
Estruturas Discretas

Profa. Dra. Helena de Medeiros Caseli
Departamento de Computação – UFSCar

Todos os direitos reservados. Nenhuma parte desta apostila poderá ser reproduzida, sejam quais forem os meios empregados, sem a permissão, por escrito, da autora.

1. Teoremas e Técnicas de Demonstração

As pedras angulares da matemática são a definição, o teorema e a prova. As *definições* especificam com precisão os conceitos em que estamos interessados, os *teoremas* afirmam exatamente o que é verdadeiro sobre esses conceitos, e as *provas* demonstram, de maneira irrefutável, a verdade dessas asserções (SCHEINERMAN, 2011, p. 1).

Neste capítulo apresenta-se uma breve contextualização de conceitos utilizados durante o curso como *definição*, *teorema*, *proposição*, *lema*, *corolário*, etc., bem como técnicas de demonstração como: *demonstração por exaustão*, *demonstração direta*, *demonstração por contraposição*, *demonstração por absurdo* e *indução matemática*.

Infelizmente, não existe uma fórmula para a construção de demonstrações nem um algoritmo geral prático para provar teoremas. Felizmente, a experiência ajuda não apenas porque você vai melhorando com a prática, mas também porque uma demonstração que funciona para um teorema pode ser, às vezes, modificada para funcionar para outro teorema diferente, porém semelhante. Como muito bem colocado por Menezes (2005), em computação, um *teorema* pode ser visto como um problema a ser resolvido e sua *demonstração*, como a solução computacional, ou seja, o algoritmo correspondente.

Os teoremas podem ser, muitas vezes, enunciados e demonstrados de maneira menos formal do que usando argumentos das lógicas proposicional e de predicados. Analogamente, demonstrações, em geral, não são escritas passo a passo com justificativas formais a cada passo. Ao invés disso, os passos principais e o raciocínio usado são esboçados em linguagem do dia a dia. A ideia é, portanto, ensinar aos estudantes como pensar claramente e apresentar a demonstração de maneira lógica. Vale ressaltar, também, que o conteúdo deste capítulo foca nos principais conceitos e estratégias de demonstração abordados neste curso de Matemática Discreta e, portanto, não é amplo nem tão detalhado quanto o que se encontra em livros específicos sobre o tema. Além disso, pressupõe-se conhecimento de Lógica obtido previamente pelo estudante em outra disciplina pré-requisito para esta.

O texto que se segue está baseado em (SCHEINERMAN, 2011), (GERSTING, 2004) e (MENEZES, 2005).

1.1. Definições

Ao iniciar o estudo da matemática nos deparamos com conceitos abstratos, não palpáveis, que exigem nossa imaginação para ganharem vida. Por exemplo, o conceito de número existe em nossa cabeça, mas como explicar o que é um número?

Os números, assim como outros objetos matemáticos, adquirem existência por meio das *definições*. Exemplo:

Definição 1.1 – Par

Um número inteiro é par se for divisível por 2.

Essa definição especifica, sem ambiguidades, o que é um número par. Porém, para que ela se torne completa é necessário definir outros conceitos subjacentes como *ser divisível*. Desse modo, as definições são, na maioria dos casos, construídas a partir de conceitos já conhecidos ou definidos previamente. Conceitos de base como *inteiro* e 2, usados na Definição 1.1, não precisam ser definidos. Assim, com a definição do que é *ser divisível* em Definição 1.2 é possível entender completamente o que é o conceito *par*.

Definição 1.2 – Divisível

Sejam a e b inteiros. Dizemos que a é *divisível* por b se existe um inteiro c , de modo que $bc = a$.

1.2. Teoremas

“Um *teorema* é uma afirmação declarativa sobre matemática para a qual existe uma *prova*” (SCHEINERMAN, 2011, p. 8). Uma *afirmação declarativa* é uma sentença que expressa uma ideia sobre como alguma coisa é. Exemplo: O povo brasileiro gosta de futebol.

O termo *prova* (ou *demonstração*) pode ser definido como uma dissertação que mostra, de maneira irrefutável (incontestavelmente correta), que uma afirmação é verdadeira. Mostrar a veracidade de uma afirmação, no contexto da matemática, envolve um procedimento muito mais rigoroso do que em outras áreas. No dia a dia, sabe-se que quase todas as afirmações consideradas verdadeiras estão limitadas ao objetivo. Se a afirmação-exemplo “O povo brasileiro gosta de futebol” foi usada pelos dirigentes da CBF para ilustrar que o Brasil era um bom candidato para a Copa do Mundo de 2014, ela pode ser considerada verdadeira apenas tendo em conta “a maioria dos brasileiros”. Contudo, essa verdade não pode ser considerada absoluta e universal.

Na matemática, provar que uma afirmação é verdadeira é provar que ela é válida para todos os elementos aos quais se refere e não apenas a alguns, mesmo que esses “alguns” sejam muitos. No exemplo anterior, é sabido que nem todo brasileiro gosta de futebol, em especial as esposas que ficam em casa cuidando das crianças para seus maridos irem “bater uma bolinha” com os amigos! Em matemática, o termo “verdadeiro” deve ser considerado absoluto, incondicional e sem exceção. Segundo Scheinerman (2011, p. 10) “os matemáticos adotaram a convenção de que uma afirmação é *verdadeira* desde que ela seja absolutamente verdadeira, sem exceção. Uma afirmação que não é absolutamente verdadeira nesse sentido estrito é chamada *falsa*.”

Assim, usando a notação da Lógica, um teorema é uma *proposição*¹ do tipo:

$$p \rightarrow q$$

que é sempre *verdadeira*, ou seja, é uma *tautologia*. Nessa notação, a *p* dá-se o nome de *hipótese* e a *q*, *tese* ou *conclusão* (MENEZES, 2005).

A palavra *teorema* tem a conotação de importância e generalidade que outros termos alternativos tendem a afrouxar (SCHEINERMAN, 2011):

- **Resultado:** uma expressão modesta para teorema;
- **Fato:** um teorema de importância bastante limitada (p.ex., $2+2=4$ é um fato);
- **Proposição:** um teorema de importância secundária. Mais importante ou mais geral que um fato, mas não tem tanto prestígio quanto um teorema;
- **Lema:** um teorema cujo objetivo principal é ajudar a provar outro teorema mais importante. Lemas são usados como partes da elaboração de uma prova complicada.
- **Corolário:** resultado com uma prova rápida, trivial, cujo passo principal é o uso de outro teorema provado anteriormente.
- **Alegação:** análogo a lema.

Formas de expressar um teorema

- **Se-então**

Se A então B

Sempre que a condição A for verdadeira, a condição B também será. A é chamada de *hipótese* e B de *conclusão* (ou *tese*).

Por exemplo, a afirmação:

“A soma de dois números inteiros pares é par.”

pode ser reformulada como:

¹ “Uma *Proposição* é uma construção (sentença, frase, pensamento) à qual se pode atribuir juízo. No caso da *Lógica Matemática*, o tipo de juízo é o verdadeiro-falso, ou seja, o interesse é na 'verdade' das proposições.” (MENEZES, 2005, p. 14).

“Se x e y são inteiros pares, então $x+y$ também é par.”

Para verificar a veracidade dessa afirmação veja que só importa demonstrar que a conclusão é verdadeira quando a hipótese é verdadeira (x e y são pares), ou seja, não importa os demais casos: quando x é ímpar, quando y é ímpar ou quando x e y (ambos) são ímpares. Inclusive, se x e y são ambos ímpares, sabemos que $x+y$ é par; porém, isso não vem ao caso na demonstração do teorema se-então apresentado anteriormente.

Esse fato se deve à tabela-verdade para a implicação se-então (SCHEINERMAN, 2011) ilustrada na Figura 1.

Condição A	Condição B	$A \rightarrow B$
Verdadeira	Verdadeira	Possível
Verdadeira	Falsa	Impossível
Falsa	Verdadeira	Possível
Falsa	Falsa	Possível

Figura 1. Tabela-verdade para a implicação.

Fonte: Adaptado de (SCHEINERMAN, 2011, p. 11).

A afirmação “Se A, então B” assegura que a condição B é verdadeira sempre que A o for, mas não faz qualquer referência a B quando A é falsa. A única circunstância em que “Se A então B” não é verdade é se A for verdadeira e B falsa.

Outras formas alternativas de expressar “Se A então B”:

- “A implica B” ou “B é implicado por A”
 - “Sempre que A, temos B” ou “B, sempre que A”
 - “A é suficiente para B” ou “A é uma condição suficiente para B”
 - “Para que B seja verdadeiro, é suficiente que tenhamos A”
 - “B é necessário para A” no sentido de que para que A seja verdadeiro é necessário que B também seja verdadeiro
 - “ $A \Rightarrow B$ ”
- **Se e Somente Se**

A se e somente se B

Essa é uma maneira concisa de expressar “Se A então B, e se B então A”. Por exemplo, a afirmação:

“Se um inteiro x é par, então $x+1$ é ímpar, e se $x+1$ é ímpar, então x é par.”

pode ser escrita como:

“Um inteiro x é par se e somente se $x+1$ é ímpar.”

A afirmação “A se e somente se B” assegura que as condições A e B devem ser ambas verdadeiras ou ambas falsas como expresso na tabela apresentada na Figura 2 (SCHEINERMAN, 2011).

Condição A	Condição B	$A \leftrightarrow B$
Verdadeira	Verdadeira	Possível
Verdadeira	Falsa	Impossível
Falsa	Verdadeira	Impossível
Falsa	Falsa	Possível

Figura 2. Tabela-verdade para a bi-implicação.
Fonte: Adaptado de (SCHEINERMAN, 2011, p. 13).

Maneiras alternativas de expressar “A se e somente se B”:

- “A sse B” em que sse é a abreviação de “se e somente se”
- “A é necessário e suficiente para B”
- “A é equivalente a B” em que, nesse caso, a “equivalência” entre A e B reside no fato de que A é verdade exatamente nas mesmas circunstâncias em que B é verdade
- “ $A \Leftrightarrow B$ ”

De modo semelhante, as expressões “e”, “ou” e “não” usadas na matemática podem ser mapeadas em suas tabelas-verdade aprendidas na Lógica.

Essas definições no contexto da teoria dos conjuntos – Cardinalidade de conjuntos finitos e Operações entre conjuntos

O número de elementos de um conjunto finito A é o tamanho de A ou cardinalidade de A e é denotado por $|A|$. Alguns resultados relacionando cardinalidade e operadores são:

Lema 1: Se A e B são conjuntos finitos disjuntos, então $A \cup B$ é finito e

$$|A \cup B| = |A| + |B|$$

Teorema 1: Se A e B são conjuntos finitos, então $A \cup B$ e $A \cap B$ são finitos e

$$|A \cup B| = |A| + |B| - |A \cap B|$$

Corolário 1: Se A, B e C são conjuntos finitos, então $A \cup B \cup C$ também é e

$$|A \cup B \cup C| = |A| + |B| + |C| - |A \cap B| - |A \cap C| - |B \cap C| + |A \cap B \cap C|$$

1.3. Técnicas de Demonstração

Como apresentado na seção anterior, os conceitos matemáticos são especificados por meio de *definições*, e *teoremas* são afirmações declarativas provadas. Então, o que é uma *prova* (ou *demonstração*)? A partir de uma afirmação que supomos verdadeira (uma *conjetura*), “uma prova é uma argumentação que mostra, de maneira indiscutível, que uma afirmação é verdadeira” (SCHEINERMAN, 2011, p. 18). Na demonstração de $P \Rightarrow Q$, a hipótese P é suposta verdadeira e, como tal, não deve ser demonstrada. As hipóteses supostas verdadeiras são as premissas sobre as quais uma demonstração é desenvolvida, ou seja, são a base para o raciocínio (MENEZES, 2005).

Existem várias técnicas para provar a veracidade de um teorema (ou demonstrar o teorema) das quais algumas serão apresentadas nesta seção por meio de exemplos simples, de afirmações já conhecidas e aceitas por todos, uma vez que a intenção não é oferecer conhecimento novo, mas sim exemplificar como uma prova é redigida.

A ideia é, a partir de uma afirmação que supomos verdadeira (conjetura), chegar à prova de que ela é realmente verdadeira seguindo uma sequência de passos lógicos e discretos (sem saltos inexplicáveis no raciocínio). Por exemplo, se a afirmação que se deseja provar é:

“Todo número primo é ímpar”

Sem muito esforço sabe-se que a afirmação é falsa. O procedimento (ou algoritmo) para se chegar a essa conclusão pode ser: (1) percorra mentalmente o conjunto dos números primos, (2) para cada número primo verifique se é ímpar. Ao se deparar com o número 2 nota-se que ele é primo e não é ímpar! Em outras palavras, a estratégia era, inicialmente, provar a afirmação porém, quando encontrou-se uma dificuldade (o 2 nesse caso) a estratégia passou a ser determinar em que consistia o problema e construir para ele um contraexemplo.

Esse é o tipo de prova mais simples: demonstração por *contraexemplo*. O contraexemplo é um tipo de demonstração da falsidade de uma afirmação que é ao mesmo tempo útil e simples. Sua relevância está no fato de que, como mencionado anteriormente, uma prova matemática da veracidade de uma afirmação não pode ser baseada em casos específicos; ela deve ser válida para rigorosamente todos os objetos a que se refere. Desse modo, basta um caso que “fure” a afirmação para que ela não seja verdadeira e, portanto, falsa. Provar que uma afirmação é falsa é o que chamamos de *refutação*. Esse tipo de prova segue o esquema apresentado a seguir (SCHEINERMAN, 2011).



Esquema de prova 1

Como refutar uma afirmação do tipo “se-então” falsa por meio de um contraexemplo.

Para refutar uma afirmação da forma “Se A, então B”:

- Ache uma situação em que A é verdadeira, mas B é falsa.

Infelizmente (ou não), a refutação por contraexemplo é uma técnica útil porém nem sempre aplicável ... Outras técnicas efetivas são apresentadas nas próximas subseções. Por ora, tenha em mente que uma prova é como um “algoritmo” com entrada, saída e passos de processamento:

Prova como um “algoritmo”

Entrada

- Uma conjectura (uma afirmação que ainda não foi provada)

Processamento = A prova

- Uma série de passos em que cada um:
 - Deve ser precisamente fundamentado, com base em definições, propriedades ou resultados já conhecidos
 - Deve também ser colocado de forma genérica, ou seja, válida para todos os objetos aos quais o teorema se refere

Saída

- O teorema, ou seja, a prova para a afirmação de entrada, quando for possível obtê-la

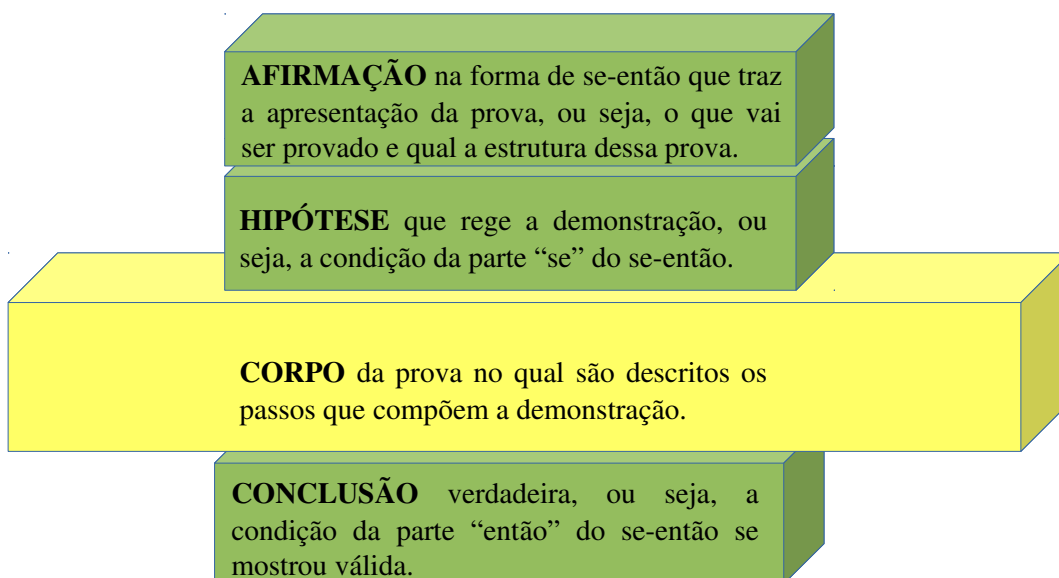


Figura 3. Estrutura básica de uma prova.

Além disso, uma prova pode ser formatada em partes conforme apresentado na Figura 3, na

qual as partes em verde são derivadas da conjectura que se deseja demonstrar e a parte em amarelo, o *corpo da prova*, é o elo de ligação entre a *hipótese* e a *conclusão* e, como tal, a parte mais importante da prova. Também pode-se incluir ao final da prova a expressão Q.E.D. (do latim *quod erat demonstrandum*) que significa "como se queria demonstrar" ou sua versão em português C.Q.D. Há, ainda, a possibilidade de substituir tal expressão por um dos símbolos ■ ou □.

1.3.1. Demonstração por exaustão

Embora “provar a falsidade por um contraexemplo” sempre funcione, “provar por um exemplo” quase nunca funciona. Uma exceção ocorre quando a conjectura é uma asserção sobre uma coleção finita. Nesse caso, a conjectura pode ser provada verificando-se que ela é verdadeira para cada elemento da coleção. Uma *demonstração por exaustão* significa que foram exauridos todos os casos possíveis (GERSTING, 2004).

Por exemplo, vamos provar a seguinte conjectura:

“Se um inteiro entre 1 e 20 é divisível por 6, então também é divisível por 3.”

Como existe apenas um número finito de casos, a conjectura pode ser provada simplesmente mostrando-se que é verdadeira para todos os inteiros entre 1 e 20:

Número	Divisível por 6?	Divisível por 3?	Número	Divisível por 6?	Divisível por 3?
1	não		11	não	
2	não		12	sim: $12 = 2 * 6$	sim: $12 = 4 * 3$
3	não		13	não	
4	não		14	não	
5	não		15	não	
6	sim: $6 = 1 * 6$	sim: $6 = 2 * 3$	16	não	
7	não		17	não	
8	não		18	sim: $18 = 3 * 6$	sim: $18 = 6 * 3$
9	não		19	não	
10	não		20	não	

1.3.2. Demonstração direta

Quando a demonstração por exaustão é inviável pode-se usar a *demonstração direta* para provar que “se P então Q”. Para tanto, supõe-se a hipótese P e deduz-se a conclusão Q. A prova direta consiste em construir uma sequência de passos baseados em definições e resultados já conhecidos, que permita nos levar da hipótese até a conclusão. Algumas estratégias de prova, nesse

caso, são: trabalhar de “frente para trás” – partindo-se da hipótese – ou de “trás para frente” – partindo-se da conclusão (SCHEINERMAN, 2011; GERSTING, 2004).

Por exemplo, uma prova direta para o fato:

“O produto de dois inteiros pares é um inteiro par.”

reescrito na forma se-então:

“Se x e y são dois inteiros pares, então o produto xy é um inteiro par.”

seria como apresentado a seguir, na qual será usada a Definição 1.2 de *ser divisível*.


Seguindo a estrutura de prova apresentada na Figura 3, a prova seria:

Prova:

Vamos mostrar que, se x e y são dois inteiros pares, então o produto xy é um inteiro par.	} AFIRMAÇÃO
Sejam x e y inteiros pares.	→ HIPÓTESE
Como x é par e y é par, pela definição de números pares temos que x é divisível por 2 e y é divisível por 2.	} CORPO
Pela definição de divisível sabemos que “ a é divisível por b se existe um inteiro c tal que $bc = a$ ” e podemos reescrever x e y como $x = 2m$ e $y = 2n$.	
Observe que $xy = 2m2n = 2(2mn)$ onde $2mn$ é um inteiro c tal que $2c = xy$.	} CONCLUSÃO
Por conseguinte, xy é divisível por 2.	
Portanto, xy é par.	→

■

Desse modo, temos o segundo esquema de prova resumido no quadro a seguir (SCHEINERMAN, 2011).

 **Esquema de prova 2**

A prova direta de um teorema “se-então”.

- Escrever a(s) primeira(s) sentença(s) da prova, apresentando a hipótese. Criar uma notação adequada (por exemplo, atribuir letras para representar variáveis).
- Escrever a(s) última(s) sentença(s) da prova, apresentando a conclusão.
- Desenredar as definições, trabalhando para a frente, a partir do começo da prova, e para trás, a partir do fim da prova.
- Avaliar o que já sabe e o que necessita. Procurar estabelecer um elo entre as duas metades de seu argumento.

De modo semelhante, um teorema na forma se-e-somente-se pode ser comprovado seguindo o esquema de prova 3 (SCHEINERMAN, 2011).



Esquema de prova 3

A prova direta de um teorema “se-e-somente-se”.

Para provar uma afirmação da forma “A se e somente se B”:

- (\Rightarrow) Prove que “se A, então B”.
- (\Leftarrow) Prove que “se B, então A”.

1.3.3. Demonstração por contraposição

Se você tentou produzir uma demonstração direta da conjectura $P \rightarrow Q$ e não conseguiu, pode tentar algumas variantes da técnica de demonstração direta. Se você puder provar o teorema $\neg Q \rightarrow \neg P$, pode concluir que $P \rightarrow Q$ usando a tautologia

$$(\neg Q \rightarrow \neg P) \rightarrow (P \rightarrow Q)$$

$\neg Q \rightarrow \neg P$ é a contrapositiva de $P \rightarrow Q$. A técnica de provar $P \rightarrow Q$ através de uma *demonstração por contraposição* é, então, fazer a demonstração direta de $\neg Q \rightarrow \neg P$ (GERSTING, 2004).

Por exemplo, para provar a conjectura:

“Se o quadrado de um inteiro é ímpar, então o inteiro tem que ser ímpar.”

Podemos reescrevê-la simbolicamente como $(x^2 \text{ ímpar}) \rightarrow (x \text{ ímpar})$.

Para fazer uma demonstração por contraposição vamos provar o contrário, ou seja, a negação da conclusão implicando na negação da hipótese: $\neg(x \text{ ímpar}) \rightarrow \neg(x^2 \text{ ímpar})$ o que é equivalente a $(x \text{ par}) \rightarrow (x^2 \text{ par})$:

Prova:

Vamos mostrar por contraposição que se o quadrado de um número inteiro é ímpar, então o inteiro tem que ser ímpar. } AFIRMAÇÃO

Seja x um inteiro par. } HIPÓTESE

Como x é par, pela definição de números pares temos que x é divisível por 2. } CORPO

Pela definição de divisível sabemos que “ a é divisível por b se existe um inteiro c tal que $bc = a$ ” e podemos reescrever x como $x = 2m$.

Observe que $x^2 = 2m2m = 2(2mn)$ onde $2mn$ é um inteiro c tal que $2c = x^2$.

Por conseguinte, x^2 é divisível por 2.

Portanto, x^2 é par. Desse modo, por contraposição, demonstramos que se o quadrado de um número inteiro é ímpar, então o inteiro é ímpar. } CONCLUSÃO

■



Esquema de prova 4

A prova por contraposição de um teorema “se-então”.

- Escrever a(s) primeira(s) sentença(s) da prova, apresentando a hipótese. Criar uma notação adequada (por exemplo, atribuir letras para representar variáveis). Deixar claro que a prova é por contraposição e, portanto, será provado que a negação da conclusão leva à negação da hipótese.
- Escrever a(s) última(s) sentença(s) da prova, apresentando a conclusão.
- Desenredar as definições, trabalhando para a frente, a partir do começo da prova, e para trás, a partir do fim da prova.
- Avaliar o que já sabe e o que necessita. Procurar estabelecer um elo entre as duas metades de seu argumento.

1.3.4. Demonstração por absurdo

Em uma *demonstração por absurdo*, supomos que a hipótese e a negação da conclusão são, ambas, verdadeiras e tentamos deduzir uma contradição dessas proposições (GERSTING, 2004).

Por exemplo, vamos demonstrar por absurdo a proposição:

“Se um número somado a ele mesmo é igual a ele mesmo, então esse número é 0.”

por meio da prova apresentada a seguir. Veja que negar a conclusão nesse caso é dizer que o número não é 0, ou seja, é diferente de 0.

Prova:

Vamos demonstrar por absurdo que se um número somado a ele mesmo é igual a ele mesmo então esse número é diferente de 0.	} AFIRMAÇÃO
Seja x um número qualquer tal que $x=x+x$.	→ HIPÓTESE
Suponha, para demonstrar por absurdo, que $x \neq 0$. Então $2x = x$ e $x \neq 0$.	} CORPO
Como $x \neq 0$ podemos dividir ambos os lados da equação $2x = x$ por x , obtendo $2 = 1$, uma contradição (um absurdo).	
Por conseguinte, $(x + x = x) \rightarrow (x = 0)$.	
Portanto, $x = 0$.	→ CONCLUSÃO

■



Esquema de prova 5

A prova por absurdo de um teorema “se-então”.

- Escrever a(s) primeira(s) sentença(s) da prova, apresentando a hipótese. Criar uma notação adequada (por exemplo, atribuir letras para representar variáveis). Deixar claro que a prova é por absurdo e, portanto, será provado que a negação da conclusão e a veracidade da hipótese, juntas, levam a um absurdo.
- Escrever a(s) última(s) sentença(s) da prova, apresentando a conclusão.

- Desenredar as definições, trabalhando para a frente, a partir do começo da prova, e para trás, a partir do fim da prova.
- Avaliar o que já sabe e o que necessita. Procurar estabelecer um elo entre as duas metades de seu argumento.

1.3.5. Demonstração por indução matemática

Essa técnica de demonstração é particularmente útil em ciência da computação. Para ilustrar como ela funciona, imagine que você está subindo uma escada infinitamente alta. Como você sabe se será capaz de chegar a um degrau arbitrariamente alto? Suponha que você faça as seguintes hipóteses sobre sua capacidade de subir:

1. Você consegue alcançar o primeiro degrau.
2. Uma vez chegando a um degrau, você sempre será capaz de chegar ao próximo.

Se a proposição 1 e o condicional 2 são ambos verdadeiros, então, pela proposição 1 você consegue chegar no primeiro degrau e, portanto, pela proposição 2, consegue chegar ao próximo (o segundo degrau, nesse caso). Novamente, pela proposição 2, se você está no segundo degrau você consegue alcançar o próximo, ou seja, você consegue chegar ao terceiro degrau. Esse raciocínio se aplica indefinidamente. Assim, você pode subir tão alto quanto quiser. Outra analogia, apresentada por Menezes (2005) é o *efeito dominó* no qual, ao derrubar a primeira peça, a primeira peça ao cair derruba a segunda, a segunda peça ao cair derruba a terceira e assim por diante como ilustra a Figura 4.

