Fundamentos da Matemática

Notas de Aula

Diego Sebastián Ledesma

Atualizado 28/03/2024

Conteúdo

1. Apresentação

Este texto está composto por minhas notas de aula para o ministério da disciplina Fundamentos da Matemática.

O conteúdo do texto está baseado em material dos seguintes livros

- Iezzi, G., Murakami, C., *Fundamentos de Matemática Elementar*, Atual Editora, 2013
- Aguilar, I.; Dias, M. Sequeiros. *A Construção dos Números Reais e Suas Extensões*. Rio de Janeiro:UFF, 2015.
- Roitman, J. *Introduction to modern set theory*. Wiley (1990).
- Saenz, J. *Fundamentos de la Matemática*. Hipotenusa (2005).
- Seymour Lipschutz - Schaum's outline of theory and problems of set theory and related topics. McGraw-Hill (1998)

e foi modificado e adapatado da forma que achei conveniente para o ministério das aulas.

O texto é de ajuda e guia sobre os tópicos que irei abordando ao longo do semestre com a maior quatidade de detalhes que consegui. No entanto, recomendo fortemente que seja feita sempre uma conferência com as fontes acima citadas.

Em elaboração

I Lógica e Conjuntos

Em elaboração

2. Proposições

Em matemática utilizamos uma linguagem com termos e expressões específicas e com significados precisos. Começamos a estudar estes termos e expressões

Definição 2.1 Uma proposição é uma sentença declarativa, por meio de palavras ou termos, e cujo conteúdo é submetido a juízo no qual poderá ser considerado Verdadeiro (V) ou Falso (F). Estes verdadeiros ou falsos correspondem ao valor lógico da proposição.

Os princípios do raciocínio lógico são os seguintes

- **Princípio da Exclusão:** uma proposição só pode ser verdadeira ou falsa, não existindo possibilidade de uma terceira opção.
- **Princípio da Identidade:** uma proposição verdadeira é verdadeira e uma falsa é falsa.
- **Princípio da não contradição:** nenhuma proposição é verdadeira e falsa simultâneamente.

Definição 2.2 Um Paradoxo ou Absurdo é uma sentença declarativa que não possue valor de verdade verdadeiro nem falso e, portanto, não é proposição.

■ **Exemplo 2.1** Alguns exemplos de paradoxos ou absurdos são :

- "Isto que escrevo é falso": Se a frase é Falsa também é Verdadeiro pois acabei de escrever algo que é falso. Por outro lado se é Falsa, também é verdadeira pois o que acabei de escrever é falso.
- "Eu só digo mentiras": Se o que disse é verdadeiro então não digo mentiras unicamente de onde a frase é falsa. Por outro lado se o que disse é falso então eu o que disse não é uma mentira de onde é verdadeira também.
- "A regra é que não há regra": Se é verdade então há uma regra que é a de não ter regras, portanto é falsa. Mas se for falsa, então há regra é portanto é verdadeira.

■

Algumas proposições tem seu valor de verdade fixo e não pode ser provado ou demonstrado.

Definição 2.3 Um axioma é uma proposição que aceitamos como verdadeira e que não admite demonstração.

Denotamos às proposições com letras O, P, Q, R.

■ **Exemplo 2.2** O que é proposição:

- P="O gelo é o estado sólido da água cristalizada no sistema cristalino hexagonal"(Verdadeiro)
- P="Em um triângulo retângulo, o comprimento da hipotenusa é sempre maior que a soma dos comprimento

dos catetos"(Falso)
- P="a soma dos ângulos internos de um triângulo retângulo no plano é menor do que π"(Falso)
- P="Brasilia é a capital do Brasil"(Verdadeiro)
- P="$5^2 = 25$"(Verdadeiro).
- P="$7 > 5$"(verdadeiro)
- P="$2 < \pi$"(verdadeiro)

O que não é proposição:
- "O número π tem propriedades tão interessantes!"(sentença exclamativa)
- "Tomara seja um número par"(sentença optativa)
- "Será que $a^2 + b^2 < a + b$?"(sentença interrogativa)
- "Faça a conta para mostrar que $(-2)^2 = 4$" (sentença imperativa)
- Opiniões não são proposições.
- Sentenças abertas também não são proposições: "quanto devo adicionar a 2 para obter 5?

■

Dadas certas proposições P e Q podemos criar novas proposições fazendo operações sobre elas. Passamos a descrever estas operações:
- **Negação:** Dada uma proposição P formamos uma nova proposição "não P" que é a negação de P e é denotada por $\neg P$.
- **Conjunção:** Dadas duas proposições P e Q formamos uma nova proposição "P e Q" e que é denotada por $P \wedge Q$.
- **Disjunção** Dadas duas proposições P e Q formamos uma nova proposição "P ou Q" e que é denotada por $P \vee Q$.
- **Condicional:** Dadas duas proposições P e Q formamos uma nova proposição "se P então Q" e que é denotada por $P \Rightarrow Q$. Neste caso P é denominada "condição suficiente ou hipótese" e Q é chamada de "condição necessária ou conclusão".
- **Bicondicional:** Dadas duas proposições P e Q formamos uma nova proposição "P se, e somente se, Q"e que é denotada por $P \Leftrightarrow Q$.

Observamos que com estas operações lógicas podemos formar novas proposições a partir de proposições simples. Chamamos estas proposições de proposições compostas.

■ **Exemplo 2.3** Sejam P, Q, R, S proposições, então

$$P \vee [(Q \wedge \neg R) \Rightarrow S] \Leftrightarrow (Q \wedge P)$$

é um exemplo de proposição composta. ■

■ **Exemplo 2.4** Considere as proposições
- P="O gelo é o estado sólido da água cristalizada no sistema cristalino hexagonal"(Verdadeiro)
- Q="Beber água quente ou chá mata o coronavírus"(Falso)

Então, por exemplo,
- $\neg P$ ="O gelo **não** é o estado sólido da água cristalizada no sistema cristalino hexagonal"
- $P \wedge Q$ ="O gelo é o estado sólido da água cristalizada no sistema cristalino hexagonal **e** Beber água quente ou chá mata o coronavírus"
- $P \vee Q$ ="O gelo é o estado sólido da água cristalizada no sistema cristalino hexagonal **ou** Beber água quente ou chá mata o coronavírus"
- $P \Rightarrow Q$ ="Se O gelo é o estado sólido da água cristalizada no sistema cristalino hexagonal **então** Beber água quente ou chá mata o coronavírus"
- $P \Leftrightarrow Q$ ="O gelo é o estado sólido da água cristalizada no sistema cristalino hexagonal **se, e somente se,** Beber água quente ou chá mata o coronavírus"

■

■ **Exemplo 2.5** Considere as proposições
- P ="3/4 é um número racional".
- Q = "3 é um número impar".

- $R =$ "5 é um número primo".

Então

- $P \wedge Q =$"$3/4$ é um número racional **e** 3 é um número impar".
- $\neg P \vee Q =$"$3/4$ **não** é um número racional **ou** 3 é um número impar".
- $\neg(\neg P) =$"**não** é verdade que $3/4$ **não** é um número racional".
- $\neg((\neg P \Rightarrow Q) =$"**não** é verdade que se $3/4$. **não** é um número racional **então** 3 é um número impar".
- $(P \wedge Q) \Rightarrow R =$"se $3/4$ é um número racional **e** 3 é um número impar **então** 5 é um número primo".
- $(R \vee (\neg Q)) \Rightarrow \neg P =$"Se 5 é um número primo **ou** 3 **não** é um número impar **então** $3/4$ **não** é um número racional".

■

Obs.

O sistema lógico que estamos trabalhando só temos, como vimos, dois valores de verdade (V ou F) no entanto há outros sistemas lógicos em que o número de valores de verdade pode ser maior. Existe, por exemplo, a lógica de $n \in \mathbb{N}$ valores de verdade para a lógica de E. Post ou a lógica difusa ou Fuzzy em que há tantos valores de verdade como pontos no intervalo real $[0,1]$.

Em elaboração

3. Tabelas da Verdade

Como dizemos anteriormente, uma proposição tem um valor de verdade (Verdadeira ou Falsa). Vamos ver agora qual é o valor de verdade das proposições compostas obtidas a partir das operações negação, conjunção, disjunção, condicional e bicondicional.

Junto a isto vamos construir um dispositivo muito útil no estudo da lógica matemática que são as tabelas da verdade. Com elas poderemos definir valor lógico de uma proposição composta em função dos valores de verdade das proposições que a compõem.

- **Negação:** Para a negação temos a seguinte regra,
  - se uma proposição P é verdadeira, então a negação dela, $\neg P$ será falsa.
  - se uma proposição P é falsa, então a negação dela, $\neg P$ será verdadeira.

  Podemos resumir isto na seguinte tabela.

P	$\neg P$
V	F
F	V

- **Conjunção:** Para a conjunção temos a seguinte regra: Sejam P e Q duas proposições, então a proposição $P \wedge Q$ é verdadeira se, e somente se, P e Q são verdadeiras.
  Podemos resumir isto na seguinte tabela.

P	Q	$P \wedge Q$
V	V	V
V	F	F
F	V	F
F	F	F

- **Disjunção:** Para a disjunção temos a seguinte regra: Sejam P e Q duas proposições, então a proposição $P \vee Q$ é falsa se, e somente se, P e Q são falsas.
  Podemos resumir isto na seguinte tabela.

P	Q	$P \vee Q$
V	V	V
V	F	V
F	V	V
F	F	F

- **Condicional:** Para o condicional temos a seguinte regra: Sejam P e Q duas proposições, então a proposição $P \Rightarrow Q$ é falsa se, somente se, P e verdadeiro e Q é falso.
  Podemos resumir isto na seguinte tabela.

P	Q	$P \Rightarrow Q$
V	V	V
V	F	F
F	V	V
F	F	V

- **Bicondicional:** Para a proposição bicondicional temos então a seguinte regra: $P \Leftrightarrow Q$ é verdadeira se os valores de verdade de P e Q coincidem e falsa no caso contrário
  Podemos resumir isto na seguinte tabela.

P	Q	$P \Leftrightarrow Q$
V	V	V
V	F	F
F	V	F
F	F	V

Com estas tabelas básicas podemos formar as tabelas das proposições compostas (uma proposição formada a partir de outras proposições utilizando conectivos lógicos, veremos isto depois) seguindo o seguinte roteiro: Dada uma uma formula proposicional construímos uma tabela-verdade da seguinte forma

- Na linha superior colocamos as subfórmulas da fórmula proposicional. Dispondo de menor a maior na formação da proposição.
- Para cada subformula teremos uma coluna.
- As proposições básicas sobre as quais esta construida a proposição por meio das operações lógicas são colocadas nas primeiras colunas.
- Completamos as linhas em função dos valores de verdade das proposições básicas. Observar que se temos k proposições básicas, teremos 2^k linhas.

Assim por exemplo: Se a proposição é $(P \vee Q) \wedge R$ teremos como tabela da verdade

P	Q	R	$(P \vee Q)$	$(P \vee Q) \wedge R$
V	V	V	V	V
V	V	F	V	F
V	F	V	V	V
V	F	F	V	F
F	V	V	V	V
F	V	F	V	F
F	F	V	F	F
F	F	F	F	F

4. Cálculo Proposicional

Como vimos anteriormente a partir de proposições simples podemos formar, utilizando operadores lógicos, proposições compostas.

O conjunto das proposições munido das operações negação, conjunção, disjunção formam uma álgebra que é a chamada álgebra proposicional. Com ela podemos fazer "contas". Passamos agora estudar essa álgebra.

Uma **fórmula proposicional** é uma regra, construída a partir de um número finito de conectivos lógicos, que pode ser aplicada a um conjunto de proposições,

$$P(Q_1,\ldots,Q_k).$$

Nesse caso a regra P é a fórmula e as entradas $Q_1,\ldots,Q_k$ são as variáveis. Ao aplicar uma fórmula proposicional

$$P(Q_1,\ldots,Q_k)$$

a um conjunto de proposições fixas $R_1,\ldots,R_k$ teremos uma proposição

$$P(R_1,\ldots,R_k).$$

A proposição assim obtida é chamada de **proposição composta**, isto é, uma proposição composta é uma proposição P que é obtida ao aplicar uma fórmula proposicional a um conjunto de proposições.

Dada uma fórmula proposicional $P(Q_1,\ldots,Q_k)$ e um conjunto de proposições $R_1,\ldots,R_k$ produzimos uma proposição composta

$$P = P(R_1,\ldots,R_k),$$

o valor lógico de P é obtido em função dos valores lógicos das proposições $R_1,\ldots,R_k$ e das tabelas da verdade para os conectivos lógicos utilizando para definir P.

■ **Exemplo 4.1** Por exemplo

- Considere a fórmula

  $$P_1(P) = \neg(\neg(P).$$

  Quando aplicada a uma proposição específica, por exemplo,

  $$P = \text{"}5 < 6\text{"},$$

teremos

$$P_1(P) = \neg(\neg(5 < 6)).$$

Em particular, se P é falsa então $P_1(P)$ será falsa.

- Considere a fórmula

$$P_1(P,Q) = P \wedge (P \Rightarrow Q).$$

Quando aplicada, por exemplo às proposições

$$P = \text{"O número } \pi \text{ é irracional"} \quad Q = \text{"}\pi < 5\text{"}$$

teremos

$$P_1(P,Q) = \text{"O número } \pi \text{ é irracional e se número } \pi \text{ é irracional então } \pi < 5 \text{ ."}$$

Em particular se P é falsa, para qualquer valor lógico que assuma Q a proposição $P_1(P,Q)$ será falsa.

- Considere a fórmula

$$P_1(P,Q,R) = R \vee (P \wedge Q).$$

Quanto aplicada, por exemplo, às proposições

$$P = \text{"}5 < \pi\text{"} \quad Q = \text{"5 é número impar"} \quad R = \text{"2 divide a 3"}$$

teremos,

$$P_1(P,Q,R) = \text{"2 divide a 3 ou} \pi < 5 \text{ e 5 é número impar"}$$

Se R é verdadeira então para qualquer valor lógico que assuumam P e Q a proposição $P_1(P,Q,R)$ será verdadeira.

■

A seguir estabelecemos um critério de equivalência entre as fórmulas proposicionais.

Definição 4.1 Duas fórmulas proposicionais $P_1(Q_1,\ldots,Q_k)$ e $P_2(Q_1,\ldots,Q_k)$, são ditas lógicamente equivalentes se elas assumem valores lógicos iguais para quaisquer escolha dos valores lógicos que podem assumir as variáveis $Q_1,\ldots,Q_k$.

Para provar que duas fórmulas proposicionais são equivalentes podem ser utilizadas tabelas da verdade. A seguir vemos alguns exemplos que mostrar algumas equivalência básicas de fórmulas proposicionais.

- **Dupla Negação:** "$\neg(\neg P) = P$"
  De fato

P	$\neg P$	$\neg(\neg P)$
V	F	V
F	V	F

- **Idempotência:**

$$\text{"}P \vee P = P\text{"} \quad \text{e} \quad \text{"}P \wedge P = P\text{"}.$$

De fato

P	$P \vee P$	$P \wedge P$
V	V	V
F	F	F

- **Comutatividade:**

  "$P \vee Q = Q \vee P$" e "$P \wedge Q = Q \wedge P$".

  A prova disto segue imediato da definição de conjunção e disjunção.
- **Associatividade:**

  "$(P \vee Q) \vee O = P \vee (Q \vee O)$" e "$(P \wedge Q) \wedge O = P \wedge (Q \wedge O)$".

  Mostramos uma, pois a outra se prova de forma similar.

P	Q	O	$(P \vee Q)$	$(Q \vee O)$	$P \vee (Q \vee O)$	$(P \vee Q) \vee O$
V	V	V	V	V	V	V
V	V	F	V	V	V	V
V	F	V	V	V	V	V
V	F	F	V	F	V	V
F	V	V	V	V	V	V
F	V	F	V	V	V	V
F	F	V	F	V	V	V
F	F	F	F	F	F	F

- **Distributividade:**

  "$P \vee (Q \wedge O) = (P \vee Q) \wedge (P \vee O)$" e "$P \wedge (Q \vee R) = (P \wedge Q) \vee (P \vee O)$".

  Novamente mostramos um pois o outro é análogo

P	Q	O	$(P \vee Q)$	$(P \vee O)$	$(Q \wedge O)$	$P \vee (Q \wedge O)$	$(P \vee Q) \wedge (P \vee O)$
V	V	V	V	V	V	V	V
V	V	F	V	V	F	V	V
V	F	V	V	V	V	V	V
V	F	F	V	V	F	V	V
F	V	V	V	V	V	V	V
F	V	F	V	F	F	F	F
F	F	V	F	V	F	F	F
F	F	F	F	F	F	F	F

- **Leis de De Morgan:**

  "$\neg(P \vee Q) = (\neg P) \wedge (\neg Q)$" e "$\neg(P \wedge Q) = (\neg P) \vee (\neg Q)$".

  Novamente mostramos uma, a outra é análoga.

P	Q	$\neg P$	$\neg Q$	$(P \vee Q)$	$\neg(P \vee Q)$	$(\neg P) \wedge (\neg Q)$
V	V	F	F	V	F	F
V	F	F	V	V	F	F
F	V	V	F	V	F	F
F	F	V	V	F	V	V

- **Lei de exclusão:** "$(P \vee \neg P) \wedge Q = Q$"

P	$\neg P$	$(P \vee \neg P)$	Q	$(P \vee \neg P) \wedge Q$
V	F	V	V	V
V	F	V	F	F
F	V	V	V	V
F	V	V	F	F

- **Lei de dominação:** Se Q é uma proposição verdadeira então

$$"P \vee Q = Q" \quad \text{e} \quad "P \wedge Q = P".$$

De fato

P	Q	$(P \vee Q)$
V	V	V
F	V	V

e

Q	P	$(P \wedge Q)$
V	V	V
V	F	F

Obs. Da mesma forma que provamos as equivalências acima, podemos mostrar as seguintes:

- $P \Rightarrow Q = (\neg P \vee Q)$. De fato

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

Trataremos, daqui para frente, a identidade

$$P \Rightarrow Q = \neg P \vee Q$$

de definição do condicional ($\Rightarrow$).

- $P \Leftrightarrow Q = [(P \Rightarrow Q) \wedge (Q \Rightarrow P)]$. De fato

P	Q	$P \Rightarrow Q$	$Q \Rightarrow P$	$P \Leftrightarrow Q$	$(P \Rightarrow Q) \wedge (Q \Rightarrow P)$
V	V	V	V	V	V
V	F	F	V	F	F
F	V	V	F	F	F
F	F	V	V	V	V

Trataremos, daqui para frente, a identidade

$$P \Leftrightarrow Q = (P \Rightarrow Q) \wedge (Q \Rightarrow P)$$

de definição do bicondicional ($\Leftrightarrow$).

Obs. A fórmula proposicional dada pelo condicional

$$R_1(P,Q) = (P \Rightarrow Q)$$

é equivalente a

$$R_2(P,Q) = \{\neg[P \wedge (\neg Q)]\}.$$

Para ver isto utilizamos as identidades acima

$$\begin{aligned} P \Rightarrow Q &= \neg P \vee Q \\ &= \neg[P \wedge (\neg Q)]. \end{aligned}$$

A partir da proposição condicional podemos definir as seguintes proposições

- **Recíproca:** Dada uma proposição condicional $P \Rightarrow Q$ definimos a proposição recíproca por $Q \Rightarrow P$.
- **Inversa:** Dada uma proposição condicional $P \Rightarrow Q$ definimos a proposição inversa por $\neg P \Rightarrow \neg Q$.

- **Contrapositiva:** Dada uma proposição condicional $P \Rightarrow Q$ definimos a proposição contrapositiva por $\neg Q \Rightarrow \neg P$. A fórmula da contrapositiva é equivalente ao condicional. De fato, se

$$R_1(P,Q) = (P \Rightarrow Q) \quad \text{e} \quad R_2(P,Q) = (\neg Q \Rightarrow \neg P),$$

utilizando as regras acima vemos que

$$\begin{aligned} P \Rightarrow Q &= \neg P \vee Q \\ &= \neg(\neg Q) \vee (\neg P) \\ &= \neg Q \Rightarrow \neg P. \end{aligned}$$

Lema 4.1 Se R é uma proposição falsa então $P \wedge R$ é falsa e $P \vee R = P$.

Demonstração. De fato, se R é falsa $\neg R$ é verdadeira. Utilizando a lei de dominação temos

$$\begin{aligned} \neg(P \wedge R) &= \neg P \vee \neg R \\ &= \neg R \quad \rightarrow \quad \text{De onde } R \text{ falsa garante } P \wedge R \text{ é falsa.} \end{aligned}$$

Para a segunda, vemos que

$$\begin{aligned} \neg(P \vee R) &= \neg P \wedge \neg R \\ &= \neg P \quad \rightarrow \quad \text{De onde } R \text{ é falsa garante } (P \vee R) = P. \end{aligned}$$

■

Lema 4.2 A fórmula proposicional

$$R_1(P) = P \vee \neg P$$

é sempre verdadeira para qualquer valor que possa assumir P, e a fórmula proposicional

$$R_2(P) = P \wedge \neg P$$

é sempre falsa para qualquer valor que possa assumir P.

Demonstração. Para mostrar que $P \vee \neg P$ é sempre verdadeira observamos que

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

Da mesma forma, $P \wedge \neg P$ é sempre falsa. De fato,

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

■

Definição 4.2 Uma fórmula proposicional $Q = Q(P_1, \ldots, P_k)$ é uma

- Tautologia quando o seu valor de verdade é Verdadeiro independentemente dos valores de verdade que possam assumir as variáveis $P_1, \ldots, P_k$ que a compõem.
- Contradição quando o seu valor de verdade é Falso independentemente dos valores de verdade que possam assumir as variáveis $P_1, \ldots, P_k$ que a compõem.
- Contingência se não for Tautologia nem Contradição.

Obs. As Tautologias recebem o nome de Leis da lógica.

■ **Exemplo 4.2** • Dadas P e Q proposições, vamos mostrar que a fórmula

$$R(P,Q) = [(P \Rightarrow Q) \wedge \neg Q] \Rightarrow \neg P$$

é uma tautologia.
De fato, construindo a tabela de verdade vemos que:

P	Q	$\neg Q$	$P \Rightarrow Q$	$(P \Rightarrow Q) \wedge \neg Q$	$\neg P$	$[(P \Rightarrow Q) \wedge \neg Q] \Rightarrow \neg P$
V	V	F	V	F	F	V
V	F	V	F	F	F	V
F	V	F	V	F	V	V
F	F	V	V	V	V	V

• Dadas P e Q proposições, vamos mostrar que a fórmula

$$R(P,Q) = P \wedge \neg(Q \vee P)$$

é uma contradição.
De fato, construindo a tablea de verdade vemos que:

P	Q	$Q \vee P$	$\neg(Q \vee P)$	$P \wedge \neg(Q \vee P)$
V	V	V	F	F
V	F	V	F	F
F	V	V	F	F
F	F	F	V	F

■

Com as leis e resultados acima podemos fazer contas com as proposições. Vejamos a seguir alguns exemplos.

■ **Exemplo 4.3** Vamos mostrar que as seguintes equivalências entre fórmulas proposicionais

• $[(P \wedge Q) \Rightarrow R] = [P \Rightarrow (Q \Rightarrow R)]$ (esta fórmula é conhecida como **Lei de exportação**).
De fato

$$\begin{aligned}
(P \wedge Q) \Rightarrow R &= \neg(P \wedge Q) \vee R \quad \text{(definição de } \Rightarrow) \\
&= (\neg P \vee \neg Q) \vee R \quad \text{(De Morgan)} \\
&= \neg P \vee (\neg Q \vee R) \quad \text{(associatividade)} \\
&= \neg P \vee (Q \Rightarrow R) \quad \text{(definição de } \Rightarrow) \\
&= P \Rightarrow (Q \Rightarrow R) \quad \text{(definição de } \Rightarrow).
\end{aligned}$$

• $[(P \wedge \neg Q) \Rightarrow \neg(P \wedge R \Rightarrow \neg Q)] = [Q \wedge (P \Rightarrow R)]$
De fato,

$$\begin{aligned}
(P \vee \neg Q) \Rightarrow \neg[(P \wedge R) \Rightarrow \neg Q] &= \neg(P \vee \neg Q) \vee \neg[\neg(P \wedge R) \vee \neg Q) \quad \text{(definição de } \Rightarrow) \\
&= (\neg P \wedge Q) \vee [(P \wedge R) \wedge Q] \quad \text{(De Morgan)} \\
&= [\neg P \vee (P \wedge R)] \wedge Q \quad \text{(distributividade)} \\
&= [(\neg P \vee P) \wedge (\neg P \vee R)] \wedge Q \quad \text{(associatividade)} \\
&= [(\neg P \vee R)] \wedge Q \quad \text{(pois } (\neg P \vee P) \text{ é Verdadeira)} \\
&= Q \wedge (P \Rightarrow R) \quad \text{(definição de } \Rightarrow).
\end{aligned}$$

• Vamos ver como expressar a fórmula do condicional e do bicondicional utilizando somente a negação e a disjunção.

$$\begin{aligned}
P \Rightarrow Q &= \neg(\neg(P \Rightarrow Q)) \quad \text{(dupla negação)} \\
&= \neg[P \wedge (\neg Q)] \quad \text{(definição de } \Rightarrow) \\
&= \neg P \vee Q \quad \text{(De Morgan)}.
\end{aligned}$$

Para o bicondicional temos, pelo visto para o condicional e a definição, que

$$\begin{aligned}
P \Leftrightarrow Q &= (P \Rightarrow Q) \wedge (Q \Rightarrow P) \\
&= (\neg P \vee Q) \wedge (\neg Q \vee P) \quad \text{(definição de } \Rightarrow) \\
&= \neg[\neg(\neg P \vee Q) \vee \neg(\neg Q \vee P)] \quad \text{(relação vista acima e De Morgan)}
\end{aligned}$$

■

Lema 4.3 — Leis da Absorção. Sejam P e Q proposições, então

$$P \vee (P \wedge Q) = P \quad \text{e} \quad P \wedge (P \vee Q) = P,$$

Demonstração. Observamos que se R é uma proposição que sempre é verdadeira, temos que

$$\begin{aligned} P \vee (P \wedge Q) &= (P \wedge R) \vee (P \wedge Q) \quad (R \text{ é verdadeira}) \\ &= P \wedge (R \vee Q) \quad (\text{distributividade}) \\ &= P \wedge R \quad (R \text{ é verdadeira}) \\ &= P \quad (R \text{ é verdadeira}). \end{aligned}$$

Também

$$\begin{aligned} P \wedge (P \vee Q) &= \neg[\neg P \vee \neg(P \vee Q)] \quad (\text{dupla negação}) \\ &= \neg[\neg P \vee (\neg P \wedge \neg Q)] \quad (\text{De Morgan}) \\ &= \neg[\neg P] \quad (\text{resultado anterior}) \\ &= P \quad (\text{dupla negação}). \end{aligned}$$

■

Em elaboração

5. Argumentação Lógica

A argumentação lógica é uma organização ou estruturação de proposições pela qual, junto com as regras da lógica, chegamos a uma conclusão ou solução. Ela é importante pois nos permite, principalmente, encontrar o caminho correto para a resolução de um problema. No entanto, claramente, ajuda na resolução de problemas práticos do dia a dia.

