Universidade de Caxias do Sul
Centro de Ciências Exatas e Tecnologia
Departamento de Informática

Matemática Discreta

Márcia Rodrigues Notare

Caxias do Sul, julho de 2003.

ÍNDICE

1 TEORIA DOS CONJUNTOS

Definição de Conjunto: um conjunto é uma coleção de zero ou mais objetos distintos, chamados elementos do conjunto, os quais não possuem qualquer ordem associada. Em outras palavras, é uma ***coleção não-ordenada*** de objetos.

Exemplo: A = {branco, azul, amarelo}

Em um conjunto, a ordem dos elementos não importa e cada elemento deve ser listado apenas uma vez.

Podemos definir um conjunto de diferentes formas:

Denotação por Extensão: os elementos são listados exaustivamente.
Exemplo: Vogais = {a, e, i, o, u}

Denotação por Compreensão: definição de um conjunto por propriedades comuns aos objetos. De forma geral, escreve-se {x | P(x)}, onde P(x) representa a propriedade.
Exemplo: Pares = {*n* | *n* é par}, que representa o conjunto de todos os elementos *n*, tal que *n* é um número par.

Ainda podemos especificar um conjunto omitindo alguns elementos que estão implícitos na notação adotada. Veja exemplos:

Dígitos = {0, 1, 2, 3, ..., 9}
Pares = {0, 2, 4, 6, ...}

1.1 Relação de Pertinência

- Se *a* é elemento de um conjunto A, então podemos escrever:

$$a \in A$$

e dizemos que *a* pertence ao conjunto A.

- Se *a* não é elemento de um conjunto A, então podemos escrever:

$$a \notin A$$

e dizemos que *a* não pertence ao conjunto A.

Exemplo: Considerando o conjunto Vogais = {a, e, i, o, u}, podemos dizer que:
- e $\in$ Vogais
- m $\notin$ Vogais

Considerando o conjunto B = {x | x é brasileiro}, temos que:
- Pelé $\in$ B
- Bill Gates $\notin$ B

1.2 Alguns Conjuntos Importantes

O Conjunto Vazio é um conjunto que não possui elementos e pode ser denotado por $\varnothing$ ou { }.

Ainda temos:

- N, que representa o conjunto dos números naturais;
- Z, que representa o conjunto dos números inteiros;
- Q, que representa o conjunto dos números racionais;
- I, que representa o conjunto dos números irracionais;
- R, que representa o conjunto dos números reais;
- C, que representa o conjunto dos números complexos.

Definição de Alfabeto: um alfabeto é um conjunto finito, ou seja, um conjunto que pode ser denotado por extensão. Os elementos de uma alfabeto são chamados de símbolos ou caracteres.

Definição de Palavra: uma palavra sobre um alfabeto é uma seqüência finita de símbolos do alfabeto, justapostos.

ε palavra vazia
Σ alfabeto
Σ^* conjunto de todas as palavras possíveis sobre o alfabeto Σ

Exemplos:
- $\varnothing$ é um alfabeto
- {a, b, c, d} é uma alfabeto
- N não é um alfabeto
- ε é uma palavra sobre {a, b, c]
- ε é uma palavra sobre $\varnothing$
- $\varnothing^* = \{\varepsilon\}$

Aplicações na Computação

Chamamos de ***Linguagem Formal*** a um conjunto de palavras sobre um alfabeto. Portanto, podemos entender que uma ***linguagem de programação*** é o conjunto de todos os seus possíveis programas e que um programa é uma palavra da linguagem de programação.

1.3 Relação de Inclusão

Se todos os elementos de um conjunto A são também elementos de um conjunto B, então dizemos que:

$\boxed{A \subseteq B}$ A está contido em B

ou que

$\boxed{B \supseteq A}$ B contém A

Neste caso, podemos dizer que ***A é um subconjunto de B***.

Por outro lado, se $A \subseteq B$ e $A \neq B$, ou seja, existe $b \in B$ tal que $b \notin A$, então dizemos que:

$\boxed{A \subset B}$ A está contido propriamente em B

ou que

$\boxed{B \supset A}$ B contém propriamente A

Neste caso, dizemos que ***A é um subconjunto próprio de B***.

Exemplos:
- $\{1, 2, 3\} \subseteq \{3, 2, 1\}$
- $\{1, 2\} \subseteq \{1, 2, 3\}$
- $\{1, 2\} \subset \{1, 2, 3\}$

Definição de Conjunto Universo: denotado por U, é o conjunto que contém todos os conjuntos que estão sendo considerados, ou seja, define o contexto de discussão. Dessa forma, U não é um conjunto fixo e, para qualquer conjunto A, temos que $A \subseteq U$.

1.4 Igualdade de Conjuntos

Dois conjuntos A e B são ditos iguais se, e somente se, possuem os mesmos elementos, ou seja:

$$\boxed{A = B \leftrightarrow (A \subseteq B \wedge B \subseteq A)}$$

Exemplos:

- $\{0,1,2\} = \{x \in \mathrm{N} \mid x \geq 0 \wedge x < 3\}$
- $\mathrm{N} = \{x \in \mathrm{Z} \mid x \geq 0\}$
- {a, b, c} = {a, b, b, c, c, c}

1.5 Pertinência x Inclusão

Os elementos de um conjunto podem ser conjuntos. Portanto, preste atenção nos conceitos de pertinência e inclusão.

Exemplos: Considere o conjunto S = {a, b, c, d, ∅, {0}, {1, 2}}. Então:

- $\{a\} \notin S$
- $\{a\} \subseteq S$
- $\emptyset \in S$
- $\emptyset \subseteq S$
- $\{0\} \in S$
- $\{1,2\} \in S$
- $\{a, b, c, d\} \notin S$
- $\{a, b, c, d\} \subseteq S$

2 INTRODUÇÃO À LÓGICA MATEMÁTICA

Lógica é o estudo dos princípios e métodos usados para distinguir sentenças verdadeiras de falsas.

Definição de Proposição: uma proposição é uma construção que se pode atribuir juízo, ou seja, que pode ser apenas verdadeira ou falsa.

São exemplos de proposições:
- Quatro é maior do que cinco.
- Ela é muito inteligente.
- São Paulo é uma cidade grande

Exemplos que não são proposições:
- Como vai você?
- Como isso pode acontecer!
- Bom dia!

2.1 Conectivos Lógicos

As proposições podem ser simples (atômicas) ou compotas e os conectivos têm a função de combinar sentenças simples para formar sentenças compostas.

Proposição Atômica: são proposições que não podem ser decompostas em proposições mais simples.

Proposição Composta: são proposições mais complexas, compostas por proposições mais simples através dos conectivos lógicos (ou operadores lógicos).

Exemplos:
- Animais são peludos **e** aves têm penas.
- Vou comprar um carro **ou** uma bicicleta.
- **Se** chover **então** ficarei em casa.
- Um triângulo é equilátero **se e somente se** tiver os três lados iguais.

2.1.1 Negação

A negação de uma proposição é construída a partir da introdução da palavra ***não*** ou ***não é o caso que***.

Exemplos:
- Brasil **não** é um país.
- **Não é o caso que** quatro é maior do que cinco.

Considerando que P denota uma proposição, então sua negação é denotada por:

$\neg P$ ou $\sim P$ (lê-se "*não P*")

Interpretamos a negação da seguinte forma: se P é verdadeira, então ¬P é falsa; se P é falsa, então ¬P é verdadeira.

Para visualizar os valores lógicos de um conectivo utilizamos a tabela-verdade, que descreve as possíveis combinações dos valores lógicos das proposições.

P	¬ P
V	**F**
F	**V**

2.1.2 Conjunção

Uma conjunção é verdadeira se ***ambos*** seus conjunctos são verdadeiros. Caso contrário, é falsa. É denotada por:

$\boxed{P \wedge Q}$ (lê-se "*P e Q*")

A seguir a tabela-verdade da conjunção.

P	Q	P ∧ Q
V	V	**V**
V	F	**F**
F	V	**F**
F	F	**F**

2.1.3 Disjunção

Uma disjunção é verdadeira se ***pelo menos um*** dos seus disjunctos for verdadeiro. Caso contrário, é falsa. É denotada por:

$\boxed{P \vee Q}$ (lê-se "*P ou Q*")

A tabela-verdade da disjunção está apresentada a seguir.

P	Q	P ∨ Q
V	V	**V**
V	F	**V**
F	V	**V**
F	F	**F**

2.1.4 Condicional (Implicação)

O condicional é falso se seu antecedente for verdadeiro e seu conseqüente for falso. Caso contrário, ele é verdadeiro. É denotado por:

$\boxed{P \rightarrow Q}$ (lê-se "*se P então Q*")

Observe: a expressão "**P → Q**" assegura que: **não é o caso que P e não Q**. Verbalizando, se considerarmos a expressão:

"Se esfriar, então chove" (P → Q)

podemos interpretá-la como sendo:

"Não é o caso que esfria e não chove" ¬(P ∧ ¬Q)

Assim, podemos dizer que um enunciado da forma **P → Q** tem o ***mesmo significado*** (semântica) que um enunciado da forma **¬(P ∧ ¬Q)**, ou seja, ambos são verdadeiros sob as mesmas condições. Portanto, podemos obter a tabela-verdade de P → Q construindo a tabela verdade de ¬(P ∧ ¬Q).

P	Q	P → Q
V	V	**V**
V	F	**F**
F	V	**V**
F	F	**V**

2.1.5 Bicondicional

O bicondicional, denotado por $\boxed{P \leftrightarrow Q}$, tem o mesmo significado que (P $\rightarrow$ Q) $\wedge$ (Q $\rightarrow$ P). Assim, a tabela-verdade de (P $\leftrightarrow$ Q) pode ser obtida construindo a tabela-verdade de (P $\rightarrow$ Q) $\wedge$ (Q $\rightarrow$ P).

P	**Q**	**P $\leftrightarrow$ Q**
V	V	**V**
V	F	**F**
F	V	**F**
F	F	**V**

2.2 Fórmulas Bem-Formadas

Fórmulas bem-formadas (well formed formula - wff) são sentenças lógicas construídas corretamente sobre o alfabeto cujos símbolos são conectivos, parênteses e letras sentenciais.

Exemplos:
- $\neg$P, P $\wedge$ Q, P $\vee$ Q, P $\rightarrow$ Q, P $\leftrightarrow$ Q
- P $\vee \neg$Q
- (P $\wedge \neg$Q) $\rightarrow$ R
- $\neg$(P $\wedge$ Q) $\leftrightarrow$ ($\neg$P $\vee\neg$Q)

2.3 Tabelas-verdade para wffs

Para construir uma tabela-verdade para uma wff, escrevemos as letras sentenciais à esquerda da tabela e a fórmula à direita da tabela. Devemos completar com todas as possibilidades de valores verdade para as letras sentenciais. A seguir, devemos identificar o ***operador principal***, pois é ele que determina o valor-verdade para toda a fórmula. Por fim, completamos a tabela com os valores-verdade para os operadores, sub-wffs e por fim para a wff (operador principal).

Veja os exemplos abaixo, observando os passos de construção:

1. Construa a tabela-verdade para a fórmula $\neg\neg$**P**.
   a) preenchemos a coluna letra sentencial P, completando-se os possíveis valores-verdade que P pode assumir;
   b) preenchemos a coluna da ocorrência de P na fórmula (na wff);
   c) preenchemos o sinal de negação imediatamente à esquerda de P;
   d) preenchemos o segundo sinal de negação, que é o operador principal e, portanto, determina o valor-verdade da fórmula.

P	$\neg$	$\neg$	**P**
V	**V**	F	V
F	**F**	V	F

2. Construa a tabela-verdade para a fórmula $\neg$**P** $\vee$ **Q**.

P	**Q**	$\neg$ **P**	$\vee$	**Q**
V	V	F	**V**	V
V	F	F	**F**	F
F	V	V	**V**	V
F	F	V	**V**	F

Observe que o operador principal da fórmula acima é $\vee$ e, portanto, deve ter sua coluna como última a ser preenchida. Assim:

a) preenchemos as colunas das letras sentenciais P e Q (à esquerda da tabela);
b) preenchemos as colunas da ocorrência de $\neg$P e Q;
c) por fim, preenchemos a coluna $\vee$, que é o operador principal e, portanto, determina o valor verdade da fórmula.

3. Construa a tabela verdade para a fórmula **(P $\vee$ Q) $\wedge$ $\neg$(P $\wedge$ Q)**.

P	**Q**	**P**	$\vee$	**Q**	$\wedge$	$\neg$	**P**	$\wedge$	**Q**
V	V	V	V	V	**F**	F	V	V	V
V	F	V	V	F	**V**	V	V	F	F
F	V	F	V	V	**V**	V	F	F	V
F	F	F	F	F	**F**	V	F	F	F

O operador principal dessa fórmula é o $\wedge$ (veja: (P $\vee$ Q) $\wedge$ $\neg$(P $\wedge$ Q)). Assim a coluna deste operador determina o valor-verdade da fórmula. Então, as etapas de construção são como segue:
a) preenchemos as colunas das letras sentenciais P e Q (à esquerda da tabela);
b) preenchemos as colunas da ocorrência de P e Q na fórmula;
c) preenchemos as colunas da ocorrência de $\vee$ e $\wedge$ na fórmula (mas não o $\wedge$ principal);
d) preenchemos a coluna da ocorrência da negação do operador $\wedge$;
e) finalmente, preenchemos a coluna do operador principal $\wedge$, que determina o valor-verdade da fórmula. (Observe que o operador principal $\wedge$ conecta as colunas de $\vee$ e $\neg$).

4. Construa a tabela verdade para a fórmula **P $\vee$ $\neg$P**.

P	**P**	$\vee$	$\neg$**P**
V	V	**V**	F
F	F	**V**	V

5. Construa a tabela verdade para a fórmula **P $\wedge$ $\neg$P**.

P	**P**	$\wedge$	$\neg$**P**
V	V	**F**	F
F	F	**F**	V

Uma fórmula que assume sempre o valor lógico V, como no exemplo 4, é denominada uma ***tautologia***. Uma tautologia é intrinsecamente verdadeira pela sua própria estrutura, ou seja, é verdadeira independentemente dos valores lógicos atribuidos as suas letras sentenciais. Por outro lado, uma fórmula que assume sempre o valor lógico F, como no exemplo 5, é denominada uma ***contradição***. Uma contradiação é intrinsecamente falsa pela sua própria estrutura, ou seja, é falsa independentemente dos valores lógicos atribuidos as suas letras sentenciais.