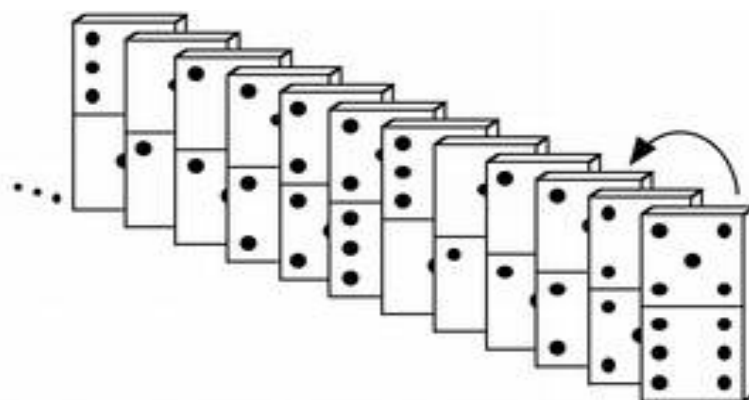


Figura 4. Ilustração gráfica do efeito dominó.

Fonte: (MENEZES, 2005, p. 160).

Ambas as hipóteses (1 e 2) são necessárias. Se apenas a primeira proposição fosse verdadeira, você não teria nenhuma garantia de passar do primeiro degrau (ou da primeira peça do

dominó) e, se apenas a segunda fosse verdadeira, você poderia não ser capaz de começar nunca.

Vamos supor que os degraus da escada estejam numerados pelos inteiros positivos (maiores que 0): 1, 2, 3, etc. Agora pense sobre uma propriedade específica que um número possa ter. Ao invés de “chegar a um degrau arbitrariamente alto”, podemos falar sobre um inteiro positivo arbitrário tendo essa propriedade. Vamos usar a notação $P(n)$ para dizer que um inteiro positivo n tem a propriedade P . As duas proposições que precisamos provar são:

1. $P(1)$ (1 tem a propriedade P)
2. Para qualquer inteiro positivo k , $P(k) \rightarrow P(k + 1)$ (se qualquer número tem a propriedade P , o próximo também tem)

Se pudermos provar ambas as proposições 1 e 2, então $P(n)$ é válida para qualquer inteiro positivo n , da mesma forma que você poderia subir até um degrau arbitrário da escada.

O fundamento para argumentos desse tipo é o *primeiro princípio da indução matemática*.

Indução matemática

A *indução matemática* é uma propriedade que pode ser definida com base no conjunto $\mathbb{N}^* = \{1, 2, 3, \dots\}$ e é usada em muitas demonstrações.

Princípio da Indução Matemática I

Seja P uma proposição definida nos inteiros positivos \mathbb{N}^* . Suponha que P tem as seguintes propriedades:

- i) $P(1)$ é verdade
- ii) $P(k+1)$ é verdade sempre que $P(k)$ é verdade

Então, $P(n)$ é verdade para todo inteiro positivo n .

Ao fazer uma demonstração por indução, o estabelecimento da veracidade da proposição i) é chamado de *base da indução* ou *passo básico* da demonstração por indução. O estabelecimento da veracidade de $P(k) \rightarrow P(k+1)$ é o *passo indutivo*. Quando supomos que $P(k)$ é verdade para provar o passo indutivo, $P(k)$ é chamada de *hipótese de indução*.

Nas outras técnicas de demonstração, podemos começar com uma hipótese e juntar diversos fatos até chegarmos à conclusão. De fato, mesmo que a nossa conjectura esteja ligeiramente incorreta, podemos ver qual deve ser a conclusão correta ao fazer a demonstração. Na indução matemática, no entanto, precisamos saber desde o início qual é a forma exata da propriedade $P(n)$ que queremos estabelecer. A indução matemática, portanto, não é uma técnica de demonstração

exploratória – pode apenas confirmar uma conjectura correta.

Exemplo: Capítulo 2 item 2.3.

Princípio da Indução Matemática II

Seja P uma proposição definida nos inteiros positivos \mathbb{N}^* tal que:

i') $P(1)$ é verdade

ii') $P(r)$ é verdade para todo r , $1 \leq r \leq k \rightarrow P(k+1)$ verdade

Então, $P(n)$ é verdade para todo inteiro positivo n .

Os dois princípios são equivalentes, ou seja, se aceitamos como válido o primeiro princípio, então o segundo também é válido e vice-versa.

Por exemplo, vamos demonstrar por indução a proposição:

“Se n é um número natural então n é menor do que 2 elevado a n .”

por meio da prova apresentada a seguir.²

Prova:

Vamos demonstrar por indução que se n é um número natural então n é menor do que 2 elevado a n , ou seja: $n < 2^n$.

i) *Base da indução*: Seja $k = 0$. Então $0 < 2^0 = 1$. Portanto, $P(0)$ é verdade.

ii) *Passo indutivo*: Suponha que, para algum número natural k , $P(k)$: $k < 2^k$ é verdade. Vamos provar que para qualquer número natural $k+1$, $P(k+1)$ também é verdade, ou seja, que $k+1 < 2^{k+1}$.

Reescrevendo:

$$k+1 < 2^{k+1} \leq 2^k + 2^k = 2 * 2^k = 2^{k+1}$$

Portanto, para qualquer n número natural tem-se que $n < 2^n$.

AFIRMAÇÃO

HIPÓTESE

CORPO

CONCLUSÃO



Esquema de prova 6

A prova por indução de um teorema “se-então”.

- Escrever a(s) primeira(s) sentença(s) da prova, apresentando a hipótese. Criar uma notação adequada (por exemplo, atribuir letras para representar variáveis).
- Escrever a(s) última(s) sentença(s) da prova, apresentando a conclusão.
- Provar a *Base da indução*.
- Supor como verdadeira a *Hipótese de indução* e provar o *Passo indutivo* usando a Base de indução previamente provada.
- Avaliar o que já sabe e o que necessita. Procurar estabelecer um elo entre as duas metades de seu argumento.

² O conjunto dos números naturais ou inteiros não-negativos \mathbb{N} , diferente de \mathbb{N}^* , engloba o 0, ou seja, $0 \in \mathbb{N}$.

Resumindo

Técnica de Demonstração	Abordagem para provar $P \rightarrow Q$	Observações
Demonstração por exaustão	Demonstre $P \rightarrow Q$ para todos os casos possíveis	Pode ser usada apenas para provar um número finito de casos
Demonstração direta	Suponha P , deduza Q	Abordagem padrão – o que se deve tentar em geral
Demonstração por contraposição	Suponha $\neg Q$, deduza $\neg P$	Use essa técnica se $\neg Q$ parece dar mais munição do que P
Demonstração por absurdo	Suponha $P \rightarrow \neg Q$, deduza uma contradição	Use essa técnica quando Q disser que alguma coisa não é verdade
Demonstração por indução	Prove para o caso base da indução; suponha a hipótese de indução e prove o passo indutivo	Use a base de indução juntamente com a hipótese de indução para provar o passo indutivo

2. Teoria dos Conjuntos

A teoria dos conjuntos é uma das pedras fundamentais da matemática. Muitos conceitos em matemática e em ciência da computação podem ser expressos de maneira conveniente na linguagem de conjuntos. Operações podem ser efetuadas em conjuntos para gerar novos conjuntos. Embora a maioria dos conjuntos de interesse para cientistas da computação sejam finitos ou enumeráveis, existem conjuntos que têm tantos elementos que não podem ser enumerados. A teoria dos conjuntos é o tema deste capítulo.

2.1. Conjuntos - definições iniciais

Um **conjunto** é definido, intuitivamente, como uma coleção de objetos não ordenada e sem repetição (SCHEINERMAN, 2011).

Embora não seja uma regra, em geral, todos os objetos em um conjunto têm alguma propriedade em comum. Com base nesta propriedade sabe-se que qualquer objeto que tem essa propriedade pertence ao conjunto e qualquer objeto que não tem essa propriedade não pertence ao conjunto.

Como mencionado, os objetos de um conjunto não possuem nenhuma ordem de apresentação e cada um é listado apenas uma vez; é redundante listá-lo de novo. Assim, $\{1, 2, 3\}$, $\{1, 1, 2, 3\}$ e $\{3, 2, 1\}$ são o mesmo conjunto. Resumindo: não interessa a ordem em que os objetos de um conjunto são listados nem se eles são repetidos, importa apenas quais objetos fazem parte do conjunto ou não (SCHEINERMAN, 2011).

Exemplos:

- o conjunto formado por todas as mulheres da sala
- o conjunto formado por todos(as) os(as) corinthianos(as) da sala
- o conjunto formado por todas as pessoas com mais de 65 anos na sala

Notação e Pertinência

Usaremos letras maiúsculas para denotar conjuntos e o símbolo \in para denotar pertinência em um conjunto. Assim, $b \in B$ significa que b pertence a B , ou b é um **elemento** (ou um **membro**) do conjunto B ou ainda que b está em B . Contrariamente, $c \notin B$ significa que c não pertence ao conjunto B .

Usaremos chaves ($\{\}$) para indicar um conjunto, ou seja, os elementos que o formam e

separaremos esses elementos com vírgula.

Exemplo:

- Seja $B = \{1, 2, 3, 4, 5\}$ então $1 \in B$ e $6 \notin B$

Cardinalidade de conjuntos

A **cardinalidade** (ou **tamanho**) de um conjunto A é o número de elementos desse conjunto e é denotada pelas barras de valor absoluto em torno do símbolo do conjunto: $|A|$.

Exemplos:

- Se $B = \{1, 2, 3, 4, 5\}$ então $|B| = 5$
- $E = \{a, b\}$ então $|E| = 2$

Um conjunto finito possui cardinalidade finita (um inteiro) enquanto um conjunto infinito possui cardinalidade infinita.

Alguns conjuntos especiais

É conveniente usar uma notação padrão para determinados conjuntos, de modo que possamos nos referir mais facilmente a eles:

\mathbb{N} = conjunto dos números naturais ou inteiros não-negativos (note que $0 \in \mathbb{N}$)

\mathbb{Z} = conjunto dos números inteiros

\mathbb{Q} = conjunto dos números racionais (formados pela divisão de dois inteiros a/b com $b \neq 0$)

\mathbb{R} = conjunto dos números reais

Descrição de conjuntos

A maneira mais simples de descrever um conjunto é listando seus elementos entre chaves. Para um **conjunto finito** (um conjunto com n elementos para algum inteiro positivo n), podemos fazer isso simplesmente listando todos os n elementos, como fizemos com os exemplos anteriores. Para os **conjuntos infinitos**, no entanto, não é possível listar todos os seus elementos um a um, embora seja possível, às vezes, indicar a forma geral listando os primeiros elementos. Por exemplo, o conjunto S de todos os inteiros positivos pares poderia ser indicado como $S = \{2, 4, 6, 8, \dots\}$.

Há, portanto, três maneiras de descrever um conjunto:

1. Listar total ou parcialmente os elementos desse conjunto (como apresentado nos exemplos anteriores). Essa forma de definição de um conjunto é denominada *denotação por extensão* e só é possível para conjuntos finitos, ou seja, com número finito de elementos (MENEZES, 2005).

2. Usar recorrência para descrever como gerar os elementos desse conjunto, ou seja, explicita-se um elemento desse conjunto e descreve-se os outros elementos em termos de elementos já conhecidos. Por exemplo, o conjunto S composto por todos os inteiros positivos pares poderia ser indicado, usando recorrência, como:

i. $2 \in S$

ii. Se $n \in S$, então $(n + 2) \in S$

3. Descrever uma propriedade que caracteriza os elementos desse conjunto. Por exemplo, o conjunto S composto por todos os inteiros positivos pares poderia ser indicado como

$$S = \{x \mid x \text{ é um inteiro positivo par}\}$$

que se lê “o conjunto de todos os x tal que x é um inteiro positivo par”. Essa opção é conhecida como *denotação por compreensão* e faz uso da notação de conjunto que tem a forma geral:

$$\{\text{variável de referência} \mid \text{condições}\}$$

Existem conjuntos para os quais a primeira maneira não funciona; a segunda é, muitas vezes, difícil de usar e a terceira, em geral, é a melhor opção. Por exemplo, o que o conjunto $\{3, 5, 7, \dots\}$ representa? O conjunto dos números ímpares maiores do que 1 ou o conjunto de inteiros primos ímpares? Portanto, esta opção de listar parcialmente os elementos de um conjunto deve ser usada apenas quando não houver ambiguidade.

Conjunto vazio

É aquele que não possui elementos. É denotado por \emptyset ou $\{\}$.

Exemplo:

- Se $S = \{x \mid x \in \mathbb{N} \text{ e } x < 0\}$, então $S = \emptyset$.

Note que \emptyset , o conjunto que não tem elementos, é diferente de $\{\emptyset\}$, o conjunto cujo único elemento é o conjunto vazio!

Igualdade de conjuntos

Dois conjuntos são iguais se e somente se contêm exatamente os mesmos elementos.

Exemplos:

- $B = \{1, 2, 3, 4, 5\}$ é igual a $C = \{5, 4, 3, 2, 1\}$
- $E = \{1, 2\}$ é igual a $F = \{2, 1, 4/2, 5/5\}$

Lembre-se que um conjunto não se altera se seus elementos forem repetidos ou reordenados.

Assim, para provar que dois conjuntos A e B são iguais, deve-se mostrar que todo elemento de A é também elemento de B e vice-versa. Por exemplo, podemos utilizar o esquema de prova 3 apresentado no Capítulo 1 para provar que os conjuntos A e B a seguir são iguais:

$$A = \{ x \in \mathbb{Z} \mid x \text{ é par} \}$$

$$B = \{ y \in \mathbb{Z} \mid y = a + b, \text{ em que } a \text{ e } b \text{ são ímpares} \}$$

Prova:

Vamos provar que $A = \{ x \in \mathbb{Z} \mid x \text{ é par} \}$ e $B = \{ y \in \mathbb{Z} \mid y = a + b, \text{ em que } a \text{ e } b \text{ são ímpares} \}$ são iguais, ou seja, $A = B$.

(\Rightarrow)

Suponha que $x \in A$. Portanto, x é par.

De acordo com a definição de número par, tem-se que x é divisível por 2. Desse modo, é possível reescrever x como $x = 2y$ para algum inteiro y .

Observe que $2y+1$ e -1 (por que $-1 = 2*(-1)+1$) são ímpares e, como $x = 2y = (2y+1) + (-1)$, constatamos que x é a soma de dois números ímpares.

Portanto, $x \in B$.

(\Leftarrow)

Suponha que $x \in B$. Portanto, x é a soma de dois números ímpares a e b .

Por definição de ímpar, existe um inteiro c tal que $a = 2c+1$ e $b = 2d+1$.

Observe $x = a + b = 2c + 1 + 2d + 1 = 2c + 2d + 2 = 2(c + d + 1)$.

Como c e d são inteiros, também o é $c + d + 1$. Logo, por definição de divisível, $x = (a+b)$ é divisível por 2. Por conseguinte, x é par.

Portanto, $x \in A$. ■

Conjunto Universo

O conjunto universo define o contexto dos objetos em discussão e é denotado por U .

Exemplo:

- O conjunto $A = \{2, 4, 6, 8, \dots\}$ pode ser entendido como um conjunto definido sobre o conjunto universo U dos números naturais ($U = \mathbb{N}$), ou dos inteiros ($U = \mathbb{Z}$).

Quando não houver margem a dúvidas, o conjunto universo não precisa ser especificado.

Subconjunto

A é subconjunto de B se todo elemento de A também é elemento de B . Diz-se que A está contido em B ($A \subseteq B$) ou B contém A ($B \supseteq A$). Caso contrário, indica-se que A não está contido em B ($A \not\subseteq B$) ou B não contém A ($B \not\supseteq A$).

Se $A \subseteq B$ mas $A \neq B$, ou seja, existe pelo menos um elemento de B que não pertence a A , então A é um **subconjunto próprio** de B e denota-se por $A \subset B$ ($B \supset A$).

Exemplos:

- $\mathbb{N} \subseteq \mathbb{Z} \subseteq \mathbb{Q} \subseteq \mathbb{R}$
- $A = \{1, 7, 9, 15\}$, $B = \{7, 9\}$ e $C = \{7, 9, 15, 20\}$
 $B \subseteq A$, $B \subseteq C$, $B \subset A$, $A \not\subseteq C$, $\{7\} \subset A$, $\emptyset \subseteq C$ (uma vez que \emptyset não possui elemento, a proposição é automaticamente verdadeira)

\subseteq e \in

\subseteq e \in possuem significados relacionados, porém diferentes.

$x \in A$ significa que x é elemento de A e a notação $A \subseteq B$ significa que todo elemento de A também é elemento de B . Assim, $\emptyset \subseteq \{1, 2, 3\}$ é verdadeiro mas $\emptyset \in \{1, 2, 3\}$ é falso.



Compilador x Pertinência à Linguagem

Um compilador de uma linguagem de programação é um programa que traduz programas, ou seja, ele tem como entrada um programa em uma linguagem de programação (linguagem fonte) e gera como saída a versão traduzida deste programa em código executável (na linguagem alvo). O processo de tradução pode ser dividido em etapas de análise do programa de entrada (fonte) e a síntese do código de saída (alvo). As etapas de análise (léxica, sintática e semântica), basicamente, verificam se o programa fonte p pertence à linguagem fonte L , ou seja, se $p \in L$.



Subconjunto e noção de herança em programação orientada a objetos

Suponha que $B = \{x \mid P(x)\}$ e que $A \subseteq B$. Como todo elemento de A também pertence a B e P é uma propriedade que caracteriza os elementos de B , todo elemento de A também tem essa propriedade P . Em outras palavras, os elementos de A “herdam” a propriedade P . Essa é a mesma noção de “herança” que temos em uma linguagem de programação orientada a objetos para um tipo descendente, ou subtipo, ou tipo derivado. O tipo descendente herda todas as propriedades e operações do tipo ascendente.

**Algumas propriedades importantes de conjuntos**

- i) para todo conjunto A , tem-se que $\emptyset \subseteq A \subseteq U$ (todo conjunto é subconjunto do conjunto universo e contém o conjunto vazio)
- ii) para todo conjunto A , $A \subseteq A$ (todo conjunto é subconjunto de si mesmo)
- iii) se $A \subseteq B$ e $B \subseteq C$ então $A \subseteq C$
- iv) $A = B$ se e somente se $A \subseteq B$ e $B \subseteq A$ (provar a inclusão nas duas direções é a maneira usual de estabelecer a igualdade de dois conjuntos)

**Esquema de prova 7**

Provar que um conjunto é subconjunto de outro.

Mostrar que $A \subseteq B$:

- Seja $x \in A$. *(início da prova)*
- Demonstra-se que todo elemento de A é também elemento de B . *(corpo da prova)*
- Portanto, $x \in B$ e, assim, $A \subseteq B$.

Provando que A é subconjunto de B e que A é subconjunto próprio de B

Suponha que $B = \{x \mid P(x)\}$, para provar que $A \subseteq B$ mostramos que $P(x)$ é válida para qualquer elemento arbitrário $x \in A$.

Suponha que $B = \{x \mid P(x)\}$, para provar que $A \subset B$ mostramos que os elementos de A têm alguma propriedade adicional não compartilhada por todos os elementos de B .

Exemplo:

- Sejam

$$A = \{x \mid x \in \mathbb{R} \text{ e } x^2 - 4x + 3 = 0\}$$

$$B = \{x \mid x \in \mathbb{N} \text{ e } 1 \leq x \leq 4\}$$

Prove que $A \subset B$.

Prova:

Seja $x \in A$. Então $x \in \mathbb{R}$ e $x^2 - 4x + 3 = 0$ ou, reescrevendo, $(x - 1)(x - 3) = 0$, o que nos dá $x = 1$ ou $x = 3$. Em qualquer um dos casos, $x \in \mathbb{N}$ e $1 \leq x \leq 4$ de modo que $x \in B$. Portanto, $A \subseteq B$. Além disso, tem-se que o número 4 pertence a B ($x \leq 4$) mas não pertence a A , logo $A \subset B$.

Provando a igualdade de dois conjuntos

Usando, para isso a propriedade iv) $A = B$ se e somente se $A \subseteq B$ e $B \subseteq A$.

Exemplo:

- Prove que $\{x \mid x \in \mathbb{N} \text{ e } x^2 < 15\} = \{x \mid x \in \mathbb{N} \text{ e } 2x < 7\}$.

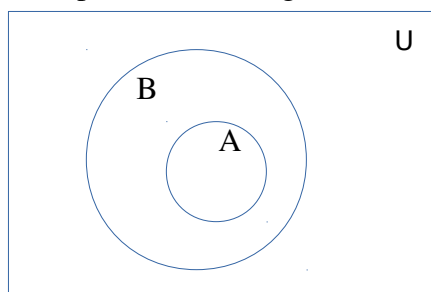
Prova:

Sejam $A = \{x \mid x \in \mathbb{N} \text{ e } x^2 < 15\}$ e $B = \{x \mid x \in \mathbb{N} \text{ e } 2x < 7\}$. Para provar que $A = B$ vamos provar que $A \subseteq B$ e $B \subseteq A$.

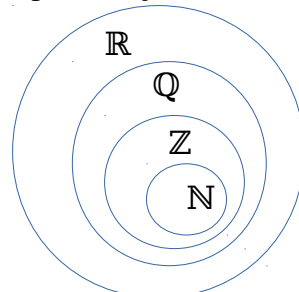
- Para $A \subseteq B$ escolhemos um elemento arbitrário de A e mostramos que ele satisfaz a característica dos elementos de B . Seja $x \in A$. Então x é um inteiro não-negativo que satisfaz a propriedade $x^2 < 15$. Os inteiros não-negativos cujos quadrados são menores do que 15 são 0, 1, 2 e 3, logo esses são os elementos de A . O dobro de cada um dos elementos de A ($2x$) é 0, 2, 4 e 6, respectivamente, ou seja, um número menor do que 7. Portanto, todo elemento de A pertence a B e $A \subseteq B$.
- Para $B \subseteq A$ tem-se que todo elemento de B é um inteiro não-negativo cujo dobro é menor do que 7. Esses números são 0, 1, 2 e 3, cujos quadrados são respectivamente 0, 1, 4, e 9, ou seja, números menores do que 15. Logo, $B \subseteq A$.
- Provando que A é subconjunto de B e que B é subconjunto de A , provamos que $A = B$.

2.2. Diagrama de Venn e Operações entre conjuntos

Um diagrama de Venn é uma representação pictórica de conjuntos. Foram assim chamados em homenagem ao matemático britânico do século XIX, John Venn. Nessa representação, um retângulo é usado para representar o conjunto universo enquanto os demais conjuntos são representados por discos. A Figura 3 traz um exemplo dessa representação.



a) $A \subseteq B$



b) $N \subseteq Z \subseteq Q \subseteq R$

Figura 3. Exemplo de diagrama de Venn para conjuntos que são subconjuntos de outros.

Operações entre conjuntos

Seja U o conjunto de todos os estudantes da UFSCar. Seja A o conjunto de estudantes de ciência da computação e seja B o conjunto de estudantes de administração. Ambos, A e B , pertencem a U . Um novo conjunto de estudantes pode ser definido consistindo em todos que são alunos de ciência da computação ou de administração (ou ambos), este conjunto é a **união** de A e B . Um outro conjunto que pode ser definido como aquele formado pelos alunos que cursam, ao mesmo tempo, ciência da computação e administração. Esse conjunto (que pode ser vazio) é chamado de a **intersecção** de A e B .

Definições

– União

A união de dois conjuntos A e B , denotada por $A \cup B$, é o conjunto de todos os elementos que pertencem a A ou a B :

$$A \cup B = \{ x \mid x \in A \text{ ou } x \in B \}$$

– Intersecção

A intersecção de dois conjuntos A e B , denotada por $A \cap B$, é o conjunto dos elementos que pertencem a A e a B :

$$A \cap B = \{ x \mid x \in A \text{ e } x \in B \}$$

– Conjunto disjunto

Dois conjuntos são disjuntos se não compartilham elementos comuns, ou seja, se $A \cap B = \emptyset$, A e B são ditos **disjuntos**. Os conjuntos disjuntos também são denominados *conjuntos independentes* ou *conjuntos mutuamente exclusivos* (MENEZES, 2005).

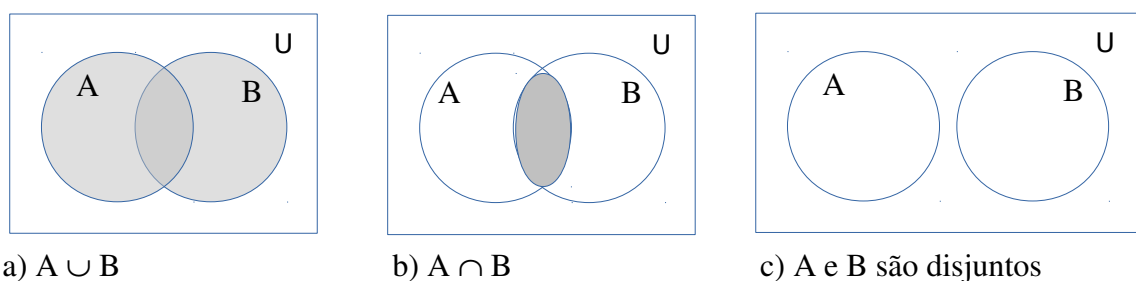


Figura 4. Diagrama de Venn para as operações de união (a) e intersecção (b) e a ilustração de conjuntos disjuntos (c).

– **Complementar** ou **Complementar absoluto**

O complementar de um conjunto A , denotado por A^c ou por A' , é o conjunto dos elementos que pertencem a U mas não pertencem a A :

$$A' = \{ x \mid x \in U \text{ e } x \notin A \}$$

– **Diferença** ou **Complementar relativo**

A diferença entre dois conjuntos A e B , denotada por $A \setminus B$ ou $A - B$, é o conjunto dos elementos que pertencem a A mas não pertencem a B :

$$A - B = \{ x \mid x \in A \text{ e } x \notin B \}$$

Essa operação pode ser reescrita como:

$$A - B = \{ x \mid x \in A \text{ e } x \in B' \} \text{ ou}$$

$$A - B = A \cap B'$$

– **Diferença simétrica**

A diferença simétrica dos conjuntos A e B , denotada por $A \oplus B$, consiste em todos os elementos que pertencem a A ou B mas não a ambos:

$$A \oplus B = (A \cup B) - (A \cap B)$$

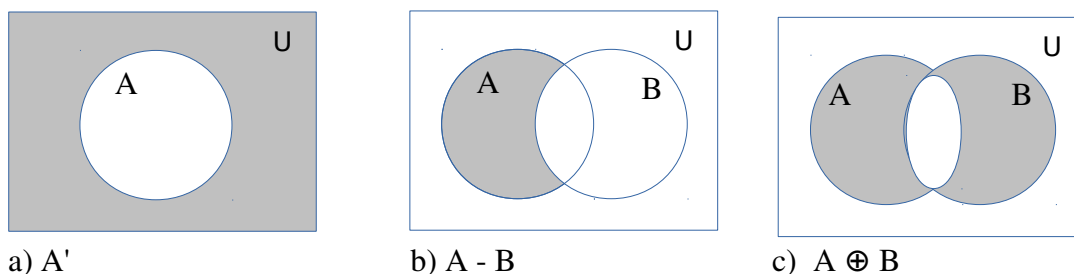


Figura 5. Diagrama de Venn para as operações de complementar (a), diferença (b) e diferença simétrica (c).