Definição 5.1 Sejam P e Q duas proposições. Dizemos que P implica logicamente Q (ou P implica Q) e o denotamos por

$$P \vdash Q.$$

se a proposição composta

$$P_1(P,Q) = [P \Rightarrow Q]$$

é verdadeira.

Obs. Lembramos que se P e Q são duas proposições temos que a tabela da verdade do condicional é

P	Q	$P \Rightarrow Q$
V	V	V
V	F	F
F	V	V
F	F	V

Portanto, para que o condicional seja verdadeira temos que pedir que se P é verdadeira, então Q é verdadeira. Veremos isso com mais detalhes depois.

Definição 5.2 • Um raciocínio ou argumento lógico é a afirmação de que uma proposição C, chamada conclusão, é consequência de outras proposições, $P_1, \ldots, P_n$, chamadas premissas. Neste caso, denotamos

$$\{P_1, \cdots, P_n\} \vdash C$$

- Um argumento é **válido** ou correto se a conjunção das premisas implica lógicamente a conclusão, isto é, se a fórmula

  $$Q_1(P_1,\ldots,P_n,C) = [P_1 \wedge \cdots \wedge P_n \Rightarrow C]$$

  é verdadeira quando avaliada em $P_1,\ldots,P_n,C$ ou, equivalentemente,

  $$P_1 \wedge \cdots \wedge P_n \vdash C.$$

  Neste caso a conclusão é chamada de Teorema.
- Uma **falácia** e um raciocínio que não é válido.

Vamos mostrar agora, utilizando o que foi visto acima, duas regras canônicas da argumentação lógica: As regras de Modus Ponens e Modus Tollens.

Observamos que estas regras são na verdade fórmulas que valem sempre que as componentes forem substituidas por proposições com seus respectivos valores de verdade.

- A regra **Modus Ponendo Ponens** (do Latim "maneira que afirma afirmando") ou afirmação do antecedente. Chamamos esta regra de modus ponens por simplicidade. Esta regra pode ser escrita da seguinte forma: sejam P e Q duas proposições então

  $$\{P \Rightarrow Q,\ P\} \vdash Q.$$

  Para isto, considere proposição

  $$R(P,Q) = P \wedge (P \Rightarrow Q)$$

  e vamos mostrar que R implica lógicamente Q, isto é, $R \vdash Q$. Construímos a tabela

P	Q	$P \Rightarrow Q$	R	$R \Rightarrow Q$
V	V	V	V	V
V	F	F	F	V
F	V	V	F	V
F	F	V	F	V

  Portanto a fórmula $S(P,Q) = [R(P,Q) \Rightarrow Q]$ é uma tautologia, de onde segue que $R(P,Q)$ implica lógicamente Q para quaisquer valores de P e Q.
  Um exemplo da regra de Modus ponens é a seguinte

  "Se hoje é domingo então não trabalho. Hoje é domingo. Logo, não trabalho."

  Podemos também mostrar este argumento utilizando as regras de cálculo proposicional, para isto observamos que

  $$\begin{aligned}
  [(P \Rightarrow Q) \wedge P] \Rightarrow Q &= [(\neg P \vee Q) \wedge P] \Rightarrow Q \quad \text{(definição } \Rightarrow\text{)} \\
  &= [(\neg P \wedge P) \vee (Q \wedge P)] \Rightarrow Q \quad \text{(associatividade)} \\
  &= (Q \wedge P) \Rightarrow Q \quad \text{(dominação)} \\
  &= \neg(Q \wedge P) \vee Q \quad \text{(definição } \Rightarrow\text{)} \\
  &= (\neg Q \vee \neg P \vee Q) \quad \text{(De Morgan)} \\
  &= (\neg Q \vee Q) \vee \neg P \quad \text{(associatividade)}
  \end{aligned}$$

  que é uma tautologia pois $\neg Q \vee Q = \neg(Q \wedge \neg Q)$ é verdadeira.
- A regra de **Modus Tollendo Tollens** (do Latim: "maneira que nega por negação") ou negação do consequente. Chamamos esta regra de modus tollens por simplicidade. Esta regra pode ser escrita na forma

  $$\{P \Rightarrow Q,\ \neg Q\} \vdash \neg P$$

Para isto, considere proposição

$$R(P,Q) = \neg Q \wedge (P \Rightarrow Q)$$

e vamos mostrar que R implica lógicamente Q, isto é, $R \vdash Q$. Construímos a tabela

P	Q	$P \Rightarrow Q$	$\neg Q$	R	$\neg P$	$R \Rightarrow \neg P$
V	V	V	F	F	F	V
V	F	F	V	F	F	V
F	V	V	F	F	V	V
F	F	V	V	V	V	V

Portanto a fórmula $S(P,Q) = [R(P,Q) \Rightarrow \neg P]$ é uma tautologia, de onde segue que $R(P,Q)$ implica lógicamente $\neg P$ para quaisquer valores de P e Q.
Um exemplo da regra de Modus Tollens é a seguinte

"Se hoje é domingo então não trabalho. Trabalho. Logo, hoje não é domingo."

Podemos também mostrar este argumento utilizando as regras de cálculo proposicional, para isto observamos que

$$\begin{aligned}
[(P \Rightarrow Q) \wedge \neg Q] \Rightarrow \neg P &= [(\neg P \vee Q) \wedge \neg Q] \Rightarrow \neg P \quad \text{(definição } \Rightarrow\text{)} \\
&= [(\neg P \wedge \neg Q) \vee (Q \wedge \neg Q)] \Rightarrow \neg P \quad \text{(distributividade)} \\
&= [(\neg P \wedge \neg Q)] \Rightarrow \neg P \quad \text{(pois } (Q \wedge \neg Q) \text{ é Falsa e dominação)} \\
&= \neg(\neg P \wedge \neg Q) \vee \neg P \quad \text{(definição } \Rightarrow\text{)} \\
&= (P \vee Q) \vee \neg P \quad \text{(De Morgan)} \\
&= Q \vee (P \vee \neg P) \quad \text{(asociatividade)}
\end{aligned}$$

que é uma tautologia pois $\neg P \vee P = \neg(P \wedge \neg P)$ é verdadeira.

Associadas a estas regras temos duas falácias ou argumentos inválidos que são de uso cotidiano na forma de raciocinar:

- **Falácia da afirmação do consequênte:** É muito similar a Modus Ponens. A fórmula proposicional da mesma é

  $$\{P \Rightarrow Q,\ Q\} \vdash P$$

  Para ver que o argumento é inválido temos que mostrar que a fórmula do argumento não é uma tautologia. De fato, se

  $$R(P,Q) = (P \Rightarrow Q) \wedge Q$$

  temos

P	Q	$P \Rightarrow Q$	R	$R \Rightarrow P$
V	V	V	V	V
V	F	F	F	V
F	V	V	V	F
F	F	V	F	V

  Um exemplo desta falácia é o seguinte argumento

  "Se hoje é domingo então não trabalho. Não trabalho. Logo, hoje é domingo."

  Veja que, neste caso,

  $P =$ "Hoje é domingo" $\quad Q =$ "Não trabalho"

  e argumento não se sustenta precisamente quando P é falso e Q verdadeiro, pois pode ser segunda-feira e, no caso, também não trabalhar.

- **Falácia da negação do antecedente:** É muito similar a Modus Tollens. A fórmula proposicional da mesma é

$$\{P \Rightarrow Q,\ \neg P\} \vdash \neg Q$$

Para ver que o argumento é inválido temos que mostrar que a fórmula do argumento não é uma tautologia. De fato, se

$$R(P,Q) = (P \Rightarrow Q) \wedge (\neg P)$$

temos

P	Q	$P \Rightarrow Q$	$\neg P$	R	$\neg Q$	$R \Rightarrow \neg Q$
V	V	V	F	F	F	V
V	F	F	F	F	V	V
F	V	V	V	V	F	F
F	F	V	V	V	V	V

Um exemplo da falácia é o seguinte argumento

"Se hoje é domingo então não trabalho. Hoje não é domingo. Logo, trabalho."

Veja que, neste caso,

$P =$ "Hoje é domingo" $\quad Q =$ "Não trabalho"

e argumento não se sustenta precisamente quando P é falso e Q verdadeiro, pois pode ser segunda-feira e, no caso, também não trabalhar.

Obs. Estas duas falácias vistas acima são a mais comuns em argumentação de prova. Principalmente nos resultados em que temos que provar que uma propriedade vale para todo elemento de um conjunto. A falácia surge ao argumentar que como "vale para um caso particular vale para todo". Isto é uma falácia do tipo afirmação do consequente, pois a argumentação correta é que se "vale para todo elemento do conjunto, vale para o caso particular". Isto ficará mais claro quando sejam vistos os quatificadores.

A seguir estudamos alguns exemplos de regras de argumentos lógicos com as mesmas técnicas que estudamos acima.

■ **Exemplo 5.1** • Considere as seguintes fórmulas proposicionais

$$P_1 = (P \Rightarrow Q) \quad P_2 = (R \Rightarrow \neg Q) \quad P_3 = R \quad C = (\neg P)$$

e o argumento

$$\{P_1,\ P_2,\ P_3\} \vdash C.$$

A tabela de verdade associada a este argumento é

P	Q	R	P_1	P_2	$P_1 \wedge P_2 \wedge P_3$	C	$P_1 \wedge P_2 \wedge P_3 \Rightarrow C$
V	V	V	V	F	V	F	V
V	V	F	V	V	F	F	V
V	F	V	F	V	F	F	V
V	F	F	F	V	F	F	V
F	V	V	V	V	V	V	V
F	V	F	V	V	F	V	V
F	F	V	V	V	V	V	V
F	F	F	V	V	F	V	V

portanto o argumento é válido. Um exemplo deste tipo de argumento é
- P ="hoje é dia 15".
- Q ="amanhã é dia 16"
- R ="hoje é dia 13"

Então
- P_1 ="Se hoje é dia 15 então amanhã é dia 16"
- P_2 ="Se hoje é dia 13 amanhã não é dia 16"
- P_3 ="Hoje é dia 13"
- C ="Hoje não é dia 15"

e o argumento seria:

"Se hoje é dia 15 então amanhã é dia 16. Se hoje é dia 13 amanhã não é dia 16. Hoje é dia 13. Logo, hoje não é dia 15."

Podemos também mostrar que este argumento é valido utilizando as regras de cálculo proposicional, para isto observamos que

$$\begin{aligned}
P_1 \wedge P_2 \wedge P_3 \Rightarrow \neg P &= (P \Rightarrow Q) \wedge (R \Rightarrow \neg Q) \wedge R \Rightarrow \neg P \\
&= (\neg P \vee Q) \wedge (\neg R \vee Q) \wedge R \Rightarrow \neg P \quad \text{(definição } \Rightarrow\text{)} \\
&= (\neg P \vee Q) \wedge [(\neg R \vee Q) \wedge R)] \Rightarrow \neg P \quad \text{(associatividade)} \\
&= (\neg P \vee Q) \wedge [(\neg R \wedge R) \vee (Q \wedge R)] \Rightarrow \neg P \quad \text{(distributividade)} \\
&= (\neg P \vee Q) \wedge (Q \wedge R) \Rightarrow \neg P \quad \text{(dominação)} \\
&= (\neg P \wedge Q \wedge R) \vee (Q \wedge Q \wedge R) \Rightarrow \neg P \quad \text{(distributividade)} \\
&= (\neg P \wedge Q \wedge R) \vee (Q \wedge R) \Rightarrow \neg P \quad \text{(idempotência)} \\
&= [\neg P \wedge (Q \wedge R)] \vee (Q \wedge R) \Rightarrow \neg P \quad \text{(associatividade)} \\
&= \neg P \Rightarrow \neg P \quad \text{(absorção)} \\
&= (P \vee \neg P) \quad \text{(definição } \Rightarrow\text{)}
\end{aligned}$$

que é claramente uma tautologia.

- Considere as seguintes fórmulas proposicionais

$$P_1 = (P \Rightarrow Q) \quad P_2 = (Q \Rightarrow R) \quad C = (P \Rightarrow R)$$

e o argumento

$$\{P_1,\ P_2\} \vdash C.$$

Éste argumento é conhecido como Silogismo Hipotético. A tabela de verdade associada a este argumento é

P	Q	R	P_1	P_2	$P_1 \wedge P_2$	C	$P_1 \wedge P_2 \Rightarrow C$
V	V	V	V	V	V	V	V
V	V	F	V	F	F	F	V
V	F	V	F	V	F	V	V
V	F	F	F	V	F	F	V
F	V	V	V	V	V	V	V
F	V	F	V	F	F	V	V
F	F	V	V	V	V	V	V
F	F	F	V	V	V	V	V

portanto o argumento é válido. Um exemplo deste tipo de argumento é
- P ="ontem foi dia 14".
- Q ="hoje é dia 15"

– R ="amanhã é dia 16"

Então

– P_1 ="Se ontem foi dia 14 então hoje é dia 15".
– P_2 ="Se hoje é dia 15 então amanhã é dia 16".
– C ="Se ontem foi dia 14 então amanhã é dia 16".

e o argumento seria:

"Se ontem foi dia 14 então hoje é dia 15. Se hoje é dia 15 então amanhã é dia 16. Logo, se ontem foi dia 14 então amanhã é dia 16."

Podemos também mostrar que este argumento é valido utilizando as regras de cálculo proposicional, para isto observamos que

$$\begin{aligned}
P_1 \wedge P_2 \Rightarrow C &= [(P \Rightarrow Q) \wedge (Q \Rightarrow R)] \Rightarrow (P \Rightarrow R) \\
&= [(P \Rightarrow Q) \wedge (\neg Q \vee R)] \Rightarrow (\neg P \vee R) \quad \text{(definição } \Rightarrow\text{)} \\
&= [(P \Rightarrow Q) \wedge \neg Q] \vee [(P \Rightarrow Q) \wedge R)] \Rightarrow (\neg P \vee R) \quad \text{(Distributividade)} \\
&= [\neg P] \vee [(P \Rightarrow Q) \wedge R)] \Rightarrow (\neg P \vee R) \quad \text{(Modus Tollens)} \\
&= [\neg P] \vee [(\neg P \vee Q) \wedge R)] \Rightarrow (\neg P \vee R) \quad \text{(definição } \Rightarrow\text{)} \\
&= [\neg P \vee (\neg P \vee Q)] \wedge [\neg P \vee R] \Rightarrow (\neg P \vee R) \quad \text{(Distributividade)} \\
&= \neg[\,[\neg P \vee (\neg P \vee Q)] \wedge [\neg P \vee R]\,] \vee (\neg P \vee R) \quad \text{(definição } \Rightarrow\text{)} \\
&= \neg[\neg P \vee (\neg P \vee Q)] \vee [\neg(\neg P \vee R)] \vee (\neg P \vee R) \quad \text{(De Morgan)}
\end{aligned}$$

Que é uma tautologia pois $[\neg(\neg P \vee R)] \vee (\neg P \vee R)$ é sempre Verdadeira.

■

Nos detemos um pouco na questão de como utilizamos, em matemática, a argumentação lógica para provar que um determinado argumento

$$\{P_1, \ldots, P_n\} \vdash C,$$

é válido. Neste caso sabemos que o que temos que provar é que a proposição

$$Q(P_1, \ldots, P_n, C) = [P_1 \wedge \cdots \wedge P_n \Rightarrow C],$$

onde $P_1, \ldots, P_n$ são as premisas e C é a conclusão, é verdadeira. A proposição $Q(P_1, \ldots, P_n, C)$ tem a seguinte tabela da verdade

$P_1 \wedge \cdots \wedge P_n$	C	$P_1 \wedge \cdots \wedge P_n \Rightarrow C$
V	V	V
V	F	F
F	V	V
F	F	V

Portanto, para mostrar que o argumento é válido, temos que ver que **NUNCA OCORRE** o caso em que

$$P_1 \wedge \cdots \wedge P_n : \text{Verdadeira} \quad \text{e} \quad C : \text{Falsa}$$

Isto pode ser feito de diferentes formas:

- **Forma Direta:** Assumindo que $P_1 \wedge \cdots \wedge P_n$ é verdadeira (portanto cada uma das P_i são verdadeiras) chegamos, utilizando as ferramentas matemáticas que dispomos, o cálculo proposicional e/ou tabelas da verdade, que a única posibilidade para a conclusão C é ser uma proposição verdadeira.

- **Forma Indireta:** Utilizando a equivalência contrapositiva,

$$\begin{aligned} P_1 \wedge \cdots \wedge P_n \Rightarrow C &= \neg(P_1 \wedge \cdots \wedge P_n) \vee C \\ &= C \vee \neg(P_1 \wedge \cdots \wedge P_n) \\ &= \neg(\neg C) \vee \neg(P_1 \wedge \cdots \wedge P_n) \\ &= \neg C \Rightarrow \neg(P_1 \wedge \cdots \wedge P_n). \end{aligned}$$

cuja tabela da verdade é

$P_1 \wedge \cdots \wedge P_n$	C	$\neg C$	$\neg(P_1 \wedge \cdots \wedge P_n)$	$\neg C \Rightarrow \neg(P_1 \wedge \cdots \wedge P_n)$
V	V	F	F	V
V	F	V	F	F
F	V	F	V	V
F	F	V	V	V

Desta forma, para mostrar que o argumento é válido devemos mostrar que se assumimos a C como sendo falsa chegamos, utilizando as ferramentas matemáticas que dispomos, o cálculo proposicional e/ou tabelas da verdade, a que a única posibilidade para $\neg(P_1 \wedge \cdots \wedge P_n)$ seja ser uma proposição verdadeira e portanto, o que está grifado em verde não acontece.

- **Redução ao Absurdo:** O método consiste em mostrar a partir de supostos que alguma das proposições que constituem o argumento não pode ser uma proposição, o que é um absurdo ou paradoxo. Ele se baseia em que a negação de uma tautologia é uma contradição. Como

$$\neg(P_1 \wedge \cdots \wedge P_n \Rightarrow C) = \neg(\neg(P_1 \wedge \cdots \wedge P_n) \vee C) = P_1 \wedge \cdots \wedge P_n \wedge \neg C$$

a ideia é provar que

$$P_1 \wedge \cdots \wedge P_n \wedge (\neg C)$$

é um contradição lógica. Fazendo a tabela da verdade vemos que,

$P_1 \wedge \cdots \wedge P_n$	C	$\neg C$	$P_1 \wedge \cdots \wedge P_n \wedge \neg C$
V	V	F	F
V	F	V	V
F	V	F	F
F	F	V	F

e portanto, deve-se mostrar que o que está grifado em verde não acontece.

Assim, este caso consiste em mostrar utilizando as ferramentas matemáticas que dispomos, o cálculo proposicional e/ou tabelas da verdade, que se assumimos que as P_i são verdadeiras e C falsa chegamos a que uma das proposições que compõem o argumento (geralmente C, mas pode ser alguma das P_i também) tem dois valores de verdade (Verdadeiro e Falso) simultáneamente violando o princípio de exclusão. De onde segue que esta não pode ser uma proposição, o que é um absurdo que provém dos supostos. Consequêntemente o grifado em verde não pode acontecer.

Dado um determinado argumento que devemos provar escolheremos a forma em que vamos mostrá-lo. A forma que será empregada na demonstração depende do contexto. Muitas vezes uma é mais conveniente respeito das outras por ser mais simples de ser aplicada.

De forma geral,

- Se vamos mostrar que $P \vdash Q$ mostramos $P \Rightarrow Q$ é verdadeira e, portanto, que nunca ocorre o caso em que P é verdadeira e Q é falsa.
- Se vamos mostrar que $P = Q$ então devemos mostrar que $P \vdash Q$ e que $Q \vdash P$, isto é, que o bicondicional $P \Leftrightarrow Q$ é uma verdadeira e, portanto, nunca ocorre o caso em que as proposições tem valores lógicos diferentes.

■ **Exemplo 5.2** • A gente aplica algum dos três métodos no dia a dia: Suponha, por exemplo, que você mora numa kitnet (casas maiores requerem mais pasos porém o raciocínio é similar) e você tem que sair e precisa das chaves porque está trancado do lado de dentro. Então, para buscar a chave, o raciocínio que você aplica é

"Se a chave não está na sala então está no banheiro".

Vamos mostrar que este raciocínio é válido das três formas vistas acima.
Primeiramente, denotamos por

$$P_1 = \text{"Há uma chave"}, \quad P_2 = \text{"A chave não está na sala"},$$

$$C = \text{"A chave está no banheiro"}.$$

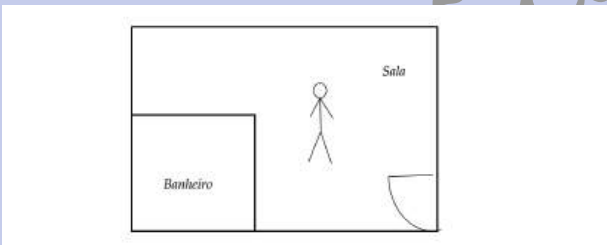
O argumento então é

$$\{P_1, P_2\} \vdash C,$$

e queremos mostrar que é válido, isto é, provar que

$$Q(P_1, P_2, C) = [P_1 \wedge P_2 \Rightarrow C]$$

é verdadeira.
Assumimos que P_1 é sempre verdadeira pois sabemos que há uma chave.



- Direta: Assumimos $P_1 \wedge P_2$ como verdadeira. Então, como a casa tem 2 cómodos, se a chave não está na sala (P_1 é verdadeira) tem que estár no outro cómodo. Como este cómodo é o banheiro ela deve estar no banheiro. De onde C é verdadeira.
- Indireta: (similar à direta só que na outra direção). Assumimos que C é falsa. Então a chave não está no banheiro. Novamente, como a casa tem dois cómodos, então deve estar no outro cómodo, que é a sala. De onde a chave está na sala e, portanto, P_2 é falsa. De onde $P_1 \wedge P_2$ é falsa.
- Absurdo: Neste caso assumimos $P_1 \wedge P_2 \wedge \neg C$ é verdadeira, isto é, que a chave não está na sala e que também não está no banheiro. Portanto, como a casa tem dois cómodos, não pode estar na casa. Mas a gente estava dentro da casa e teve que abrir a porta. De onde segue que a casa não tem chave. Isto é um absurdo (pois sabemos que há uma chave) que provém de supor que a chave não está no banheiro.

- Considere as proposições
$P_1 =$ "o número natural N é divisível por 2"
$P_2 =$ "o número natural N é divisível por 3"
$C =$ "o número natural N é divisível por 6"
Queremos mostrar que $\{P_1,\ P_2\} \vdash C$ é um argumento válido. Ou, dito de outra forma, que

"Se o número natural N é divisível por 2 e o número natural N é divisível por 3 então o número natural N é divisível por 6"

Vamos mostrar isto das três formas deferentes vistas acima:

- Direta. Assuma que P_1 e P_2 são verdadeiras, isto é, que o número natural N é tal que $N = 2 \cdot r$ e $N = 3 \cdot k$ então, como $(2,3) = 1$ existe um $t \in \mathbb{N}$ tal que $k = 2 \cdot t$. Portanto

$$N = 3 \cdot k = 3 \cdot 2 \cdot t = 6 \cdot t.$$

de onde C é verdadeira.