2.4 Equivalência

Dizemos que duas fórmulas P e Q são equivalentes se a fórmula P $\leftrightarrow$ Q é uma tautologia. Denotamos essa propriedade por

$$\boxed{P \Leftrightarrow Q}$$

A seguir, exemplos de algumas equivalências tautológicas importantes, onde 1 representa uma tautologia e 0 representa uma contradição:

- Comutatividade:	$A \vee B \Leftrightarrow B \vee A$	$A \wedge B \Leftrightarrow B \wedge A$
- Associatividade:	$(A \vee B) \vee C \Leftrightarrow A \vee (B \vee C)$	$(A \wedge B) \wedge C \Leftrightarrow A \wedge (B \wedge C)$
- Distributividade:	$A \vee (B \wedge C) \Leftrightarrow (A \vee B) \wedge (A \vee C)$	$A \wedge (B \vee C) \Leftrightarrow (A \wedge B) \vee (A \wedge C)$
- Elemento Neutro:	$A \vee 0 \Leftrightarrow A$	$A \wedge 1 \Leftrightarrow A$
- Complementares:	$A \vee \neg A \Leftrightarrow 1$	$A \wedge \neg A \Leftrightarrow O$
- DeMorgan:	$\neg(A \vee B) \Leftrightarrow \neg A \wedge \neg B$	$\neg(A \wedge B) \Leftrightarrow \neg A \vee \neg B$

💻 **Aplicações na Computação**

Os conectivos lógicos E (AND), OU (OR) e NÃO (NOT), respectivamente $\wedge$, $\vee$ e $\neg$, estão disponíveis em muitas linguagens de programação. Eles agem sobre combinações e expressões verdadeiras e falsas para produzir um valor lógico final. Tais valores lógicos permitem a decisão do fluxo de controle em programas de computador. Assim, em uma ramificação condicional de um programa, se o valor lógico da expressão condicional for verdadeiro, o programa executará um trecho do seu código; se o valor lógico da expressão condicional for falso, ele execurá outro trecho do seu código. Se a expressão condicional for substituída por outra expressão equivalente mais simples, o valor lógico não será afetado, assim como o fluxo de controle do programa, mas o novo código será mais fácil de ser entendido e poderá ser executado mais rapidamente.

Veja o exemplo a seguir:

```
if ((x < y) and not ((x < y) and (z < 1000)))
   do AlgumaCoisa;
else
   do OutraCoisa;
```

Nesse exemplo, a expressão condicional tem a forma $A \wedge \neg(A \wedge B)$, onde A é "x < y" e B é "z < 1000". Podemos simplificar essa expressão utilizando as equivalências vistas anteriormente.

$A \wedge \neg(A \wedge B) \Leftrightarrow$	
$A \wedge (\neg A \vee \neg B) \Leftrightarrow$	(DeMorgan)
$(A \wedge \neg A) \vee (A \wedge \neg B) \Leftrightarrow$	(Distributividade)
$0 \vee (A \wedge \neg B) \Leftrightarrow$	(Complemetar)
$(A \wedge \neg B) \vee 0 \Leftrightarrow$	(Comutatividade)
$A \wedge \neg B$	(Elemento Neutro)

Podemos então reecrever a proposição da seguinte forma:

```
if ((x < y) and not (z < 1000))
   do AlgumaCoisa;
else
   do OutraCoisa;
```

2.5 Quantificadores

Wffs formadas apenas pelos cinco operadores lógicos ($\neg \wedge \vee \rightarrow \leftrightarrow$) têm possibilidade limitada de expressões. Por exemplo, não conseguiríamos simbolizar a sentença "Para todo x, x>0" como sendo uma proposição verdadeira sobre os inteiros positivos. Portanto novos conceitos, como o de quantificador, deve ser introduzido.

Quantificadores são frases do tipo ***para todo***, ***para cada*** ou ***para algum***, isto é, frases que dizem "quantos objetos" apresentam determinada propriedade.

Quantificador Universal: é simbolizado por $\forall$ e lê-se *para todo*, *para qualquer* ou *para cada*. Assim, a sentença acima pode ser simbolizada por:

$$\boxed{(\forall x)(x > 0)}$$

O valor lógico da expressão (∀x)(x>0) depende do domínio dos objetos sobre os quais estamos nos referindo, que chamamos de ***conjunto universo***. Qual seria o valor lógico da expressão (∀x)P(x) em cada uma das seguintes interpretações?

- P(x) é a propriedade que x é amarelo e o conjunto universo é o conjunto de todos os botões-de-ouro.
- P(x) é a propriedade que x é amarelo e o conjunto universo é o conjunto de todas as flores.
- P(x) é a propriedade que x é positivo ou negativo e o conjunto universo é conjunto de todos os inteiros.

Quantificador Existencial: é simbolizado por ∃ e lê-se *existe, existe algum, para pelo menos um, para algum.* Assim, a expressão

$$\boxed{(\exists x)(x > 0)}$$

pode ser lida como "existe um x tal que x é maior do que zero".

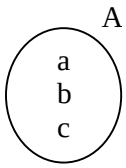
A expressão (∀x)(∃y)Q(x, y) é lida como "para todo x existe um y tal que Q(x, y)". Considerando que o conjunto universo é conjuntos dos números inteiros e que Q(x, y) é a propriedade x < y, a expressão diz que para todo inteiro x existe um inteiro maior. Esta expressão é verdadeira. Entretanto, se invertermos a ordem dos quantificadores escrevendo (∃y)(∀x)Q(x, y), a mesma interpretação diz que existe um inteiro y que é maior que qualquer outro inteiro x. Neste caso, o valor lógico da expressão é falso. Isto ressalta o fato de que a ordem dos quantificadores é importante!

3 ÁLGEBRA DE CONJUNTOS

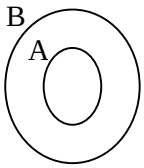
Entendemos que uma álgebra é constituída de operações definidas sobre um conjunto. Dessa forma, uma Álgebra de Conjuntos é constituída por operações definidas para todos os conjuntos.

Podemos representar conjuntos e suas operações através de figuras geométricas, como elipses e retângulos, chamados ***Diagramas de Venn***. Usualmente, os retângulos são utilizados para representar o conjunto universo e as elipses para representar os demais conjuntos.

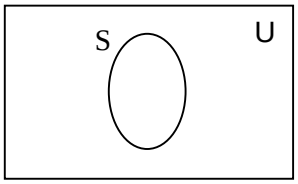
Por exemplo, as figuras abaixo representam:



O conjunto A = {a, b, c}



$A \subseteq B$



$S \subseteq U$

A relação de inclusão é transitiva, ou seja:

$$A \subseteq B \wedge B \subseteq C \Rightarrow A \subseteq C$$

Prova: Suponha A, B e C conjuntos quaisquer tal que $A \subseteq B$ e $B \subseteq C$.
Seja $a \in A$. Então, temos que

$a \in A$	
$a \in B$	pela definição de subconjunto ($A \subseteq B$)
$a \in C$	pela definição de subconjunto ($B \subseteq C$)

Logo, para qualquer elemento $a \in A$, temos que $a \in C$. Assim, pela definição de subconjunto, temos que $A \subseteq C$.

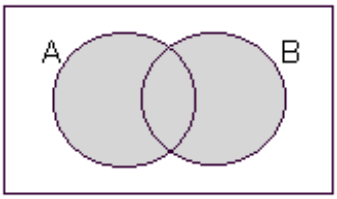
3.1 Operação de União

Sejam A e B conjuntos. A ***união*** dos conjuntos A e B, denotada por $A \cup B$, é como segue:

$$A \cup B = \{x \mid x \in A \vee x \in B\}$$

Em outras palavras, a união de dois conjuntos A e B considera todos os elementos que pertencem ao conjunto A ou ao conjunto B, ou seja, resulta em um conjunto cujos elementos pertencem a pelo menos um dos dois conjuntos.

A operação de união pode ser visualizada através de um diagrama de Venn, como mostrado a seguir.



Exemplos:

- Dados os conjuntos D = {0, 1, 2, 3, 4, 5, 6, 7, 8, 9} e V = {a, e, i, o, u}, temos que
$$D \cup V = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, a, e, i, o, u\}$$

- Dados os conjuntos $A = \{x \in N \mid x > 2\}$ e $B = \{ x \in N \mid x^2 = x\}$, temos que
$$A \cup B = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, ...\}$$

- Considere R, Q e I. Temos que
$$R \cup Q = R$$
$$R \cup I = R$$
$$Q \cup I = R$$

- Para qualquer conjunto universo U e qualquer $A \subseteq U$, temos que
$$\varnothing \cup \varnothing = \varnothing$$
$$U \cup \varnothing = U$$
$$U \cup A = U$$
$$U \cup U = U$$

3.1.1 Propriedades da União

Elemento Neutro: $A \cup \varnothing = \varnothing \cup A = A$

Prova:

Seja $x \in (A \cup \varnothing)$.

$x \in (A \cup \varnothing) \Leftrightarrow$

$x \in A \vee x \in \varnothing \Leftrightarrow$ (definição de união)

$x \in A$ (elemento neutro)

Logo, $A \cup \varnothing = A$

Analogamente, seja $x \in (\varnothing \cup A)$.

$x \in (\varnothing \cup A) \Leftrightarrow$

$x \in \varnothing \vee x \in A \Leftrightarrow$ (definição de união)

$x \in A \vee x \in \varnothing \Leftrightarrow$ (comutatividade)

$x \in A$ (elemento neutro)

Logo, $\varnothing \cup A = A$

Idempotência: $A \cup A = A$

Prova:

Seja $x \in (A \cup A)$.

$x \in (A \cup A) \Leftrightarrow$

$x \in A \vee x \in A \Leftrightarrow$ (definição de união)

$x \in A$ (idempotência do conectivo $\vee$)

Logo, $A \cup A = A$

Comutatividade: $A \cup B = B \cup A$
Prova:
Caso 1: Seja $x \in A \cup B$.
$x \in A \cup B \Rightarrow$
$x \in A \vee x \in B \Rightarrow$ (definição de união)
$x \in B \vee x \in A \Rightarrow$ (comutatividade do conectivo $\vee$)
$x \in (B \cup A)$ (definição de união)

Logo, pela definição de inclusão, $(A \cup B) \subseteq (B \cup A)$.

Caso 2: Seja $x \in B \cup A$.
$x \in B \cup A \Rightarrow$
$x \in B \vee x \in A \Rightarrow$ (definição de união)
$x \in A \vee x \in B \Rightarrow$ (comutatividade do conectivo $\vee$)
$x \in A \cup B$ (definição de união)

Logo, $(B \cup A) \subseteq (A \cup B)$. Portanto, pela definição de igualdade de conjuntos, podemos concluir que $A \cup B = B \cup A$.

Associatividade: $A \cup (B \cup C) = (A \cup B) \cup C$
Prova:
Caso 1: Seja $x \in A \cup (B \cup C)$.
$x \in A \cup (B \cup C) \Rightarrow$
$x \in A \vee x \in (B \cup C) \Rightarrow$ (definição de união)
$x \in A \vee (x \in B \vee x \in C) \Rightarrow$ (definição de união)
$(x \in A \vee x \in B) \vee x \in C \Rightarrow$ (associatividade do conectivo $\vee$)
$x \in (A \cup B) \vee x \in C \Rightarrow$ (definição de união)
$x \in (A \cup B) \cup C$ (definição de união)

Logo, pela definição de inclusão, temos que $A \cup (B \cup C) \subseteq (A \cup B) \cup C$.

Caso 2: Seja $x \in (A \cup B) \cup C$.
$x \in (A \cup B) \cup C \Rightarrow$
$x \in (A \cup B) \vee x \in C \Rightarrow$ (definição de união)
$(x \in A \vee x \in B) \vee x \in C \Rightarrow$ (definição de união)
$x \in A \vee (x \in B \vee x \in C) \Rightarrow$ (associatividade do conectivo $\vee$)
$x \in A \vee x \in (B \cup C) \Rightarrow$ (definição de união)
$x \in A \cup (B \cup C)$ (definição de união)

Logo, $(A \cup B) \cup C \subseteq A \cup (B \cup C)$. Portanto, pela definição de igualdade de conjuntos, podemos concluir que $A \cup (B \cup C) = (A \cup B) \cup C$.

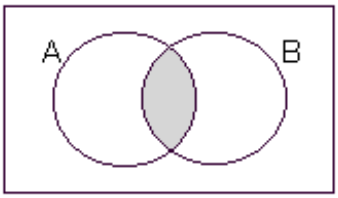
3.2 Operação de Interseção

Sejam A e B conjuntos. A ***interseção*** dos conjuntos A e B, denotada por $A \cap B$, é como segue:

$$A \cap B = \{x \mid x \in A \wedge x \in B\}$$

Em outras palavras, a interseção de dois conjuntos A e B considera todos os elementos que pertencem ao conjunto A e ao conjunto B, ou seja, resulta em um conjunto cujos elementos pertencem aos conjuntos A e B, simultaneamente.

A operação de interseção pode ser visualizada através de um diagrama de Venn, como mostrado a seguir.



Exemplos:

- Dados os conjuntos D = {0, 1, 2, 3, 4, 5, 6, 7, 8, 9}, V = {a, e, i, o, u} e P = {0, 2, 4, 6, 8, ...}, temos que

$$D \cap P = \{0, 2, 4, 6, 8\}$$
$$D \cap V = \varnothing$$

Chamamos conjuntos cuja interseção é o conjunto vazio de ***conjuntos disjuntos***.

- Dados os conjuntos $A = \{x \in N \mid x > 2\}$ e $B = \{ x \in N \mid x^2 = x\}$, temos que

$$A \cap B = \varnothing \qquad \text{(conjuntos disjuntos)}$$

- Considere R, Q e I. Temos que

$$R \cap Q = Q$$
$$R \cap I = I$$
$$Q \cap I = \varnothing$$

- Para qualquer conjunto universo U e qualquer conjunto $A \subseteq U$, temos que

$$\varnothing \cap \varnothing = \varnothing$$
$$U \cap A = A$$
$$U \cap \varnothing = \varnothing$$
$$U \cap U = U$$

3.2.1 Propriedades da Interseção

Elemento Neutro: $A \cap U = U \cap A = A$

Idempotência: $A \cap A = A$

Comutatividade: $A \cap B = B \cap A$

Associatividade: $A \cap (B \cap C) = (A \cap B) \cap C$

As provas são análogas à operação de união e ficam sugeridas como exercício.

Propriedades que envolvem União e Interseção

a) Distributividade da Interseção sobre a União: $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$

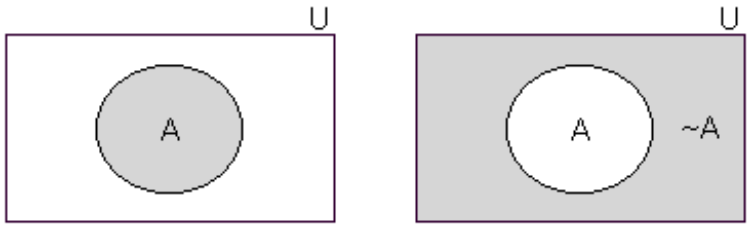
b) Distributividade da União sobre a Interseção: $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$

3.3 Operação Complemento

Suponha o conjunto universo U. O ***complemento*** de um conjunto $A \subseteq U$, denotado por $\boxed{\sim A}$, é como segue:

$$\boxed{\sim A = \{x \in \cup \mid x \notin A\}}$$

A operação complemento pode ser visualizada através de um diagrama de Venn, como mostrado a seguir.