Exemplos:

- Sejam $A = \{1, 3, 5, 7, 9\}$ e $B = \{3, 5, 6, 10, 11\}$

a) $A \cup B = \{1, 3, 5, 6, 7, 9, 10, 11\}$

b) $A \cap B = \{3, 5\}$

c) $A - B = \{1, 7, 9\}$

d) $A \oplus B = \{1, 6, 7, 9, 10, 11\}$

- Dado o enunciado “o conjunto formado por todos os alunos da UFSCar que jogam futebol e cursam ciência da computação ou engenharia da computação”, usando as

operações apresentadas anteriormente, e considerando-se que:

U = conjunto formado por todos os alunos da UFSCar

A = conjunto formado pelos alunos da UFSCar que jogam futebol

B = conjunto formado pelos alunos de ciência da computação

C = conjunto formado pelos alunos de engenharia da computação

tal conjunto poderia ser representado como $A \cap (B \cup C)$ ou $(A \cap B) \cup (A \cap C)$.

2.3. Classes de conjuntos, conjuntos de conjuntos e partições

Classes de conjuntos

Uma **classe de conjuntos** ou **coleção de conjuntos** é um conjunto de conjuntos. São usados geralmente quando queremos tratar de alguns subconjuntos de um dado conjunto. Uma coleção de conjuntos pode ser denotada entre colchetes ou entre chaves.

Uma **subclasse** ou **subcoleção** é formada por alguns conjuntos de uma classe de conjuntos.

Exemplos:

Seja $S = \{1, 2, 3, 4\}$

- A é a classe de subconjuntos de S que contêm exatamente três elementos de S .

$A = [\{1, 2, 3\}, \{1, 2, 4\}, \{1, 3, 4\}, \{2, 3, 4\}]$

- B é a classe de subconjuntos de S que contêm três elementos sendo um deles o número 2.

$B = [\{1, 2, 3\}, \{1, 2, 4\}, \{2, 3, 4\}]$

B é subclasse de A

Conjunto das partes ou conjunto potência

Para um conjunto S podemos formar um novo conjunto cujos elementos são os subconjuntos de S . Esse novo conjunto é chamado o **conjunto das partes** ou **conjunto potência** de S e é denotado por 2^S ou $\wp(S)$:

$$\wp(S) = \{X \mid X \subseteq S\}$$

Exemplo:

- Para $S = \{0, 1\}$, $\wp(S) = \{\emptyset, \{0\}, \{1\}, \{0, 1\}\}$

Note que os elementos do conjunto das partes de um conjunto são conjuntos. Para qualquer conjunto S , $\wp(S)$ sempre tem, pelo menos, \emptyset e S como elementos já que sempre é verdade que $\emptyset \subseteq S$ e $S \subseteq S$.

Se S é infinito, o conjunto das partes de S também é. O número de elementos do conjunto das partes de S é 2 elevado à cardinalidade de S , ou seja, se S possui n elementos então $\wp(S)$ tem 2^n elementos.

Provando por indução que se S possui n elementos então $\wp(S)$ tem 2^n elementos.

Base da indução. Para a base da indução tomamos $n = 0$. O único conjunto com zero elementos é \emptyset . O único subconjunto de \emptyset é \emptyset , logo $\wp(\emptyset) = \{\emptyset\}$ um conjunto com $1 = 2^0$ elementos.

Passo indutivo. Vamos supor que para qualquer conjunto com k elementos o conjunto de suas partes tem 2^k elementos. Seja S um conjunto com $k + 1$ elementos. Retire 1 desses elementos, por exemplo, x . O conjunto que resta é um conjunto com k elementos, logo, pela hipótese de indução, seu conjunto de partes tem 2^k elementos. Cada um desses elementos também pertence a $\wp(S)$. Os únicos elementos de $\wp(S)$ ainda não incluídos são os que contêm x . Todos os subconjuntos contendo x podem ser encontrados colocando-se x em todos os subconjuntos que não o contêm (que são, no total, 2^k). Assim, teremos 2^k subconjuntos contendo x . Juntos, temos 2^k subconjuntos não contendo x e 2^k contendo x ou, no total: $2^k + 2^k = 2 * 2^k = 2^{k+1}$ subconjuntos. Portanto, $\wp(S)$ tem 2^{k+1} elementos. ■

A Figura 3 ilustra graficamente a demonstração do passo indutivo:

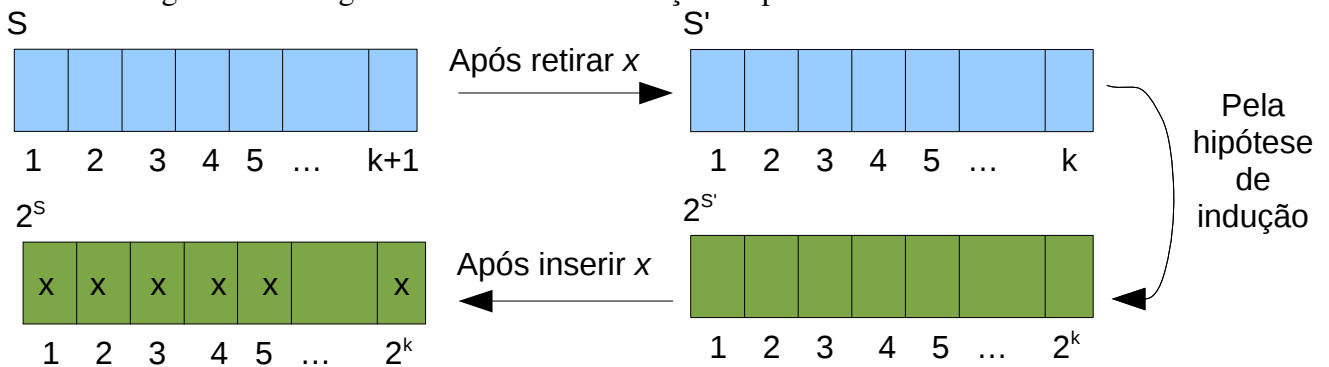


Figura 6. Ilustração gráfica do passo indutivo. Em azul o conjunto de elementos e em verde o conjunto das partes.

Partições

Uma **partição** de um conjunto S é uma coleção de subconjuntos disjuntos não-vazios cuja união é igual a S . Em outras palavras, uma partição do conjunto A é uma coleção $\{A_i\}$ de subconjuntos não vazios de A tais que:

- i) cada a em A pertence a algum dos A_i
 ii) os conjuntos em $\{A_i\}$ são disjuntos dois a dois, isto é, se $A_i \neq A_j$ então $A_i \cap A_j = \emptyset$

Uma partição pode ser representada em diagrama de Venn como:

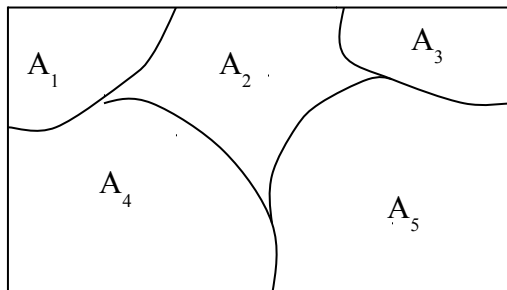


Figura 7. Diagrama de Venn de uma partição de conjuntos.

Os subconjuntos de uma partição são chamados de **células**.

Exemplo:

Seja $A = \{1, 2, 3, 4, 5, 6, 7, 8, 9\}$

– $B = \{\{1, 2, 3\}, \{5, 8, 9\}, \{4, 6, 7\}\}$

é

partição

– $C = \{\{1, 2, 3\}, \{5, 3, 8, 9\}, \{4, 6, 7\}\}$ não é partição porque as células não são disjuntas

– $D = \{\{1, 2, 3\}, \{5, 8, 9\}, \{6, 7\}\}$ não é partição porque a união das células não é

A

Generalização de operações entre conjuntos

Considere um número finito de conjuntos A_1, A_2, \dots, A_m . A união e intersecção desses conjuntos é, respectivamente, denotada e definida por:

$$A_1 \cup A_2 \cup \dots \cup A_m = \cup = \{x \mid x \in A_i \text{ para algum } A_i\}$$

$$A_1 \cap A_2 \cap \dots \cap A_m = \cap = \{x \mid x \in A_i \text{ para todo } A_i\}$$

Generalizações para coleções de conjuntos

Seja A uma coleção de conjuntos. A união e intersecção de conjuntos na coleção A são denotadas e definidas, respectivamente, por:

$$\cup (A \mid A \in A) = \{x \mid x \in A \text{ para algum } A \in A\} \text{ e}$$

$$\cap (A \mid A \in A) = \{x \mid x \in A \text{ para todo } A \in A\}.$$

2.4. Identidades envolvendo conjuntos

Existem muitas igualdades entre conjuntos envolvendo as operações de união, intersecção, diferença e complementação que são verdadeiras para todos os subconjuntos de cada conjunto U . Como elas são independentes dos subconjuntos particulares utilizados, essas igualdades são chamadas de identidades (ou leis).

Tabela 1: Identidades básicas envolvendo conjuntos.

1a. $A \cup A = A$	1b. $A \cap A = A$	(leis de idempotência)
2a. $A \cup B = B \cup A$	2b. $A \cap B = B \cap A$	(leis de comutatividade)
3a. $(A \cup B) \cup C = A \cup (B \cup C)$	3b. $(A \cap B) \cap C = A \cap (B \cap C)$	(leis de associatividade)
4a. $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$	4b. $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$	(leis de distributividade)
5a. $A \cup \emptyset = A$	5b. $A \cap U = A$	(leis de identidade)
6a. $A \cup U = U$	6b. $A \cap \emptyset = \emptyset$	
7a. $A \cup A' = U$	7b. $A \cap A' = \emptyset$	(leis dos complementares)
8a. $U' = \emptyset$	8b. $\emptyset' = U$	
9a. $(A')' = A$		(lei da involução)
10a. $(A \cup B)' = A' \cap B'$	10b. $(A \cap B)' = A' \cup B'$	(leis de DeMorgan)

Essas identidades básicas podem ser usadas para provar outras identidades envolvendo conjuntos. Contudo, para usar uma identidade é necessário que a expressão que se deseja demonstrar seja exatamente da mesma forma que a identidade. Exemplo:

- Provando a identidade $[C \cap (A \cup B)] \cup [(A \cup B) \cap C'] = A \cup B$

$$[C \cap (A \cup B)] \cup [(A \cup B) \cap C']$$

$$= [(A \cup B) \cap C] \cup [(A \cup B) \cap C'] \quad (2b)$$

$$= (A \cup B) \cap (C \cup C') \quad (4b)$$

$$= (A \cup B) \cap U \quad (7a)$$

$$= A \cup B \quad (5b)$$

Dualidade

O **dual** de cada identidade da Tabela 1 também faz parte dessa tabela. A identidade dual é obtida permutando-se \cup com \cap e U com \emptyset . Por exemplo, o dual da identidade $[C \cap (A \cup B)] \cup [(A \cup B) \cap C'] = A \cup B$ é:

$$[C \cup (A \cap B)] \cap [(A \cap B) \cup C'] = A \cap B$$



Conjuntos contáveis e não-contáveis e Teoria da Computação

Um conjunto é **contável** quando é possível designar um elemento como sendo o primeiro, um outro como sendo o segundo e assim por diante. Nos conjuntos finitos, o número de elementos é sua cardinalidade. Porém, mesmo em conjuntos infinitos é possível, às vezes, selecionar um elemento como o primeiro, outro como segundo e assim por diante. Nesse caso, todos os elementos do conjunto aparecerão na lista em algum momento e esse conjunto infinito é dito **enumerável**. Por exemplo, o conjunto dos números naturais (\mathbb{N}) é infinito e enumerável já que é possível enumerar seus elementos: 0, 1, 2, 3, ...

Tanto os conjuntos finitos quanto os enumeráveis são conjuntos contáveis, pois podemos contar ou enumerar todos os seus elementos. Assim, ser contável não implica em dizer qual o número total de elementos do conjunto, mas sim ser capaz de dizer “esse é o primeiro elemento”, “esse é o segundo” e assim por diante.

Existem, no entanto, conjuntos infinitos que são não-contáveis (ou não-enumeráveis). Um conjunto não-enumerável é tão grande que não há maneira de se contar os elementos e obter todo o conjunto nesse processo. Por exemplo, o conjunto de todos os números reais entre 0 e 1 não é enumerável. Uma maneira de demonstrar esse fato é usando o **método de diagonalização de Cantor** – veja demonstração na página 141 de (GERSTING, 2004).

A existência de conjuntos não-enumeráveis é fundamental na Teoria da Computação, já que a notação de computabilidade (aquilo que pode ser computado por computador) está relacionada ao conjunto de linguagens (ou problemas) recursivamente enumeráveis.

Resumindo

Conceitos aprendidos nesse capítulo

- conjunto - uma coleção de objetos não ordenada e sem repetição
- elemento ou membro - um objeto que pertence ao conjunto
- conjunto finito - um conjunto com n elementos para algum inteiro positivo n
- conjunto infinito - um conjunto que não é finito
- cardinalidade (ou tamanho) de um conjunto - número de elementos desse conjunto
- conjunto vazio (\emptyset) - aquele que não possui elementos
- conjunto universo (U) - define o contexto dos objetos em discussão
- subconjunto - A é subconjunto de B ($A \subseteq B$ ou $B \supseteq A$) se todo elemento de A também é elemento de B
- subconjunto próprio - se $A \subseteq B$ mas $A \neq B$, ou seja, existe pelo menos um elemento de B que não pertence a A
- união de dois conjuntos A e B ($A \cup B$) - conjunto de todos os elementos que pertencem a A ou a B
- intersecção de dois conjuntos A e B ($A \cap B$) - conjunto dos elementos que pertencem a A e a B
- conjuntos disjuntos - aqueles que não compartilham elementos comuns
- complementar de um conjunto (A') - conjunto dos elementos que pertencem a U mas não pertencem a A
- diferença entre dois conjuntos A e B ($A - B$) - conjunto dos elementos que pertencem a A mas não pertencem a B
- diferença simétrica entre dois conjuntos A e B ($A \oplus B$) - conjunto de todos os elementos que pertencem a A ou B mas não a ambos
- classe de conjuntos ou coleção de conjuntos (denotada entre colchetes ou entre chaves) - conjunto de conjuntos
- subclasse ou subcoleção - formada por alguns conjuntos de uma classe de conjuntos
- conjunto das partes ou conjunto potência de S (2^S ou $\wp(S)$) - formado pelos subconjuntos de S
- partição de um conjunto S - uma coleção de subconjuntos disjuntos não-vazios cuja união é igual a S
- dual de uma identidade - identidade obtida permutando-se \cup com \cap e U com \emptyset

3. Relações sobre Conjuntos

No capítulo 2 vimos a Teoria dos Conjuntos na qual são apresentadas definições, propriedades e operações em um conjunto e entre conjuntos. Contudo, um conjunto por si mesmo não é muito interessante até fazermos algo com seus elementos. Por exemplo, podemos efetuar diversas operações aritméticas em elementos do conjunto \mathbb{Z} . Poderíamos subtrair dois inteiros ou considerar o negativo de um inteiro. A subtração, por exemplo, age em dois inteiros x e y sendo que $x - y$ gera apenas uma resposta que sempre será um número inteiro. Assim, a subtração é efetuada em um **par ordenado** de números.

Intuitivamente, uma **relação** pode ser entendida como uma comparação entre objetos. Dois objetos podem ou não estar relacionados por alguma regra. Por exemplo, algumas relações comuns na matemática e na computação são: menor do que, é paralelo a, é subconjunto de, etc. Esses são exemplos de relações binárias, ou seja, que ocorrem entre dois objetos. Existem também relações unárias (envolvendo apenas um objeto), ternárias (envolvendo três objetos), quaternárias (envolvendo quatro objetos) e assim por diante.

Na computação, o conceito e relação ou derivados (funções) está presente em diversas construções como Banco de Dados Relacional e Redes de Petri (MENEZES, 2005). No contexto dessa disciplina, alguns tipos de relações importantes serão abordadas: (i) as relações de equivalência, (ii) as relações de ordem e (iii) as funções (capítulo 4).

Porém, antes de falar de cada um deles, há dois conceitos que precisam ser apresentados: **par ordenado** e **produto cartesiano**.

3.1. Par ordenado e Produto Cartesiano

Par ordenado

Um **par ordenado** é um par de elementos (lista de dois elementos) da forma (x, y) onde x é o primeiro elemento do par e y é o segundo.

A ordem é importante em um par ordenado. Assim, os conjuntos $\{1, 2\}$ e $\{2, 1\}$ são iguais, mas os pares ordenados $(1, 2)$ e $(2, 1)$ não são. Você provavelmente já viu a aplicação de pares ordenados como coordenadas de um ponto no plano. O ponto $(1, 2)$ é diferente do ponto $(2, 1)$.

Dois pares ordenados (x, y) e (u, v) são iguais, ou seja $(x, y) = (u, v)$, apenas quando $x = u$ e $y = v$. Portanto $(a, b) \neq (b, a)$ a menos que $a = b$.

Exemplos:

- Dado que $(2x-y, x+y) = (7, -1)$ e usando a definição da igualdade de pares ordenados, é possível encontrar os valores de x e y resolvendo as equações $2x-y=7$ e $x+y=-1$. Assim, temos que $y = -3$ e $x = 2$.
- Seja $A = \{3, 4\}$. É possível listar todos os pares ordenados (x, y) de elementos de A : $(3,3), (3,4), (4,4), (4,3)$.

Produto Cartesiano

O **produto cartesiano** de dois conjuntos A e B , denotado por $A \times B$, é o conjunto de todos os pares ordenados com o primeiro elemento em A e o segundo elemento em B :

$$A \times B = \{ (x, y) \mid x \in A \text{ e } y \in B \}$$

Utiliza-se A^2 para denotar $A \times A$.

Exemplos:

- $\mathbb{R} \times \mathbb{R} = \mathbb{R}^2$ é o conjunto dos pares ordenados de números reais que, na representação geométrica, contém os pontos do plano.
- Sejam $A = \{1, 2\}$ e $B = \{3, 4\}$,
 - $A \times B = \{(1, 3), (1, 4), (2, 3), (2, 4)\}$
 - $B \times A = \{(3, 1), (3, 2), (4, 1), (4, 2)\}$
 - $A^2 = \{(1, 1), (1, 2), (2, 1), (2, 2)\}$

Importante:

- A ordem dos conjuntos altera o resultado do produto cartesiano. Assim, $A \times B \neq B \times A$ e, portanto, a operação de produto cartesiano é não-comutativa. Analogamente, $(A \times B) \times C \neq A \times (B \times C)$ a operação de produto cartesiano também é não-associativa.
- Para dois conjuntos A e B finitos, o número de elementos no produto cartesiano é o produto do número de elementos nos dois conjuntos: $|A \times B| = |A| * |B|$.
- O produto cartesiano pode ser estendido para qualquer número finito de conjuntos. Para quaisquer conjuntos A_1, A_2, \dots, A_n , o conjunto de todas as n -tuplas (a_1, a_2, \dots, a_n) onde $a_1 \in A_1, a_2 \in A_2, \dots, a_n \in A_n$ é chamado de produto cartesiano de A_1, A_2, \dots, A_n :

$$A_1 \times A_2 \times \dots \times A_n \text{ ou } \prod_{i=1}^n A_i$$

Uma n -tupla ordenada (a_1, a_2, \dots, a_n) não deve ser confundida com um conjunto $\{a_1,$

a_2, \dots, a_n já que na n -tupla ordenada, a ordem é importante.

3.2. Relações

Se descobrirmos que duas pessoas, Caetano e Bethânia, estão relacionadas, entenderemos que existe alguma conexão familiar entre elas, ou seja, que o par (Caetano, Bethânia) se diferencia de outros pares ordenados de pessoas porque existe uma relação que elas satisfazem, neste caso, a relação de irmãos. O análogo matemático é distinguir determinados pares ordenados de objetos de outros pares ordenados porque as componentes dos pares diferenciados satisfazem alguma relação que os outros não satisfazem.

Por exemplo, para $A = \{1, 2, 3\}$, o produto cartesiano $A \times A = \{(1, 1), (1, 2), (1, 3), (2, 1), (2, 2), (2, 3), (3, 1), (3, 2), (3, 3)\}$. Se estivermos interessados na relação de igualdade, então os elementos $(1, 1)$, $(2, 2)$ e $(3, 3)$ seriam escolhidos pois são os únicos pares ordenados cujos elementos são iguais. Por outro lado, se estivermos interessados na relação de um número ser menor do que o outro então escolheríamos os pares ordenados $(1, 2)$, $(1, 3)$ e $(2, 3)$.

Definição

Sejam A e B conjuntos. Uma **relação** (ou relação binária) de A para B é um subconjunto de $A \times B$.

$$R \subseteq A \times B$$

ou $R: A \rightarrow B$, em que A é denominado *domínio*, *origem* ou *conjunto de partida* de R e B é o *contradomínio*, *codomínio*, *destino* ou *conjunto de chegada* de R (MENEZES, 2005). Dizemos que R é uma *relação sobre* (ou *em*) A quando $R \subseteq A \times A$ e dizemos que R é uma *relação de A para B* se $R \subseteq A \times B$ (SCHEINERMAN, 2011).

Uma relação é, portanto, um conjunto de pares ordenados. Usamos a notação $x R y$ para indicar que o par ordenado (x, y) satisfaz a relação R e, portanto, dizemos que x é R -relacionado a y ou, simplesmente, que x relaciona-se com y . A relação R pode ser definida com palavras ou simplesmente listando-se os pares ordenados que satisfazem R . É importante notar que a relação é definida com base no domínio A , no contradomínio B e no conjunto de pares R , ou seja, qualquer alteração de um desses itens leva a uma outra relação.

Exemplos:

– Sejam $A = \{1, 2, 3, 4\}$ e $B = \{4, 5, 6, 7\}$

– $C = \{(1, 1), (2, 2), (3, 3), (4, 4)\}$

relação sobre (ou em) A

- $D = \{(1, 2), (3, 2)\}$ relação em A
 - $E = \{(1, 4), (1, 5), (4, 7)\}$ relação de A para B
 - $F = \{(4, 4), (5, 2), (6, 2), (7, 3)\}$ relação de B para A
 - $G = \{(1, 7), (7, 1)\}$ é uma relação, mas não é de A para B nem de B para A
- Para cada uma das relações R definidas a seguir em \mathbb{N} , apenas os pares ordenados que pertencem a R aparecem sublinhados ():
- a) $x R y \leftrightarrow x = y + 1$;¹ (2, 2), (2, 3), (3, 3), (3, 2)
 - b) $x R y \leftrightarrow x \text{ divide } y$; (2, 4), (2, 5), (2, 6)
 - c) $x R y \leftrightarrow x \text{ é ímpar}$; (2, 3), (3, 4), (4, 5), (5, 6)
 - d) $x R y \leftrightarrow x > y^2$; (1, 2), (2, 1), (5, 2), (6, 4), (4, 3)

É possível definir relações que envolvam mais do que dois conjuntos. Por exemplo, sejam $A = \{1, 2, 3\}$, $B = \{a, b, c\}$ e $C = \{x, y\}$ e R uma relação sobre $A \times B \times C$: $R = \{(1, b, y), (1, c, x), (2, b, x), (2, b, y), (3, a, y)\}$. De forma geral, dados n conjuntos A_1, A_2, \dots, A_n , uma relação n -ária R pode ser definida sobre o produto cartesiano $A_1 \times A_2 \times \dots \times A_n$ sendo que R será formada por n -tuplas da forma (a_1, a_2, \dots, a_n) tal que $a_1 \in A_1, a_2 \in A_2, \dots, a_n \in A_n$.

Quando uma relação é definida entre elementos de um mesmo conjunto, $R \subseteq A \times A$, a relação também é denominada de *endorrelação* ou *autorrelação*.

Operações

Como uma relação é um conjunto (de pares ordenados), todas as operações sobre conjuntos se aplicam às relações.

Exemplo:

- Sejam R e S duas relações em \mathbb{N} definidas por $x R y \leftrightarrow x = y$ e $x S y \leftrightarrow x < y$. Então
 - a relação $R \cup S$ é descrita como: $x (R \cup S) y \leftrightarrow x \leq y$
 - a relação R' é descrita como: $x R' y \leftrightarrow x \neq y$
 - a relação S' é descrita como: $x S' y \leftrightarrow x \geq y$
 - o conjunto que representa a relação $R \cap S$ é: $R \cap S = \emptyset$

1 O símbolo \leftrightarrow indica *se e somente se*.

2 Um número natural x divide outro número natural y quando o resultado da divisão de y/x é um número natural.

Representação gráfica de relações

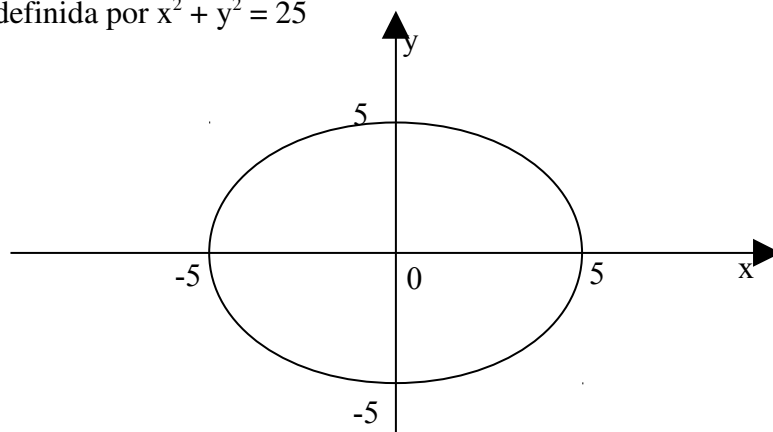
Assim como as operações entre conjuntos podem ser representadas usando o Diagrama de Venn, as relações sobre conjuntos também possuem representações gráficas. Essas representações auxiliam a compreensão de quais elementos de cada conjunto estão relacionados.

– Pontos no plano

Considere uma relação S no conjunto dos números reais, \mathbb{R} . S é um subconjunto de $\mathbb{R} \times \mathbb{R} = \mathbb{R}^2$. Como \mathbb{R}^2 pode ser representado pelo conjunto de pontos no plano S pode, então, ser representado assinalando os pontos no plano que pertencem a S .

Exemplo:

- S definida por $x^2 + y^2 = 25$



– Conjuntos Finitos

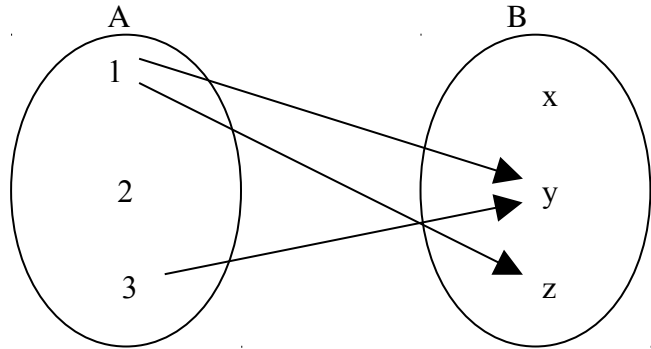
Sejam A e B conjuntos finitos e R uma relação de A para B . R pode ser representada por:

- **Matriz retangular** - com linhas nomeadas pelos elementos de A e colunas pelos elementos de B . Cada posição da matriz terá 1 ou 0, dependendo se a ($a \in A$) está ou não relacionado com b ($b \in B$), respectivamente.
- **Diagrama de setas (Diagrama de Venn)** - com elementos de A e B em dois discos disjuntos e uma seta de a para b onde $a \in A$ e $b \in B$ sempre que a estiver relacionado com b .