- Indireta. Assuma que C é falsa, e $\neg C$ verdadeira, isto é , que $N = 6\cdot k + r$ com $0 < r < 6$.
  Modo 1: Se $2|r$ (P_1 verdadeira) então $3 \not| r$ pois, se dividisse teríamos que $6|r$, o que não acontece. Portanto P_2 é falsa e, consequêntemente $P_1 \wedge P_2$ é falsa, de onde $\neg(P_1 \wedge P_2)$ é verdadeira.
  Modo 2: Se $3|r$ (P_2 verdadeira) então $2 \not| r$ pois, se dividisse teríamos que $6|r$, o que não acontece. Portanto P_1 é falsa e, consequêntemente $P_1 \wedge P_2$ é falsa, de onde $\neg(P_1 \wedge P_2)$ é verdadeira.
- Absurdo: Assuma que P_1 e P_2 são verdadeiras e C é falsa, isto é que $2|N$, $3|N$ e $N = 6k + r$ com $0 < r < 6$. Então, como $2|N$ temos que $N = 2m$ pois e, como $3|n$ e $(2,3) = 1$ temos que $m = 3m'$ de onde $N = 6m'$. De onde obtemos que C é verdadeira e falsa ao mesmo tempo, e portanto não pode ser uma proposição, o que é um absurdo que provém do fato de supor que C é falsa.

- Considere as proposições
  $P_1 =$ "N^2 um inteiro múltiplo divisível por 3"
  $C =$ "N é um número inteiro divisível por 3"
  Queremos mostrar que $P_1 \vdash C$ é um argumento válido. Ou, dito de outra forma, que

  "Se N^2 um inteiro múltiplo divisível por 3 então N é um número inteiro divisível por 3"

  Vamos mostrar isto das três formas deferentes vistas acima, mas antes de começar observamos que se N é um número inteiro então, do algoritmo da divisão,

  $$N = 3\cdot k + r \quad k \in \mathbb{Z}, \quad 0 \leq r < 3$$

  portanto

  $$N^2 = 3\cdot(3\cdot k^2 + 2\cdot k) + r^2$$

  onde

  $$r^2 = \begin{cases} 0 & \text{se} \quad r = 0 \\ 1 & \text{se} \quad r = 1 \\ 4 & \text{se} \quad r = 2 \end{cases}$$

  - Direta. Assuma que P_1 é verdadeira então $r^2 = 0$, de onde $r = 0$. Portanto 3 divide a N e C é verdadeira.
  - Indireta. Assuma que C é falsa, e $\neg C$ verdadeira. Pelo visto no começo, isto garante que $N = 3\cdot k + r$ com $r = 1$ ou $r = 2$. De onde P_1 é falsa
  - Absurdo: Assuma que P_1 é verdadeira e C é falsa. Então, $N = 3\cdot k$ e $N^2 = 3\cdot k' + r^2$ para $r^2 = 1$, ou $r^2 = 4$. Pelo visto no começo, a segunda afirmação garante que $N = 3\cdot l + r$ para $r = 1$ ou $r = 2$, de onde segue que N não pode ser divisível por 3 e portanto P_1 também é falsa, o que é um absurdo.

■

Em elaboração

6. Quantificadores

Existem frases declarativas que não há como dizer se são verdadeiras ou falsas pois dependem do valor que assume uma variável para que possam ser consideradas como proposição. Estas são chamadas de funções proposicionais. Para definir corretamente o conceito de função proposicional precisamos da noção de conjunto.

A noção de conjunto, elemento e pertinência, são conceito básicos da matemática e aceitos sem definição. Algo similar ao que acontece com pontos, retas, etc., na geometria. No entanto, podemos dizer que

- Um agrupamento, classe, coleção ou sistema é, em geral, um conjunto.
- Cada membro ou objeto que entra na formação do conjunto é chamado de elemento do conjunto.
- Se A é um conjunto e a um elemento que entra na formação do conjunto A dizemos que a pertence a A e escrevemos $a \in A$. Caso contrário, dizemos que a não pertence a A e escrevemos $a \notin A$.
- Um conjunto é dito Universal se ele contém todos os elementos que estão em discusão. Geralmente denotamos a este conjunto por A ou U.

A teoria de conjuntos se constrói então a partir destes três conceitos básicos: conjunto, elemento e relação de pertenência.

Vamos denotar por letras maiúsculas $A,\ B,\ C\ldots$ aos conjuntos e por minúsculas $a,\ b, c\ \ldots$ aos elementos dos conjuntos.

Obs. Se definirmos os elementos de um conjunto a partir de uma propriedade de seus elementos de forma descuidada, podemos ter problemas. Por exemplo, considere

$$\mathscr{O} = \{X \text{ conjunto},\ X \notin X\}$$

Observamos que dizer que X conjunto tal que $X \notin X$ ou $X \in X$ não é absurdo. De fato

- Seja A o conjunto de todos os carros, como A não é um carro temos que $A \notin A$.
- Seja A o conjunto das ideias abstratas é um conjunto que, por ser uma ideia abstrata, é um conjunto satisfaz $A \in A$.

No entanto, $\mathscr{O}$ não é um conjunto. De fato, se assumimos que é conjunto, observamos que:

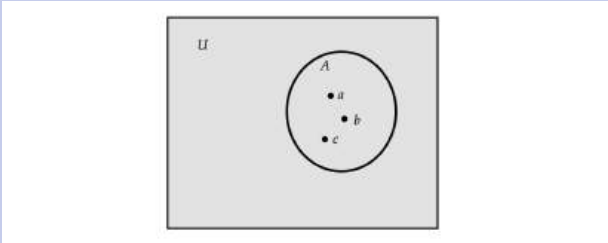
- Se $\mathscr{O} \in \mathscr{O}$ então, da definição, $\mathscr{O} \notin \mathscr{O}$.
- Por outro lado $\mathscr{O} \notin \mathscr{O}$ então $\mathscr{O} \in \mathscr{O}$. O que é uma contradição.

O problema parte de admitir que $\mathscr{O}$ é conjunto. Este problema é conhecido como Paradoxo de Russel. Em particular, decorre disto que a coleção de todos os conjuntos não é um conjunto.

Para representar gráficamente conjuntos,utilizamos os diagramas de Venn (em honor a John Venn, matemático inglés). Para isso começamos desenhando um quadrado que é o conjunto universal U e dentro dele utilizamos

uma linha fechada que não possui auto-intersecção para representar o conjunto A. Dentro dela, utilizando pontos, representamos os elementos do conjunto A.

■ **Exemplo 6.1** Se $A = \{a,\ b,\ c\}$ então



■

Outra forma de representar os conjuntos é por listando todos seus elementos entre chaves. Por exemplo,

$$A = \{a,b,c,d,\ \ldots\}.$$

Estudaremos na próxima seção a teoria de conjuntos com mais detalhes.

Definição 6.1 Uma função proposicional é uma sentença declarativa que possui uma variável aberta e, ao substituir esta variável por um valor se torna uma proposição.

A função proposicional esta composta de um conjunto A e de um juizo declarativo $P(x)$, onde x é a variável, que toma valores em um conjunto A chamado universo discursivo.

O domínio de verdade de P é conjunto que denotamos por $\mathrm{Dom}(P)$ dado por

$$\mathrm{Dom}(P) = \{a \in A,\ P(a) \text{ é verdadeira}\}$$

Denotamos a função proposicional por $(A,P(x))$ ou simplesmente $P(x)$ quando damos por subentendido o conjunto A.

■ **Exemplo 6.2**
- $P(x) =$ "$x^2 = 9$" e $A = \mathbb{N}$. Seu dominio de verdade é $\mathrm{Dom}(P) = \{3\}$.
- $P(x) =$ "$x \leq 5$" e $A = \mathbb{N} \cup \{0\}$. Seu dominio de verdade é $\mathrm{Dom}(P) = \{0,1,2,3,4,5\}$.
- $P(x) =$ "x é o melhor time de futebol do mundo"e $A = \{\text{times de futebol}\}$. Seu dominio de verdade é $\mathrm{Dom}(P) = \{\text{Boca Juniors}\}$.

■

Se temos uma função proposicional $(A,P(x))$ podemos nos perguntar para quantos elementos de A a proposição é verdadeira?. As respostas podem ser: todos, alguns, um e nenhum. Passamos agora a ver estes quantificadores.

Formalmente, se P é um proposição, existem dois quantificadores

- Quantificador universal (ou para todo): que é simbolizado por

  $$\forall x,\ P$$

  e se lê, "para todo x temos P".

  A proposição assim construída será verdadeira se para todo valor que pode assumir x, P for verdadeira.
- Quantificador de existencia (ou existe): que é simbolizado por

  $$\exists\, x,\ P = \neg[\forall\, x,\ \neg P]$$

  e se lê, "existe x tal que P" ou "não é verdade que para todo x temos que P é falsa".

  A proposição assim construída será verdadeira se existe um valor que pode assumir x tal que P é verdadeira.

Com estes quantificadores construimos os chamados de **quantificadores delimitados** como segue: Seja $(A,P(x))$ uma função proposicional

- Quantificador Universal delimitado: **"Para todo x em A, $P(x)$ é verdadeira. "**
  A notação para esta expressão é

  $$\forall\, x \in A,\ P(x) := \forall x,\ [(x \in A) \Rightarrow P(x)].$$

  Neste caso a proposição é verdadeira se $P(x)$ é verdadeira para todo $x \in A$.
- Quantificador Existencial delimitado: **"Existe x em A tal que $P(x)$ é verdadeira. "**
  A notação para esta expressão é

  $$\exists\, x \in A,\ P(x) := \exists x,\ [(x \in A) \wedge P(x)].$$

  Neste caso a proposição é verdadeira se $P(x)$ é verdadeira para, pelo menos, um $x \in A$.
- Quantificador Existencial de unicidade delimitado: **"Existe um único x em A tal que $P(x)$ é verdadeira."**
  A notação para esta expressão é
  $\exists!\, x \in A,\ P(x) \equiv \exists\, x \in A, \forall\, y \in A, [(P(x) \wedge P(y)) \Leftrightarrow (x = y)]$.
  Neste caso a proposição é verdadeira se $P(x)$ é verdadeira para um único $x \in A$.

Obs. Os quantificadores permitem transformam uma função proposicional em uma proposição.

■ **Exemplo 6.3**

- A proposição:

  $$P = \text{"para todo número real } x\text{, se } x^2 = 1 \text{ então } x \in \{-1,1\}\text{"}$$

  pode ser escrita

  $$P = \forall\, x,\ x \in \mathbb{R} \Rightarrow (x^2 = 1 \Rightarrow x \in \{-1,1\})$$

  a negação dela seria

  $$\begin{aligned} \neg P &= \exists\, x,\ x \in \mathbb{R} \wedge \neg[x^2 = 1 \Rightarrow x \in \{-1,1\}] \\ &= \exists\, x,\ x \in \mathbb{R} \wedge (x^2 = 1) \wedge [x \notin \{-1,1\}] \end{aligned}$$

- A proposição:

  $$P = \text{"existe um número real } x \text{ tal que } x^2 = 1 \text{ e } x \in \{-1,1\}\text{"}$$

  pode ser escrita

  $$P = \exists\, x,\ x \in \mathbb{R} \wedge \{(x^2 = 1) \wedge [x \in \{-1,1\}]\}.$$

  Sua negação dela seria

  $$\begin{aligned} \neg P &= \forall\, x,\ \neg\left[\, x \in \mathbb{R} \wedge \{(x^2 = 1) \wedge [x \in \{-1,1\}]\}\right] \\ &= \forall\, x,\ x \notin \mathbb{R} \vee (x^2 \neq 1) \vee [x \notin \{-1,1\}]. \end{aligned}$$

- A proposição:

  $$P = \text{"Existe um número natural maior que 5"}$$

  pode ser escrita

  $$P = \exists x,\ x \in \mathbb{N} \wedge (x > 5).$$

  Sua negação seria

  $$\neg P = \forall x,\ x \in \mathbb{N} \Rightarrow (x \leq 5).$$

- A proposição:

  $$P = \text{"Todo número natural divisível por 2 é par"}$$

pode ser escrita

$$P = \forall\, x,\ x \in \mathbb{N} \Rightarrow (\ 2|x\ \Rightarrow\ x \text{ é par.})$$

Sua negação seria

$$\neg P = \exists\, x,\ x \in \mathbb{N} \wedge \neg(\ 2|x\ \Rightarrow\ x \text{ é par.})$$

■

Para negar as proposições construidas com quantificadores temos a seguinte regra de De Morgan que segue da definição: Dada P uma proposição temos

$$\begin{aligned} \neg[\forall x,\ P] &= \neg[\neg(\exists\, x, (\neg P))] \\ &= \exists\, x,\ (\neg P). \end{aligned}$$

Da regra acima, decorre a seguinte regra:

$$\begin{aligned} \neg[\exists\, x,\ P] &= \neg[\exists\, x,\ \neg(\neg(P))] \\ &= \neg[\neg(\forall x,\ \neg P)] \\ &= \forall x,\ \neg P. \end{aligned}$$

Com isto, podemos mostrar que

$$\begin{aligned} \neg[\exists\, x \in A,\ P(x)] &= \neg[\exists\, x,\ (x \in A \wedge P(x))] \\ &= \forall\, x,\ [\neg(x \in A) \vee \neg P(x)] \\ &= \forall\, x,\ \neg(x \in A) \vee \neg P(x) \\ &= \forall\, x.\ (x \in A) \Rightarrow \neg P(x) \\ &= \forall x \in A,\ \neg P(x). \end{aligned}$$

e que

$$\begin{aligned} \neg[\forall\, x \in A,\ P(x)] &= \exists\, x,\ \neg[(x \in A \Rightarrow P(x))] \\ &= \exists\, x,\ \neg[\neg(x \in A) \vee P(x)] \\ &= \exists\, x,\ (x \in A) \wedge (\neg P(x)) \\ &= \exists\, x \in A,\ \neg P(x). \end{aligned}$$

Chegamos assim nas seguintes regras:

- $\neg[\forall\, x \in A,\ P(x)] = \exists\, x \in A,\ \neg P(x)$
- $\neg[\exists\, x \in A,\ P(x)] = \forall\, x \in A,\ \neg P(x)$

■ **Exemplo 6.4** Considere as seguintes funções proposicionais:

- a)

  "Existe $x \in \mathbb{R}$ tal que $x^2 + 1 = 16$."

  Escrevemos

  $$\exists x \in \mathbb{R},\ x^2 + 1 = 16$$

  e sua negação

  $$\begin{aligned} \neg[\exists x \in \mathbb{R},\ x^2 + 1 = 16] &= \forall x \in \mathbb{R},\ \neg(x^2 + 1 = 16) \\ &= \forall x \in \mathbb{R},\ x^2 + 1 \neq 16. \end{aligned}$$

- b)

"para todo $x \in \mathbb{R}$ tal que $x^2 - 1 = 24$ temos $x + 1 \geq 6$."

Escrevemos

$$\forall x \in \mathbb{R},\ x^2 + 1 = 16 \Rightarrow x + 1 \geq 6$$

e sua negação

$$\begin{aligned} \neg[\forall x \in \mathbb{R},\ x^2+1 = 16 \Rightarrow x+1 \geq 6] &= \exists\, x \in \mathbb{R},\ \neg(x^2+1 = 16 \Rightarrow x+1 \geq 6) \\ &= \exists\, x \in \mathbb{R},\ \neg[\neg(x^2+1 = 16) \vee (x+1 \geq 6)] \\ &= \exists\, x \in \mathbb{R},\ (x^2+1 = 16) \wedge \neg(x+1 \geq 6) \\ &= \exists\, x \in \mathbb{R},\ (x^2+1 = 16) \wedge (x+1 < 6). \end{aligned}$$

■

A demonstração das proposições com quantificadores pode ser feita de forma direta ou provando que sua negação é falsa.

■ **Exemplo 6.5** • $\forall\, x \in (1, +\infty),\ x < x^2$.

Seja $x > 1$ então

$$x^2 = x \cdot x > x \cdot 1 = x$$

• $\exists x \in \mathbb{N}$ tal que $2x > 201$.
Seja $x = 101$ então $2(101) = 202 > 201$.

■

No caso de querermos demonstrar a falsidade das proposições

• com quantificador universal: se utiliza o método de contraexemplo. Ou seja, para mostrar que

$$\forall x \in A,\ P(x)$$

é falsa se procura um elemento $a \in A$ tal que $\neg P(a)$ é verdadeira. Tal elemento, se existir, recebe o nome de contraexemplo.

• com quantificador existêncial: se prova diretamente a não existência do elemento ou se prova que a negação dela é verdadeira.

■ **Exemplo 6.6** • $\forall\, x \in (0, +\infty),\ x < x^2$.

Seja $x = 1/2$ então

$$x^2 = \frac{1}{4} < \frac{1}{2} = x$$

portanto a proposição é falsa.

• $\exists x \in (0, 100)$ tal que $2x > 201$.

– Direto: Se $0 < x < 100$ então $0 < 2x < 200$ portanto $2x < 200 < 201$. de onde a proposição é falsa.

– Negação: provamos que

$$\begin{aligned} \neg[\exists x \in (0,100),\ 2x > 201] &= \forall x \in (0,100), \neg[2x > 201] \\ &= \forall x \in (0,100), 2x \leq 201. \end{aligned}$$

De fato, se $0 < x < 100$ então $0 < 2x < 200 \leq 201$. Portanto a negação da proposição é verdadeira e, consequêntemente, a proposição é falsa.

■

Com isto podemos construir a seguinte tabela que relaciona como mostrar que a veracidade ou falsidade das proposições com um quatificador.

Proposição	Quando é Verdadeira	Quando é Falsa
$\forall\, a \in A,\ P(a)$	Para todo $a \in A$ $P(a)$ é verdadeira	Existe $a \in A$ para o qual $P(a)$ é falsa.
$\exists\, a \in A,\ P(a)$	Existe $a \in A$ para o qual $P(a)$ é verdadeira	Para todo $a \in A$ $P(a)$ é falsa.

Observamos que nada temos falado das proposições com o quantificador $\exists!$. Isto porque ele é construido a partir da conjunção de duas proposições com quantificadores.

Passamos a estudar proposições com dois quantificadores. De modo geral, estas proposições podem-se resumir a quatro casos. Dada $P(a,b)$ uma função proposicional em um universo U e $A,\ B$ conjuntos em U, temos as seguintes proposições

- $\forall\, a \in A,\ \forall\, b \in B,\ P(a,b)$.
- $\forall\, a \in A,\ \exists\, b \in B,\ P(a,b)$.
- $\exists\, a \in A, \forall\, b \in B,\ P(a,b)$.
- $\exists\, a \in A, \exists\, b \in B,\ P(a,b)$.

Obs. É fácil ver que

$$\forall\, a \in A,\ \forall\, b \in B,\ P(x,y) = \forall\, b \in B,\ \forall\, a \in A,\ P(a,b).$$

De fato se para todo $a \in A$ temos $\forall\, b \in B, P(a,b)$ então $P(a,b)$ é verdadeira para todo $a \in A$ e $b \in B$. De onde segue que para todo $b \in B$ temos que $\forall\, a \in A,\ P(a,b)$ é veraddeira. De forma similar, temos que

$$\exists\, a \in A, \exists\, b \in B,\ P(a,b) = \exists\, b \in B,\ \exists\, a \in A,\ P(a,b).$$

Pois se existe $a \in A$ tal que $\exists\, b \in B,\ P(a,b)$ é verdadeira, então existem $a \in A$ e $b \in B$ tal que $P(a,b)$ é verdadeira. De onde segue que é equivalente a dizer que existe $b \in B$ tal que $\exists\, A \in A,\ P(a,b)$ é verdadeira.

No entanto, observamos que, de forma geral, temos

$$\forall\, a \in A,\ \exists\, b \in B,\ P(a,b) \neq \exists\, b \in B,\ \forall\, a \in A,\ P(a,b).$$

Sabemos que

$$\{\exists\, b \in B,\ \forall\, a \in A,\ P(a,b)\} \vdash \forall\, a \in A,\ \exists\, b \in B,\ P(a,b).$$

De fato, se existe b tal que para todo $a \in A$ temos que $P(a,b)$ é verdadeira então para todo $a \in A$ existe $b \in B$ tal que $P(a,b)$ é verdadeira.

Para ver que o argumento

$$\{\forall\, a \in A,\ \exists\, b \in B,\ P(a,b)\} \vdash \exists\, b \in B,\ \forall\, a \in A,\ P(a,b).$$

não é válido de forma geral, mostramos dois contraexemplos:

- Seja $A = \{\text{Doenças}\}$ e $B = \{\text{Médico especialista}\}$ e $P(a,b)$ a função proposicional

  $$P(a,b) = \text{"}b \text{ trata a doença } a\text{"}.$$

  E agora observemos as proposições:

  $$Q_1 : \forall\, a \in A,\ \exists\, b \in B,\ P(a,b) \quad = \quad \begin{array}{l}\text{Para toda doença existe um médico}\\ \text{especialista que trata ela.}\end{array}$$

  e, por outro lado

  $$Q_2 : \exists\, b \in B,\ \forall\, a \in A,\ P(a,b) \quad = \quad \begin{array}{l}\text{existe um médico especialista}\\ \text{que trata todas as doenças.}\end{array}$$

  Claramente Q_1 não implica lógicamente Q_2 pois Q_1 é verdadeira e Q_2 é falsa.
- Considere $A = (0,\infty)$ e $B = (0,\infty)$ e $P(a,b) : a \cdot b = 1$. Claramente para todo $a \in (0,\infty)$ existe $b \in (0,\infty)$ tal que $a \cdot b = 1$. No entanto vejamos que não existe $b \in B$ tal que para todo $a \in A$ temos $a \cdot b = 1$. Para provar isto fazemos pelo absurdo. Assuma que um tal $b \in (0,\infty)$ existe então para $a = 1$ temos

  $$b \cdot a = b \cdot 1 = 1 \ \Rightarrow\ b = 1$$

  de onde $b = 1$. Por outro lado, para $a = 2$ temos

  $$b \cdot a = b \cdot 2 = 1 \ \Rightarrow\ b = \frac{1}{2}.$$

  De onde b assuma dois valores diferentes, o que é um absurdo.

Como no caso de um quantificador, indicamos como negar proposições com mais de um quantificador. Assim, utilizamos o visto acima junto as Leis de De Morgan para obter

- $$\begin{aligned}\neg[\forall\, x\in A,\ \forall\, y\in B,\ P(x,y)] &= \exists\, x\in A,\ \neg[\forall\, y\in B,\ P(x,y)]\\ &= \exists\, x\in A,\ \exists\, y\in B,\ \neg P(x,y)\end{aligned}$$
- $$\begin{aligned}\neg[\forall\, x\in A,\ \exists\, y\in B,\ P(x,y)] &= \exists\, x\in A,\ \neg[\exists\, y\in B,\ P(x,y)]\\ &= \exists\, x\in A,\ \forall\, y\in B,\ \neg P(x,y)\end{aligned}$$
- $$\begin{aligned}\neg[\exists\, x\in A,\ \forall\, y\in B,\ P(x,y)] &= \forall\, x\in A,\ \neg[\forall\, y\in B,\ P(x,y)]\\ &= \forall\, x\in A, \exists\, y\in B,\ \neg P(x,y)\end{aligned}$$
- $$\begin{aligned}\neg[\exists\, x\in A,\ \exists\, y\in B,\ P(x,y)] &= \forall\, x\in A,\ \neg[\exists\, y\in B,\ P(x,y)]\\ &= \forall\, x\in A, \forall\, y\in B,\ \neg P(x,y)\end{aligned}$$

Com isto podemos construir a seguinte tabela que relaciona como mostrar que a veracidade ou falsidade das proposições com dois quatificadores.

Proposição	Quando é Verdadeira	Quando é Falsa
$\forall\, a\in A,\ \forall\, b\in B,\ P(a,b)$	Para todo $a\in A$ e $b\in B$ tal que $P(a,b)$ é verdadeira	Existe um $a\in A$ e um $b\in B$ tal que $P(a,b)$ é falsa.
$\forall\, a\in A,\ \exists\, b\in B,\ P(a,b)$	Para todo $a\in A$ existe um $b\in B$ tal que $P(a,b)$é verdadeira	Existe um $a\in A$ tal que para todo $b\in B$ temos $P(a,b)$ é falsa .
$\exists\, a\in A,\ \forall\, b\in B,\ P(a,b)$	Existe um $a\in A$, para todo $b\in B$, tal que $P(a,b)$ é verdadeira	Para todo $a\in A$ existe $b\in B$ tal que $P(a,b)$ é falsa.
$\exists\, a\in A,\ \exists\, b\in B,\ P(a,b)$	Existe um $a\in A$ e existe um $b\in B$ tal que $P(a,b)$ é verdadeira	Para todo $a\in A$ e para todo $b\in B$ temos $P(a,b)$ é falsa.

■ **Exemplo 6.7** • Considere a proposição

$P =$"As necessidades da maioria se sobrepõem às necessidades da minoria"

Vamos a descrever a proposição com quantificadores. Começamos definindo o conjunto

$A = \{$necessidades das pessoas$\}$

e as funções proposicionais

$M(x) =$ "x é necessidade da maioria" $\quad N(x) =$ "x é necessidade da minoria"

$P(x,y) =$ "x se sobrepõe a y".

Então escrevemos

$$\forall\, x\in A,\ \forall\, y\in A,\ (M(x)\wedge N(y))\Rightarrow P(x,y).$$

A negação é

$$\begin{aligned}&\neg[\forall\, x\in A,\ \forall\, y\in A,\ (M(x)\wedge N(y))\Rightarrow P(x,y)]\\ =\ &\exists\, x\in A, \neg[\,\forall\, y\in A,\ (M(x)\wedge N(y))\Rightarrow P(x,y)]\\ =\ &\exists\, x\in A,\ \exists\, y\in A,\ \neg[(M(x)\wedge N(y))\Rightarrow P(x,y)]\\ =\ &\exists\, x\in A,\ \exists\, y\in A,\ [(M(x)\wedge N(y))\wedge\neg P(x,y)],\end{aligned}$$

que poderíamos traduzir a

$\neg P =$"Há uma necessidade de muitos que se não se sobrepõe a uma necessidade de poucos."