Exemplos:

- Dados o conjunto universo U = {0, 1, 2, 3, 4, 5, 6, 7, 8, 9} e o conjunto A = {0, 1, 2}, temos que

$$\sim A = \{3, 4, 5, 6, 7, 8, 9\}$$

- Dados o conjunto universo U = N e o conjunto A = {0, 1, 2}, temos que

$$\sim A = \{x \in \mathbb{N} \mid x > 2\}$$

- Para qualquer conjuntos universo U, temos que

$$\sim \varnothing = U$$
$$\sim U = \varnothing$$

- Considerando R como conjunto universo, temos que

$$\sim Q = I$$
$$\sim I = Q$$

- Suponha U qualquer. Então para qualquer conjunto $A \subseteq U$, temos que

$$A \cup \sim A = U$$
$$A \cap \sim A = \varnothing$$
$$\sim \sim A = A$$

Podemos provar o último caso da seguinte forma:

Suponha um elemento $x \in A$.
$x \in A \Rightarrow$
para ~A, $x \notin A$, ou seja $\neg(x \in A) \Rightarrow$ (definição de complemento)
para ~ ~A, $\neg\neg(x \in A)$, ou seja, $x \in A$.

3.3.1 Propriedades de DeMorgan

a) $\sim(A \cup B) = \sim A \cap \sim B \quad \Leftrightarrow \quad A \cup B = \sim(\sim A \cap \sim B)$
b) $\sim(A \cap B) = \sim A \cup \sim B \quad \Leftrightarrow \quad A \cap B = \sim(\sim A \cup \sim B)$

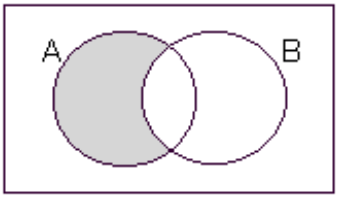
3.4 Operação de Diferença

Sejam A e B conjuntos. A ***diferença*** entre os conjuntos A e B, denotada por $\boxed{A - B}$, é como segue:

$$\boxed{A - B = \{x \mid x \in A \wedge x \notin B\}}$$

Em outras palavras, a diferença entre dois conjuntos A e B considera todos os elementos que pertencem ao conjunto A e que não pertencem ao conjunto B.

A operação de diferença pode ser visualizada através de um diagrama de Venn, como mostrado a seguir.



Exemplos:

- Dados os conjuntos D = {0, 1, 2, 3, 4, 5, 6 ,7 , 8, 9}, V = {a, e, i, o, u} e P = {0, 2, 4, 6, 8, ...}, temos que

$$D - V = D$$
$$D - P = \{1, 3, 5, 7, 9\}$$

- Dados os conjuntos $A = \{x \in \mathbb{N} \mid x > 2\}$ e $B = \{x \in \mathbb{N} \mid x = x^2\}$, temos que

$$A - B = \{3, 4, 5, 6, 7, ...\}$$
$$B - A = \{0, 1\}$$

- Dados os conjuntos R, Q e I, temos que

$$R - Q = I$$
$$R - I = Q$$
$$Q - I = Q$$

- Para qualquer conjunto universo U e qualquer conjunto $A \subseteq U$, temos que

$$\varnothing - \varnothing = \varnothing$$
$$U - \varnothing = U$$
$$U - A = {\sim}A$$
$$U - U = \varnothing$$

3.5 Conjunto das Partes

Dado conjunto A, temos que:

- $A \subseteq A$
- $\varnothing \subseteq A$
- Se $x \in A$, então $\{x\} \subseteq A$

A operação unária, que aplicada a um conjunto A, resulta num conjunto constituído de todos os subconjuntos de A é denominada ***conjunto das partes de A*** e é denotada por:

$$\boxed{P(A) = \{X \mid X \subseteq A\}}$$

Exemplo: Dados os conjuntos A = {a}, B = {a, b} e C = {a, b, c}, temos que

- $P(\varnothing) = \{\varnothing\}$
- $P(A) = \{\varnothing, \{a\}\}$
- $P(B) = \{\varnothing, \{a\}, \{b\}, \{a, b\}\}$
- $P(C) = \{\varnothing, \{a\}, \{b\}, \{c\}, \{a, b\}, \{a, c\}, \{b, c\}, \{a, b, c\}\}$

Se o número de elementos de um conjunto X é n, então o números de elementos de P(X) é 2^n.

3.6 Produto Cartesiano

Antes de definirmos a operação produto cartesiano, vamos definir uma seqüência: uma seqüência de n elementos é definida como sendo uma n-upla ordenada, ou seja, n objetos em ordem fixa. Particularmente, dizemos que uma 2-upla é uma par ordenado e é representada por $\langle x, y \rangle$ ou (x, y).

Observação: A ordem dos elementos é importante! Logo, $\langle x, y\rangle \neq \langle y, x\rangle$.

Sejam A e B conjuntos. O ***produto cartesiano*** de A por B é como segue:

$$\boxed{A \times B = \{\langle a, b\rangle \mid a \in A \wedge b \in B\}}$$

Denotamos o produto cartesiano de um conjunto A por ele mesmo como $\boxed{A \times A = A^2}$.

Exemplos: Dados os conjuntos A = {a}, B = {a, b} e C = {0, 1, 2}, temos que:

- $A \times B = \{\langle a,a\rangle, \langle a,b\rangle\}$
- $B \times C = \{\langle a,0\rangle, \langle a,1\rangle, \langle a,2\rangle, \langle b,0\rangle, \langle b,1\rangle, \langle b,2\rangle\}$
- $C \times B = \{\langle 0,a\rangle, \langle 0,b\rangle, \langle 1,a\rangle, \langle 1,b\rangle, \langle 2,a\rangle, \langle 2,b\rangle\}$
- $A^2 = \{\langle a,a\rangle\}$
- $B^2 = \{\langle a,a\rangle, \langle a,b\rangle, \langle b,a\rangle, \langle b,b\rangle\}$
- $A \times \mathrm{N} = \{\langle a,0\rangle, \langle a,1\rangle, \langle a,2\rangle, ...\}$
- $(A \times B) \times C = \{\langle\langle a,a\rangle,0\rangle, \langle\langle a,a\rangle,1\rangle, \langle\langle a,a\rangle,2\rangle, \langle\langle a,b\rangle,0\rangle, \langle\langle a,b\rangle,1\rangle, \langle\langle a,b\rangle,2\rangle\}$
- $A \times (B \times C) = \{\langle a,\langle a,0\rangle\rangle, \langle a,\langle a,1\rangle\rangle, \langle a,\langle a,2\rangle\rangle, \langle a,\langle b,0\rangle\rangle, \langle a,\langle b,1\rangle\rangle, \langle a,\langle b,2\rangle\rangle\}$
- $A \times \varnothing = \varnothing$
- $\varnothing \times A = \varnothing$
- $\varnothing^2 = \varnothing$

Observações:

- Não-comutatividade: $A \times C \neq C \times A$
- Não-associatividade: $(A \times B) \times C \neq A \times (B \times C)$

Propriedades que envolvem Produto Cartesiano, União e Interseção

a) Distributividade sobre a União: $A \times (B \cup C) = (A \times B) \cup (A \times C)$

b) Distributividade sobre a Interseção: $A \times (B \cap C) = (A \times B) \cap (A \times C)$

3.7 União Disjunta

Sejam A e B conjuntos. A ***união disjunta*** dos conjuntos A e B, denotada por $\boxed{A + B}$, é como segue:

$$\boxed{A + B = \{\langle a, A\rangle \mid a \in A\} \cup \{\langle b, B\rangle \mid b \in B\}}$$

onde os pares ordenados $\langle a, A\rangle$ e $\langle b, B\rangle$ representam $\langle \textit{elemento}, \textit{identificação}\rangle$.

Também podemos denotar a união disjunta da seguinte forma:

$$\boxed{A + B = \{a_A \mid a \in A\} \cup \{b_B \mid b \in B\}}$$

Exemplos: Dados os conjuntos D = {0, 1, 2, 3, 4, 5, 6, 7, 8, 9}, V = {a, e, i, o, u}, P = {0, 2, 4, 6, ...} e A = {a, b, c}, temos que:

- D + V = $\{0_D, 1_D, 2_D, 3_D, 4_D, 5_D, 6_D, 7_D, 8_D, 9_D, a_V, e_V, i_V, o_V, u_V\}$
- D + P = $\{0_D, 1_D, 2_D, 3_D, 4_D, 5_D, 6_D, 7_D, 8_D, 9_D, 0_P, 2_P, 4_P, 6_P, ...\}$
- $\varnothing + \varnothing = \varnothing$
- A + $\varnothing$ = $\{a_A, b_A, c_A\}$
- A + A = $\{a_0, b_0, c_0, a_1, b_1, c_1\}$

4 RELAÇÕES

4.1 Relação Binária

Dados dois conjuntos A e B, uma relação binária R de A em B é um subconjunto de um produto cartesiano $A \times B$, ou seja $R \subseteq A \times B$, onde:

- A é o domínio, origem ou conjunto de partida de R
- B é o contra-domínio, destino ou conjunto de chegada de R

Para $R \subseteq A \times B$, se $\langle a,b \rangle \in R$, então afirmamos que "a relaciona-se com b". Podemos denotar uma relação R da seguinte forma: $R : A \to B$ e, para um elemento $\langle a,b \rangle \in R$, podemos denota-lo como aRb.

Exemplos: Sejam A = {a}, B = {a, b} e C = {0, 1, 2}. São exemplos de relações:

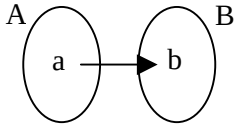
- $\varnothing$ é uma relação de A em B
- $A \times B = \{\langle a,a \rangle, \langle a,b \rangle\}$ é uma relação de A em B
- Relação de Igualdade de A em A: $\{\langle a,a \rangle\}$
- Relação "menor" de C em C: $\{\langle 0,1 \rangle, \langle 0,2 \rangle, \langle 1,2 \rangle\}$
- Relação de C em B: $\{\langle 0,a \rangle, \langle 1,b \rangle\}$
- $\subseteq : P(B) \to P(B)$
- $\leq : C \to C$
- $= : A \to A$

Endorrelação ou Auto-Relação: dado um conjunto A, uma relação do tipo $R : A \to A$ é dita uma Endorrelação ou Auto-Relação. Assim, temos que origem e destino são o mesmo conjunto e podemos denota-la por $\langle A, R \rangle$.

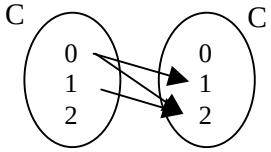
Exemplos: Seja A um conjunto. Então, são endorrelações:

- $\langle \mathrm{N}, \leq \rangle$
- $\langle \mathrm{Z}, \leq \rangle$
- $\langle Q, = \rangle$
- $\langle P(A), \subseteq \rangle$
- $\langle P(R), \subset \rangle$

Uma relação binária pode ser representada no diagrama de Venn, como mostram as figuras abaixo.



par $\langle a,b \rangle$ de $R : A \to B$



$\langle C, < \rangle = \{\langle 0,1 \rangle, \langle 0,2 \rangle, \langle 1,2 \rangle\}$

A seguir, algumas definições referentes ao conceito de relação:

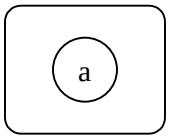
a) $\langle a,b\rangle \in R$: dizemos que *R* está definida para *a* e que *b* é a imagem de *a*.
b) Domínio de definição: é o conjunto de todos os elementos de A para os quais *R* está definida.
c) Conjunto imagem: conjunto de todos os elementos de B que estão relacionados com algum elemento de A.

Exemplos: Dados os conjuntos A = {a}, B = {a, b} e C = {0, 1, 2}, temos que
- para a endorelação $\langle C,< \rangle$, o domínio de definição é o conjunto {0, 1} e o conjunto imagem é o conjuto {1, 2]
- para a relação $=: A \to B$, o domínio de definição é o conjunto {a} e o conjunto imagem também é o conjunto {a}.

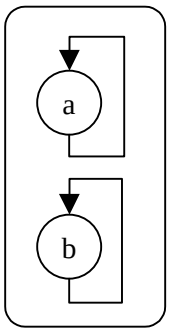
4.2 Endorrelação como Grafo

Toda endorrelação $R : A \to A$ pode ser representada como um grafo, onde:
a) cada elemento do conjunto A é representado como um nodo do grafo;
b) cada par $\langle a,b\rangle$ da relação é representada como uma aresta do grafo, com origem em *a* e destino em *b*.

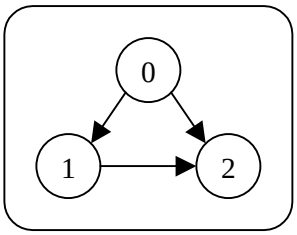
Exemplos:



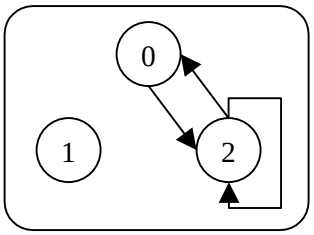
$\varnothing: A \to A$



$=: B \to B = \{\langle a,a\rangle, \langle b,b\rangle\}$



$\langle C,< \rangle = \{\langle 0,1\rangle, \langle 0,2\rangle, \langle 1,2\rangle\}$



$R : C \to C$ tal que $R = \{\langle 0,2\rangle, \langle 2,0\rangle, \langle 2,2\rangle\}$

4.3 Relação como Matriz

Sejam A = {a_1, a_2, ..., a_n} e B = {b_1, b_2, ..., b_m} dois conjuntos finitos. A representação da relação $R : A \to B$ como matriz é como segue:
a) o número de linhas é n (número de elementos do domínio);
b) o número de colunas é m (número de elementos da imagem);
c) a matriz resultante possui m x n células;
d) cada uma das m x n células possuem um valor lógico associado;
e) se $\langle a_i, b_j \rangle \in R$, então a posição determinada pela linha *i* e pela coluna *j* da matriz contém valor verdadeiro (1); caso contrário, seu valor será falso (0).

Exemplo: Dados os conjuntos A = {a}, B = {a, b} e C = {0, 1, 2}, temos que

$\varnothing$	a
a	0

$\varnothing: A \to A$

=	a	b
a	1	0
b	0	1

$\langle B, = \rangle$

<	0	1	2
0	0	1	1
1	0	0	1
2	0	0	0

$\langle C, < \rangle$

R	0	1	2
0	0	0	1
1	0	0	0
2	1	0	1

$R : C \to C$ tal que $R = \{\langle 0,2 \rangle, \langle 2,0 \rangle, \langle 2,2 \rangle\}$

$A \times B$	a	b
a	1	1

$A \times B = A \to B$

S	a	b
0	1	0
1	0	1
2	0	0

$S = \{\langle 0, a \rangle, \langle 1, b \rangle\}: C \to B$

$\subseteq$	$\varnothing$	{a}	{b}	{a, b}
$\varnothing$	1	1	1	1
{a}	0	1	0	1

$\subseteq: P(A) \to P(B)$

4.4 Propriedades das Relações

Uma endorrelação binária em um conjunto A pode ter determinadas propriedades. A seguir serão apresentadas as propriedades que envolvem as endorrelações.