Exemplo:

- Sejam $A = \{1, 2, 3\}$ e $B = \{x, y, z\}$ conjuntos finitos. A relação $R = \{(1, y), (1, z), (3, y)\}$ de A para B pode ser representada graficamente como

	x	y	z
1	0	1	1
2	0	0	0
3	0	1	0

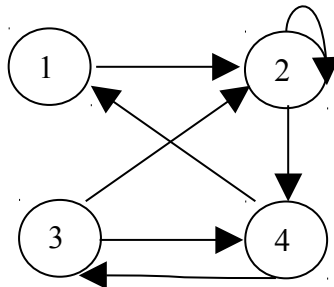


– **Grafos orientados para uma autorrelação**

Seja R uma autorrelação, ou seja, uma relação de um conjunto finito A nele mesmo. Os elementos do conjunto são representados por vértices do grafo e as setas são inseridas de cada elemento a para um elemento b sempre que a estiver relacionado a b . Esse diagrama é chamado **grafo orientado da relação**.

Exemplo:

- Sejam $A = \{1, 2, 3, 4\}$ um conjunto finito e $R = \{(1, 2), (2, 2), (2, 4), (3, 2), (3, 4), (4, 1), (4, 3)\}$ uma relação em A



Relações e modelo relacional de Banco de Dados

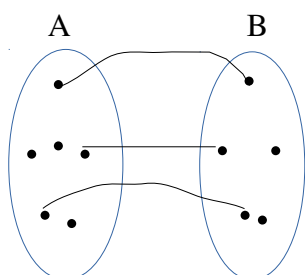
O **modelo relacional** é um modelo de dados que se baseia no princípio em que todos os dados estão guardados em tabelas (ou, matematicamente falando, relações). Toda sua definição é teórica e baseada na lógica de predicados e na teoria dos conjuntos.

É possível, então, fazer uma analogia entre os tipos de relações da matemática e do modelo relacional. Assim, considerando-se a relação R de A para B como o conjunto de pares ordenados da forma (x, y) , então

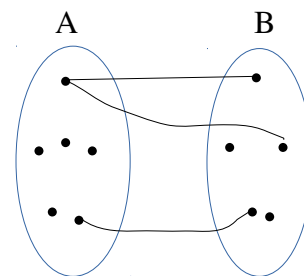
- Uma relação é **um para um** se cada primeiro elemento e cada segundo elemento

aparecem apenas uma vez na relação.

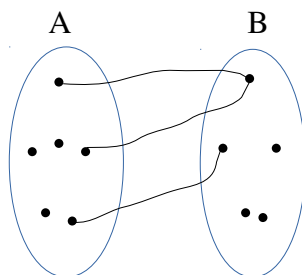
- Uma relação é **um para muitos** se algum primeiro elemento aparece mais de uma vez, isto é, se x aparece em mais de um par.
- Uma relação é **muitos para um** se algum segundo elemento y aparece em mais de um par.
- Uma relação é **muitos para muitos** se pelo menos um x aparece em mais de um par e pelo menos um y aparece em mais de um par.



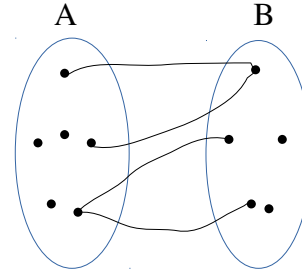
um para um (1-1)



um para muitos (1-n)



muitos para um (n-1)



muitos para muitos (n-n)

Note que nem todos os valores de A precisam ser elementos de algum par ordenado em R .

Algumas relações interessantes

– Relação de igualdade

Seja A um conjunto qualquer. A relação de igualdade sobre A , também chamada de identidade ou relação diagonal em A , é definida por $\{(a, a) \mid a \in A\}$.

Exemplo:

- Dado o conjunto $A = \{1, 2, 3, 4\}$, a relação de igualdade em A é $R = \{(1, 1), (2, 2), (3, 3), (4, 4)\}$

– **Relação inversa**

Seja R uma relação qualquer de um conjunto A para um conjunto B . A relação inversa de R , também chamada de relação dual ou relação oposta, denotada por R^{-1} , é a relação de B para A obtida invertendo-se a ordem de todos os pares ordenados em R .

$$R^{-1} = \{(x, y) \mid (y, x) \in R\}$$

Exemplo:

- Sejam $A = \{1, 2, 3\}$ e $B = \{x, y, z\}$ conjuntos e $R = \{(1, y), (1, z), (3, y)\}$ uma relação de A para B então $R^{-1} = \{(y, 1), (z, 1), (y, 3)\}$ é a relação inversa de R , de B para A

Proposição: Seja R uma relação. Então $(R^{-1})^{-1} = R$.

Como R , R^{-1} e $(R^{-1})^{-1}$ são todos conjuntos, para provar essa proposição podemos utilizar um esquema de prova baseado na propriedade que diz que $A = B$ se e somente se $A \subseteq B$ e $B \subseteq A$, como apresentado no Capítulo 2. Alternativamente essa prova pode ser escrita no esquema de prova apresentado a seguir (SCHEINERMAN, 2011).



Esquema de prova 8

Provar que dois conjuntos são iguais.

Sejam A e B os conjuntos. Para provar que $A = B$, temos o seguinte esquema:

- Suponhamos que $x \in A$... Portanto, $x \in B$.
- Suponhamos que $x \in B$... Portanto, $x \in A$.
- Portanto, $A = B$.

Prova:

Vamos provar que o inverso de uma relação inversa de R é a própria R , ou seja, que $(R^{-1})^{-1} = R$.

Para tanto, suponhamos que $(x, y) \in R$. Então, pela definição de relação inversa tem-se que $(y, x) \in R^{-1}$. Novamente, pela definição de relação inversa, se $(y, x) \in R^{-1}$ então $(x, y) \in (R^{-1})^{-1}$.

Agora vamos supor que $(x, y) \in (R^{-1})^{-1}$. Então, pela definição de relação inversa tem-se que $(y, x) \in R^{-1}$. Novamente, pela definição de relação inversa, se $(y, x) \in R^{-1}$ então $(x, y) \in R$.

Demonstramos que $(x, y) \in R \Leftrightarrow (x, y) \in (R^{-1})^{-1}$.

Portanto, $(R^{-1})^{-1} = R$. ■

3.3. Propriedades de autorrelações

Uma relação em um conjunto A (uma autorrelação) pode ter determinadas propriedades. Por exemplo, a relação R de igualdade em A , $x R y \leftrightarrow x = y$, tem três propriedades:

1. para qualquer $x \in A$, $x = x$, ou seja $(x, x) \in R$;
2. quaisquer que sejam $x, y \in A$, se $x = y$ então $y = x$, ou seja, $(x, y) \in R \rightarrow (y, x) \in R$;
3. quaisquer que sejam $x, y, z \in A$, se $x = y$ e $y = z$ então $x = z$, ou seja, $[(x, y) \in R \text{ e } (y, z) \in R] \rightarrow (x, z) \in R$.

Essas três propriedades fazem com que a relação de igualdade seja, respectivamente, reflexiva, simétrica e transitiva.

Definições

Seja R uma relação definida em um conjunto A . Então,

- R é *reflexiva* se para todo $x \in A$ temos $x R x$
- R é *simétrica* se para todo $x, y \in A$ temos $x R y \rightarrow y R x$
- R é *transitiva* se para todo $x, y, z \in A$ temos $(x R y \wedge y R z) \rightarrow x R z$.³
- R é *antissimétrica* se para todo $x, y \in A$ temos $(x R y \wedge y R x) \rightarrow x = y$
- R é *antirreflexiva* (ou *irreflexiva*) se para todo $x \in A$ temos x não R -relacionado com x

Veja que uma relação pode ser não reflexiva (quando existir um x que não se relaciona consigo mesmo) e não antirreflexiva (quando existir um x que se relaciona consigo mesmo) ao mesmo tempo, já que em ambas as definições necessariamente para todos os elementos do conjunto A a relação deve (reflexiva) ou não (antirreflexiva) existir.

Veja que as propriedades de simetria e antissimetria para relações não são exatamente opostas. Antissimétrica não significa não simétrica. Uma relação não é simétrica se algum (x, y) pertence à relação mas (y, x) não. Assim, as relações podem ser simétricas e não antissimétricas, antissimétricas e não simétricas, podem ser ao mesmo tempo simétricas e antissimétricas ou podem não ser nem simétrica nem antissimétrica.

Enquanto as propriedades reflexiva e antirreflexiva devem ser satisfeitas por todos os elementos do conjunto A , as demais relações envolvem apenas aqueles elementos especificados na premissa (lado esquerdo de \rightarrow); ou seja, se não houver uma premissa, não há a necessidade da

³ \wedge = e lógico

conclusão (lado direito de \rightarrow).

Exemplos:

- Relação = (igualdade) sobre \mathbb{Z} é
 - reflexiva: qualquer inteiro é igual a si mesmo
 - não antirreflexiva: pois é reflexiva
 - simétrica: se $x = y$ então $y = x$
 - antissimétrica: se $x = y$ e $y = x$ então x e y são o mesmo elemento
 - transitiva: se $x = y$ e $y = z$ então $x = z$
- Relação \leq (menor ou igual) sobre \mathbb{Z} é
 - reflexiva: para qualquer inteiro x , é verdade que $x \leq x$
 - não antirreflexiva: pois é reflexiva
 - não simétrica: $x \leq y \nrightarrow y \leq x$
 - antissimétrica: se $x \leq y$ e $y \leq x$, então $x = y$
 - transitiva: $x \leq y$ e $y \leq z$ implicam $x \leq z$
- Relação $<$ (estritamente menor que) sobre \mathbb{Z} é
 - antirreflexiva: pois por exemplo, $3 < 3$ é falso
 - não reflexiva: pois é antirreflexiva
 - não simétrica: $x < y \nrightarrow y < x$
 - antissimétrica: não há premissa para ser verificada ($x R y \wedge y R x$), ela é sempre falsa pois não há par (x, y) e (y, x) , portanto, é verdadeira a propriedade
 - transitiva: $x < y$ e $y < z$ implicam $x < z$
- Relação $|$ (divide) sobre \mathbb{N}^* é
 - reflexiva: para qualquer número natural x (veja que x não é 0 pois $0 \notin \mathbb{N}^*$), x divide ele mesmo resultando no número natural 1
 - não antirreflexiva: pois é reflexiva
 - não simétrica: por exemplo, 2 divide 4 mas 4 não divide 2
 - antissimétrica: se x e y são números naturais com $x | y$ e $y | x$ então $x = y$
 - transitiva: se x divide y e y divide z então x divide z
- Relação $|$ (divide) sobre \mathbb{Z}^* é
 - reflexiva: para qualquer número inteiro x (veja que x não é 0 pois $0 \notin \mathbb{Z}^*$), x

divide ele mesmo resultando no número inteiro 1

- não antirreflexiva: pois é reflexiva
- não simétrica: por exemplo, 3 divide 9 mas 9 não divide 3
- não antissimétrica: por exemplo, $3 \mid -3$ e $-3 \mid 3$ mas $3 \neq -3$
- transitiva: por exemplo, $2 \mid 4$ e $4 \mid 8$ então $2 \mid 8$
- Relação de inclusão de conjuntos (\subseteq) é
 - reflexiva: já que todo conjunto é subconjunto de si mesmo
 - não antirreflexiva: pois é reflexiva
 - não simétrica: já que $A \subseteq B$ não implica $B \subseteq A$
 - antissimétrica: já que se $A \subseteq B$ e $B \subseteq A$ então $A = B$
 - transitiva: já que se $A \subseteq B$ e $B \subseteq C$ então $A \subseteq C$

Tabela 2: Resumo das propriedades das auto-relações exemplificadas.

	=	\leq	<	\mid sobre \mathbb{N}^*	\mid sobre \mathbb{Z}^*	\subseteq
Reflexiva	✓	✓		✓	✓	✓
Antirreflexiva			✓			
Simétrica	✓					
Antissimétrica	✓	✓	✓	✓		✓
Transitiva	✓	✓	✓	✓	✓	✓

Importante:

- As propriedades são atributos de uma relação R definida em um conjunto A . O conhecimento do conjunto A é fundamental para que se determine se a relação é ou não reflexiva, enquanto que para as outras propriedades é suficiente olhar apenas para os pares ordenados em R

Exemplo:

Considere a relação $R = \{(1, 1), (1, 2), (2, 2), (2, 3), (3, 3)\}$.

- R é reflexiva? A resposta depende do conjunto no qual ela está definida. Por exemplo,
 - Se R é uma relação no conjunto $\{1, 2, 3\}$: SIM, ela é reflexiva
 - Se R é uma relação sobre todo o \mathbb{Z} : NÃO, ela não é reflexiva pois há

vários outros elementos de \mathbb{Z} para os quais nada é especificado na relação R

- R é simétrica? A resposta pode ser dada olhando-se apenas os pares ordenados em R o que, nesse caso, nos dá a resposta NÃO já que, por exemplo, $(2, 1)$ não está em R

3.4. Relação de equivalência

Seja R uma relação em um conjunto A . Dizemos que R é uma **relação de equivalência** em A se R é reflexiva, simétrica e transitiva. A relação de igualdade ($x R y \leftrightarrow x = y$) apresentada anteriormente é, portanto, uma relação de equivalência. Na verdade, as relações de equivalência são relações que apresentam forte semelhança com a relação de igualdade, ou seja, objetos relacionados por uma relação de equivalência são objetos parecidos.

Exemplos:

- O produto cartesiano de um conjunto A por ele mesmo, $A \times A$, é uma relação de equivalência. Por exemplo, para $A = \{1, 2, 3\}$ $A^2 = \{(1, 1), (1, 2), (1, 3), (2, 1), (2, 2), (2, 3), (3, 1), (3, 2), (3, 3)\}$, ou seja, uma relação:
 - reflexiva pois $(1, 1), (2, 2), (3, 3) \in A^2$
 - simétrica pois $(1, 2), (2, 1), (1, 3), (3, 1), (2, 3), (3, 2) \in A^2$
 - transitiva pois $(1, 2), (2, 3), (1, 3) \in A^2, (1, 3), (3, 2), (1, 2) \in A^2$ etc.
- A relação “tem o mesmo tamanho que” definida sobre o conjunto das partes de um conjunto A qualquer. Assim, para dois conjuntos B e $C \in 2^A$ tem-se que $B R C$ se e somente se $|B| = |C|$.
- Em \mathbb{N} , $x R y \leftrightarrow x + y$ é par
- Em $\{0, 1\}$, $x R y \leftrightarrow x = y^2$
- Em $\{x \mid x \text{ é um aluno dessa turma}\}$, $x R y \leftrightarrow$ “ x senta-se na mesma fila que y ”
- Em $\{1, 2, 3\}$, $R = \{(1, 1), (2, 2), (3, 3), (1, 2), (2, 1)\}$

Classes de equivalência

Seja R uma relação de equivalência em um conjunto A e seja $a \in A$. A classe de equivalência de a , denotada por $[a]$, é o conjunto de todos os elementos do conjunto A que estão R -relacionados com a ; isto é,

$$[a] = \{x \mid x \in A \text{ e } x R a\}$$

Qualquer $b \in [a]$ é dito representante da classe de equivalência. Uma classe de equivalência pode usar o nome de qualquer de seus elementos. Uma relação de equivalência sempre determina classes de equivalência sobre o conjunto em que está definida.

Exemplos:

- Dado o conjunto $A = \{a, b, c\}$ e a relação de equivalência $R = \{(a, a), (b, b), (c, c), (a, c), (c, a)\}$, o conjunto $[a] = \{a, c\}$. Esse conjunto também pode ser chamado de $[c]$.
- Dado o conjunto $A = \{1, 2, 3, 4, 5\}$ e a relação de equivalência $R = \{(1, 1), (2, 2), (1, 2), (2, 1), (1, 3), (3, 1), (3, 2), (2, 3), (3, 3), (4, 4), (5, 5), (4, 5), (5, 4)\}$, por exemplo, o conjunto $[3] = \{1, 2, 3\}$ e o $[4] = \{4, 5\}$.
- No caso em que $x R y \leftrightarrow$ "x senta-se na mesma fila que y", suponha que João, Carlinhos, José, Judite e Téo sentam-se todos na terceira fila. Então, a classe de equivalência de João é $[João] = \{João, Carlinhos, José, Judite, Téo\}$, ou seja, todos os colegas que sentam na mesma fila que João. Além disso, $[João] = [Téo] = [Judite]$ e assim por diante.

Classes de equivalência e Partições

As relações de equivalência têm uma forte relação com as partições de conjuntos (veja capítulo 2).⁴ Note que ou duas classes de equivalência não têm nenhum elemento em comum ou, se têm um elemento comum, então tem todos, ou seja, são idênticas. Em outras palavras, as classes de equivalência são disjuntas duas a duas (SCHEINERMAN, 2011). Assim, qualquer relação de equivalência determina uma partição no conjunto em que está definida. Por exemplo, ao agrupar todos os alunos no conjunto $A = \{x \mid x \text{ é um aluno dessa turma}\}$ de acordo com a relação R , $x R y \leftrightarrow$ "x senta-se na mesma fila que y" chegamos à figura a seguir:

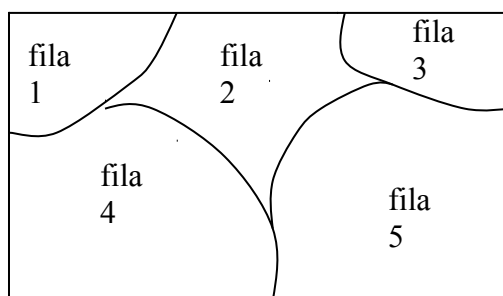


Figura 8. Diagrama de Venn que representa uma partição do conjunto de alunos via relação de equivalência $x R y \leftrightarrow$ "x senta-se na mesma fila que y".

Dividimos o conjunto A em subconjuntos de tal maneira que todos na turma pertencem a

⁴ Uma partição de um conjunto A é uma coleção de subconjuntos disjuntos não-vazios cuja união é igual a A .

um, e apenas um, subconjunto (ou seja, a apenas uma fila). Os subconjuntos que compõem a partição, chamados algumas vezes de **blocos** da partição, são formados agrupando-se os elementos relacionados.

Teorema 3.1

Seja R uma relação de equivalência em um conjunto A . As classes de equivalência de R são subconjuntos não vazios de A , disjuntos dois a dois, cuja união é A .

Reescrevendo esse teorema para incluir a definição de partição:

Reescrevendo o Teorema 3.1

Seja R uma relação de equivalência em um conjunto A . O conjunto das classes de equivalência de A pela R é uma partição de A . Especificamente:

- (i) para cada $a \in A$, temos $a \in [a]$
- (ii) $[a] = [b]$ se e somente se $(a,b) \in R$
- (iii) se $[a] \neq [b]$, então $[a]$ e $[b]$ são disjuntos

Em outras palavras, em (i) temos que o elemento pertence a sua própria classe de equivalência, ou seja, está relacionado consigo mesmo já que toda relação de equivalência é reflexiva. Em (ii) sabe-se que a classe de equivalência de dois elementos são iguais se eles se relacionam entre si já que, neste caso, um necessariamente faz parte da relação do outro já que toda relação de equivalência é simétrica. Por fim, (iii) é uma decorrência de (ii), pois se as classes de equivalência $[a]$ e $[b]$ fossem iguais, haveria relação entre a e b – $(a,b) \in R$ – e as classes compartilhariam os mesmos elementos, ou seja, $[a] \cap [b] \neq \emptyset$ fazendo $[a]$ e $[b]$ não disjuntos.

Exemplo:

- A relação de equivalência em \mathbb{N} , $x R y \leftrightarrow "x + y \text{ é par}"$ divide \mathbb{N} em duas classes de equivalência. Se x é um número par, então, para todo número par y , $x + y$ é par e $y \in [x]$. Todos os números pares formam uma classe. Se x é ímpar, então, para todo número ímpar y , $x + y$ é par e $y \in [x]$. Todos os números ímpares formam uma segunda classe. A partição é representada abaixo:

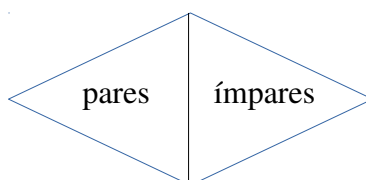


Figura 9. Partição do conjunto dos números naturais definida via relação de equivalência $x R y \leftrightarrow "x + y \text{ é par}"$.

Conjunto quociente

A coleção de todas as classes de equivalência de elementos de A por uma relação de equivalência R é chamada de **conjunto quociente** de A por R e é denotada por A/R :

$$A/R = \{[a] \mid a \in A\}$$

Exemplos:

- Dado o conjunto $A = \{a, b, c\}$ e a relação de equivalência $R = \{(a, a), (b, b), (c, c), (a, c), (c, a)\}$ as classes de equivalência são: $[a] = \{a, c\} = [c]$ e $[b] = \{b\}$. Assim, o conjunto quociente $A/R = \{[a], [b]\}$
- Dado o conjunto $A = \{1, 2, 3, 4, 5\}$ e a relação de equivalência $R = \{(1, 1), (2, 2), (1, 2), (2, 1), (1, 3), (3, 1), (3, 2), (2, 3), (3, 3), (4, 4), (5, 5), (4, 5), (5, 4)\}$ as classes de equivalência são: $[1] = \{1, 2, 3\} = [2] = [3]$ e $[4] = \{4, 5\} = [5]$. Assim, o conjunto quociente $A/R = \{[1], [4]\}$.

O Teorema 3.1 pode, ainda ser reescrito usando o conceito de Conjunto Cociente como:

“Seja R uma relação de equivalência em um conjunto A . O quociente A/R é uma partição de A .”



Utilidade das classes de equivalência

A divisão de um conjunto em classes de equivalência é útil porque é conveniente, em muitas situações, subir o nível de abstração e tratar as classes como entidades.

Por exemplo, seja $F = \{a/b \mid a, b \in \mathbb{Z}, b \neq 0\}$. Portanto, F é o conjunto de todas as frações. Duas frações como $1/2$ e $2/4$ são ditas equivalentes. Formalmente, a/b é equivalente a c/d , denotado por $a/b \sim c/d$ se, e somente se, $ad = bc$. Vamos mostrar que a relação \sim em F é uma relação de equivalência:

- $a/b \sim a/b$ já que $ab = ba \Rightarrow \sim$ é reflexiva
- se $a/b \sim c/d$ então $ad = bc$ ou $cb = da$ e $c/d \sim a/b \Rightarrow \sim$ é simétrica
- se $a/b \sim c/d$ e $c/d \sim e/f$ então $ad = bc$ e $cf = de$. Multiplicando a primeira equação por f e a segunda por b obtemos $adf = bcf$ e $bcf = bde$. Logo, $adf = bde$ ou, dividindo ambos os lados por d : $af = be$. Portanto, $a/b \sim e/f \Rightarrow \sim$ é transitiva

Algumas amostras de classes de equivalência de F por essa relação de equivalência são:

$$[1/2] = \{ \dots, -3/-6, -2/-4, -1/-2, 1/2, 2/4, 3/6, 4/8, 5/10, \dots \}$$

$$[3/10] = \{ \dots, -9/-30, -6/-20, -3/-10, 3/10, 6/20, 9/30, \dots \}$$

O conjunto \mathbb{Q} dos números racionais pode ser considerado como sendo o conjunto de todas as classes de equivalência de F . Um único número racional, como $[1/2]$, pode ser representado por muitas frações. Por exemplo, para somar $[1/2] + [3/10]$ procuramos por representantes das classes que tenham o mesmo denominador e somamos esses representantes. Assim, para somar $[1/2] + [3/10]$ representamos $[1/2]$ por $5/10$ e $[3/10]$ por $3/10$ resultando em $8/10$ e, normalmente, escreve-se $[8/10]$ como $[4/5]$.

Esse procedimento é tão familiar que, em geral, escreve-se $1/2 + 3/10 = 4/5$; de qualquer forma, as classes de frações estão sendo manipuladas através de seus representantes.

3.5. Relação de ordem

Enquanto uma relação de equivalência estabelece uma relação entre elementos parecidos, uma relação de ordem reflete a noção intuitiva de ordenação, de sequência, de sucessão (MENEZES, 2005).

Relações de ordem parcial

Uma relação R em um conjunto A é dita um ordenamento parcial ou uma **ordem parcial** se R é reflexiva, antissimétrica e transitiva. Além disso, uma relação de ordem parcial R é chamada de **ordem parcial estrita** se ela é antirreflexiva, antissimétrica e transitiva.

Exemplos:

- A relação de inclusão de conjuntos, \subseteq , é uma ordem parcial em qualquer coleção de conjuntos já que:
 - a. é reflexiva ($A \subseteq A$ para todo conjunto A)
 - b. é antissimétrica (se $A \subseteq B$ e $B \subseteq A$, então $A = B$)
 - c. é transitiva (se $A \subseteq B$ e $B \subseteq C$, então $A \subseteq C$)
- A relação $<$ (estritamente menor que) sobre os inteiros é uma ordem parcial estrita:
 - a. é antirreflexiva (pois para todo inteiro, ele não é menor do ele mesmo, por exemplo, $3 < 3$ é falso)

b. é transitiva (por exemplo, $3 < 4$ e $4 < 5$ então $3 < 5$)

c. é antissimétrica como consequência das duas propriedades anteriores, uma vez que sendo transitiva tem-se que se $x R y$ e $y R x$ (premissa da antissimetria) implicaria em $x R x$ o que seria impossível já que a relação é antirreflexiva. Assim, nunca ocorrerá $x R y$ e $y R x$ e a antissimetria é válida

Outros exemplos de ordem parcial:

- Em \mathbb{N} , $x R y \leftrightarrow x \leq y$
- Em \mathbb{Z}^+ , $x R y \leftrightarrow x$ divide y
- Em $\{0, 1\}$, $x R y \leftrightarrow x = y^2$

Conjunto parcialmente ordenado

Se R é uma ordem parcial no conjunto A , então o par ordenado (A, R) é chamado um **conjunto parcialmente ordenado** ou poset (*partially ordered set*) ou, ainda, PO. Denotaremos um conjunto parcialmente ordenado arbitrário por (A, \preceq) ; em qualquer caso particular, \preceq tem algum significado preciso como "menor ou igual a", "é subconjunto de" ou outra relação de ordem parcial.