Observamos que há uma forma melhor de descrever esta proposição definindo o que significa ser maioria e minoria, em função da cardinalidade do conjunto de pessoas.

- Considere a proposição

  "Existe um barbeiro que barbeia a todos aqueles, e somente aqueles que não se barbeiam."

  Se consideramos o conjunto dos homens como sendo A e as funções proposicionais

  $$P(x) = \text{"}x \text{ é barbeiro"}, \qquad B(x,y) = \text{"}x \text{ barbeia } y\text{"}$$

  Destacamos que
  - "existe um barbeiro": $\exists\, x \in A,\ P(x)$
  - "que barbeia a todos aqueles, e somente aqueles, que não se barbeiam": pode ser traduzida como $\forall\, y \in A,\ \neg B(y,y) \Leftrightarrow B(x,y)$.

  A frase então, pode ser escrita

  $$Q = \exists\, x \in A,\ \{P(x) \wedge [\forall\, y \in A, \neg B(y,y) \Leftrightarrow B(x,y)]\}\text{"}$$

  Veremos abaixo que isto pode ser escrito como

  $$Q = \exists\, x \in A,\ \forall\, y \in A,\ [P(x) \wedge (\neg B(y,y) \Leftrightarrow B(x,y)))]\text{"}$$

  A negação de P é

  $$\neg Q = \forall\, x \in A,\ \exists\, y \in A,\ \{\neg P(x) \vee \neg[\neg B(y,y) \Leftrightarrow B(x,y)]\}\text{"}$$

  que é igual a

  $$\neg Q = \forall\, x \in A,\ \exists\, y \in A,\ \{\neg P(x) \vee [B(y,y) \Leftrightarrow B(x,y)]\}\text{"}.$$

- Consideramos o universo como sendo os números reais

  "Para todo $\varepsilon > 0$ existe um $\delta > 0$ para todo $x \in \mathbb{R}$ tal que se $|x-2| < \delta$ então $|2\cdot x - 4| < \varepsilon$."

  Escrevemos

  $$\forall\, \varepsilon > 0,\ \exists\, \delta > 0,\ \forall\, x \in \mathbb{R}\ |x-2| < \delta \Rightarrow |2\cdot x - 4| < \varepsilon$$

  Observamos que

  $$\varepsilon > 0 = \varepsilon \in (0,\infty), \quad \text{e que} \quad \delta > 0 = \delta \in (0,\infty).$$

  A negação da proposição P é

  $$\begin{aligned}
  &\neg[\forall \varepsilon > 0,\ \exists\, \delta >,\ \forall\, x \in \mathbb{R}\ ,\ |x-2| < \delta \Rightarrow |2\cdot x - 4| < \varepsilon] \\
  &= \exists\, \varepsilon > 0\ \neg[\ \exists\, \delta > 0,\ \forall\, x \in \mathbb{R}\ ,\ |x-2| < \delta \Rightarrow |2\cdot x - 4| < \varepsilon] \\
  &= \exists\, \varepsilon > 0\ \ \forall\, \delta > 0,\ \neg[\ \forall\, x \in \mathbb{R}\ |x-2| < \delta \Rightarrow |2x - 4| < \varepsilon] \\
  &= \exists\, \varepsilon > 0\ \ \forall\, \delta > 0,\ \exists x \in \mathbb{R},\ \neg[\ |x-2| < \delta \Rightarrow |2x - 4| < \varepsilon] \\
  &= \exists\, \varepsilon > 0\ \ \forall\, \delta > 0,\ \exists x \in \mathbb{R},\ \neg[\neg(|x-2| < \delta) \vee (|2\cdot x - 4| < \varepsilon)] \\
  &= \exists\, \varepsilon > 0,\ \forall\, \delta > 0,\ \exists x \in \mathbb{R},\ (\neg(\neg(|x-2| < \delta)) \wedge (\neg[|2\cdot x - 4| < \varepsilon]) \\
  &= \exists\, \varepsilon > 0,\ \forall\, \delta > 0,\ \exists x \in \mathbb{R},\ (|x-2| < \delta) \wedge (|2\cdot x - 4| \geq \varepsilon).
  \end{aligned}$$

  Portanto

  $$\neg P = \exists\, \varepsilon > 0,\ \forall \delta > 0,\ \exists x \in \mathbb{R},\ (|x-2| < \delta) \wedge (|2\cdot x - 4| \geq \varepsilon).$$

  A proposição é verdadeira. De fato, se para todo $x \in \mathbb{R}$ tal que
  $|x-2| < \delta$ temos $|2\cdot x - 4| < 2\cdot\delta$
  Então dado $\varepsilon > 0$ existe $\delta = \frac{\varepsilon}{2} > 0$ tal que se $x \in \mathbb{R}$ tal que $|x-2| < \delta$ então $|2\cdot x - 4| < \varepsilon$.
  Temos provado assim que

  $$\forall\, \varepsilon > 0,\ \exists\, \delta > 0.\ \forall\, x \in \mathbb{R},\ |x-2| < \delta \Rightarrow |2\cdot x - 4| < \varepsilon.$$

- Para mostrar a falsidade de uma proposição com mais de um quantificador se procede de forma similar ao caso de um, isto é, se mostra um contraexemplo ou se prova que a negação dela é verdadeira.
  Vamos mostrar que a proposição

  $$\forall \varepsilon > 0,\ \exists\ \delta > 0,\ \forall\, x \in \mathbb{R},\ 0 < |x| < \delta \Rightarrow |\sin(1/x) - 1| < \varepsilon$$

  é falsa. Novamente observamos que

  $$\varepsilon > 0 = \varepsilon \in (0,\infty), \quad \text{e que} \quad \delta > 0 = \delta \in (0,\infty).$$

  Para mostrar a falsidade de P provamos que a negação dela é verdadeira, isto é

  $$\begin{aligned} & \neg[\forall \varepsilon > 0, \exists \delta > 0,\ \forall\, x \in \mathbb{R},\ 0 < |x| < \delta \Rightarrow |\sin(1/x) - 1| < \varepsilon] \\ = \ & \exists\ \varepsilon > 0\ \neg[\exists \delta > 0,\ \forall\, x \in \mathbb{R},\ 0 < |x| < \delta \Rightarrow |\sin(1/x) - 1| < \varepsilon] \\ = \ & \exists\ \varepsilon > 0,\ \forall\ \delta > 0,\ \neg[\ \forall\, x \in \mathbb{R},\ 0 < |x| < \delta \Rightarrow |\sin(1/x) - 1| < \varepsilon] \\ = \ & \exists\ \varepsilon > 0\ \forall\ \delta > 0,\ \exists x \in \mathbb{R},\ \neg[0 < |x| < \delta \Rightarrow |\sin(1/x) - 1| < \varepsilon] \\ = \ & \exists\ \varepsilon > 0\ \forall\ \delta > 0,\ \exists x \in \mathbb{R},\ (0 < |x| < \delta) \wedge |\sin(1/x) - 1| \geq \varepsilon \end{aligned}$$

  Provamos então que

  $$\neg P = \exists\ \varepsilon > 0\ \forall\ \delta > 0,\ \exists x \in \mathbb{R},\ (0 < |x| < \delta) \wedge |\sin(1/x) - 1| \geq \varepsilon$$

  De fato, considere $\varepsilon = \frac{1}{2}$ e $\delta > 0$ qualquer. Seja $k \in \mathbb{N}$ tal que $\delta > \frac{1}{k}$ e, portanto, $0 < |x_0| = \frac{1}{k\pi} < \delta$ e

  $$|\sin(1/x_0) - 1| = 1 > \frac{1}{2}.$$

  Portanto, temos mostrado que existe $\varepsilon = 1/2$ tal que para todo δ existe $x_0 = \frac{1}{k\pi} \in \mathbb{R}$ com $\frac{1}{k\pi} < \delta$ tal que $0 < |x_0| < \delta$ e

  $$|\sin(1/x_0) - 1| = 1 > \frac{1}{2}.$$

  Portanto $\neg P$ é verdadeira e P é falsa.

■

A seguir vamos estudar em detalhe como se comportam os quantificadores com respeito a conjunção e disjunção de proposições. Isto pode ser omitido em uma primeira leitura.

Proposição 6.1 Sejam $(U, P(x))$ e $(U, Q(x))$ duas funções proposicionais. Então

- $\forall\, x \in A,\ (P(x) \wedge Q(x)) = (\forall\, x \in A,\ P(x)) \wedge (\forall\, x \in A,\ Q(x))$
- $\exists\, x \in A,\ (P(x) \vee Q(x)) = (\exists\, x \in A,\ P(x)) \vee (\exists\, x \in A,\ Q(x))$

Demonstração. Mostramos cada uma delas por separado. Para a primeira observamos que se $P(a) \wedge Q(a)$ é verdadeira para todo $a \in A$ se, e somente se temos que $P(a)$ é verdadeira e $Q(a)$ é verdadeira (da tabela de verdade da conjunção) e isto ocorre se, e somente se, $P(a)$ é verdadeira para todo $a \in A$ e $Q(a)$ é verdadeira para todo $a \in A$. Isto prova a primeira identidade.

Para provar a segunda, utilizamos a que acabamos de provar junto com a dupla negação.

$$\begin{aligned} \exists\, x \in A,\ (P(x) \wedge Q(x)) &= \neg[\neg(\exists\, x \in A,\ (P(x) \wedge Q(x)))] \\ &= \neg[\forall\, x \in A,\ \neg(P(x) \vee Q(x)] \\ &= \neg[\forall\, x \in A,\ (\neg P(x)) \wedge (\neg Q(x))] \\ &= \neg[(\forall\, x \in A,\ \neg P(x)) \wedge (\forall\, x \in A,\ \neg Q(x))] \\ &= \neg[(\forall\, x \in A,\ \neg P(x))] \vee \neg[(\forall\, x \in A,\ \neg Q(x))] \\ &= (\exists\, x \in A,\ P(x)) \vee (\exists\, x \in A,\ Q(x)). \end{aligned}$$

■

Corolário 6.1 Seja P uma proposição e $(U, Q(x))$ uma função proposicional. Então
- $\forall\, x \in A,\ (P \wedge Q(x)) = P \wedge (\forall x \in A,\ Q(x))$,
- $\exists x \in A,\ (P \vee Q(x)) = P \vee (\exists\, x \in A,\ Q(x))$.

Demonstração. Segue inmediato da proposição anterior ao observar que

$$\forall\, x \in A,\ P = P \qquad \exists\, x \in A,\ P = P.$$

■

Obs. A proposição $\exists!\ a \in A,\ P(a)$ pode ser escrita

$$\begin{aligned} \exists!\ a \in A,\ P(a) &= \exists\, a \in A,\ [P(a) \wedge (\ \forall\, b \in A,\ (P(b) \Leftrightarrow (b = a)\ )] \\ &= \exists\, a \in A,\ \forall\, b \in B,\ [P(a) \wedge (P(b) \Leftrightarrow (b = a)\ )] \end{aligned}$$

e sua negação é

$$\begin{aligned} \neg[\exists!\ a \in A,\ P(a)] &= \neg\{\exists\, a \in A,\ \forall\, b \in B,\ [P(a) \wedge (P(b) \Leftrightarrow (b = a)\ )]\} \\ &= \forall\, a \in A,\ \exists\, b \in A,\ \neg[P(a) \wedge (P(b) \Leftrightarrow (b = a)\ )] \\ &= \forall\, a \in A,\ \exists\, b \in A,\ (\neg P(a)) \vee \neg[(P(b) \Leftrightarrow (b = a)\ )] \\ &= \forall\, a \in A,\ \exists\, b \in A,\ (\neg P(a)) \vee \neg[\ [(\neg P(b)) \vee (b = a)] \wedge [\neg(b = a) \vee P(b)]\ ] \\ &= \forall\, a \in A,\ \exists\, b \in A,\ (\neg P(a)) \vee [P(b) \wedge (b \neq a)] \vee [(b = a) \wedge \neg P(b)] \\ &= \forall\, a \in A,\ \exists\, b \in A,\ \neg P(a) \vee [P(b) \wedge (b \neq a)] \end{aligned}$$

onde, na última linha, temos utilizado que

$$[(b = a) \wedge \neg P(b)] = \neg P(a).$$

Proposição 6.2 Sejam $(U, P(x))$ e $(U, Q(x))$ duas funções proposicionais. Então
- $[(\forall\, x \in A,\ P(x)) \vee (\forall\, x \in A,\ Q(x))] \Rightarrow \forall\, x \in A,\ (P(x) \vee Q(x))$
- $\exists\, x \in A,\ (P(x) \wedge Q(x)) \Rightarrow [(\exists\, x \in A,\ P(x)) \wedge (\exists\, x \in A,\ Q(x))]$

As recíprocas, em geral, são falsas.

Demonstração. Para a primeira observamos que se

$$[(\forall\, x \in A,\ P(x)) \vee (\forall\, x \in A,\ Q(x))]$$

é verdadeira então para todo $a \in A$ temos, da tabela da verdade da disjunção, que $P(a)$ é verdadeira ou $Q(a)$ é verdadeira, de onde $Q(a) \vee P(a)$ é verdadeira. Portanto $\forall\, x \in A,\ (P(x) \vee Q(x))$ é verdadeira.

Para a segunda, observamos que

$$\begin{aligned} \exists\, x \in A,\ (P(x) \wedge Q(x)) &= \neg[\neg(\exists\, x \in A,\ (P(x) \wedge Q(x)))] \\ &= \neg[\forall\, x \in A,\ \neg(P(x) \wedge Q(x))] \\ &= \neg[\forall\, x \in A,\ (\neg P(x) \vee \neg Q(x))] \\ &\Rightarrow \neg[(\forall\, x \in A,\ \neg P(x)) \vee (\forall\, x \in A,\ \neg Q(x))] \quad \text{(contrapositiva do item anterior)} \\ &= [(\exists\, x \in A,\ P(x)) \wedge (\exists\, x \in A,\ Q(x))] \end{aligned}$$

Para ver que as recíprocas são falsas em geral defina

$P(x) =$ "x é um número natural par"

$Q(x) =$ "x é um número natural impar"

Então

$$\forall\, x \in \mathbb{N},\ (P(x) \vee Q(x)) \quad \text{e} \quad [(\exists\, x \in \mathbb{N},\ P(x)) \wedge (\exists\, x \in \mathbb{N},\ Q(x))]$$

são verdadeiras e, no entanto,

$$[(\forall\, x \in \mathbb{N},\ P(x)) \vee (\forall\, x \in \mathbb{N},\ Q(x))] \quad \text{e} \quad \exists\, x \in \mathbb{N},\ (P(x) \wedge Q(x))$$

são falsas. ■

Corolário 6.2 Seja P uma proposição e $(U, Q(x))$ uma função proposicional. Então
- $\forall\, x \in A,\ (P \vee Q(x)) = P \vee (\forall x \in A,\ Q(x))$,
- $\exists x \in A,\ (P \wedge Q(x)) = P \wedge (\exists\, x \in A,\ Q(x))$.

Demonstração. Para o primeiro item observamos que somente devemos mostrar que

$$\forall\, x \in A,\ (P \vee Q(x)) \Rightarrow P \vee (\forall x \in A,\ Q(x)).$$

Mas isto é imediato pois se $\forall\, x \in A,\ (P \vee Q(x))]$ é verdadeira então pode acontecer que P é verdadeira, em cujo caso $P \vee (\forall x \in A,\ Q(x))$ ou P é falsa, em cujo caso $Q(x)$ é verdadeira, e portanto, $P \vee (\forall x \in A,\ Q(x))$ é verdadeira.

Para o segundo item, utilizamos qua regra que acabamos de provar vale junto com a dupla negação. Vemos então que

$$\begin{aligned}
\exists x \in A,\ (P \wedge Q(x)) &= \neg[\neg(\exists x \in A,\ (P \wedge Q(x)))] \\
&= \neg[\forall x \in A,\ \neg(P \wedge Q(x))] \\
&= \neg[\forall x \in A,\ (\neg P) \vee (\neg Q(x))] \\
&= \neg[\ (\neg P) \vee (\forall x \in A,\ \neg Q(x))] \\
&= P \wedge (\exists\, x \in A,\ Q(x)).
\end{aligned}$$

■

Corolário 6.3 Sejam $(U, P(x))$ e $(U, Q(x))$ funções proposicionais. Então
- $[(\forall\, x \in A,\ P(x)) \vee (\forall\, x \in A,\ Q(x))] = \forall\, x \in A,\ \forall y \in A\ (P(x) \vee Q(y))$
- $\exists\, x \in A,\ \exists\, y \in A\ (P(x) \wedge Q(y)) = [(\exists\, x \in A,\ P(x)) \wedge (\exists\, x \in A,\ Q(x))]$

Demonstração. Para o primeiro observamos que

$$\begin{aligned}
\forall\, x \in A,\ \forall y \in A\ (P(x) \vee Q(y)) &= \forall\, x \in A,\ [P(x) \vee\ (\forall y \in A,\ Q(y))] \\
&= (\forall\, x \in A,\ P(x) \vee\ (\forall y \in A,\ Q(y))] \\
&= (\forall\, x \in A,\ P(x) \vee\ (\forall x \in A,\ Q(x))].
\end{aligned}$$

De forma similar se demostra a segunda identidade. ■

Em elaboração

7. Conjuntos

Vimos, na seção anterior, uma breve introdução à teoria de conjuntos. Em particular, observamos que a teoria chega rápidamente em paradoxos se for feita de forma descuidada. Para evitar esta problemática, no século XX foram propostos varios sistemas axiomáticos com o intuito de promover uma teoria dos conjuntos sem os paradoxos da teoria ingênua dos conjuntos (como o paradoxo de Russell). Um destes sistemas, são os axiomas de Zermelo-Fraenkel (em homenagem aos matemáticos Ernst Zermelo e Abraham Fraenkel).

Sabemos, no entanto, por um resultado de K. Gödel (ver, para um leitura compreensível, o trabalho *Godel's Proof* de E. Nagel e J. Newman) que estes axiomas não podem ser provados dentro da teoria e, mais ainda, se queremos uma teoria livre de paradoxos (isto é, consistente) então teremos uma teoria incompleta (isto é, incapaz de provar todas suas afirmações), pois teremos que postular um número infinito de axiomas para evitar paradoxos visto que a aparição deles é inevitável. O postulado de axiomas se traduz, na prática, em um humilde reconhecimento da nossa limitação na capacidade de determinar se as afirmações dos paradoxos são verdadeiras ou falsas.

Nessa linha, enunciamos os axiomas de Zermelo-Fraenkel que formam a base da teoria de conjuntos, embora não nos deteremos muito sobre eles. O objetivo de fazer isto é que o estudante tome ciência da existência de uma teoria mais profunda sobre conjuntos e que deve ser levada em consideração ao se fazer um estudo sério e cuidadoso.

Nos axiomas de Zermelo-Fraenkel todo elemento é visto como sendo também um conjunto. Os axiomas são:

- **Axioma da existência:** Existe o conjunto vazio, que é conjunto que não possui elementos.
- **Axioma da extensão:** Dois conjuntos são iguais se eles têm os mesmos elementos.
- **Axioma da regularidade:** Todo conjunto não-vazio A contém algúm elemento x tal que A e x são disjuntos, isto é $\{A\}$ e $\{x\}$ são disjuntos.
- **Axioma de especificação:** Se U é um conjunto e $P(x)$ é uma função proposicional com domínio em A, então existe um subconjunto A de U que contém os elementos a de U para o qual $P(a)$ é verdadeira.
- **Axioma do par:** Se A e B são conjuntos (não necessariamente distintos) então existe um conjunto no qual A e B são elementos.
- **Axioma da união:** Para todo conjunto A existe um conjunto U tal que todo elemento que pertence a um elemento de A é um elemento de U.
- **Axioma da substituição:** Seja $P(a,b)$ uma propriedade do tipo: para todo a existe um b para o qual $P(a,b)$ é verdadeira, então: Para todo conjunto A existe um conjunto B tal que para todo $a \in A$ existe $b \in B$ para o qual $P(a,b)$ é verdadeira.
- **Axioma do infinito:** Existe um conjunto U que tem o conjunto vazio como elemento, e que, para todo

elemento y, ele contém seu sucessor $s(y) = y \cup \{y\}$.

- **Axioma da potência:** Para todo conjunto A existe um conjunto B que tem como elementos todo subconjunto de A.

Observamos que:

- No axioma da existência podemos considerar o conjunto como sendo aquele que contém o conjunto vazio, isto é, $A = \{\{\emptyset\}\}$.
- O axioma da regularidade garante nenhum conjunto pode ser membro dele mesmo, isto é, que não existe conjuntos da forma $X = \{X\}$ e, junto ao axioma do par, também não existem conjuntos da forma $X = \{\emptyset, X\}$.

  Demonstração. Se $A \in A$ então $\{A\}$ não contém um elemento disjunto de $\{A\}$ pois o único elemento é o próprio A, contradizendo o axioma da regularidade. ■

- No axioma de especificação, a restrição a U é necessária para evitar o paradoxo de Russell e suas variantes. Em outras palavras, a função proposicional precisa, primeiramente, do contexto no qual vai ser formulada.
- Do axioma do par decorre que se temos dois elementos então existe um conjunto que os contém.
- O axioma da substituição garante a existência do conjunto imagem para uma função (veremos isto depois).
- O axioma do infinito garante a existência de um conjunto infinito. Como sabemos que existe um conjunto então temos a existência dos sucessores.
- O axioma da potência garante a existência do conjunto de partes.

De forma geral, podemos determinar conjuntos de duas formas

- Por extensão: Nesta forma se listam todos os elementos do conjunto. Em geral se colocam, entre chaves, como por exemplo

  $$A = \{1, 2, 3, 4, 5, \cdots\}$$

  $$B = \{2, 4, 6, 8, 10, \cdots\}$$

- Por compreensão (ou axioma de especificação): Definindo uma propriedade de seus elementos. Como o conjunto de verdade $\mathrm{Dom}(P)$ de uma função proposicional $P(x)$ que tem como domínio um conjunto universal. Assim se $(U, P(x))$ temos que o conjunto $\mathrm{Dom}(P)$ é

  $$\mathrm{Dom}(P) = \{x \in U,\ P(x) \text{ é verdadeira}\}.$$

  Por exemplo

  $$A = \{n,\ n \text{ é um número natural}\}$$

  $$B = \{n,\ n \text{ é um número natural par}\}$$

Obs. Se temos um universo U, podemos "definir"o conjunto vazio por especificação como sendo o conjunto

$$\emptyset = \{x \in U,\ x \neq x\}.$$

Como não existe nenhum objeto diferente de si mesmo, o conjunto não tem elementos.

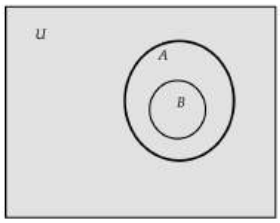
Agora, passamos definir a terminologia básica

Definição 7.1 Sejam A e B conjuntos. Dizemos que

- A é subconjunto de B, ou que A está incluso em B, e escrevemos $A \subset B$ se todo elemento de A é um elemento de B, isto é,

  $$A \subset B \Leftrightarrow (\forall x \in A,\ x \in B)$$

  Gráficamente:



- o conjunto A está incluido propriamente em B (que denotamos por $A \subsetneq B$) ou que A é um subconjunto próprio de B, se

$$[(A \subset B) \wedge (A \neq B)],$$

isto é, todo elemento de A pertence a B e existe um elemento $b \in B$ que não pertence a A.
- $(A = B) \Leftrightarrow [(A \subset B) \wedge (B \subset A)]$ (Isto, de fato, é consequência do Axioma da Extensão).

■ **Exemplo 7.1** Sejam

$$A = \{x \in \mathbb{R},\ |x+3| < 5\}$$

$$B = \{x \in \mathbb{R},\ x \geq -8\}$$

vamos mostrar que $A \subset B$. Temos que mostrar que

$$\forall x \in A \Rightarrow x \in B$$

é verdadeira. Se $x \in A$ temos que

$$\begin{aligned} |x+3| < 5 &\Leftrightarrow -5 < x+3 < 5 \\ &\Leftrightarrow -8 < x < 2 \ \Rightarrow\ x \geq -8 \end{aligned}$$

e, portanto, $x \in B$. Como o x escolhido pode ser qualquer elemento de A temos que vale para todo $x \in A$. O que prova o resultado. ■

Teorema 7.1 Para qualquer conjunto A temos que $\emptyset \subset A$.

Demonstração. Assumimos que o universo do discurso U é conhecido. A função proposicional

$$P(x) = "x \in \emptyset \Rightarrow x \in A".$$

é verdadeira para todo $a \in U$, pois $a \in \emptyset$ é sempre falsa e, consequêntemente,

$$P(a) = (a \in \emptyset \Rightarrow a \in A)$$

tem que ser verdadeira. ■

Teorema 7.2 A inclusão de conjuntos é
- Reflexiva: $A \subset A$ para todo conjunto A.
- Transitiva: Sejam A e B conjuntos tais que $[(A \subset B) \wedge (B \subset C)]$ então $(A \subset C)$.
- Antisimétrica: Sejam A e B conjuntos tais que $[(A \subset B) \wedge (B \subset A)]$ então $(A = B)$.