4.4.1 Relação Reflexiva

Sejam A um conjunto e R uma endorrelação em A. R é uma relação reflexiva se:

$$\boxed{(\forall a \in A)(aRa)}$$

A negação da propriedade reflexiva é como segue: $\boxed{(\exists a \in A)(\neg(aRa))}$

Exemplos: Dado o conjunto A = {0, 1, 2}, temos que as seguintes relações são reflexivas

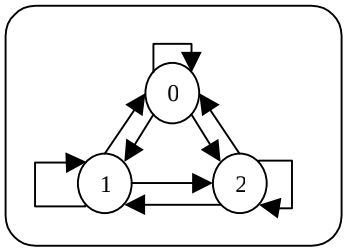
- $\langle \mathrm{N}, \leq \rangle$, pois todo elemento é igual a si mesmo
- $\langle P(A), \subseteq \rangle$, pois todo conjunto está contido em si mesmo
- $A^2 : A \to A$, pois esta relação contém os pares $\langle 0,0 \rangle, \langle 1,1 \rangle$ e $\langle 2,2 \rangle$
- $\langle A, = \rangle$, pois todo elemento é igual a si mesmo

A matriz e o grafo de uma relação reflexiva apresentam uma característica especial: a diagonal principal da matriz contém somente valores lógicos verdadeiro (1) e qualquer nodo do grafo

possui uma aresta com origem e destino nele mesmo. Veja as matrizes e grafos referentes a alguns dos exemplos apresentados acima.

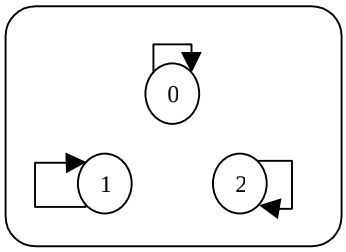
$A^2 : A \to A$

A^2	0	1	2
0	1	1	1
1	1	1	1
2	1	1	1



$\langle A, = \rangle$

=	0	1	2
0	1	0	0
1	0	1	0
2	0	0	1



4.4.2 Relação Irreflexiva

Sejam A um conjunto e R uma endorrelação em A. R é uma relação irreflexiva se:

$$\boxed{(\forall a \in A)(\neg(aRa))}$$

Exemplos: Dado o conjunto A = {0, 1, 2}, temos que as seguintes relações são irreflexivas

- $\langle \mathbb{Z}, \neq \rangle$, pois não elemento diferente de si mesmo
- $\langle P(A), \subset \rangle$, pois para a relação "está contido propriamente" os conjunto precisam se diferentes
- $\varnothing: A \to A$, pois não há nenhum elemento do tipo $\langle a, a \rangle$
- $\langle A, R \rangle$, se $R = \{\langle 0,1 \rangle, \langle 1,2 \rangle, \langle 2,1 \rangle\}$, pois não há nenhum elemento do tipo $\langle a, a \rangle$

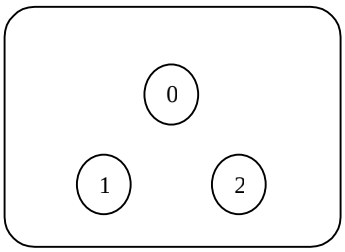
Exemplo de relação nem reflexiva, nem irreflexiva:

- $\langle A, S \rangle$, se $S = \{\langle 0,2 \rangle, \langle 2,0 \rangle, \langle 2,2 \rangle\}$

A matriz e o grafo de uma relação irreflexiva apresentam uma característica especial: a diagonal principal da matriz contém somente valores lógicos falso (0), e qualquer nodo do grafo não possui aresta com origem e destino nele mesmo. Veja as matrizes e grafos referentes a alguns dos exemplos apresentados acima.

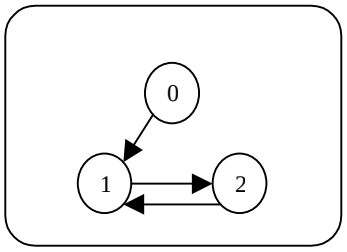
$\varnothing : A \to A$

$\varnothing$	0	1	2
0	0	0	0
1	0	0	0
2	0	0	0



$R = \{\langle 0,1\rangle, \langle 1,2\rangle, \langle 2,1\rangle\}$

R	0	1	2
0	0	1	0
1	0	0	1
2	0	1	0



4.4.3 Relação Simétrica

Sejam A um conjunto e R uma endorrelação. R é uma relação simétrica se:

$$(\forall a \in A)(\forall b \in A)(aRb \rightarrow bRa)$$

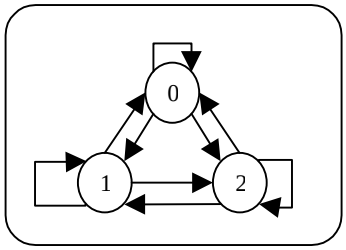
Exemplos: Dados o conjunto A = {0, 1, 2} e *X* um conjunto qualquer, temos que as seguintes relações são simétricas

- $X^2: X \rightarrow X$
- $\langle X, = \rangle$
- $\langle X, \neq \rangle$
- $\langle P(X), = \rangle$
- $\varnothing: X \rightarrow X$

A matriz e o grafo de uma relação simétrica apresentam uma característica especial: na matriz, a metade acima da diagonal principal é a imagem espelhada da metade de baixo, e, no grafo, entre dois nodos quaisquer, ou <u>não</u> existe aresta, ou existem <u>duas</u> arestas, uma em cada sentido. Veja as matrizes e grafos referentes a alguns dos exemplos apresentados acima.

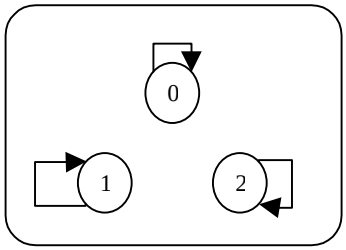
$A^2 : A \rightarrow A$

A^2	0	1	2
0	1	1	1
1	1	1	1
2	1	1	1



$\langle A, = \rangle$

=	0	1	2
0	1	0	0
1	0	1	0
2	0	0	1



4.4.4 Relação Anti-Simétrica

Sejam A um conjunto e R uma endorrelação em A. R é uma relação anti-simétrica se:

$$(\forall a \in A)(\forall b \in A)(aRb \wedge bRa \rightarrow a = b)$$

Exemplos: Dados o conjunto A = {0, 1, 2} e X um conjunto qualquer, temos que as seguintes relações são anti-simétricas

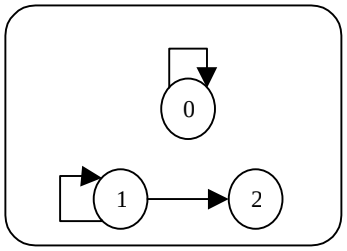
- $\langle X, = \rangle$
- $\langle P(X), = \rangle$
- $\varnothing : X \to X$
- $\langle \mathrm{N}, R \rangle$, se $R = \{\langle x, y \rangle \in \mathrm{N}^2 \mid \ y = x^2\}$

Exemplo de relação nem simétrica, nem anti-simétrica:
- $\langle A, S \rangle$, se $S = \{\langle 0,1 \rangle, \langle 1,0 \rangle, \langle 1,2 \rangle\}$

A matriz e o grafo de uma relação anti-simétrica apresentam uma característica especial: na matriz, para qualquer célula verdadeira (1) em uma das metades da matriz, a correspondente célula na outra metade é falsa (0); no grafo, entre dois nodos quaisquer, existe no máximo uma aresta. Veja a matriz e o grafo referentes a um dos exemplos apresentado acima.

$R = \{\langle 0,0 \rangle, \langle 1,1 \rangle, \langle 1,2 \rangle\}$

R	0	1	2
0	1	0	0
1	0	1	1
2	0	0	0



4.4.5 Relação Transitiva

Sejam A um conjunto e R uma endorrelação em A. R é uma relação transitiva se:

$$(\forall a \in A)(\forall b \in A)(\forall c \in A)(aRb \wedge bRc \to aRc)$$

Exemplos: Dado um conjunto X qualquer, temos que as seguintes relações são transitivas
- $X^2 : X \to X$
- $\varnothing : X \to X$
- $\langle X, = \rangle$
- $\langle \mathrm{N}, \leq \rangle$
- $\langle \mathrm{Z}, < \rangle$
- $\langle P(X), \subseteq \rangle$
- $\langle P(X), \subset \rangle$

Exemplos: Dado um conjunto X qualquer, temos que as seguintes relações <u>não</u> são transitivas
- $\langle \mathrm{Z}, \neq \rangle$
- $\langle A, R \rangle$, se $R = \{\langle 0,1 \rangle, \langle 2,0 \rangle, \langle 2,1 \rangle\}$
- $\langle A, R \rangle$, se $R = \{\langle 0,2 \rangle, \langle 2,0 \rangle, \langle 2,2 \rangle\}$

4.5 Fechos de Relações

Sejam $R: A \to A$ uma endorrelação e P um conjunto de propriedades. Então, ***o fecho de R em relação a P*** é a menor endorrelação em A que contém R e que satisfaz as propriedades de P. Se a relação R já contém as propriedades de P, então ela é a seu próprio fecho em relação a P.

$$R \subseteq FECHO - P(R)$$

4.5.1 Fecho Reflexivo

Suponha *R:* $A \to A$ uma endorrelação. Então o fecho reflexivo de R é definido como segue:

$$\boxed{Fecho - \{reflexiva\}(R) = R \cup \{\langle a,a\rangle \mid a \in A\}}$$

Exemplo: Dados o conjunto A = {1, 2, 3, 4, 5} e *R:* $A \to A$ uma endorrelação, tal que $R = \{\langle 1,2\rangle, \langle 1,5\rangle, \langle 2,3\rangle, \langle 3,4\rangle\}$, temos que

- $Fecho - \{reflexiva\}(R) = \{\langle 1,1\rangle, \langle 1,2\rangle, \langle 1,5\rangle, \langle 2,2\rangle, \langle 2,3\rangle, \langle 3,3\rangle, \langle 3,4\rangle, \langle 4,4\rangle, \langle 5,5\rangle\}$

4.5.2 Fecho Simétrico

Suponha *R:* $A \to A$ uma endorrelação. Então o fecho simétrico de R é definido como segue:

$$\boxed{Fecho - \{simétrica\}(R) = R \cup \{\langle b,a\rangle \mid \langle a,b\rangle \in R\}}$$

Exemplo: Dados o conjunto A = {1, 2, 3, 4, 5} e *R:* $A \to A$ uma endorrelação, tal que $R = \{\langle 1,2\rangle, \langle 1,5\rangle, \langle 2,3\rangle, \langle 3,4\rangle\}$, temos que

- $Fecho - \{simétrica\}(R) = \{\langle 1,2\rangle, \langle 1,5\rangle, \langle 2,1\rangle, \langle 2,3\rangle, \langle 3,2\rangle, \langle 3,4\rangle, \langle 4,3\rangle, \langle 5,1\rangle\}$

4.5.3 Fecho Transitivo

Suponha *R:* $A \to A$ uma endorrelação. Então o fecho transitivo de R é definido como segue:

a) se $\langle a,b\rangle \in R$, então $\langle a,b\rangle \in Fecho - \{transitiva\}(R)$;

b) se $\langle a,b\rangle \in Fecho - \{transitiva\}(R)$ e $\langle b,c\rangle \in Fecho - \{transitiva\}(R)$, então $\langle a,c\rangle \in Fecho - \{transitiva\}(R)$.

Exemplo: Dados o conjunto A = {1, 2, 3, 4, 5} e *R:* $A \to A$ uma endorrelação, tal que $R = \{\langle 1,2\rangle, \langle 1,5\rangle, \langle 2,3\rangle, \langle 3,4\rangle\}$, temos que

- $Fecho - \{transitiva\}(R) = \{\langle 1,2\rangle, \langle 1,3\rangle, \langle 1,4\rangle, \langle 1,5\rangle, \langle 2,3\rangle, \langle 2,4\rangle, \langle 3,4\rangle\}$

Algumas notações são importantes e podem ser utilizadas para simplificar e representar as seguintes relações:

a) $R^+ = Fecho - \{transitiva\}(R)$

b) $R^* = Fecho - \{reflexiva, transitiva\}(R)$

Portanto, considerando o exemplo acima, temos que

- $R^* = \{\langle 1,1\rangle, \langle 1,2\rangle, \langle 1,3\rangle, \langle 1,4\rangle, \langle 1,5\rangle, \langle 2,2\rangle, \langle 2,3\rangle, \langle 2,4\rangle, \langle 3,3\rangle, \langle 3,4\rangle, \langle 4,4\rangle, \langle 5,5\rangle\}$

4.6 Relação de Ordem

Intuitivamente, podemos pensar numa relação de ordem quando lembramos de uma fila no banco, de uma fila de alunos dispostos numa sala de aula, na relação "menor ou igual" no números naturais, etc.

Ordem parcial: é toda relação binária em um conjunto A que é, simultaneamente, *reflexiva*, *anti-simétrica* e *transitiva*.

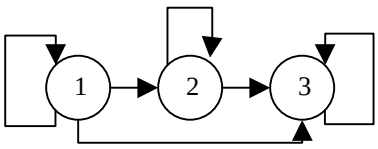
São exemplos de relação de ordem parcial:

- $\langle \mathrm{N}, \leq \rangle$
- $\langle P(\mathrm{N}), \subseteq \rangle$
- $\langle \mathrm{Z}^{+}, x\_divide\_y \rangle$

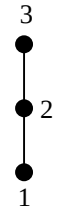
Se R é uma relação de ordem parcial em A, então dizemos que $\langle A, R \rangle$ é um conjunto parcialmente ordenado.

Se A é um conjunto finito, então podemos representar visualmente um conjunto parcialmente ordenado em A por um ***diagrama de Hasse***. Cada elemento de A é representado por um ponto (vértice) do diagrama. O diagrama de Hasse pode ser construído com base num grafo, onde as arestas que representam as relações reflexivas e transitivas ficam implícitas no diagrama. Veja o exemplo a seguir.

Exemplo: Dados o conjunto A = {1, 2, 3} e a relação de ordem $\langle A, \leq \rangle$, temos seus respectivos grafo e diagrama de Hasse representados abaixo.



(grafo)

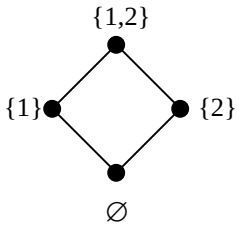


(diagrama de Hasse)

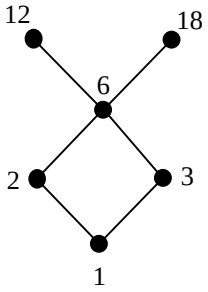
Observe que os elementos da relação são representados no diagrama em ordem crescente de baixo para cima, ou seja, como 1 ≤ 2, então o elemento 1 aparece abaixo do elemento 2. As orientação das arestas torna-se, dessa forma, desnecessária, já que a disposição dos elementos no diagrama preserva essa informação.