As ordens parciais descrevem alguma ordem mesmo quando nem todos os elementos são comparáveis, ou seja, mesmo quando a relação de ordem não é satisfeita para todos os elementos. Para passar a ideia de ordenação usamos o símbolo \preceq para ordens parciais e o símbolo $<$ para ordens parciais estritas. O inverso de $<$ é denotado por $>$ e o inverso de \preceq é \succeq . Consequentemente, se (A, \preceq) é um poset seu dual é (A, \succeq) .

Ordem total (ordem linear)

Os conjuntos parcialmente ordenados podem conter elementos não comparáveis. Esta é a característica que torna a relação de ordem algo “parcial”. Dado um conjunto parcialmente ordenado (A, R) e $x, y \in A$, dizemos que os elementos x e y são **comparáveis** se e somente se $x R y$ ou $y R x$. Se os elementos x e y não estiverem relacionados por meio da relação de ordem parcial R , então eles são **não comparáveis**.

Uma **ordem total**, ou **ordem linear**, por sua vez, é um conjunto parcialmente ordenado no qual não existem elementos não comparáveis (SCHEINERMAN, 2011).

Exemplos:

- O conjunto (\mathbb{Z}, \leq) é uma ordem total, ou seja, todos os inteiros estão relacionados entre si, dois a dois, por meio da relação “menor ou igual a” (\leq)

- O conjunto parcialmente ordenado formado pelo conjunto $Q = \{1, 3, 9, 27, 81\}$, dos divisores de 81, ordenados por divisibilidade, é uma ordem total

As ordens totais satisfazem a regra da tricotomia que define uma **relação conexa**: para todos os x e y no conjunto PO, exatamente uma das seguintes possibilidades é verdadeira

- $x \leq y$,
- $y \leq x$,
- $x = y$.

Tabela 3: Resumo das propriedades das relações de ordem. Adaptado de (MENEZES, 2005).

	Ordem parcial	Ordem parcial estrita	Ordem total	Ordem total estrita
Reflexiva	✓		✓	
Antirreflexiva		✓		✓
Antissimétrica	✓	✓	✓	✓
Transitiva	✓	✓	✓	✓
Conexa			✓	✓

Predecessor e sucessor

Se $x \leq y$ e $x \neq y$, ou seja $x < y$, dizemos que x é **predecessor** de y ou que y é **sucessor** de x . Em outras palavras, se $x R y$ e $x \neq y$, dizemos que x é **predecessor** de y e y é **sucessor** de x . Um dado y pode ter muitos predecessores mas se $x < y$ ($x R y$) e se não existe nenhum z com $x < z < y$ ($x R z$ e $z R y$) então x é o **predecessor imediato** de y ; nesse caso, também dizemos que y é o **sucessor imediato** de x .

Exemplo:

- Considere a relação $R \leftrightarrow "x \text{ divide } y"$ em $A = \{1, 2, 3, 6, 12, 18\}$. Os pares ordenados (x, y) pertencentes a essa relação são $R = \{(1, 1), (1, 2), (2, 2), (1, 3), (3, 3), (1, 6), (2, 6), (3, 6), (6, 6), (1, 12), (2, 12), (3, 12), (6, 12), (12, 12), (1, 18), (2, 18), (3, 18), (6, 18), (18, 18)\}$
 - Os predecessores de 6 são: 1, 2, 3
 - Os predecessores imediatos de 6 são: 2, 3

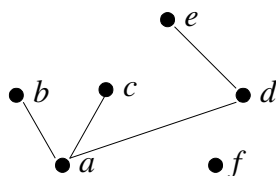
Diagrama de Hasse

Se A for finito, podemos representar visualmente um conjunto parcialmente ordenado (A, \leq) por um **diagrama de Hasse**. Cada elemento de A é representado por um ponto, denominado **nó** ou **vértice** do diagrama. Se x é o predecessor imediato de y então o nó que representa y é colocado acima do nó que representa x e os dois nós são conectados por um segmento de reta (não necessariamente na vertical).

O diagrama de Hasse de um conjunto parcialmente ordenado contém toda a informação sobre a ordem parcial. Podemos reconstruir o conjunto de pares ordenados analisando o diagrama. Os nós e os segmentos de reta no diagrama nos dão, imediatamente, os pares (predecessor, sucessor). Podemos completar o resto usando a reflexividade e a transitividade.

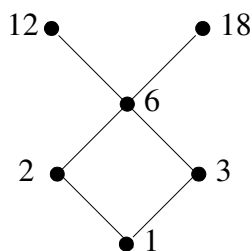
Exemplos:

- Dado o diagrama de Hasse de uma ordem parcial \leq em um conjunto $\{a, b, c, d, e, f\}$ a seguir, para se determinar os pares ordenados que compõem essa relação deve-se levar em conta que a relação é reflexiva, antissimétrica e transitiva.



Assim, podemos concluir que \leq é o conjunto $\{(a, a), (b, b), (c, c), (d, d), (e, e), (f, f), (a, b), (a, c), (a, d), (d, e), (a, e)\}$. Essa conclusão foi tomada com base: (i) na reflexividade da relação (6 primeiros pares), (ii) no que está explicitamente demonstrado pelas conexões do diagrama (4 pares seguintes) e (iii) na transitividade da relação (último par), ou seja, já que (a, d) e (d, e) estão presentes na relação, então (a, e) também deve estar.

- O diagrama de Hasse para a relação R : “ x divide y ” em $\{1, 2, 3, 6, 12, 18\}$ é apresentado a seguir



Quais seriam os pares ordenados que compõem a relação de ordem parcial representada por esse diagrama de Hasse?

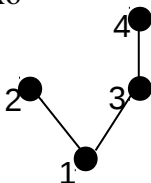
Veja que, nesse diagrama de Hasse, os elementos não comparáveis são 2 e 3 e 12 e 18, uma vez que 2 não divide 3 nem 3 divide 2, ou seja, $(2, 3)$ não pertence a R e $(3, 2)$ também não pertence a R ; algo semelhante ocorre entre 12 e 18. Os demais pares de elementos são comparáveis.

Cadeia e Anticadeia

Dado um conjunto parcialmente ordenado $P = (A, R)$ e seja C subconjunto de A ($C \subseteq A$). Dizemos que C é uma **cadeia** de P se os elementos de todos os pares em C forem comparáveis. Dizemos que C é uma **anticadeia** de P se, para todos os pares distintos de C , os elementos não são comparáveis.

Exemplos:

- Para o poset representado abaixo



- Os conjuntos $\{1, 2\}$ e $\{1, 3, 4\}$ são exemplos de cadeias
- Os conjuntos $\{2, 3\}$ e $\{2, 4\}$ são exemplos de anticadeias

Elemento mínimo e elemento máximo, minimal e maximal

Vamos considerar, novamente, um conjunto parcialmente ordenado (A, \leq) . Se existe um $y \in A$ tal que $y \leq x$ para todo $x \in A$, então y é um **elemento mínimo** (ou o **menor elemento**) do conjunto parcialmente ordenado. Se existe um $y \in A$ tal que $x \leq y$ para todo $x \in A$, então y é um **elemento máximo** (ou o **maior elemento**) do conjunto parcialmente ordenado.

Um elemento $y \in A$ é dito **minimal** se não existe $x \in A$ com $x < y$. Um elemento $y \in A$ é dito **maximal** se não existe $x \in A$ com $y < x$.

Exemplo:

- No conjunto parcialmente ordenado da relação “ x divide y ” em $\{1, 2, 3, 6, 12, 18\}$ (diagrama de Hasse apresentado anteriormente) tem-se que:
 - elemento mínimo = 1
 - elemento minimal = 1
 - elementos maximais = 12 e 18

- elemento máximo = não há

Importante:

- Se existir um elemento mínimo, ele é único e o mesmo é válido para um elemento máximo: se existir, ele é único.
- Em um diagrama de Hasse, o elemento mínimo está abaixo de todos os outros, enquanto um elemento minimal não tem elementos abaixo dele. Definições análogas podem ser feitas para o elemento máximo (ou maior elemento) e para os elementos maximais.
- O elemento mínimo é sempre minimal e o elemento máximo é sempre maximal, mas a recíproca não é verdadeira. Em um conjunto totalmente ordenado, no entanto, um elemento minimal é o elemento mínimo e um elemento maximal é o elemento máximo.

Supremo, ínfimo e reticulado

Seja (A, \leq) um conjunto parcialmente ordenado. Quaisquer que sejam x e $y \in A$, definimos como **supremo** de x e y como sendo um elemento z tal que $x \leq z$, $y \leq z$ e, se existir algum elemento z^* com $x \leq z^*$ e $y \leq z^*$ então $z \leq z^*$. Em outras palavras, o supremo é o menor dos limitantes superiores. O **ínfimo** de x e y é um elemento w tal que $w \leq x$, $w \leq y$ e se existir algum elemento w^* com $w^* \leq x$ e $w^* \leq y$ então $w^* \leq w$. Em outras palavras, o ínfimo é o maior dos limitantes inferiores.

Um **reticulado** é, então, um conjunto parcialmente ordenado no qual quaisquer dois elementos arbitrários x e y têm um supremo e um ínfimo.

Exemplo:

- De acordo com a definição acima, dos posets representados por seus diagramas de Hasse a seguir, o segundo diagrama não é um reticulado. Isso porque os elementos b e c não têm supremo. Os elementos d, e e f são limitantes superiores de b e c , no entanto não existe o menor entre eles.

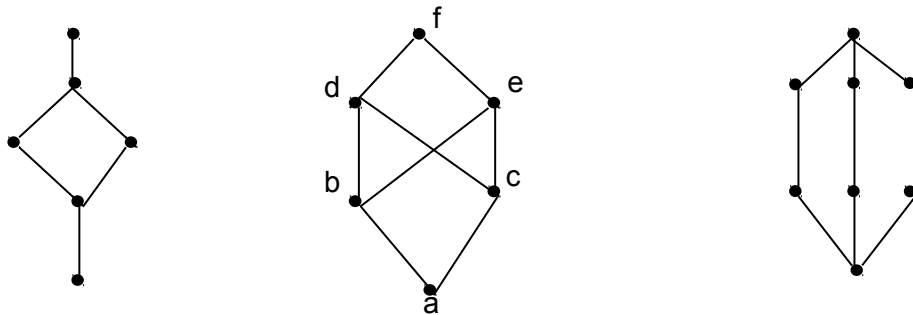


Tabela 4: Tabela que resume as propriedades das relações de equivalência e de ordem parcial

	Relação de equivalência	Relação de ordem parcial	Relação de ordem parcial estrita
Reflexiva	✓	✓	
Antirreflexiva			✓
Simétrica	✓		
Antissimétrica		✓	✓
Transitiva	✓	✓	✓
Característica	Determina uma partição	Determina uma ordenação (predecessores e sucessores)	

Resumindo

Conceitos aprendidos nesse capítulo

- par ordenado - é um par de elementos da forma (x, y) onde x é o primeiro elemento do par e y é o segundo elemento do par
- produto cartesiano de A por B ($A \times B$) - é o conjunto de todos os pares ordenados com o primeiro elemento em A e o segundo elemento em B
- relação R de A para B - é um subconjunto de $A \times B$ e $x R y$ indica que o par ordenado (x, y) satisfaz a relação R
- relação de igualdade sobre A - é definida por $\{(a, a) \mid a \in A\}$
- relação inversa de R (R^{-1}) - é a relação obtida invertendo-se a ordem de todos os pares ordenados em R
- relação reflexiva R em um conjunto A - é uma relação na qual para todo $x \in A$ temos $x R x$
- relação simétrica R em um conjunto A - é uma relação na qual para todo $x, y \in A$ temos $x R y \rightarrow y R x$
- relação transitiva R em um conjunto A - é uma relação na qual para todo $x, y, z \in A$ temos $(x R y \wedge y R z) \rightarrow x R z$
- relação antissimétrica R em um conjunto A - é uma relação na qual para todo $x, y \in A$ temos $(x R y \wedge y R x) \rightarrow x = y$
- relação de equivalência - é uma relação reflexiva, simétrica e transitiva
- classe de equivalência de $a \in A$ ($[a]$) - é o conjunto de todos os elementos do conjunto A que

estão R-relacionados com a

- conjunto quociente de um conjunto A e uma relação R (A/R) - é a coleção de todas as classes de equivalência de elementos de A por uma relação de equivalência R
- relação de ordem parcial (\preceq) - é uma relação reflexiva, antissimétrica e transitiva
- relação de ordem parcial estrita (\prec) - é uma relação de ordem parcial que não é reflexiva
- conjunto parcialmente ordenado ou poset (A, R) - é o conjunto composto por uma relação de ordem parcial R em um conjunto A
- predecessor ($x \prec y$) - x é predecessor de y se $x \prec y$. Se não existe nenhum z com $x \prec z \prec y$ então x é o predecessor imediato de y
- sucessor ($x \prec y$) - y é sucessor de x se $x \prec y$. Se não existe nenhum z com $x \prec z \prec y$ então y é o sucessor imediato de x
- diagrama de Hasse - é a representação gráfica de um poset (A, \preceq) na qual cada elemento de A é representado por um vértice do diagrama e se x é o predecessor imediato de y , o nó que representa y é colocado acima do nó que representa x e os dois nós são conectados por um segmento de reta
- relação de ordem total - é uma ordem parcial onde todo elemento do conjunto está relacionado a todos os outros elementos
- elemento mínimo ou menor elemento de um poset (A, \preceq) - é o elemento $y \in A$ tal que $y \preceq x$ para todo $x \in A$. Se existir, ele é único
- elemento máximo ou maior elemento de um poset (A, \preceq) - é o elemento $y \in A$ tal que $x \preceq y$ para todo $x \in A$. Se existir, ele é único
- elemento minimal - é o elemento $y \in A$ se não existe $x \in A$ com $x \prec y$
- elemento maximal - é o elemento $y \in A$ se não existe $x \in A$ com $y \prec x$
- supremo - é o menor dos limitantes superiores
- ínfimo - é o maior dos limitantes inferiores
- reticulado - é um poset onde dois elementos arbitrários x e y têm um supremo e um ínfimo

4. Funções

No capítulo 3 vimos o que são as relações binárias e, neste capítulo, veremos casos particulares de relações binárias: as **funções**.

Informalmente, uma **função** pode ser entendida como uma regra ou um mecanismo que transforma uma quantidade em outra (ou uma entrada em uma saída) como ilustrado na figura a seguir (SCHEINERMAN, 2011).

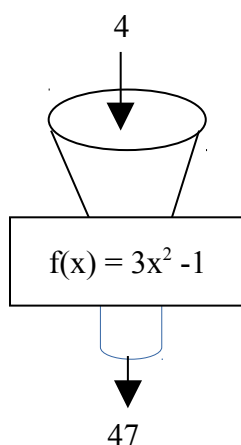
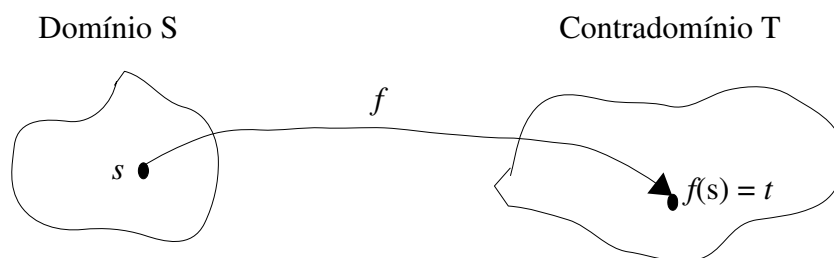


Figura 10. Ilustração de uma função como um mecanismo que transforma uma entrada em uma saída.

Uma função está composta por 3 partes:

- 1 - um conjunto de valores iniciais: o **domínio** da função;
- 2 - um conjunto de onde saem os valores associados: o **contradomínio** da função;
- 3 - a **associação** propriamente dita.

Tanto o domínio quanto o contradomínio representam conjuntos onde os valores são escolhidos. A representação gráfica desses elementos considerando-se uma função arbitrária f poderia ser:



Nessa figura, f é uma função de S em T , simbolizada por $f: S \rightarrow T$. S é, portanto, o domínio e T é o contradomínio. A associação propriamente dita é um conjunto de pares ordenados da forma (s, t) onde $s \in S$, $t \in T$ e t é o valor em T que a função associa ao valor s em S ; $t = f(s)$. Logo, a associação é um subconjunto de $S \times T$ (uma relação binária de S em T).

A propriedade dessa relação binária que a torna uma função é que todo elemento de S tem que ter um, e um único, valor em T associado, de modo que todo $s \in S$ aparece exatamente uma vez como o primeiro elemento de um par (s, t) .

Definição

Sejam S e T conjuntos. Uma **função (aplicação)** f de S em T , $f: S \rightarrow T$, é um subconjunto de $S \times T$ tal que cada elemento de S aparece exatamente uma vez como o primeiro elemento de um par ordenado. S é o **domínio** e T é o **contradomínio** da função. Se (s, t) pertence à função, então denotamos t por $f(s)$; t é a **imagem** de s sob f , s é uma **imagem inversa** de t sob f e f leva s em t . Assim, a notação $f: S \rightarrow T$ se lê “ f é uma função de S para T ” nos sugere 3 coisas: (1) f é uma função, (2) $\text{dom } f = S$ e (3) $\text{im } f \subseteq T$ (SCHEINERMAN, 2011).

Em outras palavras, uma relação f é chamada de função desde que $(a, b) \in f$ e $(a, c) \in f$ impliquem em $b = c$. O domínio de f , ou seja, o conjunto de todos os primeiros elementos possíveis dos pares ordenados de f é denotado por $\text{dom } f$; enquanto a imagem de f , ou seja, o conjunto de todos os segundos elementos possíveis dos pares ordenados de f , é denotada por $\text{im } f$. Em outra notação (SCHEINERMAN, 2011),

$$\text{dom } f = \{a \mid \exists b, (a, b) \in f\} \quad \text{e} \quad \text{im } f = \{b \mid \exists a, (a, b) \in f\} \quad \text{ou, alternativamente,}$$

$$\text{dom } f = \{a \mid f(a) \text{ está definido}\} \quad \text{e} \quad \text{im } f = \{b \mid b = f(a) \text{ para algum } a\}$$

Exemplos de funções:

- Considerando-se a função $f: \mathbb{Z} \rightarrow \mathbb{Z}$ dada por $f(x) = x^2$
 - o valor da imagem de -4, ou seja, de $f(-4)$ é 16
 - as imagens inversas de 9 são -3 e +3
 - o domínio de f é o conjunto de todos os inteiros
 - a imagem de f é o conjunto de todos os quadrados perfeitos
- Para $g: \mathbb{Z} \rightarrow \mathbb{N}$, onde g é definida por $g(x) = |x|$ (módulo de x) temos que g é uma função, pois todo número inteiro tem apenas um único valor possível para módulo. Por exemplo, $g(-3) = |-3| = 3$, $g(3) = |3| = 3$, $g(-8) = |-8| = 8$ etc.

- Seja S o conjunto de todas as cadeias de caracteres de comprimento finito. Então, a associação que leva cada cadeia em seu número de caracteres é uma função com domínio S e contradomínio \mathbb{N} (permitimos a cadeia vazia, que tem zero caractere).

Exemplos do que NÃO é função:

- Para $f: S \rightarrow T$, onde $S = T = \{1, 2, 3\}$, $f = \{(1, 1), (2, 3), (3, 1), (2, 1)\}$ temos que f não é uma função já que existem dois valores associados a $2 \in S$: 3 e 1.
- Para $h: \mathbb{N} \rightarrow \mathbb{N}$, onde h é definida por $h(x) = x - 4$ temos que h não é uma função já que para os valores 0, 1, 2 e 3 do domínio, os valores correspondentes $h(x)$ não pertencem ao contradomínio, ou seja, h não está definida para todos os valores do domínio.

A partir dos exemplos acima fica claro que uma função de S em T é um subconjunto de $S \times T$ com algumas restrições sobre os pares ordenados que contém. Pela definição de função, uma relação do tipo um para muitos (ou muitos para muitos) não pode ser uma função. Além disso, cada elemento de S tem que aparecer como um primeiro elemento.

Caraterísticas importantes

- **Consistência** - Toda vez que um número específico é fornecido como entrada para uma função, a mesma saída é retornada.
- **Valores não numéricos** - As entradas e saídas de uma função não precisam ser números (veja último exemplo acima).
- **Descrição não algébrica** - O mecanismo de uma função não precisa ser expresso em forma algébrica (veja último exemplo acima).
- **Funções de várias variáveis** - A definição de uma função inclui funções de mais de uma variável. Podemos ter uma função $f: S_1 \times S_2 \times \dots \times S_n \rightarrow T$ que associa cada n -upla de elementos (s_1, s_2, \dots, s_n) , $s_i \in S$, um único elemento de T .
- **Descrição completa** - Uma definição completa de uma função necessita que se dê o domínio, o contradomínio e a associação, na qual a associação pode ser dada por uma descrição verbal, um gráfico, uma equação ou um conjunto de pares ordenados.

Notação

Seja f uma função e seja a um objeto. A notação $f(a)$ é definida desde que exista um objeto b tal que $(a, b) \in f$. Nesse caso, $f(a) = b$. Se não existir par ordenado $(a, -)$ em f , $f(a)$ não está definida.

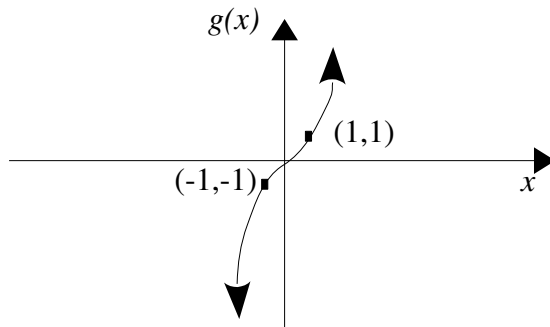
Representação gráfica de funções

- **Gráfico de funções** - Uma maneira de visualizar funções cujas entradas e saídas são números reais (\mathbb{R}).

Para traçar o gráfico de uma função, marcamos um ponto no plano com as coordenadas $(x, f(x))$ para todo $x \in \text{dom } f$. O gráfico construído dessa maneira representa uma função se qualquer reta vertical no plano intercepta o gráfico no máximo em um ponto (teste da reta vertical). Isso porque se uma reta vertical interceptar o gráfico da função em mais de um ponto significa que existe mais de um valor de saída associado a cada valor de entrada e isto contradiz a definição de função (SCHEINERMAN, 2011).

Exemplo:

- A seguir apresenta-se o gráfico para a função definida em \mathbb{R} $g(x) = x^3$

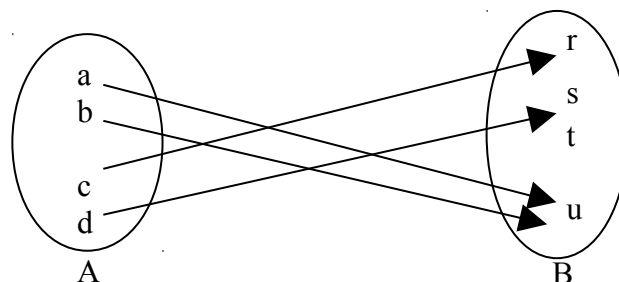


- **Diagrama de setas** - Uma maneira de representar graficamente funções $f: A \rightarrow B$ para conjuntos A e B finitos é usando os diagramas de setas vistos no Capítulo 3.

Para criar o diagrama de setas, desenha-se um conjunto de pontos para A à esquerda e um conjunto de pontos para B à direita; e traça-se uma seta de a para b quando $f(a) = b$. No diagrama de setas de uma função todo ponto à esquerda (em A) tem exatamente uma seta partindo dele e terminando à direita (em B). É possível que um ou mais elementos de B não sejam apontados por nenhuma seta no diagrama.

Exemplo:

- $f: A \rightarrow B$ e $\text{im } f = \{r, s, u\}$



Funções iguais

Duas funções são ditas iguais se têm:

1. o mesmo domínio,
2. o mesmo contradomínio e
3. a mesma associação de valores do contradomínio a valores do domínio.

Para mostrar que duas funções com o mesmo domínio e o mesmo contradomínio são iguais precisamos mostrar que a associação é a mesma. Isso pode ser feito mostrando que, dado um elemento arbitrário no domínio, ambas as funções produzem o mesmo elemento no contradomínio, isto é, elas levam esse elemento no mesmo elemento do contradomínio.

Exemplo:

- Sejam $S = \{1, 2, 3\}$ e $T = \{1, 4, 9\}$, a função $f: S \rightarrow T$ é definida por $f = \{(1, 1), (2, 4), (3, 9)\}$ e a função $g: S \rightarrow T$ é definida por

$$g(n) = \frac{\sum_{k=1}^n (4k-2)}{2}$$

Para provar que $f = g$, como ambas possuem o mesmo domínio e o mesmo contradomínio, basta provar que cada função tem o mesmo efeito em todos os elementos do domínio. Para isso, vamos demonstrar por exaustão que $g(1) = f(1) = 1$, $g(2) = f(2) = 4$ e $g(3) = f(3) = 9$:

$$g(n) = \frac{\sum_{k=1}^n (4k-2)}{2} = \frac{(4 \cdot 1 - 2)}{2} = \frac{2}{2} = 1$$

$$g(n) = \frac{\sum_{k=1}^n (4k-2)}{2} = \frac{(4 \cdot 1 - 2) + (4 \cdot 2 - 2)}{2} = \frac{2 + 6}{2} = 4$$

$$g(n) = \frac{\sum_{k=1}^n (4k-2)}{2} = \frac{(4 \cdot 1 - 2) + (4 \cdot 2 - 2) + (4 \cdot 3 - 2)}{2} = \frac{2 + 6 + 10}{2} = 9$$

Veja que a prova por exaustão só é possível, neste caso, porque o domínio é um conjunto finito de tamanho pequeno. Como seria essa prova usando indução matemática?



Algumas funções interessantes

1. Função identidade

Seja A um conjunto qualquer. A função de A em A que associa cada elemento a si mesmo é dita função identidade em A , usualmente denotada por 1_A .

$$1_A(a) = a$$

Exemplo:

- A relação de igualdade apresentada no capítulo 3, a qual é definida por $\{(a, a) \mid a \in A\}$

2. Função piso (*floor*) e função teto (*ceiling*)

A função piso $\lfloor x \rfloor$ associa a cada número real x o maior inteiro menor ou igual a x . A função teto $\lceil x \rceil$ associa a cada número real x o menor inteiro maior ou igual a x . Ambas as funções, piso e teto, são funções de \mathbb{R} em \mathbb{Z} . Se x é um inteiro, $\lfloor x \rfloor = \lceil x \rceil$; caso contrário, $\lfloor x \rfloor + 1 = \lceil x \rceil$.

Exemplos:

- $\lfloor 2,8 \rfloor = 2$ e $\lceil 2,8 \rceil = 3$
- $\lfloor -4,1 \rfloor = -5$ e $\lceil -4,1 \rceil = -4$

3. Função valor inteiro

Seja x um número real qualquer. O valor inteiro de x , escrito $\text{INT}(x)$, converte x em um inteiro truncando a parte fracionária do número. Observe que $\text{INT}(x) = \lfloor x \rfloor$ se x é positivo e $\text{INT}(x) = \lceil x \rceil$ se x é negativo.