Demonstração.
- Seja A um conjunto, então se $a \in A \Rightarrow a \in A$. Logo $A \subset A$.
- Assuma que $A \subset B$ e $B \subset C$. Então todo elemento $a \in A$ então $a \in B$, pois $A \subset B$, e como $B \subset C$ temos que $a \in C$, portanto $A \subset C$.
- Direto da definição de igualdade de conjuntos.

■

Teorema 7.3 A relação de igualdade de conjuntos é
- Reflexiva: $A = A$, para todo conjunto A.
- Simétrica: $(A = B) \Rightarrow (B = A)$.
- Transitiva: $[(A = B) \wedge (B = C)] \Rightarrow (A = C)$.

Demonstração.
- Reflexiva: Como $A \subset A$ segue inmediato do axioma da extensão.
- Simétrica: Como
$$\begin{aligned}(A = B) &\Leftrightarrow [(A \subset B) \wedge (B \subset A)] \\ &= [(B \subset A) \wedge (A \subset B)] \\ &\Leftrightarrow B = A.\end{aligned}$$
- Transitiva: $[(A = B) \wedge (B = C)] \Rightarrow (A = C)$.

■

Definição 7.2 Seja A um conjunto. O conjunto de partes de A, que denotamos por $\mathscr{P}(A)$, é aquele cujos elementos são os subconjuntos de A, isto é,

$$\mathscr{P}(A) = \{X,\ X \subset A\}.$$

Obs.
- Seja A um conjunto não vazio, então existe um elemento $a \in A$ e, portanto, $\{a\} \subset A$ e $\{a\} \in \mathscr{P}(A)$ de onde segue que $\mathscr{P}(A) \neq \emptyset$.
- Se $A \neq \emptyset$, observamos que $B = A \cup \mathscr{P}(A)$ é um conjunto não vazio com a seguinte propriedade: todo subconjunto $A' \subset A$ é um elemento e subconjunto de B.
De fato como A' é subconjunto de A temos que $A' \in \mathscr{P}(A)$ de onde $A' \in B$. Por outro lado, como A' é subconjunto de A temos que $A' \subset A$ de onde $A' \subset B$.

■ **Exemplo 7.2**
- Se $A = \{a,\ b,\ c\}$ então
$$\mathscr{P}(A) = \{\emptyset,\ \{a\},\ \{b\},\ \{c\},\ \{a,b\},\ \{a,c\},\ \{b,c\},\ A\}$$
- Se $A = \{1,\{1,2\},\{1,c\}\}$
$$\mathscr{P}(A) = \{\emptyset,\ \{1\},\ \{\{1,2\}\},\ \{\{1,c\}\},\ \{1,\ \{1,2\}\},\ \{1,\ \{1,c\}\},\ \{\{1,2\},\{1,c\}\},\ A\}$$

■

Obs. Dado $A \subset U$, o conjunto universal $\tilde{U}$ onde o conjunto de partes está não é o conjunto universal U onde A está. De fato, o conjunto $\tilde{U}$ não é conhecido e deve ser assumido pelo axioma da potência.

Teorema 7.4 Sejam A e B dois conjuntos. Então

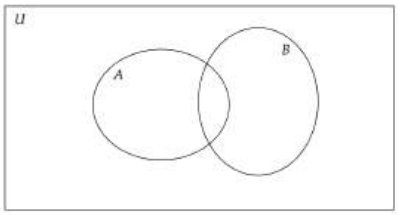
$$A \subset B \Leftrightarrow \mathscr{P}(A) \subset \mathscr{P}(B).$$

Demonstração. Temos que provar um bicondicional, então devemos provar
- $A \subset B \Rightarrow \mathscr{P}(A) \subset \mathscr{P}(B)$.
Se $X \in \mathscr{P}(A)$ então $X \subset A$ e $A \subset B$, então por um resultado anterior, $X \subset B$ e, consequêntemente $X \in \mathscr{P}(B)$.
- $(A) \subset \mathscr{P}(B) \Rightarrow A \subset B$.
Se $A \in \mathscr{P}(A) \subset \mathscr{P}$ então $A \in \mathscr{P}(B)$ portanto $A \subset B$.

■

Passamos a estudar as operações básicas da teoria de conjuntos. Sabemos, pelo axioma do par e da união, temos que dados dois conjuntos existe um conjunto U tal que A e B são subconjuntos de U. Assumimos então que conhecemos o conjunto universal U para as definições a seguir.

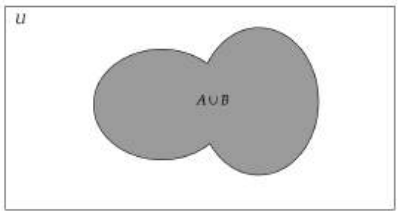
Definição 7.3 Sejam A e B dois conjuntos em um universo U.



- A união de A e B é o conjunto

$$A \cup B = \{x \in U,\ x \in A \vee x \in B\}$$

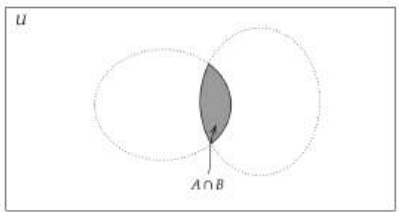
Gráficamente:



- A interseção de A e B é o conjunto

$$A \cap B = \{x \in U,\ x \in A \wedge x \in B\}$$

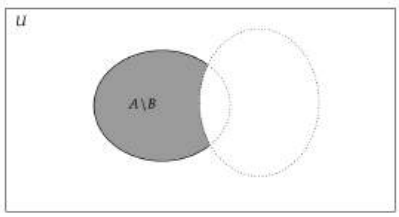
Caso $A \cap B = \emptyset$ dizemos que A e B são disjuntos.
Gráficamente:



- A diferença entre A e B é o conjunto

$$A \backslash B = \{x \in A,\ x \notin B\}$$

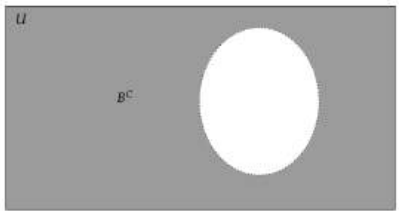
Gráficamente:



- O complemento de B em U é o conjunto

$$B^C = U \setminus B.$$

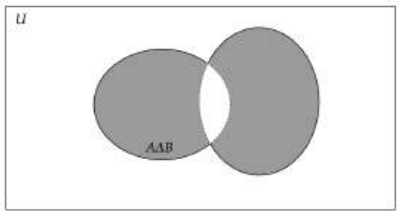
Gráficamente:



- A diferença simétrica entre A e B é o conjunto

$$A \Delta B = (A \setminus B) \cup (B \setminus A)$$

Gráficamente:



Teorema 7.5 A união e interseção de conjuntos satisfazem as seguintes propriedades

- Idempotente: $A \cup A = A$ e $A \cap A = A$ para todo conjunto A.
- Comutatividade: $A \cup B = B \cup A$ e $A \cap B = B \cap A$ para quaisquer conjuntos $A,\ B$.
- Asociatividade

$$A \cup (B \cup C) = (A \cup B) \cup C,$$

$$A \cap (B \cap C) = (A \cap B) \cap C.$$

- Distributividade: Para quaisquer conjuntos $A,\ B$ e C valem as seguintes identidades

$$A \cap (B \cup C) = (A \cap B) \cup (A \cap C),$$

$$A \cup (B \cap C) = (A \cup B) \cap (A \cup C).$$

Demonstração. • Idempotencia. Claramente $A \subset A \cup A$. Por outro lado

$$\begin{aligned} a \in A \cup A &\Leftrightarrow (a \in A) \vee (a \in A) \\ &\Leftrightarrow (a \in A) \end{aligned}$$

de onde segue que $A \cup A \subset A$. Logo $A = A \cup A$.
Para a segunda identidade, temos que $A \cap A \subset A$. Por outro lado

$$\begin{aligned} a \in A &\Leftrightarrow (a \in A) \wedge (a \in A) \\ &\Leftrightarrow (a \in A \cap A) \end{aligned}$$

de onde segue que $A \subset A \cap A$. Logo $A = A \cap A$.

- Comutatividade: Provamos uma, pois a outra é análoga.
$$\begin{aligned} x \in A \cap A &\Leftrightarrow (x \in A) \vee (x \in B) \\ &\Leftrightarrow (x \in B) \vee (x \in A) \\ &\Leftrightarrow x \in B \cap A. \end{aligned}$$
- Asociatividade: Novamente provamos uma, a outra é análoga.
$$\begin{aligned} x \in A \cup (B \cup C) &\Leftrightarrow (x \in A) \vee (x \in B \cup C) \\ &\Leftrightarrow (x \in A) \vee [(x \in B) \vee (x \in C)] \\ &\Leftrightarrow [(x \in A) \vee (x \in B)] \vee (x \in C)] \\ &\Leftrightarrow x \in (A \cup B) \cup C. \end{aligned}$$
- Distributividade: Novamente provamos uma pois a outra é análoga.

$$\begin{aligned} x \in A \cap (B \cup C) &\Leftrightarrow (x \in A) \wedge (x \in B \cup C) \\ &\Leftrightarrow (x \in A) \wedge [(x \in B) \vee (x \in C)] \\ &\Leftrightarrow [(x \in A) \wedge (x \in B)] \vee [(x \in A) \wedge (x \in C)] \\ &\Leftrightarrow (x \in A \cap B) \vee (x \in A \cap C) \\ &\Leftrightarrow x \in (A \cap B) \cup (A \cap C) \end{aligned}$$

■

Teorema 7.6 Sejam A e B dois conjuntos no universo U. Então
- $U^C = \emptyset$ e $\emptyset^C = U$.
- $A \cup A^C = U, A \cap A^C = \emptyset$.
- $\left(A^C\right)^C = A$.
- $A \subset B \Rightarrow B^C \subset A^C$.
- $(A \cup B)^C = A^C \cap B^C$
- $(A \cap B)^C = A^C \cup B^C$.
- $A \Delta B = B \Delta A$.

Demonstração.
- $U^C = \emptyset$: Claramente $\emptyset \subset U^C$. Assuma que $U^C \neq \emptyset$. Seja $x \in U^C$ então $x \notin U$ o que é uma contradição. Portanto $U^C = \emptyset$.
$\emptyset^C = U$: Claramente $\emptyset^C \subset U$. Por outro lado, se $x \in U$ então $x \notin \emptyset$ de onde $x \in \emptyset^C$, de onde segue que $U \subset \emptyset^C$. Logo $U = \emptyset^C$.
- $A \cup A^C = U$: De fato $A \cup A^C \subset U$ naturalmente. Seja $x \in U$ tal que $x \notin A$ então $x \in A^C$, portanto $x \in A \cup A^C$. De onde segue que $U \subset A \cup A^C$, e portanto $A \cup A^C = U$
$A \cap A^C = \emptyset$: Claramente $\emptyset \subset A \cap A^C$. Por outro lado se $A \cap A^C \neq \emptyset$ temos que existe $x \in A \cap A^C$ então $x \notin A$ e $x \notin A^C$. Como $A \cup A^C = U$ então $x \notin U$, o que é uma contradição. Portanto $A \cap A^C = \emptyset$.
- $\left(\left(A^C\right)\right)^C = A$:
$$\begin{aligned} x \in A &\Leftrightarrow \neg(x \in A^C) \\ A &\Leftrightarrow x \in (A^C)^C \quad (\text{pois } A \cup A^C = U). \end{aligned}$$
Logo $A = (A^C)^C$
- $A \subset B \Rightarrow B^C \subset A^C$: Assuma que $A \subset B$. Se $x \in B^C$ então $x \notin B$ de onde $x \notin A$. Portanto $x \in A^C$. Logo $B^C \subset A^C$.
- $(A \cup B)^C = A^C \cap B^C$:
$$\begin{aligned} x \in (A \cup B)^C &\Leftrightarrow \neg(x \in A \cup B) \\ &\Leftrightarrow \neg[(x \in A) \vee (x \in B)] \\ &\Leftrightarrow \neg(x \in A) \wedge \neg(x \in B)] \quad (\text{Lei de De Morgan}) \\ &\Leftrightarrow (x \in A^C) \wedge (x \in B^C) \\ &\Leftrightarrow x \in A^C \cap B^C \end{aligned}$$

- $(A\cap B)^C = A^C \cup B^C$:

$$\begin{aligned} x\in(A\cap B)^C &\Leftrightarrow \neg(x\in A\cap B)\\ &\Leftrightarrow \neg[(x\in A)\wedge(x\in B)]\\ &\Leftrightarrow \neg(x\in A)\vee\neg(x\in B)] \quad \text{(Lei de De Morgan)}\\ &\Leftrightarrow (x\in A^C)\vee(x\in B^C)\\ &\Leftrightarrow x\in A^C\cup B^C \end{aligned}$$

- A comutatividade segue da comutatividade da união: de fato

$$\begin{aligned} A\Delta B &= (A\backslash B)\cup(B\backslash A)\\ &= (B\backslash A)\cup(A\backslash B)\\ &= B\Delta A. \end{aligned}$$

■

Obs. Sejam $(P(x),U)$ e $(Q(x),U)$ duas funções proposicionais e considere os domínios de verdade

$$\text{Dom}(P)=\{x\in U,\ P(x)\text{ é verdadeira}\} \quad \text{e} \quad \text{Dom}(Q)=\{x\in U,\ Q(x)\text{ é verdadeira}\}$$

Então

- $\text{Dom}(P\vee Q)=\text{Dom}(P)\cup\text{Dom}(Q)$,
- $\text{Dom}(P\wedge Q)=\text{Dom}(P)\cap\text{Dom}(Q)$,
- $\text{Dom}(\neg P)=\text{Dom}(P)^C$,
- $\text{Dom}(P\wedge\neg Q)=\text{Dom}(P)\cap\text{Dom}(Q)^C=\text{Dom}(P)\backslash\text{Dom}(Q)$,
- $\text{Dom}(P\Rightarrow Q)=\text{Dom}(\neg P\vee Q)=\text{Dom}(P)^C\cup\text{Dom}(Q)$,
-

$$\begin{aligned} \text{Dom}(P\Leftrightarrow Q) &= \text{Dom}([P\Rightarrow Q]\wedge[Q\Rightarrow P])\\ &= [\text{Dom}(P)^C\cup\text{Dom}(Q)]\cap[\text{Dom}(P)\cup\text{Dom}(Q)^C]\\ &= [\text{Dom}(P)^C\cap(Ker(P)\cup\text{Dom}(Q)^C)]\cup[\text{Dom}(Q)\cap(\text{Dom}(P)\cup\text{Dom}(Q)^C)]\\ &= [\text{Dom}(P)^C\cap\text{Dom}(Q)^C]\cup[\text{Dom}(Q)\cap\text{Dom}(P)]\\ &= [\text{Dom}(P)\cup\text{Dom}(Q)]^C\cup[\text{Dom}(Q)\cap\text{Dom}(P)] \end{aligned}$$

8. Produto Cartesiano

Sejam A e B dois conjuntos e considere $a \in A$ e $b \in B$ definimos o par ordenado (a,b) como sendo o conjunto formado por

$$(a,b) = \{\{a\},\{a,b\}\}.$$

Neste par ordenado o elementos a e b recebem o nome de primeira e segunda coordenadas, respectivamente.

Obs.

- O par ordenado (a,b) pode ser visto como um subconjunto de $\mathscr{P}(A \cup B)$ e é, portanto, um elemento do conjunto $\mathscr{P}(\mathscr{P}(A \cup B))$.
- A relação de ordem fica clara pois

$$\{a\} \subset \{a,b\}.$$

Teorema 8.1

$$(a,b) = (c,d) \Leftrightarrow [(a = c) \wedge (b = d)].$$

Demonstração. Temos que provar o bicondicional.

- $(a,b) = (c,d) \Rightarrow [(a = c) \wedge (b = d)]$:
  Se $(a,b) = (c,d)$ temos duas posibilidades

$$\{a\} = \{c\} \wedge \{a,b\} = \{c,d\}$$

ou

$$\{a\} = \{c,d\} \wedge \{a,b\} = \{c\}$$

Se a primeira é válida temos que $a = c$ da primeira igualdade e da segunda segue que $b = d$.
Se a segunda é válida temos, da primeira igualdade que $a = c$ e $a = d$ e da segunda que $c = b$ e $c = a$.
Portanto $a = c$ e $b = d$.

- $[(a = c) \wedge (b = d)] \Rightarrow (a,b) = (c,d)$: segue da definição.

■

Corolário 8.1 Se $(a,b) = (b,a) \Rightarrow a = b$

Demonstração. Pelo visto no teorema anterior se $(a,b) = (b,a)$ então $a = b$. ■

Definição 8.1 O produto cartesiano dos conjuntos A e B é o conjunto

$$A \times B = \{(a,b) \in \mathscr{P}(\mathscr{P}(A \cup B)),\ a \in A,\ b \in B\}$$

Quando $A = B$ denotamos $A \times A$ por A^2.

■ **Exemplo 8.1**

- Seja $A = \{a,b,c\}$ e $B = \{1,2\}$ então

$$A^2 = \{(a,a),\ (a,b),\ (a,c),\ (b,a),\ (b,b),\ (b,c)\ (c,a),\ (c,b),\ (c,c)\}.$$

$$A \times B = \{(a,1),\ (a,2),\ (b,1),\ (b,2),\ (c,1),\ (c,2)\}.$$

$$B \times A = \{(1,a),\ (2,a),\ (1,b),\ (2,b),\ (1,c),\ (2,c)\}.$$

$$B^2 = \{(1,1),\ (1,2),\ (2,1),\ (2,2)\}$$

- Seja $A = \mathbb{R}$ e $B = \mathbb{N}$ então

$$A^2 = \{(x,y),\ (x \in \mathbb{R}) \wedge (y \in \mathbb{R})\}$$

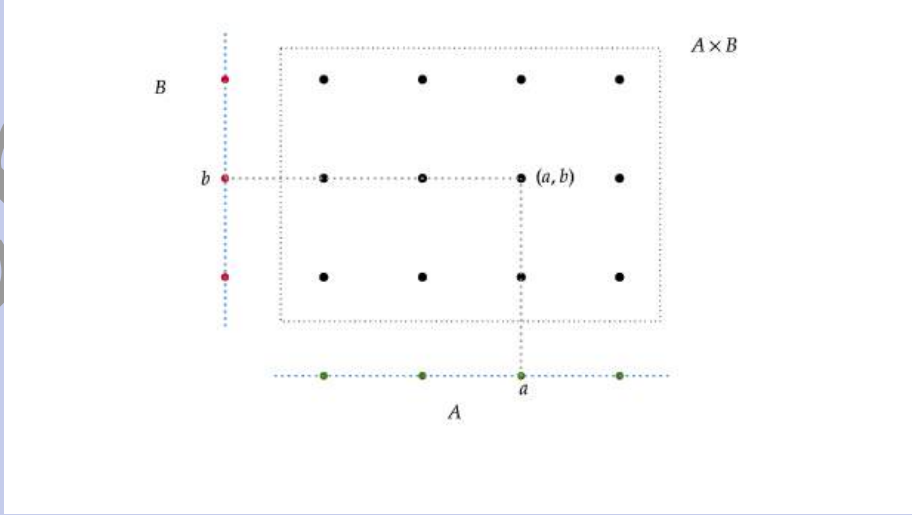
$$A \times B = \{(x,n),\ (x \in \mathbb{R}) \wedge (n \in \mathbb{N})\}$$

$$B \times A = \{(n,x),\ (x \in \mathbb{R}) \wedge (n \in \mathbb{N})\}$$

$$B^2 = \{(n,m),\ (n \in \mathbb{N}) \wedge (m \in \mathbb{N})\}$$

■

Vimos como representar os elementos de um conjunto A. Para representar gráficamente os elementos de um produto cartesiano $A \times B$ se utilizam, geralmente dois eixos, perpendiculares, um para o eixo A e outro para o B. Os elementos (a,b) são os pontos dentro do quadrado do desenho



Teorema 8.2 Sejam A, B e C conjuntos

- $A \times B = \emptyset \Leftrightarrow [A = \emptyset \vee B = \emptyset]$.
- $A \times (B \cup C) = (A \times B) \cup (A \times C)$
- $A \times (B \cap C) = (A \times B) \cap (A \times C)$

- $A \times (B \backslash C) = (A \times B) \backslash (A \times C)$

Obs. Utilizando a equivalência da contrapositiva, podemos ver que,

$$\begin{aligned} P \Leftrightarrow Q &= (P \Rightarrow Q) \wedge (Q \Rightarrow P) \\ &= (\neg Q \Rightarrow \neg P) \wedge (\neg P \Rightarrow \neg Q) \\ &= (\neg P \Rightarrow \neg Q) \wedge (\neg Q \Rightarrow \neg P) \\ &= \neg P \Leftrightarrow \neg Q. \end{aligned}$$

Demonstração. • Mostramos a proposição equivalente: $A \times B \neq \emptyset \Leftrightarrow A \neq \emptyset \wedge B \neq \emptyset$.
Primeiramente observamos que se $A \neq \emptyset$ e $B \neq \emptyset$ então $A \cup B \neq \emptyset$ e existem $a \in A$ e $b \in B$. Do axioma do par e da união $\{a\}$ e $\{a,b\}$ são subconjuntos de $A \cup B$ de onde

$$(a,b) = \{\{a\},\{a,b\}\} \in \mathscr{P}(\mathscr{P}(A \cup B)).$$

Portanto $A \times B \neq \emptyset$. Agora,

$$\begin{aligned} A \times B \neq \emptyset &\Leftrightarrow \exists\, (a,b) \in A \times B \\ &\Leftrightarrow \exists\, a \in A \wedge \exists\, b \in B \\ &\Leftrightarrow A \neq \emptyset \wedge B \neq \emptyset. \end{aligned}$$

- $A \times (B \cup C) = (A \times B) \cup (B \times C)$:

$$\begin{aligned} (a,b) \in A \times (B \cup C) &\Leftrightarrow (a \in A) \wedge (b \in B \cup C) \\ &\Leftrightarrow (a \in A) \wedge [(b \in B) \vee (b \in C)] \\ &\Leftrightarrow [(a \in A) \wedge (b \in B)] \vee [(a \in A) \wedge (b \in C)] \\ &\Leftrightarrow [(a,b) \in A \times B] \vee [(a,b) \in A \times C] \\ &\Leftrightarrow (a,b) \in (A \times B) \cup (A \times C). \end{aligned}$$

- $A \times (B \cap C) = (A \times B) \cap (B \times C)$:

$$\begin{aligned} (a,b) \in A \times (B \cap C) &\Leftrightarrow (a \in A) \wedge (b \in B \cap C) \\ &\Leftrightarrow (a \in A) \wedge [(b \in B) \wedge (b \in C)] \\ &\Leftrightarrow (a \in A) \wedge (a \in A) \wedge [(b \in B) \wedge (b \in C)] \\ &\Leftrightarrow [(a \in A) \wedge (b \in B)] \wedge [(a \in A) \wedge (b \in C)] \\ &\Leftrightarrow [(a,b) \in A \times B] \wedge [(a,b) \in A \times C] \\ &\Leftrightarrow (a,b) \in (A \times B) \cap (A \times C). \end{aligned}$$

- $A \times (B \backslash C) = (A \times B) \backslash (A \times C)$:

$$\begin{aligned} (a,b) \in A \times (B \backslash C) &\Leftrightarrow (a \in A) \wedge (b \in B \backslash C) \\ &\Leftrightarrow (a \in A) \wedge [(b \in B) \wedge \neg(b \in C)] \\ &\Leftrightarrow (a \in A) \wedge (a \in A) \wedge [(b \in B) \wedge \neg(b \in C)] \\ &\Leftrightarrow [(a \in A) \wedge (b \in B)] \wedge [(a \in A) \wedge \neg(b \in C)] \\ &\Leftrightarrow [(a,b) \in A \times B] \wedge \neg[(a,b) \in A \times C] \\ &\Leftrightarrow (a,b) \in (A \times B) \backslash (A \times C). \end{aligned}$$

■

Observamos que, utilizando o produto cartesiano, podemos fazer as seguintes reduções.

Corolário 8.2 Sejam $(U,P(x))$ e $(U,Q(x))$ funções proposicionais. Então
- $\forall\, x \in A,\ \forall\, y \in B,\ P(x,y) = \forall (x,y) \in A \times B,\ P(x,y)$.
- $\exists\, x \in A,\ \exists\, y \in B,\ P(x,y) = \exists\, (x,y) \in A \times B,\ P(x,y)$.

Demonstração. Se, para todo $(a,b) \in A \times B$ temos que $P(a,b)$ é verdadeira então seja $a \in A$ e $b \in B$ temos que $(a,b) \in A \times B$ e, portanto, $P(a,b)$ é verdadeira. De onde para todo $a \in A$ e para todo $b \in B$ temos que $P(a,b)$ é verdadeira.

Por outro lado, para todo $a \in A$ e para todo $b \in B$ temos que $P(a,b)$ é verdadeira então dado $(a,b) \in A \times B$ temos que, como $a \in A$ e $b \in B$, $P(a,b)$ é verdadeira, de onde para todo $(a,b) \in A \times B$ temos que $P(a,b)$ é verdadeira.