Exemplos:

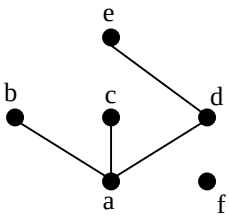
- Dada a relação de ordem $\langle P(\{1,2\}), \subseteq \rangle$, seu diagrama de Hasse está representado abaixo.



- Dados o conjunto A = {1, 2, 3, 6, 12, 18} e a relação de ordem "x divide y", o diagrama de Hasse está representado abaixo.



- Dado o diagrama de Hasse a seguir,



temos que o conjunto dado pela relação de ordem é $\{\langle a,a\rangle,\langle a,b\rangle,\langle a,c\rangle,\langle a,d\rangle,\langle a,e\rangle,\langle b,b\rangle,\langle c,c\rangle,\langle d,d\rangle,\langle d,e\rangle,\langle e,e\rangle,\langle f,f\rangle\}$.

4.6.1 Elemento Mínimo

Suponha A um conjunto e $\langle A,R\rangle$ uma relação de ordem. Dizemos que *m* é elemento mínimo de R se

$$\boxed{(\forall a\in A)(mRa)}$$

4.6.2 Elemento Minimal

Suponha A um conjunto e $\langle A,R\rangle$ uma relação de ordem. Dizemos que *m* é elemento minimal de R se

$$\boxed{(\forall a\in A)(\langle a,m\rangle\notin R)}$$

4.6.3 Elemento Máximo

Suponha A um conjunto e $\langle A,R\rangle$ uma relação de ordem. Dizemos que *m* é elemento máximo de R se

$$\boxed{(\forall a\in A)(aRm)}$$

4.6.4 Elemento Maximal

Suponha A um conjunto e $\langle A,R\rangle$ uma relação de ordem. Dizemos que *m* é elemento maximal de R se

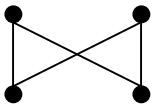
$$\boxed{(\forall a\in A)(\langle m,a\rangle\notin R)}$$

Exemplo: Dados o conjunto A = {1, 2, 3, 6, 12, 18} e a relação de ordem "x divide y", cujo diagrama de Hasse já foi apresentado anteriormente, temos que

- 1 é elemento mínimo, pois está relacionado com todos os outros elementos de A;
- 1 é elemento minimal, pois não há elemento que relaciona-se com ele;
- 12 e 18 são elementos maximais, pois não existem elementos com os quais eles relacionam-se;

- não há elemento máximo, pois não há elemento que se relaciona com todos os outros elementos de A.

Exemplo: Desenhe um diagrama de Hasse para um conjunto parcialmente ordenado com quatro elementos, tais que existam dois elementos minimais, dois elementos maximais, não existam elementos mínimo e máximo e cada elemento está relacionado com dois outros elementos.
Um possível diagrama é o apresentado a seguir:



4.7 Relação de Equivalência

A relação de equivalência nos dá a noção de igualdade semântica, ou seja, de elementos que apresentam um mesmo significado.

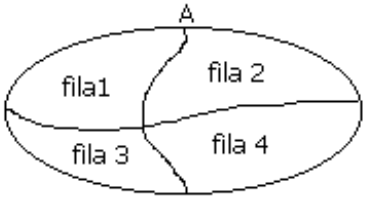
Relação de Equivalência: é toda relação binária em um conjunto A que é, simultaneamente, *reflexiva*, *simétrica* e *transitiva*.

São exemplos de relações de equivalência:

- $\langle X, = \rangle$
- $\langle A, R \rangle$, se A = {0, 1} e $aRb \leftrightarrow a = b^2$

Partição de um Conjunto: uma partição de um conjunto A é um conjunto de subconjuntos disjuntos não-vazios cuja união é igual ao conjunto A.

Para visualizar uma partição, suponha um conjunto A = {x | x é aluno de Matemática Discreta} e a relação $xRy \leftrightarrow \langle A, x\_\text{sen}ta\_na\_mesma\_fila\_que\_y \rangle$. Ao agruparmos todos os alunos do conjunto A que estão relacionados entre si, obtemos a figura abaixo. Observe que o conjunto A foi divido em subconjuntos tais que todos os alunos da turma pertencem a um, e somente um, subconjunto.



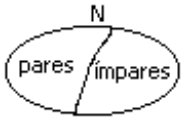
Qualquer relação de equivalência divide o conjunto onde está definida em uma partição. Os subconjuntos que compõem a partição são formados agrupando-se os elementos relacionados, como no caso dos alunos da turma de Matemática Discreta.

Classes de Equivalência: se *R* é uma relação de equivalência em um conjunto A e se $a \in$ A, denotamos por [*a*] o conjunto de todos os elementos relacionados a *a* em A e o chamamos de *classe de equivalência de a*. Dessa forma, podemos escrever que

$$[a] = \{x \mid x \in A \wedge aRx\}$$

Teorema: uma relação de equivalência R em um conjunto A determina uma partição de A e uma partição de A determina uma relação de equivalência em A.

Exemplo: Considere o conjunto dos números naturais e a relação de equivalência $\langle \mathrm{N}, "x + y \_ é \_ par" \rangle$. Tal relação divide o conjunto N em duas partes, ou seja, em duas classes de equivalências. Se *x* é par, então *x* + *y* é par, para todo número par; se *x* é ímpar, então *x* + *y* é ímpar para todo número ímpar. Assim, todos os números pares formam uma classe de equivalência e todos os números ímpares formam uma segunda classe de equivalência. Podemos representar essa partição de N como mostra figura abaixo.



Observe que as classes de equivalência podem ser representadas por qualquer objeto pertencente à ela:
- classe dos pares: [2] = [6] = [1034] = {0, 2, 4, 6, ...}
- classe dos ímpares: [1] = [11] = [2451] = {1, 3, 5, 7, ...}

Exemplo: Para cada uma das relações a seguir, descreva as classes de equivalência correspondentes.

a) $\langle \mathrm{N}, = \rangle$

Possui *n* classes de equivalência, tais que cada classe de equivalência contém um único elemento.
[*n*] = {*n*}

b) Em A = {1, 2, 3} e $R = \{\langle 1,1\rangle, \langle 2,2\rangle, \langle 3,3\rangle, \langle 1,2\rangle, \langle 2,1\rangle\}$

As classes de equivalência são as seguintes:
[1] = {1, 2} = [2]
[3] = {3}

4.7.1 Congruência em Z

Considere o conjunto dos números inteiros Z e um número inteiro $m > 1$. Dizemos que *x* é congruente a *y* módulo *m*, denotada por

$$\boxed{x \equiv y (\mathrm{mod}\, m)}$$

se $x - y$ é divisível por *m*, ou seja, se $x = y + km$ para algum inteiro *k*.

A relação de congruência em Z define uma relação de equivalência em Z. Para verificar que isso é válido, temos que mostrar que a relação de congruência em Z é uma relação reflexiva, simétrica e transitiva. Acompanhe o raciocínio a seguir: para qualquer inteiro *x*, temos que $x \equiv x (\mathrm{mod}\, m)$, pois $x - x = 0$ é divisível por *m*. Logo, temos que a relação é *reflexiva*. Suponha que $x \equiv y (\mathrm{mod}\, m)$, então $x - y$ é divisível por *m*. Então $-(x - y) = y - x$ também é divisível por *m*. Logo, temos que a relação é *simétrica*. Suponha agora que $x \equiv y (\mathrm{mod}\, m)$ e que $y \equiv z (\mathrm{mod}\, m)$, então $x - y$ e $y - z$ são divisíveis por *m*. Então, temos que a soma $(x - y) + (y - z) = x - z$ também é divisível por *m*. Logo, $x \equiv z (\mathrm{mod}\, m)$ e a relação é *transitiva*. Assim, mostramos que a relação de congruência módulo *m* em Z é, simultaneamente, reflexiva, simétrica e transitiva e, portanto, é uma relação de equivalência.

4.8 Relação Inversa

Seja uma relação *R: A* $\rightarrow$ *B*. Então, a ***relação inversa*** é como segue:

$$R^{-1} : B \to A = \{\langle b,a\rangle \mid \langle a,b\rangle \in R\}$$

Exemplos:

- Dados os conjuntos A = {a, b} e B = {2, 3, 4} e a relação $R : B \to A = \{\langle 2,a\rangle, \langle 3,b\rangle\}$, temos que a relação inversa de *R*, R^{-1} é dada por
$$R^{-1} : A \to B = \{\langle a,2\rangle, \langle b,3\rangle\}$$
- Dados o conjunto C = {2, 3, 4} e a relação $\langle C, <\rangle$, a relação inversa pode ser visualizada no diagrama a seguir:

$<: C \to C$ $\qquad$ $<^{-1} =>: C \to C$

4.9 Composição de Relações

Sejam *A*, *B* e *C* conjuntos, e *R: A* $\to$ *B* e *S: B* $\to$ *C* relações. A ***composição de R e S***, denotada por $R \circ S : A \to C$, é tal que

$$(\forall a \in A)(\forall b \in B)(\forall c \in C)(aRb \wedge bSc \to a(R \circ S)c)$$

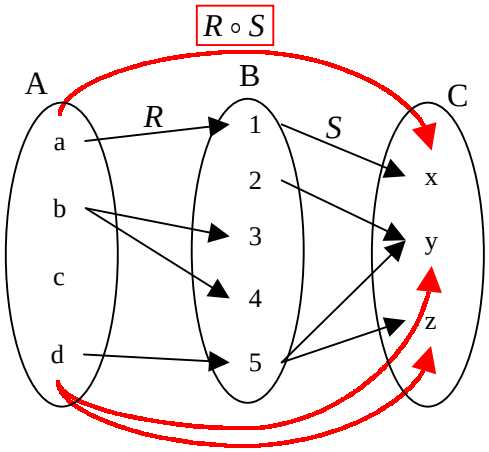
Ou seja,

$$R \circ S = \{\langle a,c\rangle \mid \exists b \in B \wedge \langle a,b\rangle \in R \wedge \langle b,c\rangle \in S\}$$

Exemplo: Dados os conjuntos A = {a, b, c, d}, B = {1, 2, 3, 4, 5} e C = {x, y, z} e as relações $R : A \to B = \{\langle a,1\rangle, \langle b,3\rangle, \langle b,4\rangle, \langle d,5\rangle\}$ e $S : B \to C = \{\langle 1,x\rangle, \langle 2,y\rangle, \langle 5,y\rangle, \langle 5,z\rangle\}$, temos que a composição de *R* e *S* é como segue

$$R \circ S = \{\langle a,x\rangle, \langle d,y\rangle, \langle d,z\rangle\}$$

e pode ser visualizada no diagrama a seguir:



A composição de relações é ***associativa***, ou seja:

Sejam as relações *R: A* $\to$ *B*, *S: B* $\to$ *C* e *T: C* $\to$ *D*. Então, temos que

$$(T \circ S) \circ R = T \circ (S \circ R) = T \circ S \circ R$$

4.9.1 Composição de Relações como Produto de Matrizes

A composição de relações pode ser vista como o produto de matrizes. Veja o exemplo a seguir.

Exemplo: Sejam R e S relações em X = {a, b, c} definidas por $R = \{\langle a,b\rangle, \langle a,c\rangle, \langle b,a\rangle\}$ e $S = \{\langle a,c\rangle, \langle b,a\rangle, \langle b,b\rangle, \langle c,a\rangle\}$. Determinaremos a composição de R e S através da multiplicação das correspondentes matrizes. Abaixo, temos as correspondentes matrizes que representam as relações R e S.

R	a	b	c
a	0	1	1
b	1	0	0
c	0	0	0

S	a	b	c
a	0	0	1
b	1	1	0
c	1	0	0

A multiplicação das matrizes R e S é dada como segue:

$$R \cdot S = \begin{pmatrix} 0+1+1 & 0+1+0 & 0+0+0 \\ 0+0+0 & 0+0+0 & 1+0+0 \\ 0+0+0 & 0+0+0 & 0+0+0 \end{pmatrix} = \begin{pmatrix} 2 & 1 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \end{pmatrix}$$

Assim, temos que a composição $R \circ S$ é dada pela matriz $R \cdot S$, ou seja, $R \circ S = \{\langle a,a\rangle, \langle a,b\rangle, \langle b,c\rangle\}$.

5 TIPOS DE RELAÇÕES

Vamos estudar agora os diferentes tipos de relações.

5.1 Relação Funcional

Uma relação binária $R: A \rightarrow B$ é uma ***relação funcional*** se, e somente se:

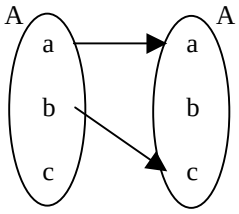
$$\boxed{(\forall a \in A)(\forall b_1 \in B)(\forall b_2 \in B)(aRb_1 \wedge aRb_2 \rightarrow b_1 = b_2)}$$

Em outras palavras, temos que para uma relação ser funcional, cada elemento do conjunto origem deve estar relacionado a, no máximo, um elemento do conjunto destino.

Exemplo: Dada a relação $X^2: Z \rightarrow Z$, tal que $X^2 = \{\langle x, y\rangle \in Z^2 \mid y = x^2\}$, temos que, para cada inteiro *x*, existe no máximo um inteiro *y* tal que $y = x^2$.

A matriz de uma relação funcional tem uma característica particular: cada linha da matriz pode conter no máximo um valor lógico verdadeiro (1).

Podemos também visualizar uma relação funcional no diagrama de Venn. Considerando a relação $R: A \rightarrow A$, tal que $R = \{\langle a, a\rangle, \langle b, c\rangle\}$ e A = {a, b, c}, temos que o correspondente diagrama é como segue:



Observe que, de fato, cada elemento do conjunto origem está relacionado a, no máximo, um elemento do conjunto destino (o que significa que podem haver elementos da origem não relacionados a algum elemento do destino).

5.2 Relação Injetora

Relação injetora é o conceito dual (inverso) de relação funcional.

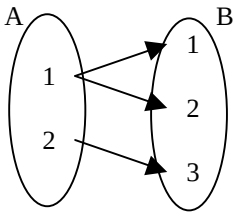
Uma relação binária $R: A \rightarrow B$ é uma ***relação injetora*** se, e somente se:

$$\boxed{(\forall b \in B)(\forall a_1 \in A)(\forall a_2 \in A)(a_1Rb \wedge a_2Rb \rightarrow a_1 = a_2)}$$

Em outra palavras, temos que, para um relação ser injetora, cada elemento do conjunto destino deve estar relacionado a, no máximo, um elemento do conjunto origem.

A matriz de uma relação injetora tem uma característica particular: existe no máximo um valor lógico verdadeiro (1) em cada coluna.