Exemplos:

- $\text{INT}(3,17) = 3$ e
- $\text{INT}(-8,5) = -8$

4. Função valor absoluto

O valor absoluto de um número real x , denotado por $\text{ABS}(x)$, ou $|x|$ é definido como sendo o maior dos valores entre x e $-x$. Observe que $\text{ABS}(0) = 0$, $\text{ABS}(x) = x$ para x positivo e $\text{ABS}(-x) = x$ para x negativo, $|x| = |-x|$.

Exemplos:

- $|-15| = 15$, $|6| = 6$ e
- $|4,56| = 4,56$

5. Função módulo ou função resto

Para qualquer inteiro x e qualquer inteiro positivo n , a função módulo n , denotada por $f(x) = x \bmod n$, associa a cada x o resto de sua divisão por n . Podemos escrever $x = qn + r$, $0 \leq r < n$, onde q é o quociente e r é o resto, de modo que o valor de $x \bmod n$ é r . Para números negativos, no entanto, deve-se dividir $|x|$ por n para obter r' . $x \bmod n = n - r'$ quando $r' \neq 0$.

Exemplos:

- $25 \bmod 7 = 4$, $25 \bmod 5 = 0$, $35 \bmod 11 = 2$, $3 \bmod 8 = 3$
- $-26 \bmod 7 = 7-5 = 2$, $-371 \bmod 8 = 8-3 = 5$, $-39 \bmod 3 = 0$

6. Função logarítmica

Seja b um número positivo. O logaritmo de qualquer número positivo x na base b ,

denotado por $\log_b x$ representa o expoente ao qual b precisa ser elevado para obter x . Isto é, $y = \log_b x$ é equivalente a $b^y = x$

Exemplos:

- $\log_2 8 = 3$ já que $2^3 = 8$
- $\log_{10} 100 = 2$ já que $10^2 = 100$
- $\log_2 64 = 6$ já que $2^6 = 64$

Para qualquer base b , definimos:

- $\log_b 1 = 0$ já que $b^0 = 1$
- $\log_b b = 1$ já que $b^1 = b$

Classes especiais de logaritmos:

- Logaritmos decimais - base 10: $\log_{10} x$ ou $\log x$
- Logaritmos naturais - base e ($e = 2,718281\dots$): $\log_e x$ ou $\ln x$
- Logaritmos binários - base 2: $\log_2 x$ ou $\lg x$

4.1. Propriedades de funções

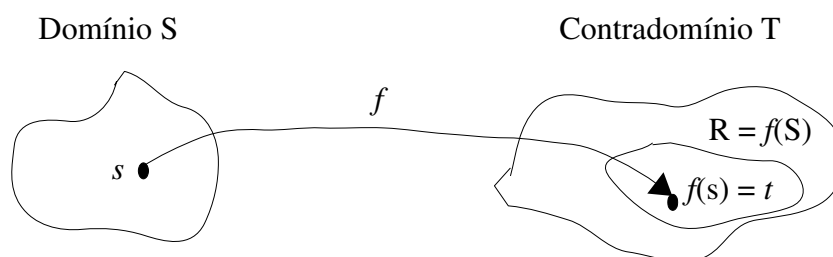
Função sobrejetora ou sobrejetiva

Uma função $f: S \rightarrow T$ é dita **sobrejetora** (ou **sobrejetiva** ou **sobre**) se sua imagem é igual a seu contradomínio. Formalmente (SCHEINERMAN, 2011, p. 230):

Definição 4.1 – Sobrejetora

Seja $f: A \rightarrow B$. Dizemos que f é *sobre* B desde que, para todo $b \in B$, exista um $a \in A$ de modo que $f(a) = b$. Em outras palavras, $\text{im } f = B$.

Considerando-se $f: S \rightarrow T$ uma função arbitrária com domínio S e contradomínio T. Parte da definição de uma função é que todo elemento de S tem uma imagem sob f e que todas as imagens são elementos de T; o conjunto R de todas as imagens é chamado de imagem da função f . Assim, $R = \{f(s) \mid s \in S\}$, ou $R = f(S)$. É claro que $R \subseteq T$ como representado graficamente a seguir:



A função é dita sobrejetora quando $R = T$, isto é, a imagem coincide com o contradomínio. Nesse caso, cada elemento de T é imagem de algum elemento de S, ou seja, não há elementos em T sem associação com algum elemento de S.

Uma função sobrejetora também é chamada de **sobrejeção**.

Exemplos:

- A função $f: \mathbb{R} \rightarrow \mathbb{R}$ definida por $f(x) = x^3$ é sobrejetora.
- A função $g: \mathbb{Z} \rightarrow \mathbb{N}$, onde g é definida por $g(x) = |x|$ (módulo de x) é sobrejetora.
- A função $h: S \rightarrow T$, onde $S = T = \{1, 2, 3\}$ e $h = \{(1, 1), (2, 1), (3, 3)\}$ não é sobrejetora pois $2 \in T$ não está associado a nenhum elemento de S já que não aparece como segundo elemento de nenhum par ordenado de h .

Provando que uma função é sobrejetora

Para toda função com imagem R e contradomínio T , temos $R \subseteq T$, ou seja, a imagem é um subconjunto do contradomínio. Assim, para mostrar que uma determinada função é sobrejetora, ou seja, que a imagem é igual a seu contradomínio, precisamos mostrar que $T \subseteq R$ resultando, então, em $R = T$.¹

Portanto, para demonstrar que uma função é sobrejetora, precisamos mostrar que um elemento arbitrário do contradomínio pertence à imagem, isto é, é a imagem de algum elemento no domínio. Por outro lado, para provar que uma função não é sobrejetora devemos produzir um contraexemplo, ou seja, um elemento no contradomínio que não é imagem de nenhum elemento do domínio.

Exemplo:

- A função $f: \mathbb{R} \rightarrow \mathbb{R}$ definida por $f(x) = x^3$ é sobrejetora. Para demonstrar essa propriedade, vamos considerar um número real arbitrário r com $x = \sqrt[3]{r}$. Como x é a raiz cúbica de um número real, sabemos que x é um número real e, portanto, pertence ao domínio de f sendo possível calcular $f(x) = (\sqrt[3]{r})^3 = r$, ou seja, r é imagem de x sob f . Logo, qualquer elemento do contradomínio (\mathbb{R}) é a imagem, sob f , de um elemento do domínio (\mathbb{R}) e, assim, provamos que a função f é sobrejetora.

Função injetora ou injetiva

Uma função $f: S \rightarrow T$ é dita **injetora** (ou **injetiva** ou **um pra um**) se nenhum elemento de T é a imagem, sob f , de dois elementos distintos de S . Formalmente (SCHEINERMAN, 2011, p. 228):

Definição 4.2 – Injetora

Uma função f é chamada *um para um* se sempre que $(x,b), (y,b) \in f$, temos que $x = y$. Em outras palavras, se $x \neq y$ então $f(x) \neq f(y)$.

¹ Relembrando: vimos, no capítulo sobre Teoria dos Conjuntos, que dois conjuntos A e B são iguais se e somente se $A \subseteq B$ e $B \subseteq A$.

Em outras palavras, a função é dita injetora se elementos diferentes do domínio S têm imagens distintas, ou seja, se $f(a) = f(b)$ então $a = b$. Uma função injetora também é chamada de **injeção**.

Exemplos:

- A função $f: \mathbb{R} \rightarrow \mathbb{R}$ definida por $f(x) = x^3$ é injetora.
- A função $g: \mathbb{R} \rightarrow \mathbb{R}$ definida por $g(x) = x^2$ não é injetora, pois, por exemplo, 4,0 é a imagem de dois valores distintos: -2,0 e 2,0.
- A função $h: S \rightarrow T$, onde $S = T = \{1, 2, 3\}$ e $h = \{(1, 1), (2, 1), (3, 3)\}$ não é injetora pois 1 e 2 $\in S$ têm a mesma imagem: 1, já que este é o segundo valor de 2 pares ordenados de h .

Provando que uma função é injetora

Para provar que uma função $f: S \rightarrow T$ é injetora, partimos da suposição de que existem elementos s_1 e s_2 de S com $f(s_1) = f(s_2)$ e mostramos que $s_1 = s_2$. Por outro lado, para provar que uma função não é injetora, produzimos um contraexemplo, ou seja, um elemento na imagem com duas imagens inversas no domínio.

Exemplos:

- A função $f: \mathbb{R} \rightarrow \mathbb{R}$ definida por $f(x) = x^3$ é injetora, pois, se x e y são números reais com $f(x) = f(y)$ então $x^3 = y^3$, o que só é possível quando $x = y$.

Função bijetora ou bijetiva

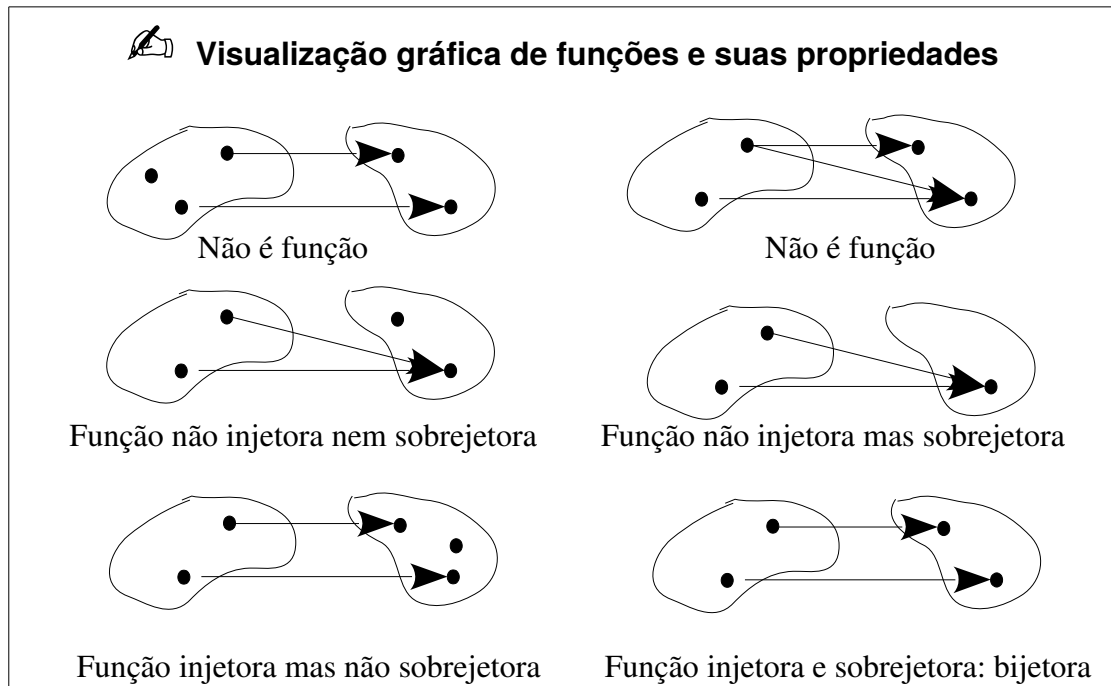
Uma função $f: S \rightarrow T$ é **bijetora** (ou **bijetiva** ou uma **bijeção**) se é, ao mesmo tempo, injetora e sobrejetora. Formalmente (SCHEINERMAN, 2011, p. 232):

Definição 4.3 – Bijetora

Uma função $f: A \rightarrow B$ é chamada *bijeção* se é ao mesmo tempo um para um e sobre.

Exemplos:

- A função $f: \mathbb{R} \rightarrow \mathbb{R}$ definida por $f(x) = x^3$ é bijetora já que vimos, anteriormente, que ela é sobrejetora e injetora.
- A função $g: \mathbb{R} \rightarrow \mathbb{R}$ definida por $g(x) = x^2$ não é bijetora pois vimos, anteriormente, que ela não é injetora.
- A função $h: \mathbb{R} \rightarrow \mathbb{R}$ definida por $h(x) = 4x - 1$ é bijetora.

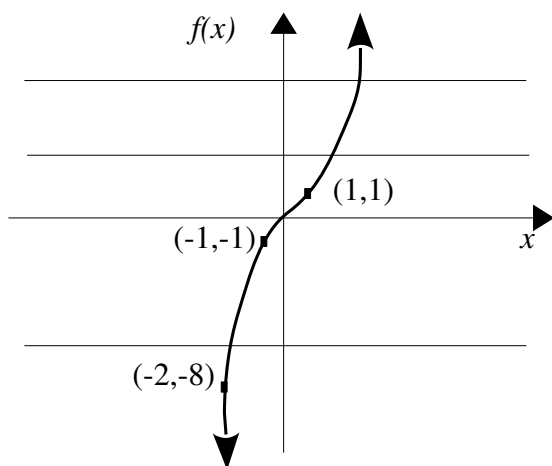


Caracterização geométrica de funções injetoras e sobrejetoras

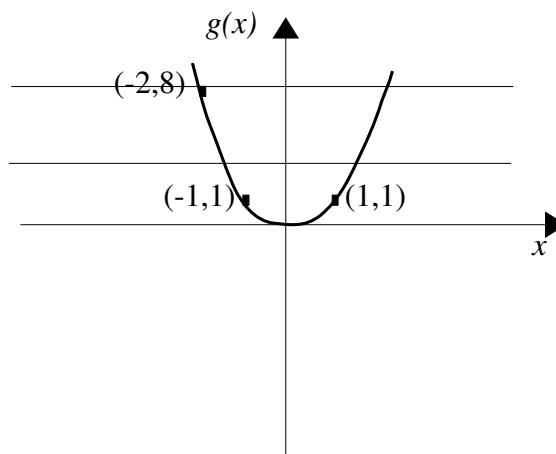
- **Função injetora:** cada reta horizontal pode interceptar o gráfico da função em no máximo um ponto
- **Função sobrejetora:** cada reta horizontal deve interceptar o gráfico da função em pelo menos um ponto
- **Função bijetora (injetora e sobrejetora):** cada reta horizontal deve interceptar o gráfico da função em exatamente um ponto

Exemplos:

- $f(x) = x^3$ é bijetora (sobrejetora e injetora), portanto uma reta horizontal intercepta o gráfico de $f(x)$ em exatamente um ponto como se pode notar pelas retas na figura abaixo
- $g(x) = x^2$ é sobrejetora, mas não é injetora, portanto uma reta horizontal intercepta o gráfico de $g(x)$ em pelo menos um ponto como se pode notar pelas retas na figura abaixo



injetora e sobrejetora, ou seja, bijetora



sobrejetora mas não injetora

4.2. Inversão e composição de funções

Função inversa

Como dito, anteriormente, as funções são um tipo especial de relações. Assim, do mesmo modo que podemos encontrar a relação inversa R^{-1} de uma relação R , podemos também considerar a inversa de uma função f , denotada por f^{-1} .²

Exemplos:

- Sejam $A = \{0, 1, 2, 3, 4\}$, $B = \{5, 6, 7, 8, 9\}$ e $f: A \rightarrow B$ definida por $f = \{(0,5), (1,7), (2,8), (3,9), (4,7)\}$. A inversa de f é $f^{-1} = \{(5,0), (7,1), (8,2), (9,3), (7,4)\}$. Veja que f^{-1} não é uma função por duas razões:
 - Tanto $(7,1)$ como $(7,4)$ estão em f^{-1}
 - $\text{dom } f^{-1} = \{5, 7, 8, 9\} \neq B$
- As funções $f(x) = b^x$ e $g(x) = \log_b x$ são a inversa uma da outra

Importante

- A inversa de uma função f de A para B não é necessariamente uma função. A inversa de f será uma função se a função f for inversível (veja definição abaixo), caso contrário, sua inversa será uma relação.

² Relembrando: vimos no capítulo 3 que a inversa de uma relação R é a relação obtida invertendo-se a ordem de todos os pares ordenados em R .

Função inversível

Uma função $f: S \rightarrow T$ é inversível se sua inversa é uma função de T para S .

Teorema: Uma função $f: S \rightarrow T$ é inversível se e somente se f é injetora e sobrejetora.

Isso porque como f é sobrejetora, todo $t \in T$ tem uma imagem inversa em S . Como f é injetora, essa imagem inversa é única. Podemos, então, associar a cada elemento $t \in T$ um único elemento em S , a saber, $s \in S$ tal que $f(s) = t$. Essa associação descreve uma função $g: T \rightarrow S$.

Assim, uma função $f: S \rightarrow T$ é dita **inversível** se a relação inversa é uma função g de T para S . Graficamente:

Exemplo:

- Dado que $f: \mathbb{R} \rightarrow \mathbb{R}$ definida por $f(x) = 3x + 4$ é uma bijeção, $f^{-1}: \mathbb{R} \rightarrow \mathbb{R}$ é definida por $f^{-1}(x) = (x - 4)/3$
 - Exemplos de pares ordenados em $f = (1, 7), (2, 10), (3, 13)$ e em $f^{-1} = (7, 1), (10, 2), (13, 3)$

Composição de funções

Sejam $f: S \rightarrow T$ e $g: T \rightarrow U$. A **função composta** $g \circ f$ é a função de S em U definida por $(g \circ f)(s) = g(f(s))$. Formalmente (SCHEINERMAN, 2011, p. 243):

Definição 4.4 – Composição de funções

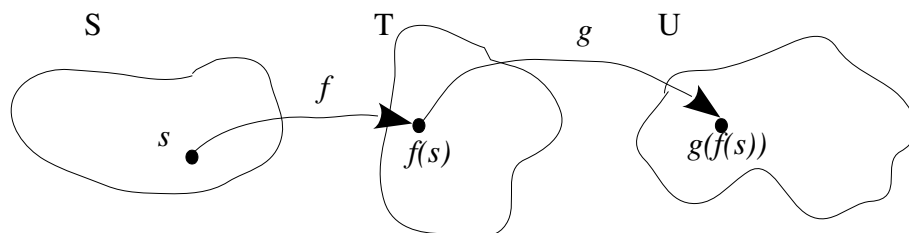
Sejam os conjuntos A, B e C e sejam $f: A \rightarrow B$ e $g: B \rightarrow C$. Então, a função $g \circ f$ é uma função de A para C definida por

$$(g \circ f)(a) = g[f(a)]$$

em que $a \in A$. A função $g \circ f$ é chamada *composição* de g e f .

Em outras palavras, para todo $s \in S$, $f(s)$ é um elemento de T , que é o domínio de g . Logo, a função g pode ser calculada em $f(s)$. O resultado de $g(f(s))$ é, portanto, um elemento de U . Assim, cria-se uma função $S \rightarrow U$, chamada composição das funções f e g e denotada por $g \circ f$.

Graficamente, essa composição pode ser ilustrada como:



Exemplo:

- Seja $f: \mathbb{R} \rightarrow \mathbb{R}$ definida por $f(x) = x^2$. Seja $g: \mathbb{R} \rightarrow \mathbb{R}$ definida por $g(x) = \lfloor x \rfloor$. Então
 - $(g \circ f)(2,3) = g(f(2,3)) = g(2,3^2) = g(5,29) = \lfloor 5,29 \rfloor = 5$
 - $(f \circ g)(2,3) = f(g(2,3)) = f(\lfloor 2,3 \rfloor) = f(2) = 2^2 = 4$

Importante

- Nem sempre é possível fazer a composição de duas funções arbitrárias; os domínios e imagens têm que ser compatíveis. Por exemplo, se $f: S \rightarrow T$ e $g: W \rightarrow Z$, onde T e W são disjuntos, então $(g \circ f)(s) = g(f(s))$ não está definida, pois $f(s)$ não pertence ao domínio de g .
- A ordem é importante na composição das funções (veja exemplo acima).
- A composição de funções preserva as propriedades das funções serem injetoras ou sobrejetoras. Portanto, a composição de duas bijeções é também uma bijeção.

4.3. Contagem de funções

Sejam A e B conjuntos finitos. Quantas funções há de A para B ? Sem perda de generalidade, podemos escolher A como o conjunto $\{1, 2, \dots, a\}$ e B como o conjunto $\{1, 2, \dots, b\}$. Toda função $f: A \rightarrow B$ pode ser escrita como

$$f = \{ (1, X), (2, X), (3, X), \dots, (a, X) \}$$

em que os X são elementos de B . De quantas maneiras podemos substituir os X com elementos de B ? Há b escolhas para o elemento X em $(1, X)$, há b escolhas para X em $(2, X)$ etc. até as b escolhas para o elemento X em (a, X) consideradas todas as escolhas anteriores. Assim, ao todo há b^a escolhas (SCHEINERMAN, 2011).

Proposição 4.1

Sejam A e B conjuntos finitos com $|A| = a$ e $|B| = b$. O número de funções de A para B é b^a .

Qual a relação entre a proposição 4.1 e as propriedades de injetividade, sobrejetividade e bijetividade?

Proposição 4.2 – Princípio da Casa do Pombo

Sejam A e B conjuntos finitos e seja $f: A \rightarrow B$. Se $|A| > |B|$, então f não é um para um. Se $|A| < |B|$, então f não é sobre.

Dessa proposição também é possível deduzir a forma contrapositiva:

- se $f: A \rightarrow B$ é um para um então $|A| \leq |B|$
- se $f: A \rightarrow B$ é sobre então $|A| \geq |B|$
- se f for ambos, ou seja, se for bijetora então $|A| = |B|$

Proposição 4.3

Sejam A e B conjuntos finitos e seja $f: A \rightarrow B$. Se f é uma bijeção então $|A| = |B|$.

**Funções definidas recursivamente (por recorrência)**

Uma função é dita recursivamente definida se a definição da função se referir à própria função. A princípio isso não parece fazer sentido - como podemos definir algo em termos de si mesmo? Porém, isso funciona porque uma definição recorrente tem duas partes:

- *Base* - Devem existir certos argumentos, chamados de valores base, nos quais a função não faça referência a si mesma;
- *Recorrência* - Cada vez que a função se referir a si própria, o argumento da função precisa estar definido com base nos casos anteriores.

Por exemplo, o fatorial de n ($n!$) é o produto de um inteiro positivo de 1 até n , inclusive. Definimos $0! = 1$. Assim temos: $0! = 1, 1! = 1, 2! = 1 \cdot 2 = 2, 3! = 1 \cdot 2 \cdot 3 = 6 \dots$ Para todo inteiro positivo n , é verdade que: $n! = n \cdot (n-1)!$ Assim, a função fatorial pode ser definida de forma recursiva como:

- 1) se $n = 0$, então $n! = 1$
- 2) se $n > 0$, então $n! = n \cdot (n-1)!$

Em 1) o valor de $n!$ é dado explicitamente, logo $n = 0$ é um valor base; enquanto, em 2), o valor de $n!$ é definido em termos de um valor menor do que n , ou seja, um valor que está mais perto do valor base.



Algoritmos, Complexidade e Funções

Um algoritmo M é uma lista finita de passos com instruções bem definidas para resolver um problema particular. Em outras palavras, um algoritmo define como determinar a saída $f(x)$ de uma dada função f com entrada x , sendo que x pode ser uma lista ou conjunto de valores. Frequentemente, pode existir mais de uma maneira de obter $f(x)$ e a escolha do melhor algoritmo pode depender da eficiência ou complexidade das opções.

Complexidade de Algoritmos

Para comparar algoritmos precisamos dispor de critérios que medem sua eficiência. Suponha que M seja um algoritmo e n o tamanho do dado de entrada. O **tempo** e o **espaço** usados pelo algoritmo são as duas medidas principais para medir a eficiência de M .

A **complexidade** de um algoritmo M é, então, a função $f(n)$ que calcula o tempo de execução e/ou o espaço de memória necessário para o algoritmo em função do tamanho n do dado de entrada. O tempo é medido contando o número de operações chave. Frequentemente, o espaço de memória requerido por um algoritmo é um múltiplo do tamanho de entrada.

A menos que seja explicitado o contrário, o termo complexidade refere-se ao tempo de execução do algoritmo. A função de complexidade $f(n)$ depende não só do tamanho n do dado de entrada mas também do tipo particular do dado. Assim, determina-se a função de complexidade $f(x)$ para alguns casos, que são normalmente os seguintes:

1. Pior caso: o maior valor possível de $f(n)$ para qualquer dado de entrada;
2. Caso Médio: o valor esperado de $f(n)$.

A análise do caso médio pressupõe certa distribuição probabilística para o dado de entrada, por exemplo, de que as permutações do conjunto de dados são igualmente prováveis. O caso médio utiliza o conceito de expectância ou valor médio E . Suponha que os números n_1, n_2, \dots, n_k ocorram com probabilidades p_1, p_2, \dots, p_k respectivamente. A expectância ou valor médio E é dado por:

$$E = n_1p_1 + n_2p_2 + \dots + n_kp_k$$

Taxa de crescimento e notação O

Sabemos, por exemplo, que se calcularmos $f(x) = x$ e $g(x) = x^2$ para valores cada vez maiores de x , os valores de g serão maiores do que os de f e a diferença é cada vez maior. Essa diferença na taxa de crescimento não vai deixar de existir se simplesmente multiplicarmos os valores de f por uma constante muito grande; não importa quão grande seja essa constante, os valores de g certamente começarão a ficar cada vez maiores do que os de f .

Por exemplo, a taxa de crescimento de algumas funções usadas normalmente na comparação de complexidade são:

		g(n)				
n	log ₂ n	n	n log ₂ n	n ²	n ³	2 ⁿ
5	3	5	15	25	125	32
10	4	10	40	100	10 ³	10 ³
100	7	100	700	10 ⁴	10 ⁶	10 ³⁰
1000	10	10 ³	10 ⁴	10 ⁶	10 ⁹	10 ³⁰⁰

Assim, seja M um algoritmo e n o tamanho do dado de entrada. A complexidade $f(n)$ de M aumenta quando n aumenta. Normalmente, examinamos a razão de crescimento de $f(n)$ comparando $f(n)$ com algumas funções padrão, como as apresentadas acima: $\log_2 n$, n , $n \log_2 n$, n^2 , n^3 , 2^n

Nessa comparação de $f(n)$ com uma função padrão utiliza-se a notação O definida como:

Sejam $f(x)$ e $g(x)$ funções arbitrárias definidas em \mathbb{R} ou em um subconjunto de \mathbb{R} ; dizemos que $f(x)$ é da ordem de $g(x)$ escrevendo $f(x) = O(g(x))$ se existem um número real k e uma constante positiva C tais que, para todo $x > k$, temos $|f(x)| \leq C|g(x)|$.

A notação acima é conhecida como **big O** ou **O grande**, já que a notação $o(g(x))$ tem um significado diferente.

Complexidade de Algoritmos Tradicionais

Assumindo que $f(n)$ e $g(n)$ são funções definidas nos inteiros positivos, então

$$f(n) = O(g(n))$$

Significa que $f(n)$ é limitada por um múltiplo constante de $g(n)$ para quase todo n .