Para provar a segunda identidade utilizamos que a primeira junto com a negação de quantificadores.

$$\begin{aligned}
\exists\, x \in A,\ \exists\, y \in B,\ P(x,y) &= \neg[\neg(\exists\, x \in A,\ \exists\, y \in B,\ P(x,y))] \\
&= \neg[\,\forall\, x \in A, \neg(\,\exists\, y \in B,\ P(x,y))] \\
&= \neg[\,\forall\, x \in A,\ \forall\, y \in B,\ \neg(P(x,y))] \\
&= \neg[\,\forall\, (x,y) \in A \times B,\ \neg(P(x,y))] \\
&= \exists\, (x,y) \in A \times B,\ \neg[\neg(P(x,y))] \\
&= \exists\, (x,y) \in A \times B,\ P(x,y).
\end{aligned}$$

■

9. Familia de conjuntos

Considere uma familia de conjuntos em um universo U dada por

$$\mathscr{F} = \{A_i,\ i \in \mathbf{I}\} \subset \mathscr{P}(U),$$

para $\mathbf{I}$ um conjunto de índices.

Dizemos que a familia $\mathscr{F}$ é finita se $\mathbf{I}$ estiver em correspondência um a um com um subconjunto $\{1,\ldots,n_0\}$ do conjunto dos números naturais e, neste caso, podemos também escrever por extenso, isto é

$$\mathscr{F} = \{A_1,\ldots,A_{n_0}\}.$$

Definição 9.1 Seja $\mathscr{F} = \{A_i,\ i \in \mathbf{I}\}$ uma familia de conjuntos de um universo U. Definimos

- a união da familia como sendo o conjunto

$$\cup_{i\in\mathbf{I}} A_i = \{x \in U,\ \exists\, i \in \mathbf{I},\ x \in A_i\}$$

- a interseção da familia como sendo o conjunto

$$\cap_{i\in\mathbf{I}} A_i = \{x \in U,\ x \in A_i\ \forall\, i \in \mathbf{I}\}$$

Teorema 9.1 Seja $\mathscr{F} = \{A_i,\ i \in \mathbf{I}\}$ uma familia de conjuntos de um universo U. Uma familia de conjuntos. Então

- $A_k \subset \cup_{i\in\mathbf{I}} A_i,\ \forall k \in \mathbf{I}$
- $\cap_{i\in\mathbf{I}} A_i \subset A_k,\ \forall k \in \mathbf{I}$
- $(\cup_{i\in\mathbf{I}} A_i)^C = \cap_{i\in\mathbf{I}} A_i^C$
- $(\cap_{i\in\mathbf{I}} A_i)^C = \cup_{i\in\mathbf{I}} A_i^C$

Demonstração.

- Se $x \in A_k$ então existe $k \in \mathbf{I}$ tal que $x \in A_k$, portanto $x \in \cup_{i\in\mathbf{I}} A_i$. Logo $A_k \subset \cup_{i\in\mathbf{I}} A_i,\ \forall\, k \in \mathbf{I}$.
- Se $x \in \cap_{i\in\mathbf{I}} A_i$ então $x \in A_i$ para todo $i \in \mathbf{I}$, portanto $x \in A_k,\ \forall k \in \mathbf{I}$.

- Observamos que

$$\begin{aligned} x \in (\cup_{i\in \mathbf{I}} A_i)^C &\Leftrightarrow \neg(x \in \cup_{i\in \mathbf{I}} A_i,) \\ &\Leftrightarrow \neg(\exists i \in \mathbf{I},\ x \in A_i,) \\ &\Leftrightarrow \forall i \in \mathbf{I},\ \neg(x \in A_i) \\ &\Leftrightarrow \forall i \in \mathbf{I},\ x \in A_i^C \\ &\Leftrightarrow \forall i \in \cap_{i\in \mathbf{I}} A_i^C. \end{aligned}$$

  Logo

$$(\cup_{i\in \mathbf{I}} A_i)^C = \cap_{i\in \mathbf{I}} A_i^C.$$

- Observamos que

$$\begin{aligned} x \in (\cap_{i\in \mathbf{I}} A_i)^C &\Leftrightarrow \neg(x \in \cap_{i\in \mathbf{I}} A_i,) \\ &\Leftrightarrow \neg(\forall i \in \mathbf{I},\ x \in A_i,) \\ &\Leftrightarrow \exists i \in \mathbf{I},\ \neg(x \in A_i) \\ &\Leftrightarrow \exists i \in \mathbf{I},\ x \in A_i^C \\ &\Leftrightarrow \forall i \in \cup_{i\in \mathbf{I}} A_i^C. \end{aligned}$$

  Logo

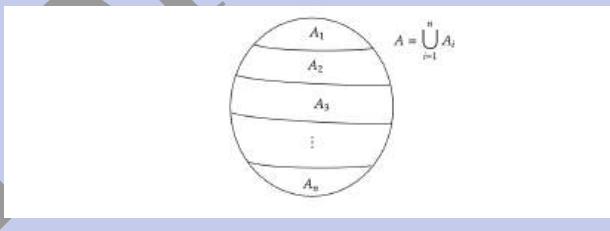
$$(\cap_{i\in \mathbf{I}} A_i)^C = \cup_{i\in \mathbf{I}} A_i^C.$$

■

Definição 9.2 Seja X um conjunto e $\mathscr{F} = \{A_i,\ i \in \mathbf{I}\}$ uma familia de subconjuntos de X. Dizemos que $\mathscr{F}$ é uma partição de X se

- $A_i \neq \emptyset$ para todo $i \in \mathbf{I}$
- $A_i \cap A_j = \emptyset$ para todo $i,\ j$ tais que $i \neq j$.
- $X = \cup_{i\in \mathbf{I}} A_i$.

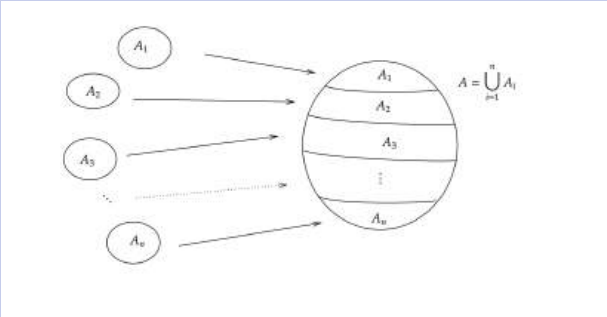
Gráficamente uma partição $\mathscr{F} = \{A_i,\ i \in \mathbf{I}\}$ de um conjunto A pode ser representada por



Se temos uma familia de conjuntos não vazios $\mathscr{F} = \{A_i,\ i \in \mathbf{I}\}$ tais que $A_i \cap A_j = \emptyset$ para $i \neq j$ então podemos formar o conjunto

$$A = \bigcup_{i\in I} A_i.$$

Neste caso, de forma natural, $\mathscr{F}$ é uma partição de A. Gráficamente



■ **Exemplo 9.1** • Se $X=\mathbb{N}$ então a familia $\mathscr{F}=\{A_1,A_2\}$ em que

$$A_1=\{n\in\mathbb{N},\ n \text{ é par}\}\quad A_2=\{n\in\mathbb{N},\ n \text{ é ímpar}\},$$

é uma partição.

- Se $X=\{a,\ b,\ c,\ d,\ e,\ g,\ f,\ h\}$ então a familia $\mathscr{F}=\{A_1,A_2,A_3,A_4\}$ em que

$$A_1=\{a,\ b,\ c\}\quad A_2=\{d\}\quad A_3=\{e,\ h\}\quad A_4=\{g,\ h\}\quad A_5=\{f\},$$

é uma partição.

Se $X=\mathbb{R}$ então a familia $\mathscr{F}=\{C_n,\ n\in\mathbb{N}\}$ em que

$$C_n=\{x\in\mathbb{R},\ n\leq|x|<n+1\}.$$

é uma partição. ■

Seja $\mathscr{F}=\{A_i,\ i\in\mathbf{I}\}$ uma familia finita para $\mathbf{I}=\{1,\cdots,n\}$. Definimos o produto cartesiano

$$X=A_1\times\cdots\times A_n$$

pelo processo a seguir:

- para $n=2$ temos definido $A_1\times A_2$.
- conhecido $A_1\times\cdots\times A_k$ para $k\geq 2$ temos que

$$A_1\times\cdots\times A_k\times A_{k+1}=(A_1\times\cdots\times A_k)\times A_{k+1}.$$

O processo acima conclui em $k=n$. Como notação, temos que os elementos do produto $A_1\times\cdots\times A_k\times A_{k+1}$ são escritos

$$((a_1,\ldots,a_k),a_{k+1})=(a_1,\ldots,a_k,a_{k+1}).$$

No caso em que todos os conjuntos que são membros da familia $\mathscr{F}$ sejam iguais, isto é,

$$\mathscr{F}=\{A_i,\ i\in\mathbf{I}\}\quad\text{com}\quad A_i=A,\quad\forall\, i\in\mathbf{I}=\{1,\cdots,n\},$$

denotamos

$$A^n=\overbrace{A\times\cdots\times A}^{n \text{ vezes}}.$$

Obs. Se a familia de conjuntos for finita, isto é for da forma $\mathscr{F}=\{A_1,\ldots,A_n\}$ então se todos os $A_i\neq\emptyset$ então podemos aplicar o axioma da união e do par n vezes e assim provar a existência das $n-$uplas $(a_1,\ldots,a_n)$. De onde $A_1\times\cdots\times A_n\neq\emptyset$. Isto pode ser feito para todo $n\in\mathbb{N}$ aplicando o proceso de indução.

Obs. De modo geral, para uma familia arbitrária de conjuntos $\mathscr{F}=\{A_i,\ i\in\mathbf{I}\}$ o produto cartesiano pode ser definido como sendo uma familia de funções

$$\prod_{i\in\mathbf{I}}A_i=\{f:\mathbf{I}\Rightarrow\cup_{i\in\mathbf{I}}A_i,\ f(i)\in A_i\}.$$

Se a familia for finita isto é $\mathbf{I}=\{1,\ldots,n\}$ para $n\in\mathbb{N}$ veremos (quando vejamos funções bijetoras) que o produto cartesiano assim definido é de certa igual ao conjunto definido acima.

■ **Exemplo 9.2** Considere a familia $\mathscr{F} = \{A_1, A_2, A_3\}$ em que

$$A_1 = A_2 = A_3 = \{a,b\} = A$$

Então

$$A^2 = A_1 \times A_2 = \{(a,a),(a,b),(b,a),(b,b)\}$$

e

$$\begin{aligned} A^3 &= A_1 \times A_2 \times A_3 \\ &= \{((a,a),a),((a,b),a),((b,a),a),((b,b),a),((a,a),b),((a,b),b),((b,a),b),((b,b),b)\} \\ &= \{(a,a,a),(a,b,a),(b,a,a),(b,b,a),(a,a,b),(a,b,b),(b,a,b),(b,b,b)\}. \end{aligned}$$

■

10. Relações

Dados A e B dois conjuntos quaisquer, estudamos formas de corresponder elementos de A com elementos de B. Tais correspondências deve conter a informação dos dois elementos então o lugar mais natural para começar esse estudo é no produto cartesiano $A \times B$.

Definição 10.1 Sejam A e B dois conjuntos.

- Uma relação de A em B é um subconjunto R do produto cartesiano $A \times B$, isto é $R \subset A \times B$.
- Neste caso, o conjunto A é dito conjunto de partida da relação e o conjunto B é dito conjunto de chegada da relação.
- Dizemos que $a \in A$ está relacionado com $b \in B$, e o denotamos por aRb ou $a \sim b$, se $(a,b) \in R$.
- No caso em que $A = B$ dizemos que R é uma relação em A.

Obs.

- Como vimos na definição, uma relação de A em B é um subconjunto R do produto cartesiano $A \times B$, portanto uma relação pode ser visto como um elemento do conjunto de partes $\mathscr{P}(A \times B)$.
- Em particular a relação correspondente a $\emptyset \subset A \times B$ é conhecida como relação nula.

■ **Exemplo 10.1**

- Seja A é o conjunto formado por um proposições $\{P_1, \ldots, P_n\}$ e de todas aquelas formadas a partir de conjunções, negações e disjunções de um número finito delas. Definimos a relação

$$R = \{(P,Q) \in A^2,\ P \Rightarrow Q \text{ é verdadeira}\}.$$

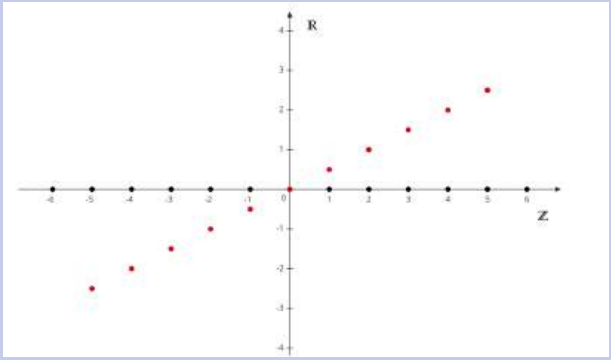
- Seja $A = \{\text{subconjuntos de um conjunto } \mathscr{U}\}$ e $W \subset A^2$ um subcojunto qualquer. Definimos a relação

$$R = \{(U,V) \in A^2,\ U \times V \subset W\}.$$

- Sejam $A = \mathbb{Z}$ e $B = \mathbb{R}$. Definimos a relação

$$R = \{(n,x) \in \mathbb{Z} \times \mathbb{R},\ (2 \cdot x = n) \wedge (-5 \leq n \leq 5)\} \subset \mathbb{Z} \times \mathbb{R}.$$

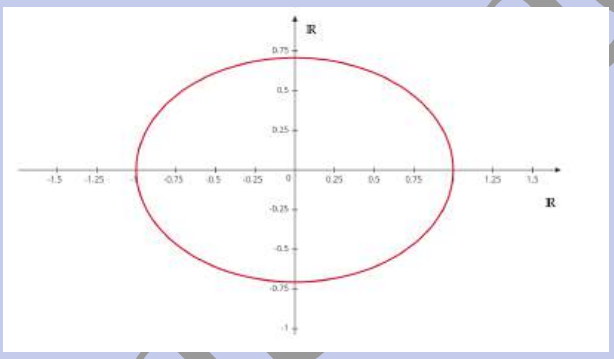
Gráficamente, a relação é o conjunto de pontos que está em vermelho.



- Sejam $A = \mathbb{R}$ e $B = \mathbb{R}$. Definimos a relação

$$R = \{(x,y) \in \mathbb{R} \times \mathbb{R},\ x^2 + 2 \cdot y^2 = 1\} \subset \mathbb{R} \times \mathbb{R}.$$

Gráficamente, a relação é o conjunto de pontos que está em vermelho.



■

Definição 10.2 Seja $R \subset A \times B$ uma relação de A em B.

- O domínio da relação é o conjunto

$$\text{Dom}(R) = \{a \in A,\ \exists\, b \in B,\ (a,b) \in R\}.$$

- A imagem da relação é o conjunto

$$\text{Img}(R) = \{b \in B,\ \exists\, a \in A,\ (a,b) \in R\}$$

■ **Exemplo 10.2**

- Seja A é o conjunto formado por um proposições $\{P_1, \ldots, P_n\}$ e de todas aquelas formadas a partir de conjunções, negações e disjunções de um número finito delas. Considere a relação

$$R = \{(P,Q) \in A^2,\ P \Rightarrow Q \text{ é verdadeira}\}.$$

Então

$$\text{Dom}(R) = A \quad \text{Img}(R) = A$$

- Seja $A = \{\text{subconjuntos de um conjunto } \mathscr{U}\}$, $W \subset A^2$ e a relação

$$R = \{(U,V) \in A^2,\ U \times V \subset W\}.$$

Então

$$\text{Dom}(R) = \{U \in A,\ \exists\, W \in A,\ (U,V) \in R\}, \quad \text{Img}(R) = \{V \in A,\ \exists\, U \in A,\ (U,V) \in R\}$$

- Sejam $A = \mathbb{Z}$, $B = \mathbb{R}$ e a relação

$$R = \{(n,x) \in \mathbb{Z} \times \mathbb{R},\ (2x = n) \wedge (-5 \leq n \leq 5)\} \subset \mathbb{Z} \times \mathbb{R}.$$

Então

$$\mathrm{Dom}(R) = \{-5,\ -4,\ -3,\ -2,\ -1,\ 0,\ 1,\ 2,\ 3,\ 4,\ 5\}$$

$$\mathrm{Img}(R) = \{-2{,}5,\ -2,\ -1{,}5,\ -1,\ -0{,}5,\ 0,\ 0{,}5,\ 1,\ 1{,}5,\ 2,\ 2{,}5\}$$

- Sejam $A = \mathbb{R}$, $B = \mathbb{R}$ e a relação

$$R = \{(x,y) \in \mathbb{R} \times \mathbb{R},\ x^2 + 2 \cdot y^2 = 1\} \subset \mathbb{R} \times \mathbb{R}.$$

Então

$$\mathrm{Dom}(R) = \{x \in \mathbb{R},\ -1 \leq x \leq 1\}$$

$$\mathrm{Img}(R) = \{y \in \mathbb{R},\ -1/\sqrt{2} \leq y \leq 1/\sqrt{2}\}$$

■

Uma forma de representar gráficamente as relações são os chamados diagramas sagitais. Nesta representação os conjuntos A e B se representam como no diagrama de Venn e se utilizam setas para indicar a relação. Por exemplo, se

$$A = \{a,b,c,d,e,f\} \quad \text{e} \quad B = \{1,2,3,4,5\},$$

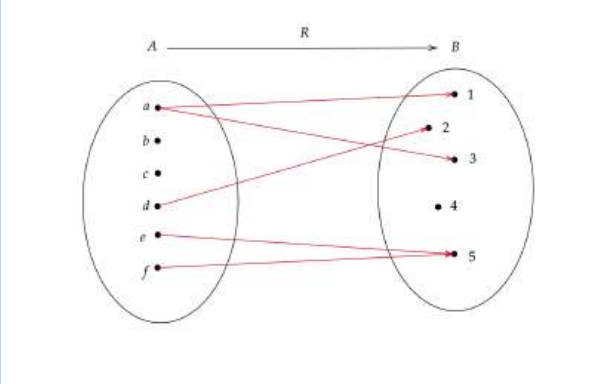
e R é a relação

$$R = \{(a,1),\ (a,3),\ (d,2),\ (e,5),\ (f,5)\}$$

tem

$$\mathrm{Dom}(R) = \{a,\ d,\ e,\ f\} \quad \text{e} \quad \mathrm{Img}(R) = \{1,\ 2,\ 3,\ 5\}$$

é representada gráficamente, por



Podemos construir relações a partir de relações já conhecidas. Para isto assuma que temos

- uma familia de conjuntos não vazios $\mathscr{F} = \{A_i,\ i \in \mathbf{I}\}$ tais que $A_i \cap A_j \neq \emptyset$
- mm conjunto não vazio B
- relações $R_i \subset A_i \times B$.

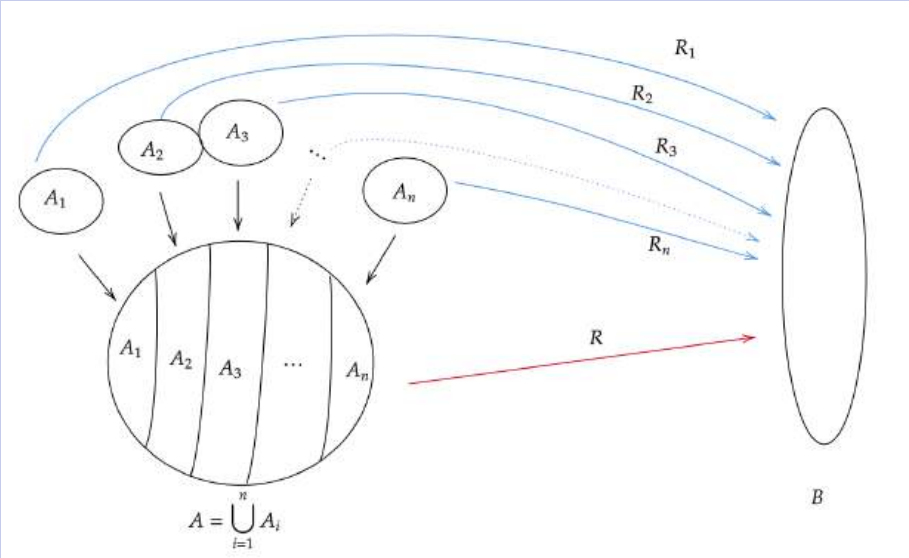
Construimos a relação $R \subset A \times B$ para

$$A = \bigcup_{i \in \mathbf{I}} A_i$$

como sendo

$$R = \{(a,b),\ \exists\, i \in \mathbf{I},\ (a,b) \in A_i\} \subset A \times B.$$

Gráficamente



Obs. Observamos que algo similar pode ser feito no caso em que $\mathscr{F}$ é uma partição de um conjunto A.

■ **Exemplo 10.3** Considere $\mathscr{F} = \{(-\infty,0),[0,1],(1,2),\{2\},(2,+\infty)\}$ e as relações

$$R_1 = \{(x,y) \in (-\infty,0) \times \mathbb{R},\ y = 2 \cdot x\}$$
$$R_2 = \{(x,y) \in [0,1] \times \mathbb{R},\ y = x^2\}$$
$$R_3 = \{(x,y) \in (1,2) \times \mathbb{R},\ y = \sin(\pi x/2)\}$$
$$R_4 = \{(2,0)\} \subset \{2\} \times \mathbb{R}$$
$$R_5 = \{(x,y) \in (2,+\infty) \times \mathbb{R},\ y = 2 - x\}$$

Então, definimos a relação em

$$A = (-\infty,0) \cup [0,1] \cup (1,2) \cup \{2\} \cup (2,+\infty) = \mathbb{R}$$

$$R = \left\{ (x,y) \in \mathbb{R} \times \mathbb{R},\ \left\{ \begin{array}{lll} y = 2 \cdot x & \text{se} & (-\infty,0) \\ y = x^2 & \text{se} & x \in [0,1] \\ y = \sin(\pi x/2) & \text{se} & x \in (1,2) \\ y = 0 & \text{se} & x = 0 \\ y = 2 - x & \text{se} & x \in (2,+\infty) \end{array} \right. \right\}$$

■

Definição 10.3 Seja $R \subset A \times B$ uma relação de A em B. A relação inversa, que denotamos por R^{-1}, é a relação de B em A definida por

$$R^{-1} = \{(b,a) \in B \times A,\ (a,b) \in R\}$$

Lema 10.1 Seja $R \subset A \times B$ uma relação de A em B então

- $\text{Dom}(R^{-1}) = \text{Img}(R)$
- $\text{Img}(R^{-1}) = \text{Dom}(R)$

Em representação sagital, podemos ver que se

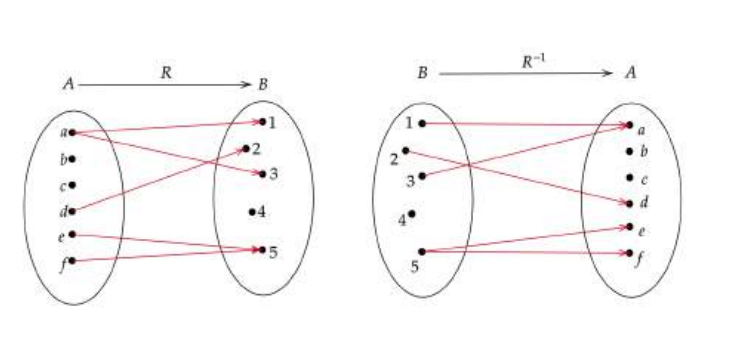
$$A = \{a,b,c,d,e,f\} \quad \text{e} \quad B = \{1,2,3,4,5\},$$

e R é a relação

$$R = \{(a,1),\ (a,3),\ (d,2),\ (e,5),\ (f,5)\}$$

então

$$R^{-1} = \{(1,a),\ (3,a),\ (2,d),\ (5,e),\ (5,f)\}$$



■ **Exemplo 10.4**

- Seja A é o conjunto formado por um proposições $\{P_1,\ldots,P_n\}$ e de todas aquelas formadas a partir de conjunções, negações e disjunções de um número finito delas. Considere

$$R = \{(P,Q) \in A^2,\ P \Rightarrow Q \text{ é verdadeira}\}.$$

Então

$$R^{-1} = \{(Q,P) \in A^2,\ P \Rightarrow Q \text{ é verdadeira}\}$$

- Seja $A = \{\text{subconjuntos de um conjunto } \mathscr{U}\}$, e $W \subset A^2$ um subcojunto e a relação

$$R = \{(U,V) \in A^2,\ U \times V \subset W\}.$$

Então

$$R^{-1} = \{(V,U) \in A^2,\ U \times V \subset W\}.$$

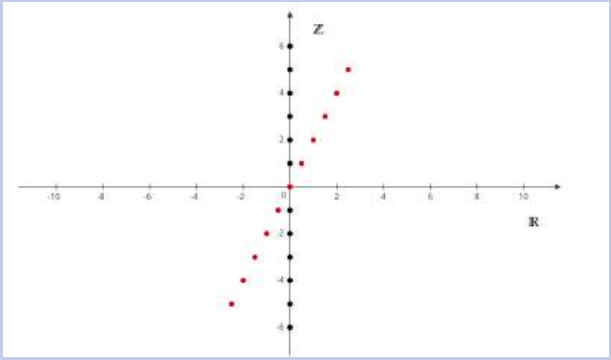
- Sejam $A = \mathbb{Z}$, $B = \mathbb{R}$ e a relação

$$R = \{(n,x) \in \mathbb{Z} \times \mathbb{R},\ (2 \cdot x = n) \wedge (-5 \leq n \leq 5)\} \subset \mathbb{Z} \times \mathbb{R}.$$

Então

$$R^{-1} = \{(x,n)) \in \mathbb{R} \times \mathbb{Z},\ (2 \cdot x = n) \wedge (-5 \leq n \leq 5)\}.$$

Gráficamente podemos representar a relação inversa como os pontos em vermelho



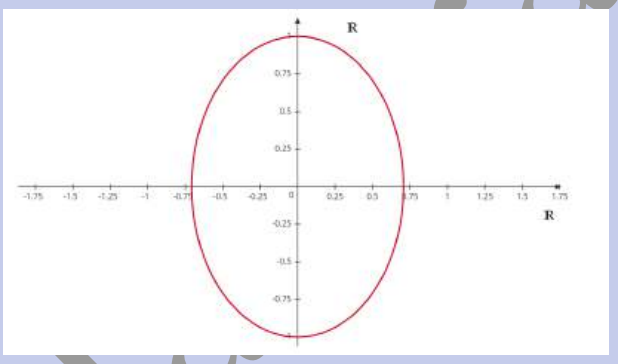
- Sejam $A = \mathbb{R}$, $B = \mathbb{R}$ e a relação

$$R = \{(x,y) \in \mathbb{R} \times \mathbb{R},\ x^2 + 2 \cdot y^2 = 1\} \subset \mathbb{R} \times \mathbb{R}.$$

Então

$$R^{-1} = \{(y,x) \in \mathbb{R} \times \mathbb{R},\ x^2 + 2 \cdot y^2 = 1\} \subset \mathbb{R} \times \mathbb{R}.$$

Gráficamente podemos representar a relação inversa como os pontos em vermelho



■

Teorema 10.1 Seja $R \subset A \times B$ uma relação de A em B. Então $(R^{-1})^{-1} = R$.