Exemplo: Dada a relação $R: A \rightarrow B$, tal que A = {1, 2}, B = {1, 2, 3} e $R = \{\langle 1,1\rangle, \langle 1,2\rangle, \langle 2,3\rangle\}$, temos que cada elemento de B está relacionado a, no máximo, um elemento de A. Veja a seguir o diagrama que representa a relação *R*.



5.3 Relação Total

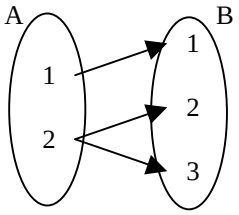
Uma relação binária $R: A \rightarrow B$ é uma ***relação total*** se, e somente se:

$$\boxed{(\forall a \in A)(\exists b \in B)(aRb)}$$

Em outras palavras, temos que para uma relação ser total, todos os elementos do conjunto origem devem estar relacionados a algum elemento do conjunto destino. O domínio de definição é o próprio conjunto A.

Na matriz de uma relação total, deve existir pelo menos um valor lógico verdadeiro em cada linha.

Exemplo: Dada a relação $R: A \rightarrow B$, tal que A = {1, 2}, B = {1, 2, 3} e $R = \{\langle 1,1\rangle, \langle 2,2\rangle, \langle 2,3\rangle\}$, temos que cada elemento de A está relacionado a algum elemento de B. Veja a seguir o diagrama que representa a relação R.



5.4 Relação Sobrejetora

Relação sobrejetora é o conceito dual (inverso) de relação total.

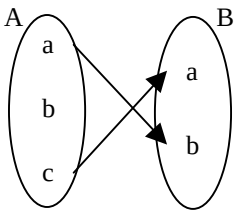
Uma relação binária $R: A \rightarrow B$ é uma ***relação sobrejetora*** se, e somente se:

$$\boxed{(\forall b \in B)(\exists a \in A)(aRb)}$$

Em outras palavras, temos que para uma relação ser sobrejetora, todos os elementos do conjunto destino devem estar relacionados a algum elemento do conjunto origem. O conjunto imagem é o próprio conjunto B.

Na matriz de uma relação sobrejetora, deve existir pelo menos um valor lógico verdadeiro em cada coluna.

Exemplo: Dada a relação $R: A \rightarrow B$, tal que A = {a, b, c}, B = {a, b} e $R = \{\langle a,b\rangle, \langle c,a\rangle\}$, temos que cada elemento de B está relacionado a algum elemento de A. Veja a seguir o diagrama que representa a relação R.



5.5 Monomorfismo

Uma relação $R: A \rightarrow B$ é um ***monomorfismo*** se, e somente se, for simultaneamente uma relação ***total*** e ***injetora***.

Dessa forma, o domínio de definição é o próprio conjunto A e cada elemento de B está relacionado com no máximo um elemento de A.

A matriz de um monomorfismo tem a seguinte característica: existe pelo menos um valor verdadeiro em cada linha da matriz (o que carateriza a relação total) e existe no máximo um valor lógico verdadeiro em cada coluna (o que carateriza a relação injetora).

Exemplo: A relação $=: A \rightarrow B$, onde A = {a} e B = {a, b}, é um monomorfismo.

5.6 Epimorfismo

Epimorfismo é o conceito dual (inverso) de monomorfismo.

Uma relação $R: A \rightarrow B$ é um ***epimorfismo*** se, e somente se, for simultaneamente uma relação ***funcional*** e ***sobrejetora***.

Dessa forma, o conjunto imagem é o próprio conjunto B e cada elemento de A está relacionado com no máximo um elemento de B.

A matriz de um epimorfismo tem a seguinte característica: existe pelo menos um valor verdadeiro em cada coluna da matriz (o que carateriza a relação sobrejetora) e existe no máximo um valor lógico verdadeiro em cada linha (o que carateriza a relação funcional).

Exemplo: São exemplos epimorfismo, sendo que onde A = {a}, B = {a, b} e C = {0, 1, 2}:

- $=: A \rightarrow A$
- $S: C \rightarrow B$, tal que $S = \{\langle 0, a\rangle, \langle 1, b\rangle\}$

5.7 Isomorfismo

Uma relação $R: A \rightarrow B$ é um ***isomorfismo*** se, e somente se, existe uma relação $S: B \rightarrow A$ tal que:

$$R \circ S = \mathrm{id}_A$$
$$S \circ R = \mathrm{id}_B$$

onde id_A é uma endorrelação de igualdade em A $\langle A, = \rangle$ e id_B é uma endorrelação de igualdade em B $\langle B, = \rangle$, chamadas de *relação identidade*.

Assim, se $R \circ S = \mathrm{id}_A$ e $S \circ R = \mathrm{id}_B$, podemos afirmar que a relação R *possui inversa*. Ainda, se existe um isomorfismo entre dois conjuntos, podemos chama-los de *conjuntos isomorfos*.

Exemplo: Dados os conjuntos $A = \{a, b, c\}$ e $B = \{e, f, g\}$ e a relação $R: A \to B$ tal que $R = \{\langle a, e\rangle, \langle b, f\rangle, \langle c, g\rangle\}$. R é um isomorfismo, pois considerando a relação inversa de R, $R^{-1} : B \to A = \{\langle e, a\rangle, \langle f, b\rangle, \langle g, c\rangle\}$, temos que

$$R \circ R^{-1} = \{\langle a, a\rangle, \langle b, b\rangle, \langle c, c\rangle\} = \mathrm{id}_A$$
$$R^{-1} \circ R = \{\langle e, e\rangle, \langle f, f\rangle, \langle g, g\rangle\} = \mathrm{id}_B$$

Logo, a relação R possui inversa e os conjuntos A e B são conjuntos isomorfos.

Teorema: Seja $R: A \to B$ uma relação. Então R é um isomorfismo se, e somente se, R for simultaneamente um monomorfismo e um epimorfismo.

Dessa forma, uma relação é um ***isomorfismo*** se, e somente se, for simultaneamente uma relação ***total***, ***injetora***, ***funcional*** e ***sobrejetora***.

Podemos observar que para uma relação ser um isomorfismo, os conjuntos origem e destino devem possuir o mesmo número de elementos.

6 FUNÇÕES PARCIAIS E TOTAIS

Uma função parcial nada mais é do que um relação que é funcional. Se a relação funcional for também total, então a denominamos de função total. Portanto, podemos dizer que toda função total é uma função parcial e que toda função parcial é uma relação. Entretanto, nem toda relação é uma função parcial, assim como nem toda função parcial é uma função total.

6.1 Função Parcial

Uma ***função parcial*** é uma relação funcional, ou seja, cada elemento do domínio está relacionado a no máximo um elemento do contra-domínio.

Um elemento pertencente à função parcial $\langle a,b\rangle \in f$ pode ser representado por $f(a)=b$.

Exemplo: Dados os conjuntos *A = {a}* e *B = {x, y}* temos que as seguintes relações são funções parcias:

- $R : B \to A = \{\langle x,a\rangle, \langle y,a\rangle\}$
- $=: B \to B$

Vale observar que a relação inversa de uma função parcial não necessariamente é uma função parcial. Se considerarmos o conjunto *A = {0, 1, 2}* e a função parcial *f: A* $\to$ *A* tal que $f = \{\langle 0,1\rangle, \langle 2,1\rangle\}$, temos que a relação inversa de *f*, $f^{-1} = \{\langle 1,0\rangle, \langle 1,2\rangle\}$ não é uma relação funcional e, consequentemente, não é uma função parcial.

Para que a relação inversa de uma relação funcional seja uma função parcial, ela deve ser também injetora (que é o dual de funcional).

6.2 Função Total

Uma ***função total*** é uma função parcial que é total. Em outras palavras, é uma função parcial definida para todos os elementos do domínio.

Se uma função é total, dizemos apenas que é uma função, ou seja, sempre que mencionarmos apenas função, estamos nos referindo a funções totais. Assim, podemos verificar as seguintes propriedades:

- Função Injetora = monomorfismo
- Função Sobrejetora = epimorfismo
- Função Bijetora = isomorfismo

Ou seja, uma função bijetora é uma função injetora e sobrejetora.

Da mesma forma que para funções parciais, a relação inversa de uma função não necessariamente é uma função. Considerando os conjuntos *A = {0, 1}* e *B = {0, 1, 2}* e a função $f : B \to A = \{\langle 0,0\rangle, \langle 1,1\rangle, \langle 2,0\rangle\}$, temos que a relação inversa de *f*, $f^{-1} = \{\langle 0,0\rangle, \langle 1,1\rangle, \langle 0,2\rangle\}$ não é uma relação funcional e, portanto, não é uma função.

Podemos considerar também a função *g: A* $\to$ *B*, tal que $g = \{\langle 0,0\rangle, \langle 1,1\rangle\}$. A inversa de *g*, $g^{-1} = \{\langle 0,0\rangle, \langle 1,1\rangle\}$ não é uma relação total e, portanto, não é uma função.

Para que a relação inversa de uma função *f* seja uma função, *f* deve ser uma função bijetora.

7 CARDINALIDADE DE CONJUNTOS

A cardinalidade de um conjunto nada mais é do que a medida de seu tamanho. Dois conjuntos A e B possuem o mesmo número de elementos ou a mesma cardinalidade, ou ainda são ditos equipotentes, denotado por

$$\boxed{\#A = \#B}$$

se existe uma correspondência um-para-um $f : A \to B$.

O conceito de cardinalidade permite definir conjuntos finitos e infinitos.

7.1 Cardinalidade Finita e Infinita

A ***cardinalidade*** de um conjunto A, representada por **#A** é:

- ***Finita***: se existe uma bijeção entre A e o conjunto {1, 2, 3, ..., *n*}, para algum $n \in \mathrm{N}$. Neste caso, **#A = *n***.
- ***Infinita***: se existe uma bijeção entre A e um subconjunto próprio de A, ou seja, se conseguimos "tirar" alguns elementos de A e ainda assim podemos estabelecer uma bijeção com A.

Exemplo: Mostre que o conjunto dos números inteiros Z é um conjunto infinito.

Para mostrar que Z é um conjunto infinito, precisamos mostrar que existe uma bijeção entre ele e um subconjunto próprio dele, como por exemplo, o conjunto dos números naturais N. Portanto, precisamos encontrar uma função bijetora $f : \mathrm{Z} \to \mathrm{N}$. Suponha $f : \mathrm{Z} \to \mathrm{N}$, tal que:

- se $a \geq 0$, então $f(a) = 2a$
- se $a < 0$, então $f(a) = |2a| - 1$

A tabela abaixo mostra os valores de *f*(*a*) e sugere o relacionamento um-para-um entre Z e N.

a	***f*(*a*)**
-4	7
-3	5
-2	3
-1	1
0	0
1	2
2	4
3	6
4	8
...	...

Temos que *f* é uma função bijetora e sabemos que N é um subconjunto próprio de Z. Portanto, Z é um conjunto infinito, como queríamos mostrar.

Vale ressaltar que nem todos os conjuntos infinitos possuem a mesma cardinalidade. Podemos dizer que um ***conjunto infinito A*** é dito:

- ***Contável***: se existe um bijeção entre A e um subconjunto infinito de N.

- ***Não-Contável***: caso contrário.

A bijeção que define o conjunto A como conjunto contável é dita enumeração de A.

Exemplo: Os conjuntos Z (inteiros) e Q (racionais) são conjuntos contáveis e os conjuntos I (irracionais) e R (reais) são conjuntos não-contáveis.

7.2 Cardinalidade dos Conjuntos Não-Contáveis

Todos os conjuntos contáveis possuem mesma cardinalidade. Entretanto, nem todos os conjuntos não-contáveis possuem a mesma cardinalidade.

Dizemos que um conjunto A tem tantos elementos quanto um conjunto B, ou seja:

$$\boxed{\#A \leq \#B}$$

quando existe uma função injetora $f : A \to B$.

Teorema Schröder-Bernstein: sejam A e B dois conjuntos tais que existem duas funções injetoras: $f_1 : A \to B$ e $f_2 : B \to A$. Então, existe uma função bijetora $g : A \leftrightarrow B$.

Conjuntos Equipotentes: Dois conjuntos A e B são ditos equipotentes quando existe uma bijeção entre eles. Logo, podemos dizer que os conjuntos A e B possuem a mesma cardinalidade.

Pela definição de conjuntos equipotentes, podemos afirmar que todos os conjuntos contáveis são equipotentes.

7.3 Cardinal

A relação estabelecida entre conjuntos equipotentes é uma relação de equivalência. Assim, podemos considerar o cardinal como uma classe de equivalência dos conjuntos equipotentes.

O cardinal do conjunto dos números naturais é representado por $\aleph_0$ (*aleph-zero*). Como qualquer conjunto infinito contável possui mesma cardinalidade que o conjunto dos números naturais, então $\aleph_0$ representa o cardinal de qualquer conjunto infinito contável e é o menor cardinal dos conjuntos infinitos.

Teorema de Cantor: o conjunto das partes de um conjunto tem sempre cardinalidade maior que este. Seja A conjunto e 2^A o conjunto das partes de A, então #A < #2^A.

Prova:

Parte 1: Vamos mostrar que #A ≤ #2^A, apresentando uma função injetora $f : A \to 2^A$. Seja $f : A \to 2^A$ uma função tal que, para todo $a \in$ A, tem-se que:

$$f(a) = \{a\}$$

f é injetora e, portanto, #A ≤ #2^A.

Parte 2: Vamos mostrar que #A ≠ #2^A, ou seja, que #A < #2^A, mostrando, por absurdo, que não existe uma função bijetora entre A e 2^A. Suponha que existe uma função bijetora $g : A \to 2^A$. Seja o seguinte subconjunto B de A:

$$B = \{a \in A \mid a \notin g(a)\}$$

Como A é um conjunto, ele pode ser um conjunto de conjuntos. Suponha $b \in$ A, tal que $g(b) = B$. Neste caso:

- se $b \in$ B, então, pela definição de B, tem-se que $b \notin g$(b) = B.
- se $b \notin g$(B), então, pela definição de B, tem-se que $b \in g$(b) = B.

O que é uma contradição! Logo, não existe uma função bijetora entre A e 2^A.

O conjunto das partes de N é equipotente ao conjunto dos números reais R. Considerando que 2^k denota o cardinal do conjunto das partes com cardinalidade k, tem-se que $2^{\aleph_0}$ é a cardinalidade do conjunto dos números reais, ou seja, é a cardinalidade do *continuum*.

Teorema: O conjunto I = [0, 1] de todos os números reais entre 0 e 1 é não-contável.

Prova (por absurdo):
Suponha I contável. Então, existe uma função bijetora $f : \mathrm{N} \to \mathrm{I}$. Seja $f(1) = a_1$, $f(2) = a_2$, $f(3) = a_3$,..., isto é, $I = \{a_1, a_2, a_3, ...\}$. Vamos listar seus elementos em uma coluna com sua expansão decimal:

$a_1 = 0, x_{11}x_{12}x_{13}x_{14}...$
$a_2 = 0, x_{21}x_{22}x_{23}x_{24}...$
$a_3 = 0, x_{31}x_{32}x_{33}x_{34}...$
$a_4 = 0, x_{41}x_{42}x_{43}x_{44}...$
...

onde $x_{ij} \in \{0,1,2,...,9\}$.