A seguir são apresentadas as complexidades de alguns algoritmos tradicionais de busca e ordenação:

- Busca linear: $O(n)$
- Busca binária: $O(\log n)$
- Bubble-sort: $O(n^2)$
- Merge-sort: $O(n \log n)$

Resumindo

Conceitos aprendidos nesse capítulo

- função ($f: S \rightarrow T$) - aplicação de um conjunto S em outro T que leva cada elemento do conjunto S em exatamente um elemento do conjunto T ; é um subconjunto de $S \times T$
- domínio de uma função f ($dom f$) - conjunto inicial de uma função (S na definição acima), ou seja, o conjunto de todos os primeiros elementos possíveis dos pares ordenados de f
- contradomínio de uma função f - conjunto final de uma função (T na definição acima)
- imagem de s sob f ($t = f(s)$) - ponto t que resulta da aplicação de uma função f a um valor s
- imagem inversa - ponto inicial de uma aplicação (s na definição anterior já que f leva s em t)
- imagem de uma função f ($im f$) - coleção de todas as imagens de pontos no domínio, ou seja, o conjunto de todos os segundos elementos possíveis dos pares ordenados de f
- gráfico de funções - uma maneira de visualizar funções cujas entradas e saídas são números reais (\mathbb{R})
- diagrama de setas - uma maneira de visualizar funções definidas de/para conjuntos finitos
- funções iguais - são aquelas com mesmo domínio, contradomínio e associação de valores do contradomínio a valores do domínio
- função identidade (1_A) - função de um conjunto A qualquer em A , que associa cada elemento a si mesmo
- função piso ou *floor* ($\lfloor x \rfloor$) - associa a cada número real x o menor inteiro maior ou igual a x
- função teto ou *ceiling* ($\lceil x \rceil$) - associa a cada número real x o maior inteiro menor ou igual a x
- função valor inteiro ($INT(x)$) - converte um número real qualquer x em um inteiro truncando a parte fracionária do número
- função valor absoluto ($ABS(x)$ ou $|x|$) - é o maior dos valores entre x e $-x$
- função módulo ou resto ($f(x) = x \bmod n$) - para qualquer inteiro x e qualquer inteiro positivo n , a função módulo n associa a cada x o resto de sua divisão por n
- função logarítmica ($\log_b x$) - o logaritmo de qualquer número positivo x na base b , denotado por $\log_b x$ representa o expoente ao qual b precisa ser elevado para obter x
- função sobrejetora (sobrejetiva) - é aquela na qual a imagem é todo o contradomínio; todo elemento no contradomínio tem uma imagem inversa
- função injetora (injetiva) - é aquela na qual dois elementos no domínio não podem ser levados

em um mesmo ponto

- função bijetora (bijetiva ou bijeção) - é aquela que é injetora e sobrejetora
- função inversa (f^{-1}) - a inversa de uma função f é a relação obtida invertendo-se a ordem de todos os pares ordenados em f , a inversa de uma função não necessariamente é uma função
- função inversível - é aquela para a qual a relação inversa é uma função; uma função é inversível se é injetora e sobrejetora
- função composta ($g \circ f$) - a função composta $g \circ f$ onde $f: S \rightarrow T$ e $g: T \rightarrow U$ é a função de S em U definida por $(g \circ f) = g(f(x))$

5. Teoria dos Números

A teoria dos números é um ramo da matemática que se tornou central na criptografia e na segurança dos computadores. Tradicionalmente, a teoria dos números se preocupa com as propriedades e relações entre os números. A aritmética modular estuda as operações básicas como adição e multiplicação no contexto dos números inteiros módulo n . A criptografia, por sua vez, é a ciência que estuda as formas de se escrever uma mensagem em código, ou seja, como transformar uma mensagem originalmente escrita com clareza em algo incompreensível de forma a permitir que apenas o destinatário autorizado a decifre e compreenda (CAVALCANTE, 2004 apud CAVALCANTE, 2005).

Nesse capítulo serão apresentados alguns teoremas e conceitos relacionados a cada um desses temas, bem como a relação entre eles. O texto que segue está fortemente baseado em (SCHEINERMAN, 2011).

5.1 Teoria dos Números

O que é a teoria dos números? Segundo Gauss (YAN, 2000):

"Mathematics is the Queen of the sciences, and number theory is the Queen of mathematics."

A teoria dos números é basicamente a teoria das propriedades dos inteiros como, por exemplo, a divisibilidade, a paridade, a relação de primos relativos, etc. A seguir são apresentadas algumas dessas propriedades.

5.1.1 Divisibilidade¹

Sejam a e b inteiros com $b \neq 0$. Dizemos que b divide a , denotado por $b|a$, se há um inteiro c tal que $a = bc$. Quando b divide a dizemos que b é divisor (ou fator) de a e a é um múltiplo de b . Se b não divide a escrevemos $b \nmid a$.

Teorema – Divisão

Sejam $a, b \in \mathbb{Z}$ com $b > 0$. Então, existe um único par de inteiros q e r tais que

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

O inteiro q é chamado **quociente** e o inteiro r é chamado **resto**. $r = 0$ se e somente se $b|a$.

Exemplos:

¹ As funções apresentadas nessa seção já foram apresentadas anteriormente no capítulo de Funções.

- Sejam $a = 23$ e $b = 10$. Então o quociente é $q = 2$ e o resto é $r = 3$, porque

$$23 = 2 * 10 + 3 \text{ e } 0 \leq 3 < 10$$

- Sejam $a = -37$ e $b = 5$. Então o quociente é $q = -8$ e o resto é $r = 3$, porque

$$-37 = -8 * 5 + 3 \text{ e } 0 \leq 3 < 5$$

Div e Mod

São operações associadas ao processo de divisão. Dados a e b , div e mod dão o quociente e o resto no problema da divisão, respectivamente. Assim, sejam $a, b \in \mathbb{Z}$ com $b > 0$. Pelo Teorema da divisão existe um único par de inteiros q e r tais que $a = qb + r$ e $0 \leq r < b$. Definimos as operações div e mod como

$$a \text{ div } b = q \quad \text{e} \quad a \text{ mod } b = r.$$

Graficamente:

$$\begin{array}{r} a \overline{) b} \\ r \quad q \end{array}$$

Exemplos:

- $11 \text{ div } 3 = 3$ $11 \text{ mod } 3 = 2$
- $23 \text{ div } 10 = 2$ $23 \text{ mod } 10 = 3$
- $-37 \text{ div } 5 = -8$ $-37 \text{ mod } 5 = 3$

Importante:

- O resto nunca é negativo. No último exemplo $-37 / 5 = -7,4$. Mas $-37 \text{ div } 5 = -8$ e $-37 \text{ mod } 5 = 3$ porque $-37 = -8 * 5 + 3$ e $0 \leq 3 < 5$
- mod tem um significado diferente na relação de equivalência modular, por exemplo $53 \equiv 23 \pmod{10}$, como explicado a seguir.

Equivalência modular e Congruência

Sejam $a, b, n \in \mathbb{Z}$ com $n > 0$. Então,

$$a \equiv b \pmod{n} \Leftrightarrow a \text{ mod } n = b \text{ mod } n.$$

Dizemos que a e b são **congruentes módulo n** se n é um divisor de $a - b$.

Além disso,

$$ax \equiv b \pmod{n} \Leftrightarrow ax - ny = b.$$

ou

$$ax \equiv b \pmod{n} \Leftrightarrow ax = b + ny.$$

Exemplo:

- Assim, $53 \equiv 23 \pmod{10}$ já que $53 \bmod 10 = 3$ e $23 \bmod 10 = 3$. Além disso, 53 e 23 são congruentes módulo 10 já que 10 é divisor de $53 - 23 = 30$.

5.1.2 Máximo divisor Comum

O máximo divisor comum de dois números $a, b \in \mathbb{Z}$, denotado por $\text{mdc}(a, b)$, é o maior inteiro que divide a e b . Assim, seja $d = \text{mdc}(a, b)$ então sabe-se que $d|a$, $d|b$ e se existir algum $c \in \mathbb{Z}$ tal que $c|a$ e $c|b$ então $c \leq d$.

Exemplos:

- $\text{mdc}(30, 24) = 6$
- $\text{mdc}(-30, -24) = 6$

Importante:

- Se a e b tem um máximo divisor comum, ele é único.

Algoritmo de Euclides para cálculo do mdc

O algoritmo de Euclides define um processo rápido para o cálculo do mdc utilizando a seguinte proposição.

Proposição 5.1.2

Sejam a e b inteiros positivos e $c = a \bmod b$. Então, $\text{mdc}(a, b) = \text{mdc}(b, c)$.

Em outras palavras, para inteiros positivos a e b temos $\text{mdc}(a, b) = \text{mdc}(b, a \bmod b)$.

Algoritmo recursivo para cálculo de mdc:

Entrada: dois inteiros positivos a e b .

Saída: $\text{mdc}(a, b)$

Passos:

1. Seja $c = a \bmod b$
2. Se $c = 0$ retorna a resposta b e para
3. Senão ($c \neq 0$), calcula-se o $\text{mdc}(b, c)$

Exemplos:

- Usando o algoritmo de Euclides para calcular $\text{mdc}(689, 234)$
 $689 \bmod 234 = 221 \Rightarrow \text{mdc}(689, 234) = \text{mdc}(234, 221)$
 $234 \bmod 221 = 13 \Rightarrow \text{mdc}(234, 221) = \text{mdc}(221, 13)$

$$221 \bmod 13 = 0 \quad \Rightarrow \text{mdc}(221, 13) = 13$$

- Usando o algoritmo de Euclides para calcular o $\text{mdc}(1281, 243)$. Faça você mesmo e verifique que a resposta é $\text{mdc}(1281, 243) = 3$.



Complexidade do Algoritmo de Euclides para cálculo de mdc

O algoritmo de Euclides não irá repetir indefinidamente já que o segundo argumento diminui em cada chamada recursiva. Assim, o algoritmo sempre termina com a resposta correta.

Além disso, ele pode ser executado em tempo polinomial, ou seja, o algoritmo de Euclides é aplicado a dois inteiros positivos a e b com $a \geq b$, então o número de divisões necessárias para encontrar $\text{mdc}(a, b)$ é $O(\log b)$.

Importante:

- Os pares de números cujo máximo divisor comum é 1 são os chamados números primos.

5.1.3 Números primos

Um inteiro positivo $p > 1$ é dito um número primo (ou apenas primo) se ele é divisível apenas por 1 e p , ou seja se p tem apenas os divisores triviais. Se $n > 1$ não é primo, então n é dito composto. Veja que, de acordo com essa definição, o inteiro positivo 1 não é nem primo nem composto.

Primos e mdc

Sejam a e b inteiros. Dizemos que a e b são relativamente primos (ou primos entre si) se e somente se $\text{mdc}(a, b) = 1$.

Exemplos:

- 23 é primo, pois seus únicos divisores são 23 e 1
- 22 não é primo, pois é divisível por 1, 2, 11 e 22

Os números primos têm propriedades especiais e interessantes e desempenham um papel fundamental no desenvolvimento da teoria dos números como, por exemplo, o teorema apresentado a seguir.

Teorema Fundamental da Aritmética

Seja n um inteiro positivo. Então, n se fatora em um produto de números primos. Além disso, a fatoração de n em primos é única, a menos da ordem dos primos.

Exemplos:

- $30 = 2 * 3 * 5 = 5 * 2 * 3 = 3 * 2 * 5$
- $38 = 2 * 19 = 19 * 2$

Lema - Sejam $a, b, p \in \mathbb{Z}$ e p primo. Se $p \mid ab$, então $p \mid a$ ou $p \mid b$.

Lema - Sejam p, q_1, q_2, \dots, q_t números primos. Se $p \mid q_1q_2\dots q_t$ então $p = q_i$ para algum $1 \leq i \leq$

t .

Importante:

- Os primos na fatoração de n não precisam ser distintos. Os primos iguais podem ser mantidos juntos, caso em que n pode ser expresso de maneira única por:

$$n = p_1^{m_1} p_2^{m_2} \dots p_r^{m_r}$$

Onde os m_i são positivos e $p_1 < p_2 < \dots < p_r$. Essa forma é conhecida como **fatoração canônica de n** .

Calculando o máximo divisor comum usando fatoração em primos

Sejam a e b inteiros positivos. Podemos fatorá-los em números primos como:

$$a = 2^{e_2} 3^{e_3} 5^{e_5} 7^{e_7} \dots \quad \text{e} \quad b = 2^{f_2} 3^{f_3} 5^{f_5} 7^{f_7} \dots$$

Exemplo:

- $24 = 2^3 3^1 5^0 7^0 \dots$

Supondo que $a \mid b$. Seja p um número primo que aparece e_p vezes na fatoração de a em números primos. Como $p^{e_p} \mid a$ e $a \mid b$ temos que $p^{e_p} \mid b$ e portanto $e_p \mid f_p$. Assim, $e_p \leq f_p$. Em outras palavras, se $a \mid b$, o número de fatores iguais a p na fatoração de a em primos é no máximo igual ao número de fatores iguais a p na fatoração de b em primos. Assim, se a e b são da forma

$$a = 2^{e_2} 3^{e_3} 5^{e_5} 7^{e_7} \dots \quad \text{e} \quad b = 2^{f_2} 3^{f_3} 5^{f_5} 7^{f_7} \dots$$

e se $d = \text{mdc}(a, b)$, então

$$d = 2^{x_2} 3^{x_3} 5^{x_5} 7^{x_7} \dots$$

onde $x_2 = \min\{e_2, f_2\}$, $x_3 = \min\{e_3, f_3\}$, $x_5 = \min\{e_5, f_5\}$, $x_7 = \min\{e_7, f_7\}$ e assim por diante.

Exemplos:

- Usando a fatoração para calcular $\text{mdc}(240, 560)$. Como

$$240 = 2^4 \cdot 3 \cdot 5$$

$$560 = 2^4 \cdot 5 \cdot 7$$

então $\text{mdc}(240, 560) = 2^4 \cdot 3^0 \cdot 5^1 \cdot 7^0 = 80$

- Calcule o mdc calculados anteriormente usando o algoritmo de Euclides, agora, usando a fatoração.

Interessante:

- Embora o método de cálculo do mdc usando fatoração pareça mais simples, não há ainda nenhum algoritmo eficiente conhecido para a fatoração de inteiros e, assim, o método mais usado para cálculo do mdc é, ainda, o algoritmo de Euclides.

5.2 Aritmética Modular

A aritmética é o estudo das operações básicas: adição, subtração, multiplicação e divisão. A aritmética modular é o estudo das operações básicas sobre um contexto diferente, que é o sistema dos números inteiros módulo n . Assim, ao invés de estarem definidas sobre o conjunto dos inteiros ou dos reais, as operações são definidas sobre o conjunto \mathbb{Z}_n .

O conjunto \mathbb{Z}_n , onde n é um inteiro positivo, é o conjunto de todos os números naturais de 0 a $n-1$, inclusive:

$$\mathbb{Z}_n = \{0, 1, 2, \dots, n - 1\}$$

As operações básicas são:

- adição mod n
- subtração mod n
- multiplicação mod n
- divisão mod n

Adição e multiplicação Modulares

Sejam n um inteiro positivo e $a, b \in \mathbb{Z}_n$. Definimos

$$a \oplus b = (a + b) \bmod n \text{ e (adição modular)}$$

$$a \otimes b = (a * b) \bmod n \text{ (multiplicação modular)}$$

Exemplos:

- Se $n = 10$, ou seja, em \mathbb{Z}_{10} :
 - $5 \oplus 5 = 0$ $5 \otimes 5 = 5$
 - $9 \oplus 8 = 7$ $9 \otimes 8 = 2$

Importante:

- As operações \oplus e \otimes dependem de contexto. Se $n=10$, $5 \oplus 5 = 0$, mas se $n=9$, $5 \oplus 5 = 1$

Propriedades das operações \oplus e \otimes

- **Fechamento** - Sejam $a, b \in \mathbb{Z}_n$, então $a \oplus b$ e $a \otimes b \in \mathbb{Z}_n$
- **Comutatividade** - Seja n inteiro com $n \geq 2$. Para todos os valores $a, b \in \mathbb{Z}_n$, temos que $a \oplus b = b \oplus a$ e $a \otimes b = b \otimes a$
- **Associatividade** - Para todos os valores $a, b, c \in \mathbb{Z}_n$, temos que $a \oplus (b \oplus c) = (a \oplus b) \oplus c$ e $a \otimes (b \otimes c) = (a \otimes b) \otimes c$
- **Elemento identidade** - Para todo $a \in \mathbb{Z}_n$, temos que $a \oplus 0 = a$ e $a \otimes 1 = a$
- **Distributividade** - Para todos os valores $a, b, c \in \mathbb{Z}_n$, temos que $a \otimes (b \oplus c) = (a \otimes b) \oplus (a \otimes c)$

Proposição

Seja n um inteiro positivo e sejam $a, b \in \mathbb{Z}_n$. Então, existe um e um só $x \in \mathbb{Z}_n$ tal que $a = b \oplus x$. O mesmo não pode ser afirmado sobre a multiplicação modular.

Subtração Modular

Sejam n um inteiro positivo e $a, b \in \mathbb{Z}_n$. Definimos

$$a \ominus b = (a - b) \bmod n \text{ e ou}$$

$$a \ominus b \text{ como o \u00fanico valor } x \in \mathbb{Z}_n \text{ tal que } a = b \oplus x$$

Exemplos:

- Se $n = 10$, ou seja, em \mathbb{Z}_{10} :
 - $3 \ominus 2 = 1$
 - $4 \ominus 9 = 5$

Inverso Modular

Seja n um inteiro positivo e $a \in \mathbb{Z}_n$. O **inverso** de a , denotado por a^{-1} , \u00e9 um elemento $b \in \mathbb{Z}_n$ tal que $a \otimes b = 1$. Um elemento de \mathbb{Z}_n que tenha inverso \u00e9 chamado invert\u00edvel.

Exemplos:

- Considere o conjunto \mathbb{Z}_{10} .
 - O elemento 0 n\u00e3o tem inverso.
 - Os elementos 2, 4, 6 e 8 n\u00e3o t\u00eam inversos.
 - Os elementos 1, 3, 7 e 9 s\u00e3o invert\u00edveis e t\u00eam apenas um inverso cada um.

Importante:

- Os elementos de \mathbb{Z}_{10} que têm inverso são precisamente os inteiros de \mathbb{Z}_{10} que são relativamente primos com 10.

Teorema (Elementos Invertíveis em \mathbb{Z}_n)

Seja n um inteiro positivo e seja $a \in \mathbb{Z}_n$, então a é invertível se e somente se a e n são relativamente primos.

Divisão Modular

Sejam n um inteiro positivo e b um elemento inversível de \mathbb{Z}_n . Seja $a \in \mathbb{Z}_n$ arbitrário.

Definimos

$$a \oslash b = a \otimes b^{-1}$$

Exemplos:

- Se $n = 10$, ou seja, em \mathbb{Z}_{10} :
 - $2 \oslash 7 = 6$
 - $3 \oslash 9 = 7$

6. Estruturas Algébricas¹

Uma **estrutura matemática** é um modelo formal cuja intenção é capturar as propriedades ou os comportamentos comuns encontrados em contextos variados. Uma **estrutura** consiste em um conjunto abstrato de objetos, junto com operações ou relações entre esses objetos obedecendo a certas regras. A estrutura da álgebra de Boole, vista na disciplina de lógica, é um modelo das propriedades e comportamentos comuns à lógica proposicional e à teoria dos conjuntos. Como um modelo formal, ela é uma entidade abstrata, uma ideia; a lógica proposicional e a teoria dos conjuntos são dois exemplos concretos dessa ideia.

Neste capítulo iremos estudar as estruturas algébricas que utilizam ideias já apresentadas em diversos capítulos desta apostila como a Teoria dos Números (Capítulo 5) e a Teoria dos Conjuntos (Capítulo 2). Para tanto, vamos iniciar com alguns conceitos pertinentes no texto que segue e está fortemente baseado em (SCHEINERMAN, 2011).

6.1 Operações

Definição

Seja A um conjunto. Uma *operação em A* é uma função cujo domínio contém $A \times A$. Assim, uma operação é uma função cuja entrada é um par de elementos de A .

Vamos começar analisando uma forma simples de aritmética: a soma. Existe um conjunto \mathbb{Z} de objetos (\mathbb{Z} denota o conjunto dos inteiros) e uma operação binária nesses objetos (a soma). A notação $[\mathbb{Z}, +]$ vai denotar o conjunto munido da operação binária. Veja que $+$ é uma operação em \mathbb{Z} porque é uma função cujo domínio inclui qualquer par de números inteiros, ou seja, o domínio é um par de elementos de $\mathbb{Z} \times \mathbb{Z}$. O mesmo não se pode dizer de \div , já que a divisão por 0 não está definida.

Em $[\mathbb{Z}, +]$, tem-se que:

$$2+(3+5) = (2+3)+5$$

é válida. Em cada um dos lados separados pelo sinal de igualdade, os inteiros permanecem na mesma ordem, mas o argumento desses inteiros, que indica a ordem em que são efetuadas as somas, muda. A mudança desses agrupamentos não altera a resposta.

¹ Esse material foi inicialmente desenvolvido pelo bolsista PESCD Adinovam Henriques de Macedo Pimenta no 2o. semestre de 2008.

Um outro tipo de equação válida em $[\mathbb{Z}, +]$ é:

$$2+3 = 3+2$$

A mudança da ordem em que os inteiros são somados não altera o resultado.

Equações do tipo :

$$0+2=2$$

$$3+0=3$$

também são válidas. Somar zero a qualquer inteiro não altera o valor daquele número.

Da mesma forma, equações como

$$2 + (-2) = 0$$

$$5 + (-5) = 0$$

$$-20 + 20 = 0$$

são válidas. Somar o negativo de um número a ele mesmo tem como resultado o 0.

Essas equações representam quatro propriedades que ocorrem com tanta frequência que possuem nomes, como apresentado a seguir.

Propriedades das operações

Seja A um conjunto e seja $*$ uma operação binária em A . **IMPORTANTE:** Aqui, o símbolo $*$ não representa a multiplicação, mas sim qualquer operação binária.

1) A operação $*$ é **associativa** se

$$\forall x, y, z \in A, \quad x*(y*z) = (x*y)*z$$

A associatividade nos permite escrever $x * y * z$ sem parênteses já que o agrupamento não é relevante. Por exemplo, as operações de soma (+) e multiplicação (x) são associativas em \mathbb{Z} , mas a subtração (-) não é já que, por exemplo, $(3-4)-7=-8$ e $3-(4-7)=6$.

2) A operação $*$ é **comutativa** se

$$\forall x, y \in A, \quad x*y = y*x$$

Por exemplo, as operações de soma (+) e multiplicação (x) são associativas em \mathbb{Z} , mas a subtração (-) não é já que, por exemplo, $3-4=-1$ e $4-3=1$.

3) $[A, *]$ tem um **elemento identidade** $i \in A$ se

$$\exists i \in A, \quad \forall x \in A, \quad x*i = i*x = x$$

Por exemplo, o 0 é o elemento identidade para soma (+) e o 1 para multiplicação (x). O elemento identidade deve funcionar em ambos os lados da operação. Veja que a operação de subtração (-) de inteiros não tem elemento identidade pois $x-0=x$ mas $0-x \neq x$. Há uma proposição

muito importante em relação ao elemento identidade:

Proposição

Seja $*$ uma operação definida em um conjunto A , então $*$ pode ter, no máximo, um elemento identidade.

4) Se $[A, *]$ tem um elemento identidade i , então cada elemento x em A tem um **inverso** (x^{-1}) em relação a $*$ se

$$\forall x \in A, \exists x^{-1} \in A, x * x^{-1} = x^{-1} * x = i$$

Por exemplo, na soma (+) sobre os inteiros o elemento identidade é o 0. Todo inteiro x tem um inverso dado por $-x$ já que $x + (-x) = (-x) + x = 0$.

Importante: Para a maioria das operações conhecidas, os elementos têm no máximo um inverso, mas é possível que um elemento tenha mais de um inverso.

5) A operação $*$ é **fechada** em A se

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

As operações de soma (+), subtração (-) e multiplicação (x) são fechadas em \mathbb{Z} , mas a subtração (-) não é fechada em \mathbb{N} já que, por exemplo, 3 e $7 \in \mathbb{N}$ mas $3 - 7 = -4 \notin \mathbb{N}$.

Nos enunciados acima, os quantificadores universais se aplicam a todo o conjunto A . Se a associatividade é válida, a equação $x * (y * z) = (x * y) * z$ é válida quaisquer que sejam x , y , e z pertencentes a A . O mesmo ocorre para a comutatividade. O quantificador existencial também se aplica a A , de modo que, se existir um elemento identidade i , ele tem que pertencer a A e, se existir um elemento inverso x^{-1} , ele tem que ser um elemento de A . Na definição de inverso, o quantificador existencial vem em segundo lugar. Para cada x existe um x^{-1} e, se mudarmos x , x^{-1} também muda, da mesma forma que o elemento inverso de 2 em $[\mathbb{Z}, +]$ é -2 e o elemento inverso de 5 é -5. Se não existe elemento identidade, não faz sentido falar sobre elementos inversos.

6.2 Grupo, grupo comutativo, monoide, semigrupo e subgrupo

Grupo

Seja $*$ uma operação definida em um conjunto G . Dizemos que o par $[G, *]$ é um **grupo** se e somente se (SCHEINERMAN, 2011, p. 391):

- O conjunto G é **fechado** sob a operação $*$, isto é, $\forall g, h \in G, g * h \in G$.

- A operação $*$ é **associativa**, isto é, $\forall g, h, k \in G, (g*h)*k = g*(h*k)$.
- Existe **um elemento identidade** $e \in G$ para $*$, isto é, $\exists e \in G, \forall g \in G, g*e = e*g = g$.
- Para todo elemento $g \in G$ existe **um elemento inverso** $h \in G$, isto é, $\forall g \in G, \exists h \in G, g*h = h*g = e$.

Veja que um grupo é um par formado por um conjunto G e uma operação $*$ nesse conjunto, o que denotamos genericamente como $[G, *]$.

Exemplo:

- $[\mathbb{Z}, +]$ é um grupo referido como "inteiros com adição" já que:
 - A adição de 2 inteiros é um inteiro \Rightarrow fechamento
 - $(x + y) + z = x + (y + z)$ \Rightarrow a adição é associativa
 - $x + 0 = x$ \Rightarrow 0 é o elemento identidade
 - $x + (-x) = 0$ \Rightarrow o inverso de todo elemento x é $-x$

Proposição

Seja $[G, *]$ um grupo. Todo elemento de G tem um inverso único em G .

Prova:

Sabemos, por definição, que todo elemento em G tem um inverso. Vamos provar por contradição que esse inverso é único, ou seja, que não é possível um elemento de G ter dois (ou mais) inversos.

Vamos supor, por contradição, que $g \in G$ tem dois inversos distintos. Sejam h e $k \in G$ inversos de g , com $h \neq k$. Isso significa que

$$g * h = h * g = g * k = k * g = i$$

onde $i \in G$ é o elemento identidade para $*$. Pela propriedade associativa presente em todo grupo tem-se que

$$h * (g * k) = (h * g) * k$$

Como consequência,

$$h * (g * k) = h * i = h \quad \text{e} \quad (h * g) * k = i * k = k$$

Logo, $h = k$, contradizendo o fato de $h \neq k$.