Demonstração. Observamos que

$$\begin{aligned}(a,b) \in (R^{-1})^{-1} &\Leftrightarrow (b,a) \in R^{-1} \\ &\Leftrightarrow (a,b) \in R.\end{aligned}$$

Portanto os conjuntos são iguais, de onde $(R^{-1})^{-1} = R$. ■

■ **Exemplo 10.5** Sejam $A = \mathbb{N}$, $B = \mathbb{Z}$ e $C = \mathbb{R}$ e as relações

$$R = \{(n,m) \in \mathbb{N} \times \mathbb{Z},\ -2n = m\},$$

e

$$S = \{(x,y) \in \mathbb{Z} \times \mathbb{R},\ x^2 = y\}$$

Construimos o conjunto

$$T = \{(n,y) \in \mathbb{N} \times \mathbb{R},\ \exists\, m \in \mathbb{Z},\ [(-2n = m) \wedge (m^2 = y)]\}.$$

que representa uma relação em $\mathbb{N} \times \mathbb{R}$. Observamos que

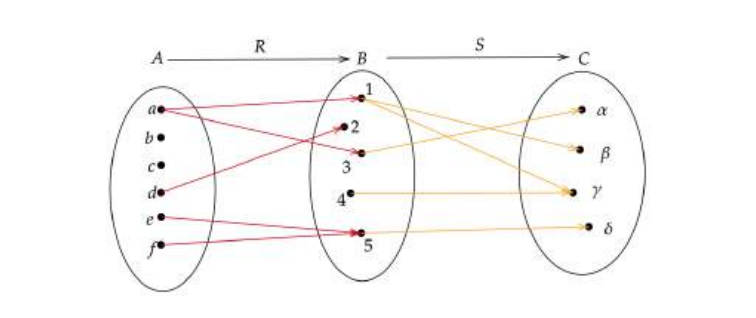
$$T = \{(n,y) \in \mathbb{N} \times \mathbb{R},\ \exists\, m \in \mathbb{Z},\ [(n,m) \in R \wedge (m,y) \in T]\}$$

■

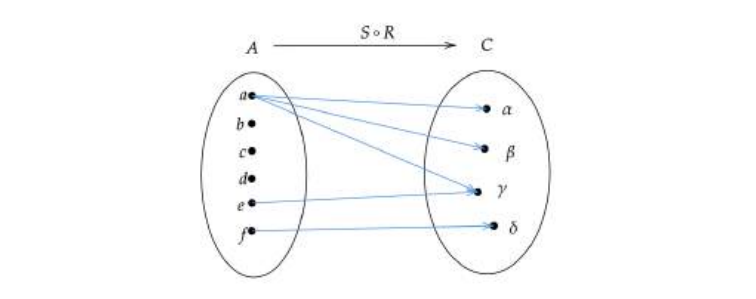
Definição 10.4 Seja R uma relação de A em B e S uma relação de B em C. A relação composta de R com S é a relação de A em C , que denotamos por $S \circ R$, e é dada por

$$S \circ R = \{(a,c) \in A \times C,\ \exists\, b \in B,\ (a,b) \in R \wedge (b,c) \in S\}$$

Em forma gráfica, podemos fazer



que nos dá uma relação



Corolário 10.1 Seja R uma relação de A em B e R^{-1} a relação inversa, então

$$R \circ R^{-1} = I_B(R) \qquad R^{-1} \circ R = I_A(R)$$

onde

$$I_A(R) = \{(a,a') \in A \times A,\ \exists\, b \in B,\ (a,b) \in R \wedge (a',b) \in R\}$$

$$I_B(R) = \{(b,b') \in B \times B,\ \exists\, a \in A,\ (a,b) \in R \wedge (a,b') \in R\}$$

Demonstração. Seguem de observar que

$$\begin{aligned}
(a,a') \in R^{-1} \circ R &\Leftrightarrow \exists\, b \in B,\ (a,b) \in R \wedge (b,a') \in R^{-1} \\
&\Leftrightarrow \exists\, b \in B,\ (a,b) \in R \wedge (a',b) \in R \\
&\Leftrightarrow (a,a') \in I_A(R).
\end{aligned}$$

$$\begin{aligned}
(b,b') \in R \circ R^{-1} &\Leftrightarrow \exists\, a \in A,\ (a,b') \in R \wedge (b,a) \in R^{-1} \\
&\Leftrightarrow \exists\, a \in A,\ (a,b') \in R \wedge (a,b) \in R \\
&\Leftrightarrow (a,a') \in I_A(R).
\end{aligned}$$

■

■ **Exemplo 10.6** • Sejam $A = \mathbb{Z}$, $B = \mathbb{N}$ e $C = \mathbb{R}$

$$R = \{(x,y) \in \mathbb{Z} \times \mathbb{N},\ y = x^2\} \subset A \times B \quad S = \{(x,y) \in \mathbb{N} \times \mathbb{R},\ y = e^x\} \subset B \times C.$$

Então um elemento (x,y) de $S\circ R$ precisa da existência de um $z\in\mathbb{N}$ tal que

$$\begin{aligned}(x,z)\in R\wedge(z,y)\in S &\Leftrightarrow (z=x^2)\wedge(y=e^z)\\ &\Leftrightarrow y=e^{x^2}\end{aligned}$$

De onde segue que

$$S\circ R=\{(x,y)\in\mathbb{Z}\times\mathbb{R},\ y=e^{x^2}\}$$

- Seja $A=B=C=\mathbb{R}$ e as relações

$$R=\{(x,y)\in\mathbb{N}\times\mathbb{R},\ y=\sin(x)\}\subset A\times B\quad S=\{(x,y),\ y=2\cdot x\}\subset B\times C.$$

Então, um elemento (x,y) de $S\circ R$ precisa da existência de um $z\in\mathbb{R}$ tal que

$$\begin{aligned}(x,z)\in R\wedge(z,y)\in S &\Leftrightarrow (z=\sin(x))\wedge(y=2\cdot z)\\ &\Leftrightarrow y=2\cdot\sin(x).\end{aligned}$$

De onde segue que

$$S\circ R=\{(x,y),\ y=2\cdot\sin(x)\}$$

- Observar que, no último exemplo, $S\circ R$ não é necessáriamente igual a $R\circ S$. De fato, se $(x,y)\in R\circ S$ então existe um $z\in\mathbb{R}$ tal que

$$\begin{aligned}(x,z)\in S\wedge(z,y)\in R &\Leftrightarrow (z=2\cdot x)\wedge(y=\sin(z))\\ &\Leftrightarrow y=\sin(2\cdot x).\end{aligned}$$

De onde segue que

$$S\circ R=\{(x,y),\ y=\sin(2\cdot x))\}$$

■

Teorema 10.2 Sejam
- R uma relação de A em B
- S uma relação de B em C, e
- T uma relação de C em D.

então

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

isto é, a composição é associativa.

Demonstração. Segue de observar que

$$\begin{aligned}(a,d)\in T\circ(S\circ R) &\Leftrightarrow \exists\, b\in B,\ (a,b)\in T\wedge[(b,d)\in S\circ R]\\ &\Leftrightarrow \exists\, b\in B,\exists\, c\in C,\ (a,b)\in T\wedge[\,(b,c)\in S\wedge(c,d)\in R]\\ &\Leftrightarrow \exists\, b\in B,\exists\, c\in C,\ [(a,b)\in T\wedge\ (b,c)\in S]\wedge(c,d)\in R]\\ &\Leftrightarrow \exists\, c\in C,\ (a,c)\in T\circ S\wedge(c,d)\in R\\ &\Leftrightarrow (a,d)\in(T\circ S)\circ R.\end{aligned}$$

■

Teorema 10.3 Seja R uma relação de A em B e S uma relação de B em C. Então

$$(R\circ S)^{-1}=S^{-1}\circ R^{-1}.$$

Demonstração. Segue de observar que

$$\begin{aligned}(c,a)\in(R\circ S)^{-1} &\Leftrightarrow (a,c)\in(R\circ S)\\ &\Leftrightarrow \exists\, b\in B,\ [(a,b)\in R]\wedge[(b,c))\in S]\\ &\Leftrightarrow \exists\, b\in B,\ [(b,a)\in R^{-1}]\wedge[(c,b))\in S^{-1}]\\ &\Leftrightarrow \exists\, b\in B,\ [(c,b))\in S^{-1}]\wedge[(b,a)\in R^{-1}]\\ &\Leftrightarrow (c,a)\in S^{-1}\circ R^{-1}.\end{aligned}$$

■

■ **Exemplo 10.7** • Sejam $A=\mathbb{Z}$, $B=\mathbb{N}$ e $C=\mathbb{R}$

$$R=\{(x,y)\in\mathbb{Z}\times\mathbb{N},\ y=x^2\}\subset A\times B\quad S=\{(x,y)\in\mathbb{Z}\times\mathbb{R},\ y=e^x\}\subset B\times C.$$

Então um elemento (x,y) de $(S\circ R)^{-1}$ precisa da existência de um $z\in\mathbb{N}$ tal que

$$\begin{aligned}(x,z)\in S^{-1}\wedge(z,y)\in R^{-1} &\Leftrightarrow (z,x)\in S\wedge(y,z)\in R\\ &\Leftrightarrow (x=e^z)\wedge(z=y^2)\\ &\Leftrightarrow (z=\ln(x))\wedge(\sqrt{z}=y)\\ &\Leftrightarrow y=\sqrt{\ln(x)}.\end{aligned}$$

De onde segue que

$$(S\circ R)^{-1}=\{(x,y)\in\mathbb{R}\times\mathbb{Z},\ y=\sqrt{\ln(x)}\}$$

- Seja $A=B=C=\mathbb{R}$ e as relações

$$R=\{(x,y)\in\mathbb{R}\times\mathbb{R},\ y=\sin(x)\}\subset A\times B$$

e

$$S=\{(x,y)\in\mathbb{R}\times\mathbb{R},\ y=2\cdot x\}\subset B\times C.$$

Então um elemento (x,y) de $(S\circ R)^{-1}$ precisa da existência de um $z\in\mathbb{R}$ tal que

$$\begin{aligned}(x,z)\in S^{-1}\wedge(z,y)\in R^{-1} &\Leftrightarrow (z,x)\in S\wedge(y,z)\in R\\ &\Leftrightarrow (x=2\cdot z)\wedge(z=\sin(y))\\ &\Leftrightarrow x=2\sin(y).\end{aligned}$$

De onde segue que

$$(S\circ R)^{-1}=\{(x,y)\in\mathbb{R}\times\mathbb{R},\ x=2\cdot\sin(y)\}$$

■

Definição 10.5 Seja R uma relação em A. Dizemos que

- a relação R é reflexiva se, e somente se, $\forall\, x\in A,\ (x,x)\in R$, (denotamos $\forall\, x\in A,\ x\sim x$),
- a relação R é simétrica se, e somente se, $\forall\ x\in A,\forall\ y\in A,\ (x,y)\in R\Rightarrow(y,x)\in R$, (denotamos $x\sim y\ \Rightarrow\ y\sim x$),
- a relação R é antisimétrica se, e somente se, $\forall\ x\in A,\forall\ y\in A,\ [(x,y)\in R\wedge(y,x)\in R]\Rightarrow x=y$, (denotamos $x\sim y\ \Rightarrow\ y\sim x$),
- a relação R é transitiva se, e somente se, $\forall\, x\in A,\forall\, y\in A\forall\, z\in A,\ [(x,y)\in R\wedge(y,z)\in R]\Rightarrow(x,z)\in R$, (denotamos $x\sim y\ \wedge\ y\sim z\ \Rightarrow\ a\sim z$.),

■ **Exemplo 10.8** • Seja $A=\{1,2\}$ e considere as relações

$$R_1=\{(1,2)\}\subset A^2,\quad R_2=\{(1,1)\}\quad R_3=\{(1,2),\ (2,1)\}$$

Observamos que

- Nenhuma é reflexiva, de fato $2 \in A$ e $(2,2)$ não está em R_i para $i = 1,2,3$
- R_2 e R_3 são simétricas: R_2 segue pois o único elemento é o $(1,1)$. No caso de R_2 temos que

$$[(1,2) \in R_2 \Rightarrow (2,1) \in R_2] \wedge [(2,1) \in R_2 \Rightarrow (1,2) \in R_2].$$

  A relação R_1 não é simétrica pois $(1,2) \in R_1$ mas $(2,1) \notin R_1$
- R_1 e R_2 são antisimétricas. De fato, no caso de R_1 pois o único elemento é $(1,2)$ de onde a condição de antisimetria se cumple. No caso de R_2 temos $(1 \sim 1) \wedge (1 \sim 1) \Rightarrow 1 = 1$.
  A relação R_3 não é antisimétrica pois

$$(1,2) \in R_3 \wedge (2,1) \in R_3,$$

  no entanto, $2 \neq 1$.
- Não é possível encontrar ternas de $(a,b) \in R_i \wedge (b,c) \in R_i \wedge (a,c) \notin R_i$ para todo $i = 1,2,3$ então as três relações são transitivas.

- Considere em $A = \{a,b,c\}$ a relação

$$R = \{(1,2),(2,1),(2,3)\}$$

  - R não é reflexiva, pois $2 \in A$ mas $(2,2) \notin R$,
  - R não é simétrica pois $(2,3) \in R$ mas $(3,2) \notin R$,
  - R não é antisimétrica pois $(1,2) \in R$ e $(2,1) \in R$ mas $1 \neq 2$.
  - R não é transitiva pois $(1,2) \in R$ e $(2,3) \in R$ mas $(1,3) \notin R$.
- Seja $U = \{(a,b) \subset \mathbb{R},\ a < b\}$ e defina

$$R = \{(A,B) \in U^2,\ A \subset B\}$$

  - a relação R é reflexiva pois, para todo $A \in U$ temos $A \subset A$ de onde $(A,A) \in R$.
  - a relação R é antisimétrica pois, $\forall A \in U,\ \forall B \in U,\ (A,B) \in R$ e $(B,A) \in R$ então $A = B$
  - a relação R é transitiva pois se $\forall A \in U,\ \forall B \in U,\ (A,B) \in R$ e $(B,C) \in R$ implica $A \subset B \subset C$ de onde $A \subset C$ e $(A,C) \in R$.
- Seja $p \in \mathbb{N}$ um número diferente de 0. Defina

$$R = \{(a,b) \in \mathbb{Z}^2,\ a,\ b \text{ tem o mesmo resto na divisão por } p\}$$

  - a relação R é reflexiva pois, para todo $a \in \mathbb{Z}$ temos que a tem o mesmo resto que b na divisão por p, de onde $(a,a) \in R$.
  - a relação R é simétrica pois, para todo $a,\ b \in \mathbb{Z}$ temos que se a tem o mesmo resto na divisão por p que b, isto é $(a,b) \in R$, então b tem o mesmo resto na divisão por p que a, de onde $(b,a) \in R$.
  - a relação R é transitiva pois se para $a,\ b,\ c \in \mathbb{Z}$ temos que a tem o mesmo resto na divisão por p que b, isto é $(a,b) \in R$, e b tem o mesmo resto na divisão por p que c, isto é $(b,c) \in R$, então a tem o mesmo resto na divisão por p que c de onde $(a,c) \in R$.

■

Definição 10.6 Seja R uma relação em A. A relação R é dita de equivalência se ela for reflexiva, simétrica e transitiva.

Se $a \in A$ definimos a clase de equivalência do elemento a como sendo o conjunto

$$[a] = \{a' \in A,\ (a,a') \in R\} = \{a' \in A,\ a \sim a'\}.$$

■ **Exemplo 10.9** •

- Seja A um conjunto e considere uma partição de A dada por

$$\mathscr{P} = \{A_i,\ i \in \mathbf{I}\}$$

  Definimos a relação R por

$$a \sim b \Leftrightarrow \exists\, i \in \mathbf{I},\ (a \in A_i) \wedge (b \in A_i).$$

  vamos ver que esta relação é de equivalência. De fato:

– É reflexiva pois para todo $a \in A$ existe um $i \in \mathbf{I}$ tal que $a \in A_i$. Portanto $a \in A_i$ e $a \in A_i$ de onde $a \sim a$.
– É simétrica pois para todo $a,\ b \in A$ se $a \sim b$ então existe um $i \in \mathbf{I}$ tal que $a \in A_i \wedge b \in A_i$, isto é, $b \in A_i \wedge a \in A_i$, de onde $b \sim a$.
– É transitiva pois se $a,\ b \in A$ tal que $a \sim b$ e $b \sim c$ então temos que existem $i,\ j \in \mathbf{I}$ tais que

$$a \in A_i \wedge b \in A_i \quad \text{e} \quad (b \in A_j) \wedge (c \in A_j)$$

portanto $b \in A_j \cap A_i$. Como $\mathscr{P}$ é partição, temos que $i = j$ de onde $c \in A_i$ e, portanto, $a \sim c$. ■

Proposição 10.1 Seja R uma relação de equivalência em A. Então
a) $a \in [a]$ para todo $a \in A$.
b) para todo $a,\ b \in A$ temos $a \sim b$ se, e somente se, $[a] = [b]$.
c) para todo $a,\ b \in A$ temos $[a] \cap [b] \neq \emptyset \Rightarrow [a] = [b]$
d) $A = \cup_{a \in A}[a]$.
Em particular, a familia formada por todas as classes de equivalência formam uma partição de A. Denotamos, por abuso de notação, esta familia por

$$\mathscr{U} = \{[a],\ a \in A\}.$$

Demonstração. a) Como a relação é simétrica $a \sim a$ para todo $a \in A$. De onde $a \in [a]$ para todo $a \in A$.
b) Dados $a,\ b \in A$, se $a \sim b$ então para todo $a' \in [a]$ temos que $a' \sim a$ e $a \sim b$. Pela transitividade da relação temos que $a' \sim b$ e, portanto $a' \in [b]$. Temos assim que $[a] \subset [b]$. De forma similar se prova que $[b] \subset [a]$ e portanto $[a] = [b]$.
Por outro lado se $[a] = [b]$ então $a \in [b]$ e, portanto, $a \sim b$.
c) Seja $c \in [a] \cap [b]$ então $c \sim a$ e $c \sim b$. Por transitividade temos então que $a \sim b$. O resultado decorre agora do item anterior .
d) Claramente $\cup_{a \in A}[a] \subset A$. Se $a \in A$ então, pelo item a) vemos que $a \in [a]$ e portanto $a \in \cup_{a \in A}[a]$. Da arbitráriedade do a escolhido temos que $A \subset \cup_{a \in A}[a]$ e portanto vale a igualdade.
A afirmação segue dos itens acima, de fato observamos que os elementos de duas clases de equivalência diferentes são disjuntos, cada elemento da familia é não vazio e, por último, a união de todas as clases de equivalência é o espaço todo. ■

Obs. Considere uma relação de equivalência R sobre um conjunto A.
- Há, em virtude do teorema anterior, uma equivalência entre partições de um conjunto e relações de equivalências.
- Cada classe de equivalência é um subconjunto de A e portanto um elemento do conjunto de partes de A, $\mathbb{P}(A)$.

Definição 10.7 Considere uma relação de equivalência R sobre um conjunto A. Seja $\mathscr{F}$ a partição de A dada pela relação de equivalência R e, na qual, cada conjunto corresponde a uma classe de equivalência. Definimos o conjunto quociente $A/\sim$ como o conjunto que tem por elementos as classes de equivalências. Por abuso de notação,

$$A/\sim = \{[a],\ a \in A\} \subset \mathscr{P}(A).$$

■ **Exemplo 10.10** • Seja $p \neq 0$ um número natural e considere

$$R = \{(a,b) \in \mathbb{Z}^2,\ a,\ b \text{ tem o mesmo resto na divisão por p}\}$$

Pelo que vimos anteriormente que a relação é de equivalência. O conjunto quociente

$$\mathbb{Z}_p = \mathbb{Z}/\sim .$$

temos então as seguintes classes

$$\begin{aligned}[0] &= \{a \in \mathbb{Z}, p|a\}\\ [1] &= \{a \in \mathbb{Z},\ \exists\, q \in \mathbb{Z},\ a = q\cdot p + 1,\}\\ &\vdots \qquad\qquad \vdots\\ [p-1] &= \{a \in \mathbb{Z},\ \exists\, q \in \mathbb{Z},\ a = q\cdot p + (p-1)\}\end{aligned}$$

- Seja $U = \{\text{Triângulos em } \mathbb{R}^{\not\perp}\}$ e definimos a relação

$$R = \{(A,B) \in U^2,\ A \text{ tem a mesma área que } B\}$$

Claramente
  - $\forall\, A \in U,\ (A,A) \in R$
  - $(A,B) \in R \Rightarrow (B,A) \in R$
  - $[(A,B) \in R \wedge (B,C) \in R] \Rightarrow (A,C) \in R.$

o quociente é $T/\sim$ está formado pelas classes

$$[A_r] = \{A \in T,\ \text{Área}(A) = r\}, \quad \forall\, r \in \mathbb{R}_{>0}.$$

em que

$$A_r = \text{triângulo com vértices em } V_1 = (0,0),\ V_2 = (0,2),\ V_3 = (r,0).$$

■

Definição 10.8 Seja R uma relação em A. Dizemos que R é uma relação de ordem (ou de ordem parcial), e a denotamos por $a \prec b$ quando $(a,b) \in R$, se ela for reflexiva, antisimétrica e transitiva.

Neste caso dizemos que o par $(A,\ \prec)$ é um conjunto ordenado. Mais ainda se a e b são dois elementos distintos de A e são tais que $a \prec b$ então dizemos que b é consecutivo de a.

Obs. As relações de ordem parcial é uma generalização da "inclusão"para conjuntos e do "menor ou igual"para números.

■ **Exemplo 10.11**

- Em $\mathbb{N}$ a relação

$$a \leq b \quad \text{se, e somente se} \quad [(a < b) \vee (a = b)]$$

é uma relação de ordem parcial. De fato ela é
  - reflexiva: para todo $a \in \mathbb{N}$ temos $a \leq a$.
  - antisimétrica: Para todo $a,\ b \in \mathbb{N}$, se $a \leq b$ e $b \leq a$ então $a = b$.
  - transitiva: para todo $a,\ b,\ c \in \mathbb{N}$, e $a \leq b$ e $b \leq c$ então $a \leq c$.
- Seja U um conjunto então considere a relação em $\mathscr{P}(U)$ dada por

$$R = \{(A,B) \in \mathscr{P}(U)^2,\ A \subset B\},$$

é uma relação de ordem parcial. De fato ela é
  - reflexiva: para todo $A \in \mathscr{P}(U)$ temos $A \subset A$.
  - antisimétrica: para todo $A,\ B \in \mathscr{P}(U)$ e $A \subset B$ e $B \subset A$ então $A = B$.
  - transitiva: para todo $A,\ B,\ C \in \mathscr{P}(U)$ se $A \subset B$ e $B \subset C$ então $A \subset C$.
- A relação em $\mathbb{Z}$ dada por

$$R = \{(p,q) \in \mathbb{Z}^2,\ p \text{ divide a } q\} \subset \mathbb{Z}^2,$$

é uma relação de ordem parcial. De fato ela é

  - reflexiva: para todo $p \in \mathbb{Z}$ temos p divide a p.
  - antisimétrica: para todo $p,\ q,\ r \in \mathbb{Z}$, se p divide a q e q divide a p então $p = q$.
  - transitiva: para todo $p,\ q,\ r \in \mathbb{Z}$, se p divide a q e q divide a r então p divide a r.
- Considere $U = \{\text{palavras de um idioma}\}$. Nesse conjunto podemos definir uma relação de equivalência (deixamos para o leitor verificar que é de equivalência)

$$a_1 \dots a_m \sim b_1 \dots b_m \quad \Leftrightarrow \quad a_1 = b_1$$

Então dividimos as palavras em classes. Cada classe contem as palavras que começam com a mesma letra, isto é, por exemplo

$$\begin{aligned} [a] &= \{\text{palavras que começam com } a\} \\ [b] &= \{\text{palavras que começam com } b\} \\ \vdots & \qquad \vdots \\ [z] &= \{\text{palavras que começam com } z\} \end{aligned}$$

Então, por exemplo para o idioma português.

$$U/\sim = \{[a],\ [b],\ \cdots,\ [z]\}$$

Também em U podemos definir a ordem dada pela ordem lexicográfica, esta relação é uma relação de ordem. Esta ordem precisa primeiro de um ordenamento das letras do alfabeto para depois induzir a ordem nas palavras. Neste caso temos a ordem em que está o diccionário.