Seja $b = 0, y_1y_2y_3y_4...$ um número real obtido da seguinte forma:

$$y_i = \begin{cases} 1 & \text{se } x_{ii} \neq 1 \\ 2 & \text{se } x_{ii} = 1 \end{cases}$$

Portanto, $b \in \mathrm{I}$. Mas

$b \neq a_1$, pois $y_1 \neq x_{11}$
$b \neq a_2$, pois $y_2 \neq x_{22}$
$b \neq a_3$, pois $y_3 \neq x_{33}$
...

Portanto, $b \notin \mathrm{I} = \{a_1, a_2, a_3, ...\}$, o que é uma contradição, já que $b \in \mathrm{I}$! Logo, a suposição de que I é contável é falsa e, portanto, I é não-contável, como queríamos provar.

8 INDUÇÃO MATEMÁTICA

Para entender intuitivamente o que é a *Indução Matemática*, vamos ilustrar a técnica:

- Você está subindo uma escada infinitamente alta. Como saber se será capaz de chegar a um degrau arbitrariamente alto?

- Suponha as seguintes hipóteses:

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

- Pela hipótese 1, você é capaz de chegar ao primeiro degrau; pela hipótese 2, você consegue chegar ao segundo; novamente pela hipótese 2, chega ao terceiro degrau; e assim sucessivamente.

Essa mesma propriedade é utilizada para provar propriedades dos números inteiros positivos! Considere que $P(n)$ denota que o número inteiro positivo n possui a propriedade P.

1. Assumimos que o número 1 tem a propriedade P: $\boldsymbol{P(1)}$
2. Supomos que a propriedade P é válida para qualquer inteiro positivo k: $\boldsymbol{P(k)}$
3. Provamos que, se a propriedade P é válida para qualquer número inteiro k, então é válida para o próximo inteiro positivo k+1: $\boldsymbol{P(k) \rightarrow P(k+1)}$

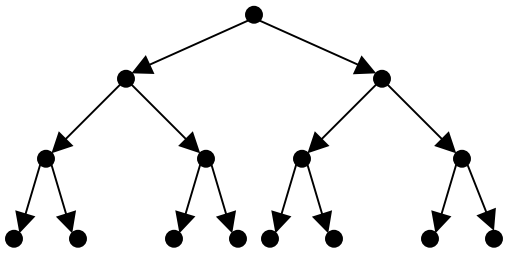
8.1 Primeiro Princípio de Indução Matemática

O *Primeiro Princípio de Indução Matemática* é formulado da seguinte forma:

1. $P(1)$ é verdade
2. $(\forall k)(P(k)$ é verdade $\rightarrow P(k+1)$ é verdade)

E com isto, provamos que a propriedade é verdadeira para todo inteiro positivo n, ou seja, que $P(n)$ é verdade.

Exemplo: Suponha que um ancestral casou-se e teve dois filhos. Vamos chamar esses dois filhos de geração 1. Suponha agora que cada um desses filhos teve dois filhos. Então a geração 2 contém quatro descendentes. Imagine que esse processo continua de geração em geração. A figura abaixo ilustra esse processo:



Geração	Descendentes
1	$2 = 2^1$
2	$4 = 2^2$
3	$8 = 2^3$
...	...

Então, podemos deduzir que:

- A geração 1 possui 2 descendentes
- A geração 2 possui 4 descendentes
- A geração 3 possui 8 descendentes
- E assim sucessivamente...

Então, podemos fazer a seguinte conjectura: *a geração n possui* 2^n *descendentes*. Ou seja, podemos escrever que:

$$P(n) = 2^n$$

Agora, vamos *provar* que nossa conjectura está correta, através do primeiro princípio de indução matemática:

Base de Indução (estabelecemos a veracidade da propriedade para n = 1):

$$P(1) = 2^1 = 2$$

Hipótese de Indução (supomos que a propriedade é válida para algum inteiro *k*, $k \geq 1$):

$$P(k) = 2^k$$

Passo de Indução (provamos que a propriedade é válida para o inteiro seguinte *k*+1, ou seja, que $P(k) \rightarrow P(k+1)$):

$$P(k+1) = 2^{k+1}$$

$P(k+1) = 2 \cdot P(k) \overset{HI}{=} 2 \cdot 2^k = 2^{k+1}$ (o número de descendentes dobra de uma geração para outra)

A tabela abaixo, resume os três passos necessários para uma demonstração que usa o primeiro princípio de indução.

Demonstração por Indução	
Passo 1	Prove a base de indução
Passo 2	Suponha $P(k)$
Passo 3	Prove $P(k+1)$

Vejamos mais alguns exemplos:

Exemplo: Prove que a equação a seguir é verdadeira para qualquer inteiro positivo *n*.

$$1 + 3 + 5 + ... + (2n-1) = n^2$$

Base de Indução - *P*(1)
Verificamos que a propriedade é válida para *n* = 1.
$P(1): 1 = 1^2$

Hipótese de Indução - *P*(*k*)
Supomos que a propriedade é válida para *n* = *k*.
$P(k): 1 + 3 + 5 + ... + (2k-1) = k^2$

Passo de Indução - *P*(*k* + 1)
Tentamos provar que a propriedade é válida para *n* = *k* + *1*, ou seja, que:
$P(k+1): 1 + 3 + 5 + ... + [2(k+1)-1] \overset{?}{=} (k+1)^2$

Para fazermos uma demonstração por indução, vamos reescrever o lado esquerdo da equação de $P(k+1)$ incluindo a penúltima parcela e usaremos a hipótese de indução para provarmos o que queremos.

$$P(k+1): 1+3+5+...+[2(k+1)-1] =$$
$$1+3+5+...+(2k-1)+[2(k+1)-1] \overset{HI}{=}$$
$$k^2+[2(k+1)-1] =$$
$$k^2+(2k+2-1) =$$
$$k^2+2k+1 =$$
$$(k+1)^2$$

Portanto, $1+3+5+...+[2(k+1)-1] = (k+1)^2$, o que mostra a validade de $P(k+1)$.

Exemplo: Prove que a equação a seguir é verdadeira para todo $n \geq 1$.

$$1+2+2^2+...+2^n = 2^{n+1}-1$$

Novamente, vamos utilizar a indução para provar a validade da propriedade.

Base de Indução - *P*(1)
Verificamos que a propriedade é válida para $n = 1$.
$P(1): 1+2 = 2^{1+1}-1$ ou $3 = 2^2-1$

Hipótese de Indução - *P*(*k*)
Supomos que a propriedade é válida para $n = k$.
$P(k): 1+2+2^2+...+2^k = 2^{k+1}-1$

Passo de Indução - *P*(*k* + 1)
Provamos que a propriedade é válida para $n = k + 1$, ou seja, que:
$$P(k+1): 1+2+2^2+...+2^{k+1} \overset{?}{=} 2^{(k+1)+1}-1$$

$$P(k+1) = 1+2+2^2+...+2^{k+1} =$$
$$1+2+2^2+...+2^k+2^{k+1} \overset{HI}{=}$$
$$2^{k+1}-1+2^{k+1} =$$
$$2\cdot(2^{k+1})-1 =$$
$$2^{k+1+1}-1$$

Portanto, $1+2+2^2+...+2^{k+1} = 2^{(k+1)+1}-1$, o que mostra que $P(k+1)$ é válida, concluindo a demonstração.

Exemplo: Prove que, para qualquer inteiro positivo *n*, $1+2+3+...+n = \frac{n\cdot(n+1)}{2}$.

Base de Indução - *P*(1)
Verificamos que a propriedade é válida para $n = 1$.

$$P(1): 1 = \frac{1 \cdot (1+1)}{2}$$

Hipótese de Indução - *P*(k)
Supomos que a propriedade é válida para $n = k$.

$$P(k): 1 + 2 + 3 + ... + k = \frac{k \cdot (k+1)}{2}$$

Passo de Indução - *P*(*k* + 1)
Provamos que a propriedade é válida para $n = k + 1$.

$$P(k+1): 1 + 2 + 3 + ... + (k+1) \stackrel{?}{=} \frac{(k+1) \cdot [(k+1)+1]}{2}$$

$$P(k+1) = 1 + 2 + 3 + ... + (k+1) =$$

$$1 + 2 + 3 + ... + k + (k+1) \stackrel{HI}{=}$$

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

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

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

$$\frac{(k+1) \cdot [(k+1)+1]}{2}$$

Nem todas as demonstrações por indução envolvem somas. Veja os exemplos a seguir.

Exemplo: Prove que, para qualquer inteiro positivo *n*, $2^n > n$.

Base de Indução - *P*(1)
Verificamos que a propriedade é válida para $n = 1$.

$$P(1): 2^1 > 1$$

Hipótese de Indução - *P*(k)
Supomos que a propriedade é válida para $n = k$.

$$P(k): 2^k > k$$

Passo de Indução - *P*(*k* + 1)
Provamos que a propriedade é válida para $n = k + 1$.

$$P(k+1): 2^{k+1} \stackrel{?}{>} k+1$$

$$2^{k+1} = 2 \cdot \underbrace{2^k > k}_{HI} \cdot 2 = k + k \geq k + 1$$

Portanto, $2^{k+1} > k+1$.

Exemplo: Prove que, para qualquer inteiro positivo *n*, $2^{2n} - 1$ é divisível por 3.

Base de Indução - *P*(1)
Verificamos que a propriedade é válida para $n = 1$.
$P(1): 2^{2\cdot 1} - 1 = 4 - 1 = 3$ é divisível por 3

Hipótese de Indução - *P*(k)
Supomos que a propriedade é válida para $n = k$.
$P(k): 2^{2k} - 1$ é divisível por 3, ou seja, que $2^{2k} - 1 = 3m$ e que, portanto, $2^{2k} = 3m + 1$

Passo de Indução - *P*(*k* + 1)
Provamos que a propriedade é válida para $n = k + 1$.
$P(k+1): 2^{2(k+1)} - 1$ é divisível por 3?

$2^{2\cdot(k+1)} - 1 =$
$2^{2k+2} - 1 =$
$(2^2 \cdot 2^{2k}) - 1 =$
$2^2 \cdot (3m+1) - 1 \overset{HI}{=}$
$12m + 4 - 1 =$
$12m + 3 =$
$3 \cdot (4m+1)$

Exemplo: Prove que $n^2 > 3n$ para $n \geq 4$.

Base de Indução - *P*(4)
Verificamos que a propriedade é válida para $n = 4$.
$P(4): 4^2 = 16 > 12 = 3 \cdot 4$

Hipótese de Indução - *P*(k)
Supomos que a propriedade é válida para $n = k$.
$P(k): k^2 > 3k, k \geq 4$

Passo de Indução - *P*(*k* + 1)
Provamos que a propriedade é válida para $n = k + 1$.
$P(k+1): (k+1)^2 \overset{?}{>} 3 \cdot (k+1)$

$(k+1)^2 =$
$k^2 + 2k + 1 \overset{HI}{>}$
$3k + 2k + 1 \geq$
$3k + 8 + 1 >$ (pois $k \geq 4$)
$3k + 3 =$
$3 \cdot (k+1)$

Exemplo: Prove que $2^{n+1} < 3^n$ para todo $n > 1$.

Base de Indução - *P*(2)
Verificamos que a propriedade é válida para $n = 2$.

$P(2): 2^{2+1} = 8 < 9 = 3^2$

Hipótese de Indução - *P*(k)
Supomos que a propriedade é válida para $n = k$.
$P(k): 2^{k+1} < 3^k, k > 1$

Passo de Indução - *P*(*k* + 1)
Provamos que a propriedade é válida para $n = k + 1$.
$P(k+1): 2^{(k+1)+1} \stackrel{?}{<} 3^{(k+1)}$

$$2^{(k+1)+1} = 2 \cdot \underbrace{2^{k+1} < 3^k}_{HI} \cdot 2 < 3^k \cdot 3 = 3^{k+1}$$

9 RECURSÃO E RELAÇÕES DE RECORRÊNCIA

9.1 Definições Recorrentes

Uma definição onde o item definido aparece como parte da definição é chamada de ***definição por recorrência***, ou ***definição recorrente***, ou ainda ***definição por indução***.

Uma definição recorrente é formada por duas partes:

1. Base ou condição básica, onde algum(s) caso(s) simples do item que está sendo definido é dado explicitamente.
2. Um passo de indução ou recorrência, onde novos casos do item que está sendo definido são dados em função de casos anteriores.

A parte 1 da definição nos permite começar, fornecendo alguns casos simples e concretos. A parte 2 nos permite construir novos casos, a partir destes mais simples e assim por diante. Daí o nome definição por indução, devido à analogia com as demonstrações por indução.

9.2 Seqüências Definidas por Recorrência

Uma seqüência S é uma lista de objetos numerados em determinada ordem. Existe um primeiro objeto, um segundo objetos, e assim por diante. S(k) denota o k-ésimo objeto da seqüência. Uma seqüência é definida por recorrência nomeando-se o primeiro valor da seqüência e depois definindo os valores subseqüentes na seqüência em termos de valore anteriores.

Exemplo: A seqüência S é definida por recorrência por

1. S(1) = 2
2. S(n) = 2S(n - 1) para $n \geq 2$

Assim, o primeiro valor da seqüência é 2; o segundo valor da seqüência é S(2) = 2S(2-1) = 2S(1) = $2 \cdot 2 = 4$; o terceiro valor da seqüência é S(3) = 2S(2) = $2 \cdot 4 = 8$; e assim por diante. Continuando a seqüência, temos

2, 4, 8, 16, 32, ...

Exemplo: Escreva os cinco primeiro valores da seqüência T, tal que:

1. T(1) = 1
2. T(n) = T(n - 1) + 3, para $n \geq 2$

1, 4, 7, 10, 13

Seqüência de Fibonacci: é uma seqüência introduzida pelo matemático italiano Fibonacci e é definida por recorrência da seguinte forma:

$F(1) = 1$
$F(2) = 1$
$F(n) = F(n-2) + F(n-1)$, para $n \geq 2$

Traduzindo, *qualquer valor da seqüência de Fibonacci, exceto os dois primeiros, é dado pela soma de seus dois valores anteriores*.

Por exemplo, podemos escrever os dez primeiros números da seqüência de Fibonacci, utilizando a sua definição por recorrência:

1, 1, 2, ,3 ,5, 8, 13, 21, 34, 55

Exemplo: Prove que, na seqüência de Fibonacci, $F(n + 4) = 3F(n +2) – F(n)$, para todo $n \geq 1$.

Podemos provar essa fórmula diretamente, sem utilizar indução matemática, usando apenas a relação de recorrência na definição dos números de Fibonacci.