Portanto, todo elemento $g \in G$ tem um inverso único em G . ■

Definição

Seja n um inteiro positivo. Definimos $\mathbb{Z}_n^* = \{ a \in \mathbb{Z} \mid \text{mdc}(a, n) = 1 \}$.

Proposição

Seja n um inteiro positivo. Então $(\mathbb{Z}_n^*, \otimes)$ é um grupo.

Exemplo:

- Para $(\mathbb{Z}_{14}^*, \otimes)$ tem-se que os elementos invertíveis em \mathbb{Z}_{14}^* são os números de \mathbb{Z}_{14}

relativamente primos com 14, ou seja: 1, 3, 5, 9, 11, 13. Assim, esses elementos juntamente com a operação \otimes formam um grupo que pode ser representado graficamente como:

\otimes	1	3	5	9	11	13
1	1	3	5	9	11	13
3	3	9	1	13	5	11
5	5	1	11	3	13	9
9	9	13	3	11	1	5
11	11	5	13	1	9	3
13	13	11	9	5	3	1

$(\mathbb{Z}_{14}^*, \otimes)$ é um grupo pois:

1. é fechado (nas células da tabela acima só existem valores de \mathbb{Z}_{14}^*),
2. \otimes é associativa (veja Capítulo 5)
3. o elemento identidade de $(\mathbb{Z}_{14}^*, \otimes)$ é o 1 (a linha do 1 e a coluna do 1 reproduzem os elementos com os quais o 1 opera)
4. todo elemento de $(\mathbb{Z}_{14}^*, \otimes)$ possui inverso, já que há um elemento identidade (1) em cada linha

Grupo comutativo (ou grupo abeliano)

Um grupo $[G, *]$ em que a operação $*$ é **comutativa**, isto é, $\forall g, h \in G, g*h = h*g$, é chamado de **grupo comutativo** ou **grupo abeliano**.²

Vale a pena ressaltar que o símbolo $*$ não denota a multiplicação, mas sim um símbolo genérico de operação. Se a operação for a soma, então o símbolo $*$ será substituído pelo símbolo $+$.

Exemplos:

- a) $[\mathbb{Z}, +]$ é um grupo comutativo com elemento identidade 0.
- b) Vamos denotar \mathbb{R}^+ como o conjunto dos números reais positivos e, agora sim, o símbolo $*$ como a multiplicação. Podemos ver que $[\mathbb{R}^+, *]$ é um grupo comutativo. A multiplicação é associativa e comutativa. O número real positivo 1 funciona como a identidade, já que

² Os grupos comutativos são chamados de abelianos em homenagem ao matemático norueguês Niels Henrik Abel (1802-1829) (SCHEINERMAN, 2011, p. 392).

$$x * 1 = 1 * x = x$$

para todo o real x positivo. Todo número real positivo x tem uma inversa em relação à multiplicação, a saber, o número real positivo $1/x$, pois

$$x * 1/x = 1/x * x = 1$$

- c) Podemos definir $M_2(\mathbb{Z})$ o conjunto de todas as matrizes 2×2 com elementos inteiros e o símbolo $+$ a soma de matrizes. Logo, esse é um grupo comutativo, pois os inteiros formam um grupo comutativo, de modo que cada elemento da matriz se comporta apropriadamente.

A soma de matrizes é comutativa porque

$$\begin{bmatrix} a_{1,1} & a_{1,2} \\ a_{2,1} & a_{2,2} \end{bmatrix} + \begin{bmatrix} b_{1,1} & b_{1,2} \\ b_{2,1} & b_{2,2} \end{bmatrix} = \begin{bmatrix} a_{1,1} + b_{1,1} & a_{1,2} + b_{1,2} \\ a_{2,1} + b_{2,1} & a_{2,2} + b_{2,2} \end{bmatrix} = \begin{bmatrix} b_{1,1} + a_{1,1} & b_{1,2} + a_{1,2} \\ b_{2,1} + a_{2,1} & b_{2,2} + a_{2,2} \end{bmatrix} = \begin{bmatrix} b_{1,1} & b_{1,2} \\ b_{2,1} & b_{2,2} \end{bmatrix} + \begin{bmatrix} a_{1,1} & a_{1,2} \\ a_{2,1} & a_{2,2} \end{bmatrix}$$

A matriz

$$\begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$$

é a identidade.

A matriz

$$\begin{bmatrix} 1 & -4 \\ 2 & 5 \end{bmatrix}$$

é a inversa da matriz

$$\begin{bmatrix} -1 & 4 \\ -2 & -5 \end{bmatrix}$$

Monoide

Se retirarmos a propriedade de existência de inverso da definição de grupo, teremos um **monoide**. Desta forma, um monoide é formado por um conjunto e uma operação associativa, fechada neste conjunto e com elemento identidade. Se o monoide tiver a propriedade comutativa ele é dito **monoide comutativo**.

Exemplos:

- a) $[\mathbb{N}, +]$ em que \mathbb{N} é o conjunto dos números naturais. Nesse caso o par é um monoide porque $+$ é associativa e fechada em \mathbb{N} , 0 (elemento identidade) pertence a \mathbb{N} e não há inverso já

que, para essa operação, os inversos seriam os números negativos os quais não fazem parte de \mathbb{N} .

b) Revisando a multiplicação de matrizes, considere A e B matrizes 2x2. A multiplicação de A por B é dada por:

$$\begin{bmatrix} a_{1,1} & a_{1,2} \\ a_{2,1} & a_{2,2} \end{bmatrix} * \begin{bmatrix} b_{1,1} & b_{1,2} \\ b_{2,1} & b_{2,2} \end{bmatrix} = \begin{bmatrix} a_{1,1} * b_{1,1} + a_{1,2} * b_{2,1} & a_{1,1} * b_{1,2} + a_{1,2} * b_{2,2} \\ a_{2,1} * b_{1,1} + a_{2,2} * b_{2,1} & a_{2,1} * b_{1,2} + a_{2,2} * b_{2,2} \end{bmatrix}$$

Agora, vamos considerar $[M_2(\mathbb{Z}), *]$, onde * denota a multiplicação de matrizes. Temos, então, que $[M_2(\mathbb{Z}), *]$ é um monoide pois é associativa e possui elemento identidade:

Provando que $[M_2(\mathbb{Z}), *]$ tem a propriedade associativa

Considerando A, B, C e D matrizes 2x2, $D=A*(B*C)$ e é dada por

$$\begin{bmatrix} a_{1,1} & a_{1,2} \\ a_{2,1} & a_{2,2} \end{bmatrix} * \begin{bmatrix} b_{1,1} & b_{1,2} \\ b_{2,1} & b_{2,2} \end{bmatrix} * \begin{bmatrix} c_{1,1} & c_{1,2} \\ c_{2,1} & c_{2,2} \end{bmatrix}$$

Sabemos que

$$\left(\begin{bmatrix} b_{1,1} & b_{1,2} \\ b_{2,1} & b_{2,2} \end{bmatrix} * \begin{bmatrix} c_{1,1} & c_{1,2} \\ c_{2,1} & c_{2,2} \end{bmatrix} \right) = \begin{bmatrix} b_{1,1} * c_{1,1} + b_{1,2} * c_{2,1} & b_{1,1} * c_{1,2} + b_{1,2} * c_{2,2} \\ b_{2,1} * c_{1,1} + b_{2,2} * c_{2,1} & b_{2,1} * c_{1,2} + b_{2,2} * c_{2,2} \end{bmatrix}$$

Logo

$$\begin{bmatrix} a_{1,1} & a_{1,2} \\ a_{2,1} & a_{2,2} \end{bmatrix} * \begin{bmatrix} b_{1,1} * c_{1,1} + b_{1,2} * c_{2,1} & b_{1,1} * c_{1,2} + b_{1,2} * c_{2,2} \\ b_{2,1} * c_{1,1} + b_{2,2} * c_{2,1} & b_{2,1} * c_{1,2} + b_{2,2} * c_{2,2} \end{bmatrix} = D$$

$$D_{1,1} = \{a_{1,1} * (b_{1,1} * c_{1,1} + b_{1,2} * c_{2,1})\} + \{a_{1,2} * (b_{2,1} * c_{1,1} + b_{2,2} * c_{2,1})\}$$

$$D_{1,2} = \{a_{1,1} * (b_{1,1} * c_{1,2} + b_{1,2} * c_{2,2})\} + \{a_{1,2} * (b_{2,1} * c_{1,2} + b_{2,2} * c_{2,2})\}$$

$$D_{2,1} = \{a_{2,1} * (b_{1,1} * c_{1,1} + b_{1,2} * c_{2,1})\} + \{a_{2,2} * (b_{2,1} * c_{1,1} + b_{2,2} * c_{2,1})\}$$

$$D_{2,2} = \{a_{2,1} * (b_{1,1} * c_{1,2} + b_{1,2} * c_{2,2})\} + \{a_{2,2} * (b_{2,1} * c_{1,2} + b_{2,2} * c_{2,2})\}$$

Agora vamos fazer para $D'=(A*B)*C$

$$\left(\begin{bmatrix} a_{1,1} & a_{1,2} \\ a_{2,1} & a_{2,2} \end{bmatrix} * \begin{bmatrix} b_{1,1} & b_{1,2} \\ b_{2,1} & b_{2,2} \end{bmatrix} \right) * \begin{bmatrix} c_{1,1} & c_{1,2} \\ c_{2,1} & c_{2,2} \end{bmatrix}$$

Sabemos que

$$\left(\begin{bmatrix} a_{1,1} & a_{1,2} \\ a_{2,1} & a_{2,2} \end{bmatrix} * \begin{bmatrix} b_{1,1} & b_{1,2} \\ b_{2,1} & b_{2,2} \end{bmatrix} \right) = \begin{bmatrix} a_{1,1} * b_{1,1} + a_{1,2} * b_{2,1} & a_{1,1} * b_{1,2} + a_{1,2} * b_{2,2} \\ a_{2,1} * b_{1,1} + a_{2,2} * b_{2,1} & a_{2,1} * b_{1,2} + a_{2,2} * b_{2,2} \end{bmatrix}$$

Logo

$$\begin{bmatrix} a_{1,1} * b_{1,1} + a_{1,2} * b_{2,1} & a_{1,1} * b_{1,2} + a_{1,2} * b_{2,2} \\ a_{2,1} * b_{1,1} + a_{2,2} * b_{2,1} & a_{2,1} * b_{1,2} + a_{2,2} * b_{2,2} \end{bmatrix} * \begin{bmatrix} c_{1,1} & c_{1,2} \\ c_{2,1} & c_{2,2} \end{bmatrix} = D$$

$$D'_{1,1} = \{(a_{1,1} * b_{1,1} + a_{1,2} * b_{2,1}) * c_{1,1}\} + \{(a_{1,1} * b_{1,2} + a_{1,2} * b_{2,2}) * c_{2,1}\}$$

$$D'_{1,2} = \{(a_{1,1} * b_{1,1} + a_{1,2} * b_{2,1}) * c_{1,2}\} + \{(a_{1,1} * b_{1,2} + a_{1,2} * b_{2,2}) * c_{2,2}\}$$

$$D'_{2,1} = \{(a_{2,1} * b_{1,1} + a_{2,2} * b_{2,1}) * c_{1,1}\} + \{(a_{2,1} * b_{1,2} + a_{2,2} * b_{2,2}) * c_{2,1}\}$$

$$D'_{2,2} = \{(a_{2,1} * b_{1,1} + a_{2,2} * b_{2,1}) * c_{1,2}\} + \{(a_{2,1} * b_{1,2} + a_{2,2} * b_{2,2}) * c_{2,2}\}$$

Como podemos verificar (exercício)

$$D_{1,1} = D'_{1,1}$$

$$D_{1,2} = D'_{1,2}$$

$$D_{2,1} = D'_{2,1}$$

$$D_{2,2} = D'_{2,2}$$

Logo, $D=D'$, ou seja, $A*(B*C) = (A*B)*C$.

Provando que $[M_2(\mathbb{Z}), *]$ possui elemento identidade

A matriz

$$\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

é um elemento identidade de $[M_2(\mathbb{Z}), *]$, já que

$$\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} * \begin{bmatrix} a & b \\ c & d \end{bmatrix} = \begin{bmatrix} a & b \\ c & d \end{bmatrix} * \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$$

Podemos ver que $[M_2(\mathbb{Z}), *]$ não é um monoide comutativo:

Provando que $[M_2(\mathbb{Z}), *]$ não é um monoide comutativo

$$\text{Para } A = \begin{bmatrix} 1 & 4 \\ 6 & -2 \end{bmatrix} \text{ e } B = \begin{bmatrix} 3 & 6 \\ 3 & 4 \end{bmatrix}$$

$$A * B = \begin{bmatrix} 15 & 22 \\ 12 & 28 \end{bmatrix} \text{ e } B * A = \begin{bmatrix} 39 & 0 \\ 27 & 4 \end{bmatrix}$$

Podemos ver que $[M_2(\mathbb{Z}), *]$ não é um grupo:

Provando que $[M_2(\mathbb{Z}), *]$ não é um grupo

Muitos elementos de $M_2(\mathbb{Z})$ não têm inverso sob a multiplicação de matrizes. Por exemplo,

se

$$\begin{bmatrix} 2 & 0 \\ 0 & 2 \end{bmatrix}$$

tiver uma matriz inversa

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix}$$

sob a multiplicação, então

$$\begin{bmatrix} 2 & 0 \\ 0 & 2 \end{bmatrix} * \begin{bmatrix} a & b \\ c & d \end{bmatrix} = \begin{bmatrix} a & b \\ c & d \end{bmatrix} * \begin{bmatrix} 2 & 0 \\ 0 & 2 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

Pela definição de multiplicação de matrizes, a única matriz que satisfaz essa equação tem $2a=1$ ou $a=1/2$, logo não é um elemento de $M_2(\mathbb{Z})$.

Semigrupo

Se retirarmos a existência de elemento identidade e a existência de inverso, teremos um **semigrupo**. Desta forma, um semigrupo é um conjunto que possui a propriedade associativa e o fechamento.

Exemplo:

- $[\mathbb{N}^*, +]$ em que \mathbb{N}^* é o conjunto dos números naturais sem o 0. Nesse caso o par é um semigrupo porque $+$ é associativa e fechada em \mathbb{N}^* e não há nem elemento identidade nem inverso.

Subgrupo

Sejam $[G, *]$ um grupo com identidade i e $A \subseteq G$. Então $[A, *]$ é um subgrupo de $[G, *]$ se satisfaz três propriedades:

- i) A é **fechado** sob $*$;
- ii) $i \in A$ sendo i a **identidade** de G ;
- iii) Todo $a \in A$ tem um **inverso** em A .

Como $[G, *]$ é grupo, então ele possui a propriedade associativa. O subgrupo $[A, *]$ herdará essa propriedade, já que, quaisquer que sejam $x, y, e z$ pertencentes a A , temos que $x, y, e z$ também pertencem a G e a equação $(x+y)+z = x+(y+z)$ é válida.

Se $[G, *]$ é um grupo com identidade i , então $\{i\}, *$ e $[G, *]$ são subgrupos de $[G, *]$. Esses são chamados de **subgrupos triviais** de $[G, *]$. Quaisquer outros subgrupos de $[G, *]$ são chamados de **subgrupos próprios**.

Exemplos:

- Para exemplificar, vamos considerar o conjunto $\mathbb{Z}_8 = \{0, 1, 2, 3, 4, 5, 6, 7\}$. Também

vamos considerar a operação *adição módulo 8*, denotada aqui por $+_8$, definida como $x +_8 y = r$, onde r é o resto da divisão de $x+y$ por 8. Por exemplo, $1 +_8 2 = 3$ e $5 +_8 4 = 1$.

Vamos representar as possíveis combinações de operação deste conjunto pela tabela a seguir:

$+_8$	0	1	2	3	4	5	6	7
0	0	1	2	3	4	5	6	7
1	1	2	3	4	5	6	7	0
2	2	3	4	5	6	7	0	1
3	3	4	5	6	7	0	1	2
4	4	5	6	7	0	1	2	3
5	5	6	7	0	1	2	3	4
6	6	7	0	1	2	3	4	5
7	7	0	1	2	3	4	5	6

Como podemos observar,

$[\mathbb{Z}_8, +_8]$ é um grupo, pois há um elemento identidade i (neste caso o 0), tal que $x +_8 i = x$, possui a propriedade associativa e cada elemento x possui seu inverso x^{-1} , tal que $x +_8 x^{-1} = i$.

Vamos agora verificar se $\{0, 2, 4, 6\}, +_8$ é subgrupo de $[\mathbb{Z}_8, +_8]$.

Podemos ver que $\{0, 2, 4, 6\}$ é fechado à $+_8$, pois para todo $x, y \in \{0, 2, 4, 6\}$, $x +_8 y$ também pertence a $\{0, 2, 4, 6\}$. Também podemos verificar que para todo x , existe um inverso x^{-1} que também pertence a $\{0, 2, 4, 6\}$. Para $x=0$, $x^{-1}=0$; para $x=2$, $x^{-1}=6$; para $x=4$, $x^{-1}=4$ e para $x=6$, $x^{-1}=2$.



Dica interessante

Veja que usando a tabela é possível verificar:

- O **elemento identidade** - está na intersecção da linha e da coluna que repetem os elementos das primeiras linha e coluna. No exemplo acima (a linha correspondente é igual à primeira linha da tabela e a coluna correspondente é igual à primeira coluna da tabela) é o elemento 0.
- A **comutatividade** - basta verificar se existe simetria em relação à diagonal principal. No exemplo acima, sim.
- O **elemento inverso** - determinado procurando na linha correspondente até encontrar a coluna onde aparece a identidade e verificando, em seguida, se a mudança de ordem ainda dá a identidade. No exemplo acima o inverso de 5 é 3 já

que $(5 + 3) \bmod 8 = 0$ (o elemento identidade).

No entanto, a **associatividade** (ou a falta dessa propriedade) não é fácil de ver na tabela.

- Subgrupos de $[\mathbb{Z}_{10}, +_{10}]$
 - $\{0\}$
 - $\{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$
 - $\{0, 5\}$
 - $\{0, 2, 4, 6, 8\}$

Dado um conjunto G e uma operação $*$, tem-se que as seguintes propriedades são satisfeitas (X) para cada estrutura:

Propriedade	Grupo comutativo	Grupo	Monoide	Monoide comutativo	Semigrupo
G é fechado sob *	X	X	X	X	X
* é associativa	X	X	X	X	X
Há elemento identidade	X	X	X	X	
Há elemento inverso	X	X			
* é comutativa	X			X	

6.3 Isomorfismo de Grupo

Dois grupos são isomorfos se são exatamente o mesmo, a menos dos nomes de seus elementos. Considere os grupos G e J definidos como $[\{1, -1\}, *]$ e $[\{u, v\}, \circ]$, respectivamente, e representados pelas tabelas abaixo:

$*$	1	-1
1	1	-1
-1	-1	1

\circ	u	v
u	u	v
v	v	u

Podemos observar que, salvo o nome dos elementos e das operações envolvidas, os dois grupos comportam-se como se fossem o mesmo grupo. Algebricamente, esse fato ocorre por causa da bijeção existente em $f: G \rightarrow J$, onde f é uma função que simplesmente troca os "nomes" dos elementos do grupo G . O "1" passa a se chamar "u" e o "-1" passa a se chamar "v". Mais formalmente temos $f(1) = u$ e $f(-1) = v$.

Dessa ideia surge a definição a seguir:

Definição

Sejam os grupos $[G, *]$ e $[H, \bullet]$, dizemos que uma função $f: G \rightarrow H$ é um *isomorfismo* (de grupo) se e somente se:

- 1) f é bijetora (um para um e sobre);
- 2) para quaisquer que sejam $x, y \in G$, $f(x*y) = f(x) \bullet f(y)$

Se existe um isomorfismo de G para H , dizemos que G é *isomorfo* a H e escrevemos $G \cong H$ (SCHEINERMAN, 2011, p. 400).

6.4 Anéis

Seja R um conjunto não vazio com duas operações binárias, uma operação de adição (denotada por $+$) e uma operação de multiplicação (denotada por $*$).³ Então R é dito um **anel**, denotado como $[R, +, *]$ se são satisfeitos os seguintes axiomas:

A1 (A adição é associativa) Para cada $a, b, c \in R$, $(a+b)+c = a+(b+c)$.

A2 (Existe um elemento identidade para a adição) Existe um elemento $0 \in R$, chamado elemento identidade, tal que $\alpha+0 = 0+\alpha = \alpha$ para todo $\alpha \in R$.

A3 (Todo elemento de R possui um inverso) Para cada $a \in R$, existe um elemento $-a \in R$ chamado de negativo de a , tal que $a+(-a) = (-a)+a = 0$.

A4 (A adição é comutativa) Para todo $a, b \in R$, $a+b = b+a$.

A5 (A multiplicação é associativa) Para cada $a, b, c \in R$, temos $(a*b*c) = a*(b*c)$.

A6 (A multiplicação é distributiva em relação a adição) .

Os axiomas A1 a A4 podem ser resumidos pela afirmação de que R é um grupo comutativo sob adição enquanto A5 especifica que R é um semigrupo sob a multiplicação. Um anel é um grupo abeliano em relação à adição com as propriedades adicionais de que as leis de fechamento, associatividade e distributividade valem para a multiplicação.

A subtração é definida em R por $a-b = a + (-b)$.

Exemplo:

- $[\mathbb{Z}, +, *]$ é um anel, o anel dos números inteiros;
- $[\mathbb{R}, +, *]$ é um anel, o anel dos números reais;

Subanel

Um subconjunto S de um anel $[R, +, *]$ é dito subanel de R se

³ O conjunto é fechado sob as operações de adição e de multiplicação.

- (i) S é subgrupo de $[\mathbb{R}, +]$
- (ii) S é subsemigrupo de $[\mathbb{R}, *]$

Isso significa que $S \neq \emptyset$ e vale $a-b \in S$ e $ab \in S$ para todos os $a, b \in S$.

Definições sobre anéis

Um anel $[A, +, *]$ chama-se:

- a) Um **anel com identidade** se existe um elemento $i \in A$ tal que $i*a=a*i=a$ para todo $a \in A$.
Em outras palavras, o semigrupo $[A, *]$ é um monoide;
- b) Anel **comutativo** se $a*b=b*a$ para todo $a, b \in A$. Em outras palavras, o semigrupo $[A, *]$ é comutativo;
- c) Anel **comutativo com identidade** se A tem as propriedades de a) e de b) simultaneamente, ou seja, $[A, *]$ é um monoide comutativo;
- d) Um **corpo**, se A é um anel comutativo com identidade $1 \neq 0$, tal que $[A, *] = A \setminus \{0\}$, ou seja, corpo é um anel no qual os elementos não-zero formam um grupo comutativo sob a multiplicação.

Exemplos:

- O anel $[2\mathbb{Z}, +, *]$ dos números inteiros pares é um anel comutativo sem elemento identidade.
- Seja R o conjunto dos números reais e $S = \{f : R \rightarrow R \mid f \text{ é uma função}\}$. Para todo $f, g \in R$, definimos $(f + g) \in R$ e $(f \cdot g) \in R$, por:

$$(f + g)(x) = f(x) + g(x), \forall x \in R$$

$$(f \cdot g)(x) = f(x) \cdot g(x), \forall x \in R.$$
 $(R, +, \cdot)$ é um **anel comutativo com identidade** i .

- $[M_2(\mathbb{Z}), +, *]$ é um anel não comutativo com elemento identidade $\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$, pois como demonstrado anteriormente $[M_2(\mathbb{Z}), +]$ é um grupo comutativo e $[M_2(\mathbb{Z}), *]$ é um monoide não comutativo com elemento identidade $\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$.
- $[\mathbb{R}, +, *]$ o anel dos números reais é um corpo.

Conceitos aprendidos nesse capítulo

- Operação associativa - uma operação $*$ é associativa se $(\forall x)(\forall y)(\forall z)[x * (y * z) = (x * y) * z]$
- Operação comutativa - uma operação $*$ é comutativa se $(\forall x)(\forall y)x * y = y * x$
- Elemento identidade - $[S, *]$ tem um elemento identidade se $(\exists i)(\forall x)(x * i = i * x = x)$
- Inverso - se $[S, *]$ tem um elemento identidade i , então cada elemento em S tem um inverso em relação a $*$ se $(\forall x)(\exists x^{-1})(x * x^{-1} = x^{-1} * x = i)$
- Fechamento - a operação $*$ é fechada em S se $\forall x, y \in S \ x * y \in S$
- Grupo - é o par $[G, *]$ (em que G é um conjunto e $*$ uma operação) onde G é fechado sob $*$, $*$ é associativa e existem elementos identidade e inverso
- Grupo comutativo (abeliano) - é um grupo em que a operação $*$ é comutativa
- Monoide - é o par $[G, *]$ onde $*$ é associativa e existe elemento identidade
- Semigrupo - é o par $[G, *]$ onde $*$ é associativa
- Subgrupo - $[A, *]$ é um subgrupo de $[G, *]$ se $[G, *]$ é um grupo, $A \subseteq G$, A é fechado sob $*$, o elemento identidade de G pertence a A e todos os elementos de A têm inverso em A
- Isomorfismo de grupo - dois grupos são isomorfos se são exatamente o mesmo, a menos dos nomes de seus elementos
- Anel - um grupo abeliano em relação à adição com as propriedades adicionais de fechamento, associatividade e distributividade em relação à multiplicação
- Corpo - um anel no qual os elementos não-zero formam um grupo abeliano sob a multiplicação

Referências

CAMARGO, H. Apostila de Estruturas Discretas.

CAVALCANTE, A. L. B. Teoria dos Números e Criptografia. *Revista Virtual*, 2005, Disponível em: [http://www.upis.br/revistavirtual/Cavalcante %20Teoria%20dos%20N%FAmeros%20e %20Criptografia 2005 UPIS.pdf](http://www.upis.br/revistavirtual/Cavalcante%20Teoria%20dos%20N%FAmeros%20e%20Criptografia%202005%20UPIS.pdf)>. Acesso em: 19 set. 2012.

DOMINGUES, Hygino Hugueros; IEZZI, Gelson. *Álgebra moderna*. 2. ed. São Paulo: Atual, 1982. 263 p.

GERSTING, J. L. *Fundamentos Matemáticos para Ciência da Computação*: um tratamento moderno da Matemática Discreta. Tradução Valéria de Magalhães Iorio. 5. ed. Rio de Janeiro: LTC, 2004. 597 p.

HEFEZ, Abramo. *Curso de álgebra*. 2. ed. Rio de Janeiro: IMPA, 1993. v.1. 221 p. -- (Coleção Matemática Universitária)

MENEZES, P. B. *Matemática Discreta para Computação e Informática*. 2. ed. Porto Alegre: Sagra Luzatto, 2005. 258 p. (Série de Livros Didáticos, n. 16).

SCHEINERMAN, E. R., *Matemática Discreta*: uma introdução. Revisão técnica de Flávio Soares Corrêa da Silva. 2. ed. norte-americana. São Paulo: Cengage Learning, 2011. 573 p.

YAN, S. Y. *Number Theory for Computing*. Springer, 381 p. 2000.