A relação de recorrência

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

pode ser reescrita na forma

$$F(n + 1) = F(n + 2) - F(n).$$

Logo, podemos utilizá-la para provar a fórmula:

$$F(n+4) = F(n+3) + F(n+2) =$$

$$\underbrace{F(n+2) + F(n+1)}_{F(n+3)} + F(n+2) =$$

$$F(n+2) + \left[\underbrace{F(n+2) - F(n)}_{F(n+1)} \right] + F(n+2) =$$

$$3F(n+2) - F(n)$$

10 ESTRUTURAS ALGÉBRICAS

O estudo de álgebra está diretamente relacionado ao estudo de operações. Portanto, iniciaremos este capítulo estudando operações e suas propriedades.

10.1 Operações

Operações Binárias: são operações cujo domínio é um conjunto resultante de um produto cartesiano. Podemos defini-la como uma função parcial do tipo:

$$\oplus : A \times B \to C$$

Operações Internas: operações internas a um conjunto A são operações cujo domínio e contra-domínio são definidos sobre um mesmo conjunto A. Uma operação binária interna ao conjunto A é uma operação do tipo:

$$\oplus : A \times A \to A$$

Operações Fechadas: uma operação fechada é uma operação total, ou seja, é uma função. Em outras palavras, é uma operação definida para todo $x \in A \times A$ e cujo resultado pertence a *A*.

Exemplos:

a) A operação de divisão nos números reais $divisão : R \times R \to R$ é uma ***operação binária interna*** a *R*, definida como segue:

$$divisão(\langle x, y \rangle) : \frac{x}{y}$$

b) A operação quadrado nos números naturais $quadrado : \mathrm{N} \to \mathrm{N}$, definida como segue, é uma ***operação interna e fechada***:

$$quadrado(n) : n^2$$

c) A operação união $\cup : P(A) \times P(A) \to P(A)$, para um dado conjunto *A*, é uma ***operação binária interna e fechada***.

10.2 Propriedade das Operações Binárias

As principais propriedades das operações binárias internas e fechadas são: *comutativa*, *associativa*, *elemento neutro* e *elemento inverso*, que serão detalhadas a seguir.

Propriedade Associativa: Seja $\oplus : A \times A \to A$ uma operação binária interna e fechada e *x*, *y*, *z* elementos quaisquer de *A*. Então, a operação $\oplus$ é ***associativa*** se:

$$(\forall x)(\forall y)(\forall z)[x \oplus (y \oplus z) = (x \oplus y) \oplus z]$$

Propriedade Comutativa: Seja $\oplus : A \times A \to A$ uma operação binária interna e fechada e *x*, *y* elementos quaisquer de *A*. Então, a operação $\oplus$ é ***comutativa*** se:

$$(\forall x)(\forall y)(x \oplus y = y \oplus x)$$

Elemento Neutro: Seja $\oplus : A \times A \to A$ uma operação binária interna e fechada e *x* elemento qualquer de *A*. Então, a operação $\oplus$ tem ***elemento neutro*** se:

$$(\exists e)(\forall x)(x \oplus e = e \oplus x = x)$$

Elemento Inverso: Seja $\oplus : A \times A \to A$ uma operação binária interna e fechada e *x* elemento qualquer de *A*. Então, a operação $\oplus$ tem ***elemento inverso*** se:

$$(\forall x)(\exists x^{-1})(x \oplus x^{-1} = x^{-1} \oplus x = e)$$

Exemplos:

a) A operação de união $\cup : P(A) \times P(A) \to P(A)$ satisfaz as propriedades ***comutativa***, ***associativa*** e ***elemento neutro*** (conjunto vazio).

b) A operação de adição nos números naturais $+ : \mathrm{N} \times \mathrm{N} \to \mathrm{N}$ satisfaz as propriedades ***comutativa***, ***associativa*** e ***elemento neutro*** (zero).

c) A operação de adição nos números inteiros $+ : \mathrm{Z} \times \mathrm{Z} \to \mathrm{Z}$, além de satisfazer as propriedades ***comutativa***, ***associativa*** e ***elemento neutro*** (zero) satisfaz também a propriedade elemento inverso, já que, para qualquer inteiro *n*, basta tomar *–n* como elemento inverso, ou seja:

$$n + (-n) = -n + n = 0$$

10.3 Grupóides

Um ***grupóide*** é uma álgebra interna (operação binária interna) cuja operação interna é ***fechada***.

Seja $\oplus : A \times A \to A$ uma operação binária e interna. Se a operação for fechada, então $\langle A, \oplus \rangle$ é um grupóide. Se, adicionalmente, a operação for ***comutativa***, então $\langle A, \oplus \rangle$ é um ***Grupóide Abeliano***.

Exemplos:

a) Seja Σ um alfabeto não-vazio. A operação de concatenação $\bullet : \Sigma^* \times \Sigma^* \to \Sigma^*$ é fechada, mas não é comutativa. Portanto, $\langle \Sigma^*, \bullet \rangle$ é um grupóide.

b) Seja *A* um conjunto. As operações de união e interseção, $\cup : P(A) \times P(A) \to P(A)$ e $\cap : P(A) \times P(A) \to P(A)$ respectivamente, são fechadas e comutativas. Portanto, $\langle P(A), \cup \rangle$ e $\langle P(A), \cap \rangle$ são grupóides abelianos.

c) As seguintes operações são grupóides abelianos:

- $\langle \mathrm{N}, + \rangle$ e $\langle \mathrm{N}, \times \rangle$
- $\langle \mathrm{Z}, + \rangle$ e $\langle \mathrm{Z}, \times \rangle$
- $\langle R, + \rangle$ e $\langle R, \times \rangle$

d) As seguintes operações não são grupóides:

- $\langle \mathrm{N}, - \rangle$
- $\langle R, \div \rangle$

10.4 Semigrupos

Um ***semigrupo*** é um grupóide cuja operação interna é associativa. Portanto, é uma álgebra cuja operação é ***fechada*** e ***associativa***.

Seja $\oplus : A \times A \to A$ um grupóide. Se $\langle A, \oplus \rangle$ for associativa, então $\langle A, \oplus \rangle$ é um semigrupo. Se, adicionalmente, a operação for ***comutativa***, então $\langle A, \oplus \rangle$ é um ***Semigrupo Abeliano***.

Exemplos:

a) A operação de concatenação $\bullet : \Sigma^* \times \Sigma^* \to \Sigma^*$ é fechada e associativa. Portanto, $\langle \Sigma^*, \bullet \rangle$ é um semigrupo.

b) As operações de união e interseção, $\cup : P(A) \times P(A) \to P(A)$ e $\cap : P(A) \times P(A) \to P(A)$ respectivamente, são fechadas, associativas e comutativas. Portanto, $\langle P(A), \cup \rangle$ e $\langle P(A), \cap \rangle$ são semigrupos abelianos.

c) As seguintes operações são semigrupos abelianos:

- $\langle \mathrm{N}, + \rangle$ e $\langle \mathrm{N}, \times \rangle$
- $\langle \mathrm{Z}, + \rangle$ e $\langle \mathrm{Z}, \times \rangle$
- $\langle R, + \rangle$ e $\langle R, \times \rangle$

d) As seguintes operações não são semigrupos:

- $\langle \mathrm{Z}, - \rangle$
- $\langle R - \{0\}, \div \rangle$

10.5 Monóides

Um monóide é um ***semigrupo*** cuja operação possui elemento neutro. Portanto, um semigrupo é, simultaneamente, ***fechado***, ***associativo*** e possui ***elemento neutro***.

Seja $\langle A, \oplus \rangle$ um semigrupo. Se $\oplus : A \times A \to A$ possui elemento neutro, então $\langle A, \oplus, e \rangle$ é um monóide. Se, adicionalmente, a operação for ***comutativa***, então $\langle A, \oplus, e \rangle$ é um ***Monóide Abeliano***.

Exemplos:

a) As operações de união e interseção, $\cup : P(A) \times P(A) \to P(A)$ e $\cap : P(A) \times P(A) \to P(A)$ respectivamente, são fechadas, associativas, comutativas e possuem elemento neutro. Portanto, $\langle P(A), \cup, \varnothing \rangle$ e $\langle P(A), \cap, A \rangle$ são monóides abelianos.

b) As seguintes operações são monóides abelianos:

- $\langle \mathrm{N}, +, 0 \rangle$ e $\langle \mathrm{N}, \times, 1 \rangle$
- $\langle \mathrm{Z}, +, 0 \rangle$ e $\langle \mathrm{Z}, \times, 1 \rangle$
- $\langle R, +, 0 \rangle$ e $\langle R, \times, 1 \rangle$

c) A operação de concatenação $\langle \Sigma^*, \bullet \rangle$ e um semigrupo e possui elemento neutro (a palavra vazia ε). Portanto, $\langle \Sigma^*, \bullet, \varepsilon \rangle$ é um monóide.

10.6 Grupos

Um ***grupo*** é um monóide cuja operação é possui elemento inverso. Portanto, um grupo é uma operação que é, simultaneamente, ***fechada***, ***associativa***, possui ***elemento neutro*** e ***elemento inverso***.

Seja $\langle A,\oplus\rangle$ um monóide. Se $\oplus : A\times A\to A$ possui elemento inverso, então $\langle A,\oplus,e\rangle$ é um grupo. Se, adicionalmente, a operação for ***comutativa***, então $\langle A,\oplus,e\rangle$ é um ***Grupo Abeliano***.

Exemplos:

a) A operação $\langle R_+^*,\times\rangle$ é um grupo abeliano, pois é uma operação fechada, associativa, comutativa, possui elemento neutro 1 e elemento inverso.

b) A operação $\langle R,\times\rangle$ não é um grupo, pois não há número real *x* tal que:

$$0\cdot x = x\cdot 0 = 1$$

Ou seja, o número 0 não possui elemento inverso!

A tabela abaixo apresenta um resumo das estruturas algébricas estudadas e suas respectivas propriedades.

	Propriedades			
Tipo de Álgebra	*Fechada*	*Associativa*	*Elemento Neutro*	*Elemento Inverso*
Grupóide				
Semigrupo				
Monóide				
Grupo				

Exemplo: Seja $\mathrm{M}_2(\mathrm{Z})$ o conjunto de todas as matrizes 2×2 com elementos inteiros. $\langle \mathrm{M}_2(\mathrm{Z}),+\rangle$ é um grupo abeliano?

Para verificarmos se a operação $\langle \mathrm{M}_2(\mathrm{Z}),+\rangle$ é um grupo abeliano, precisamos verificar quais propriedades ela satisfaz:

- $\langle \mathrm{M}_2(\mathrm{Z}),+\rangle$ é ***fechada***, pois a adição de duas matrizes 2×2 é uma matriz 2×2.

- $\langle \mathrm{M}_2(\mathrm{Z}),+\rangle$ é ***associativa***, pois

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} + \left(\begin{bmatrix} e & f \\ g & h \end{bmatrix} + \begin{bmatrix} i & j \\ k & m \end{bmatrix} \right) = \begin{bmatrix} a & b \\ c & d \end{bmatrix} + \left(\begin{bmatrix} e+i & f+j \\ g+k & h+m \end{bmatrix} \right) =$$

$$\begin{bmatrix} a+(e+i) & b+(f+j) \\ c+(g+k) & d+(h+m) \end{bmatrix} = \begin{bmatrix} (a+e)+i & (b+f)+j \\ (c+g)+k & (d+h)+m \end{bmatrix} =$$

$$\left(\begin{bmatrix} a & b \\ c & d \end{bmatrix} + \begin{bmatrix} e & f \\ g & h \end{bmatrix} \right) + \begin{bmatrix} i & j \\ k & m \end{bmatrix}$$

- $\langle M_2(Z), + \rangle$ é ***comutativa***, pois

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} + \begin{bmatrix} e & f \\ g & h \end{bmatrix} = \begin{bmatrix} a+e & b+f \\ c+g & d+h \end{bmatrix} = \begin{bmatrix} e+a & f+b \\ g+c & h+d \end{bmatrix} = \begin{bmatrix} e & f \\ g & h \end{bmatrix} + \begin{bmatrix} a & b \\ c & d \end{bmatrix}$$

- $\langle M_2(Z), + \rangle$ possui ***elemento neutro***: $\begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$

- $\langle M_2(Z), + \rangle$ possui ***elemento inverso***. Por exemplo, a inversa da matriz $\begin{bmatrix} 4 & 3 \\ 2 & 1 \end{bmatrix}$ é a matriz $\begin{bmatrix} -4 & -3 \\ -2 & -1 \end{bmatrix}$.

Portanto, $\langle M_2(Z), + \rangle$ é um grupo abeliano!

Exemplo: Seja $Z_5 = \{0,1,2,3,4\}$. Definimos a ***soma módulo 5***, denotada por $+_5$, em Z_5, como $x +_5 y = r$, onde *r* é o resto da divisão de *x* + *y* por 5. Por exemplo:

$1 +_5 2 = 3$

$3 +_5 4 = 2$, pois 3 + 4 = 7 e o resto da divisão de 7 por 5 é 2.

A ***multiplicação módulo 5*** é definida por $x \times_5 y = r$, onde *r* é o resto da divisão de $x \times y$ por 5. Por exemplo:

$2 \times_5 3 = 1$, pois $2 \times 3 = 6$ e o resto da divisão de 6 por 5 é 1.

$3 \times_5 4 = 2$, pois $3 \times 4 = 12$ e o resto da divisão de 12 por 5 é 2.

As seguintes tabelas definem $+_5$ e $\times_5$ em Z_5:

$+_5$	**0**	**1**	**2**	**3**	**4**
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

$\times_5$	**0**	**1**	**2**	**3**	**4**
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	0	2	1

Podemos verificar que $\langle Z_5, +_5 \rangle$ e $\langle Z_5, \times_5 \rangle$ são fechadas, pois todos os resultados verificados nas tabelas são elementos de Z_5.

Podemos também verificar que $\langle Z_5, +_5 \rangle$ e $\langle Z_5, \times_5 \rangle$ são comutativas, através das tabelas construídas, pois estão espelhadas em torno da diagonal principal.

Ainda é possível verificar que $\langle Z_5, +_5 \rangle$ e $\langle Z_5, \times_5 \rangle$ são associativas. Entretanto, não podemos verificar tal propriedade nas tabelas construídas.

$\langle Z_5, +_5 \rangle$ e $\langle Z_5, \times_5 \rangle$ possuem elemento neutro: o elemento neutro de $\langle Z_5, +_5 \rangle$ é 0 e o elemento neutro de $\langle Z_5, \times_5 \rangle$ é 1.

Todos os elementos de $\langle Z_5, +_5 \rangle$ possuem elemento inverso:

- o elemento inverso de 0 é 0;
- o elemento inverso de 1 é 4;
- o elemento inverso de 2 é 3;
- o elemento inverso de 3 é 2;
- o elemento inverso de 4 é 1;

Portanto, podemos afirmar que $\langle Z_5, +_5 \rangle$ é um grupo abeliano.

Entretanto, nem todos os elementos de $\langle Z_5, \times_5 \rangle$ possuem elemento inverso. Logo $\langle Z_5, \times_5 \rangle$ é um monóide abeliano.