■

Definição 10.9 Seja $(A,\ \prec)$ um conjunto ordenado.

- Dois elementos $a,\ b$ de A são comparáveis se

$$P = (a \prec b) \vee (b \prec a)$$

for verdadeira. Caso contrário, os elementos $a,\ b$ são ditos incomparáveis.
- A relação de ordem $\prec$ é dita uma relação de ordem total se

$$\forall\, a \in A\ \forall\, b \in A, \quad [a \neq b \ \Rightarrow\ (a \prec b) \vee (b \prec a)]$$

é verdadeira. Caso contrário, a relação será chamada de ordem parcial.

■ **Exemplo 10.12**

- Em $U = \mathbb{N},\ \mathbb{R}$ a relação

$$R = \{(a,b) \in \mathbb{N}^2,\ a \leq b\}$$

é uma relação de ordem total. Isto será mostrado depois.
- Seja $U = \mathscr{P}(\{a,b\})$ um conjunto então considere a relação em $\mathscr{P}(U)$ dada por

$$R = \{(A,B) \in \mathscr{P}(U)^2,\ A \subset B\},$$

é uma relação de ordem parcial que não é total pois há conjuntos que não são comparáveis, por exemplo $A = \{a\}$ e $B = \{b\}$.

■

Definição 10.10

- Um conjunto $(A, \prec)$ é dito bem ordenado se $(A, \prec)$ é um conjunto totalmente ordenado para o qual todo subconjunto não vazio tem elemento mínimo, isto é, para todo $B \subset X$ existe $b \in B$ tal que $b \leq c$ para todo $c \in B$.
- Um conjunto que admite uma relação de ordem para a qual é bem ordenado é dito um conjunto que admite uma boa ordenação.

Um fato surpreendente é o seguinte resultado que é equivalente ao axioma da escolha:

Teorema 10.4 Todo conjunto admite uma boa ordenação.

Obs. Como consequência disto é que: Existe uma boa ordem para os números reais. O problema é que não se sabe qual é essa ordem.

11. Funções

Passamos a estudar o conceito de função. Éste é um dos conceitos fundamentais da matemática e que aparece em cada uma de suas áreas. Começamos com a sua definição.

Definição 11.1 Sejam A e B dois conjuntos. Uma função f de A em B, que denotamos por $f : A \to B$ é uma relação $f \subset A \times B$ que satisfaz

- $\text{Dom}(f) = A$
- $\forall\, x \in A,\ \forall\, y,\ \forall\, z \in B,\ [(x,y) \in f \wedge (x,z) \in f] \Rightarrow (y = z)$.

Obs. A definição garante

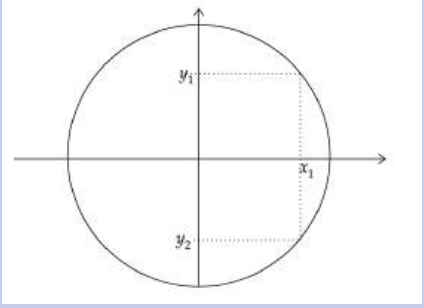
- Cada elemento do domínio da relação tem uma única imagem, isto é, se $(x,y) \in f$ então y é o único elemento de B tal que $(x,y) \in f$. É por isto que escrevemos

$$f(x) = y$$

- A relação nula associada a $\emptyset$ é uma função pois podemos ver $\emptyset = A \times \emptyset$. Portanto o domínio é A e a segunda condição é satisfeita naturalmente pois, por equivalência da contrapositiva $\forall\, x \in A,\ \forall\, y,\ \forall\, z \in B$,

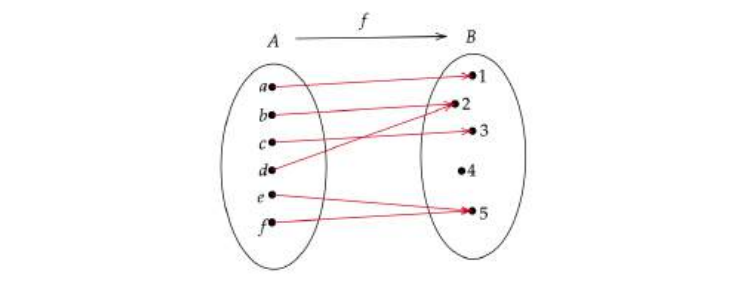
$$y \neq z \Rightarrow [(x,y) \notin f \vee (x,z) \notin f].$$

- Há relaçoes que não são funções. Por exemplo, a relação dada pelo círculo $S^1 \subset \mathbb{R}^2$.



não é função. De fato, para x_1 temos que há dois pontos y_1 e y_2 tais que (x_1, y_1) e (x_2, y_2) estão na relação.

Podemos representar a função $f : A \to B$ para $A = \{a,\ b,\ c,\ d,\ e,\ f\}$ e $B = \{1,\ 2,\ 3,\ 4,\ 5\}$ com diagramas sagitais como segue



Observamos que de cada elemento do domínio sai uma **única** seta.

Proposição 11.1 Duas funções $f,\ g : X \to Y$ são iguais se, e somente se, $f(x) = g(x)$ para todo $x \in X$.

Demonstração. Considere duas funções $f,\ g : X \to Y$ e assuma são iguais, isto é os conjuntos $f \subset X \times Y$ e $g \subset X \times Y$ são o mesmo conjunto. Então, para todo $y = f(x)$, isto é $(x,y) \in f$ temos que $(x,y) \in g$, portanto $y = g(x)$. De donde segue que $f(x) = g(x)$.

Por outro lado, se $f(x) = g(x)$ para todo $x \in X$ temos que todo $(x,y) \in f$ vale $(x,y) \in g$ e viceversa. Portanto $f = g \subset X \times Y$. ■

■ **Exemplo 11.1**

- Seja $f : A \to B$ e $b_0 \in B$. A função tal que $f(a) = b_0$ para todo $a \in A$ é chamada de função constante.
- Seja $f : A \to A$ dada por $f(a) = a$ para todo $a \in A$. Esta função é conhecida como função identidade e a denotamos por $I_A : A \to A$.
- Seja $A_0 \subset A$. Definimos a função característica $\chi_{A_0} : A \to \mathbb{N}$ por

$$\chi_{A_0}(a) = \begin{cases} 1 & \text{se} \quad a \in A_0 \\ 0 & \text{se} \quad a \notin A_0 \end{cases}.$$

■

Vamos a mostrar agora duas formas diferentes de contruir funções a partir de funções conhecidas.

- **Restrição de uma função:** Dada $f : A \to B$ uma função e $A_0 \subset A$ definimos a função $f|_{A_0} : A_0 \to B$ por

$$f|_{A_0}(a) = f(a).$$

Claramente $Dom(f|_{A_0}) = A_0$ e se

$$(x,y),\ (x,z) \in f|_{A_0}$$

então

$$(x,y),\ (x,z) \in f$$

de onde segue que $y = z$. Observamos que $f|_{A_0}$ é a única função de A_0 em B que coincide com f em A_0. De fato se $g : A_0 \to B$ tal que $g(a) = f(a) = f|_{A_0}(a)$ e, portanto $g = f|_{A_0}$.

- **Funções definidas por partes:** A ideia é construir funções sobre um espaço A a partir de funções definidas sobre uma partição. Para isto considere uma partição de $\mathscr{A} = \{A_i\ i \in \mathbf{I}\}$ de um conjunto A, isto é
  - $A_i \neq \emptyset$ para todo $i \in \mathbf{I}$
  - $A_i \cap A_j = \emptyset$ para todo $i,\ j$ tais que $i \neq j$.
  - $A = \cup_{i \in \mathbf{I}} A_i$.

e assuma que para cada A_i existe uma função

$$f_i : A_i \to B$$

Definimos $f : A \to B$ por

$$f(a) = f_i(a) \quad \text{se} \quad a \in A_i.$$

Vamos mostrar que f é função. De fato $Dom(f) = A$. Por outro lado, se $a \in A$ temos que, existe um único $A_i \in \mathscr{A}$ tal que $a \in A_i$ então, pelo fato de $f_i : A_i \to B$ ser função temos

$$f_i(a) = b_1 \quad \text{e} \quad f_i(a) = b_2 \quad \text{então} \quad b_1 = b_2.$$

■ **Exemplo 11.2** • Seja $A = (-\infty, -1] \cup (-1, 2) \cup \{2\} \cup (2, +\infty)$. Definimos então as funções f_1, f_2, f_3 e f_4 como sendo

$$f_1 : (-\infty, -1] \to \mathbb{R}, \quad x \to e^x$$

$$f_2 : (-1, 2) \to \mathbb{R}, \quad f_2(x) = x^2$$

$$f_3 : \{2\} \to \mathbb{R}, \quad f_3(2) = 5$$

$$f_4 : (2, +\infty) \to \mathbb{R}, \quad f_4(x) = \cos(x)$$

Então

$$f(x) = \begin{cases} e^x & \text{se } x \in (-\infty, -1] \\ x^2 & \text{se } x \in (-1, 2) \\ 5 & \text{se } x = 2 \\ \cos(x) & \text{se } x \in (2, +\infty) \end{cases}$$

• Seja $f : \mathbb{R} \to [1, \infty)$ definida por

$$f(x) = \begin{cases} x + 2 & \text{se } x > 0 \\ x^2 + 1 & \text{se } x \leq 0 \end{cases}$$

É fácil de ver que f é sobrejetora mas não injetora.

■

Definição 11.2 Seja $A_0 \subset A$ e seja $f : A_0 \to B$ uma função. Uma extensão de f é uma função $F : A \to B$ tal que $F|_{A_0} = f$.

■ **Exemplo 11.3** A extensão de uma função não é necessáriamente única. por exemplo $f : \{0, 1, 2, 3\} \to \mathbb{N}$ definida por $f(a) = a$ admite

$$F : \mathbb{N} \to \mathbb{N}, \quad F(a) = a$$

e

$$G : \mathbb{N} \to \mathbb{N}, \quad G(a) = \begin{cases} a & \text{se} \quad a \leq 4 \\ a^2 & \text{se} \quad a > 4 \end{cases}$$

como possíveis extensões. ■

Teorema 11.1 Sejam $f : X \to Y$ e $g : Y \to Z$ duas funções então a relação composta relação $g \circ f : X \to Z$ é função. Mais ainda, temos a seguinte regra

$$\forall\, x \in X, \quad (g \circ f)(x) = g(f(x))$$

Demonstração. É claro que

i- $Dom(g\circ f) = X$, pois f é função

ii-

$$\begin{aligned}((x,z_1)\in g\circ f)\wedge((x,z_2)\in g\circ f) &\Leftrightarrow \exists\, y_1,\, y_2\in Y,\ \{[z_1=g(y_1)\wedge y_1=f(x)]\wedge[z_2=g(y_2)\wedge y_2=f(x)]\}\\ &\Leftrightarrow \exists\, y_1,\ \{[z_1=g(y_1)\wedge y_1=f(x)]\wedge[z_2=g(y_1)\wedge y_2=f(x)]\}\\ &\quad (y_1=f(x)=y_2 \quad \text{pois } f \text{ é função}).\end{aligned}$$

De onde segue que

$$z_2 = g(y_1) = z_1 \quad \text{pois } g \text{ é função.}$$

Utilizando a regra vista acima,

$$(x,y)\in(g\circ f) \Leftrightarrow (y,f(x))\in g \Leftrightarrow y = g(f(x))$$

■

Assim como acontece com as relações, temos que vale a associatividade na composição de funções.

Proposição 11.2 Sejam $f: W\to X$, $g: X\to Y$, $h: Y\to Z$, então

$$f\circ(g\circ h) = (f\circ g)\circ h$$

Demonstração. Decorre do resultado visto para relações. ■

Obs. A composição de funções, assim como para acontece para as relações em geral, não é comutativa

■ **Exemplo 11.4** • Considere $f(x) = 2x+1$ e $g(x) = x^2+1$. Descreva a composta. Da definição segue que

$$f\circ g(x) = 2(x^2+1)+1 = 2x^2+3 \neq g\circ f(x) = (2x+1)^2+1 = 4x^2+4x+2.$$

Logo, segue que não vale a comutatividade.

- Vamos aqui exemplificar a definição 8. Considere as seguintes funções

$$f(x) = \cos(x): \mathbb{R}\to\mathbb{R}, \quad g(x) = x^2+1: \mathbb{R}\to\mathbb{R} \quad \text{e} \quad h(x) = e^x: \mathbb{R}\to\mathbb{R}.$$

Segue então que

$$\begin{aligned}&g\circ h(x) = (e^x)^2+1 = e^{2x}+1 \Rightarrow f\circ(g\circ h)(x) = \cos(e^{2x}+1)\\ &(f\circ g)(x) = \cos(x^2+1) \Rightarrow (f\circ g)\circ h(x) = \cos((e^x)^2+1) = \cos(e^{2x}+1)\end{aligned}$$

- Considere

$$f(x) = \begin{cases} x^2 & \text{se } x\in(-\infty,1]\\ e^x & \text{se } x\in(1,\infty)\end{cases} \quad \text{e} \quad g(x) = \begin{cases} x-1 & \text{se } x\in(-\infty,0]\\ 2 & \text{se } x\in[0,2]\\ x^2+1 & \text{se } x\in(2,\infty)\end{cases}$$

Observamos que

- Se $x\in(-\infty,1]$ então $x^2\in[0,\infty) = [0,2]\cup(2,\infty)$ de onde

$$f((0,1)) = (0,1) \quad \text{e} \quad f(-\infty,0] = (-\infty,0].$$

- Se $x\in(1,+\infty)$ então $e^x\in(e,\infty)$ com $e>2$

$$g\circ f(x) = \begin{cases} g(x^2) & \text{se } x\in(-\infty,1]\\ g(e^x) & \text{se } x\in(1,\infty)\end{cases} = \begin{cases} x^2+1 & \text{se } x\in(-\infty,0]\\ 2 & \text{se } x\in(0,1]\\ e^{2x}+1 & \text{se } x\in(1,\infty)\end{cases}$$

■

Definição 11.3 Uma função $f : A \to B$ é dita
- Injetora: $\forall\, a_1 \in A,\ \forall\, a_2 \in A,\ f(a_1) = f(a_2) \ \Rightarrow\ a_1 = a_2$.
- Sobrejetora: $\forall\, b \in B,\ \exists\, a \in A,\ f(a) = b$. Dito de outra forma, $\mathrm{Img}(f) = B$.
- Bijetora: Se ela for injetora e sobrejetora.

Obs. Se $f : A \to B$ é uma função bijetora então, pelo fato de ser função, para cada elemento de $a \in A$ existe um unico $b \in B$ tal que $f(a) = b$. Agora, pelo fato de ser bijetora, para cada elemento de $b \in B$ existe um único elemento de $a \in A$ tal que $f(a) = b$. Isto é, os elementos de A e B estão em correspondência biunívoca.

■ **Exemplo 11.5**
- Seja A um subconjunto de um conjunto U. Definimos

$$f : \mathscr{P}(U) \to \mathscr{P}(A), \quad f(B) = B \cap A.$$

Claramente f é sobrejetora, mas não necessáriamente injetora. De fato, por exemplo, se $U = \mathbb{N}$ e $A = \{1\}$ então

$$f(\{0,1\}) = \{1\} = f(\{1,2\}).$$

- Sejam A e B dois conjuntos disjuntos ($A \cap B = \emptyset$). Definimos

$$f : \mathscr{P}(A) \to \mathscr{P}(A \cup B), \quad f(D) = D$$

então f é injetora mas não sobrejetora pois para $B \in \mathscr{P}(A \cup B)$ não há nenhum conjunto $D \in \mathscr{P}(A)$ tal que $f(D) = B$.
- $f : \mathbb{R} \to \mathbb{R}$ dada por $f(x) = x^3$ é bijetora.
De fato, dado $y \in \mathbb{R}$ então, $x = \sqrt[3]{y}$ satisfaz $f(x) = y$ portanto é sobrejetora.
Se $f(x_1) = f(x_2)$ então $x_1^3 = x_2^3$ de onde

$$0 = (x_1^3 - x_2^3) = (x_1 - x_2)(x_1^2 + x_1x_2 + x_2^2) \ \Rightarrow (x_1 - x_2) = 0$$

e portanto $x_1 = x_2$ de onde f é injetora.
- $f : \mathbb{R} \to \mathbb{R}$ dada por $f(x) = x^2$ não é injetora nem sobrejetora.
De fato se $y < 0$ não existe $x \in \mathbb{R}$ tal que $x^2 = y$. De onde f não é sobrejetora. Por outro lado, $f(-1) = 1 = f(1)$ e, portanto não é injetora.

■

Proposição 11.3 Sejam $f : A \to B$ e $g : B \to C$ duas funções.
- Se f e g são injetoras, então $g \circ f$ é injetora.
- Se f e g são sobrejetoras, então $g \circ f$ é sobrejetora.
- Se $f \circ g$ é bijetora então g é sobrejetora e f é injetora.

Demonstração.
- Assuma que f e g são injetoras, então

$$\begin{aligned} g \circ f(x_1) = g \circ f(x_2) &\Leftrightarrow f(x_1) = f(x_2) \quad (\text{pois } g \text{ é injetora}) \\ &\Leftrightarrow x_1 = x_2 \quad (\text{pois } f \text{ é injetora}). \end{aligned}$$

de onde segue que $g \circ f$ é injetora.
- Assuma que f e g são sobrejetoras. Se $c \in C$ existe $b \in B$ tal que $g(b) = c$ pois g é sobrejetora. Como f é sobrejetora existe $a \in A$ tal que $f(a) = b$, de onde

$$c = g(b) = g(f(a) = (g \circ f)(a).$$

Portanto $g \circ f$ é sobrejetora.
- Assuma que $f \circ g$ é bijetora. Dado $c \in C$ existe $a \in A$ tal que $c = g \circ f(a) = g(f(a))$. Como $f(a) \in B$ temos que existe $b \in B$ tal que $g(b) = c$ de onde segue que g é sobrejetora.
Se $f(a_1) = f(a_2)$ temos que

$$(g \circ f)(a_1) = g(f(a_1)) = g(f(a_2)) = (g \circ f)(a_2)$$

Como $g \circ f$ é bijetora, temos que $a_1 = a_2$, de onde segue que f é injetora.

■

■ **Exemplo 11.6** Seja $f:[0,\infty)\to\mathbb{R}$ dada por $f(x)=x^2$ e $g:\mathbb{R}\to[0,\infty)$ dada por $g(x)=|x|$. Claramente f não é sobrejetora nem g é injetora, no entanto, $g\circ f:[0,+\infty)\to[0,+\infty)$ é dada por $f(x)=x$ e, portanto, é bijetora. ■

Definição 11.4 Uma função $f:A\to B$ é invertível se a relação inversa $f^{-1}:B\to A$ também é função.

Corolário 11.1 Seja $f:A\to B$ é invertível então para todo $a\in A$ e para todo $b\in B$ temos

$$f(a)=b \Leftrightarrow f^{-1}(b)=a.$$

Demonstração. A demonstração segue de observar que

$$\begin{aligned} f(a)=b &\Leftrightarrow (a,b)\in f\\ &\Leftrightarrow (b,a)\in f^{-1}\\ &\Leftrightarrow f^{-1}(b)=a. \end{aligned}$$

■

Teorema 11.2 Uma função $f:A\to B$ é invertível se, e somente se, f é bijetora. Mais ainda, f^{-1} é também bijetora.

Demonstração.

- Assuma que f é invertível e que $f(a_1)=b=f(a_2)$ então
$$(a_1,b)\wedge(a_2,b)\in f \Leftrightarrow (b,a_1)\wedge(b,a_2)\in f^{-1}.$$
Como f^{-1} é função, temos que $a_1=a_2$. Por outro lado $\mathrm{Img}(f)=Dom(f^{-1})=B$ por ser f^{-1} função. Portanto f é sobrejetora, de onde segue que é bijetora.
- Assuma agora que f é bijetora. Então $B=\mathrm{Img}(f)=Dom(f^{-1})$ pois f é sobrejetora. Por outro lado
$$(b,a_1)\wedge(b,a_2)\in f^{-1} \Leftrightarrow (a_1,b)\wedge(a_2,b)\in f,$$
Como f é injetora, temos que $a_1=a_2$. Portanto f^{-1} é função.

O restante segue de de observar que

$$\begin{aligned} (f^{-1})^{-1}(x)=y &\Leftrightarrow f^{-1}(y)=x\\ &\Leftrightarrow f(x)=y. \end{aligned}$$

de onde segue que $(f^{-1})^{-1}=f$ e, portanto f^{-1} é invertível e, pelo visto acima, bijetora. ■

Corolário 11.2 Se $f:A\to B$ e $g:B\to C$ são bijetoras, então $g\circ f$ é bijetora e, mais ainda, $(g\circ f)^{-1}=f^{-1}\circ g^{-1}$

Demonstração. Como f e g são bijetoras, por um resultado acima, temos que $g\circ f$ é sobrejetora e injetora, de onde segue que é bijetora. O restante segue de observar que

$$y=(g\circ f)(x) \Leftrightarrow g^{-1}(y)=f(x) \Leftrightarrow (f^{-1}\circ g^{-1})(y)=x,$$

de onde $(g\circ f)^{-1}(y)=(f^{-1}\circ g^{-1})(y)$ para todo $y\in C$. ■

Definição 11.5 Seja $f:A\to B$ uma função, $A_1\subset A$ e $B_1\subset B$ um subconjunto, definimos o conjunto imagem de A_1 e preimagem de B_1, como sendo

$$f(A_1)=\{f(x)\in B,\ x\in A_1\}\subset B,$$

$$f^{-1}(B_1)=\{x\in A,\ f(x)\in B_1\}\subset A.$$

Corolário 11.3 Seja $f : A \to B$ injetora e $A_2 \subset A_1 \subset A$ conjuntos. Então

$$f(A_1 \backslash A_2) = f(A_1) \backslash f(A_2).$$

Demonstração. Se $y \in f(A_1 \backslash A_2)$ então existe $x \in A_1 \backslash A_2$ tal que $f(x) = y$. Como f é injetora e $x \notin A_2$, $y \notin f(A_2)$ de onde $y \in f(A_1) \backslash f(A_2)$. Por outro lado, se $y \in f(A_1) \backslash f(A_2)$ então existe $x \in A_1$ tal que $f(x) = y$, como $y \notin f(A_2)$ e f é injetora, temos que $x \notin A_2$. ■

■ **Exemplo 11.7** Se f não é injetora não podemos garantir que o resultado acima vale. De fato seja $f : \mathbb{R} \to \mathbb{R}$ dada por $f(x) = x^2$. Considere $A_1 = \mathbb{R}$ e $A_2 = [0, \infty)$, então

$$\begin{aligned} f(A_1 \backslash A_2) &= (0, \infty) \\ f(A_1) \backslash f(A_2) &= \emptyset. \end{aligned}$$

■

Proposição 11.4 Seja $f : A \to B$ e $\mathscr{F} = \{B_i, \in \mathbf{I}\}$ então

- $f^{-1}(\cup_{i \in \mathbf{I}} B_i) = \cup_{i \in \mathbf{I}} f^{-1}(B_i)$.
- $f^{-1}(\cap_{i \in \mathbf{I}} B_i) = \cap_{i \in \mathbf{I}} f^{-1}(B_i)$.
- $f^{-1}(B_i \backslash B_j) = f^{-1}(B_i) \backslash f^{-1}(B_j)$

Demonstração. •

$$\begin{aligned} x \in f^{-1}(\cup_{i \in \mathbf{I}} B_i) &\Leftrightarrow f(x) \in \cup_{i \in \mathbf{I}} B_i \\ &\Leftrightarrow \exists\, i \in \mathbf{I},\ f(x) \in B_i \\ &\Leftrightarrow \exists\, i \in \mathbf{I},\ x \in f^{-1}(B_i) \\ &\Leftrightarrow x \in \cup_{i \in \mathbf{I}} f^{-1}(B_i). \end{aligned}$$

•

$$\begin{aligned} x \in f^{-1}(\cap_{i \in \in \mathbf{I}} B_i) &\Leftrightarrow f(x) \in \cap_{i \in \mathbf{I}} B_i \\ &\Leftrightarrow \forall\, i \in \mathbf{I},\ f(x) \in B_i \\ &\Leftrightarrow \forall\, i \in \mathbf{I},\ x \in f^{-1}(B_i) \\ &\Leftrightarrow x \in \cap_{i \in \mathbf{I}} f^{-1}(B_i). \end{aligned}$$

•

$$\begin{aligned} x \in f^{-1}(B_i \backslash B_j) &\Leftrightarrow f(x) \in (B_i \backslash B_j) \\ &\Leftrightarrow (f(x) \in B_i) \wedge (f(x) \notin B_j) \\ &\Leftrightarrow [x \in f^{-1}(B_i)] \wedge [x \notin f^{-1}(B_j)] \\ &\Leftrightarrow x \in f^{-1}(B_i) \backslash f^{-1}(B_j) \end{aligned}$$

■

Se $f : A \to B$ é injetora podemos pensar que, de alguma forma, $A \subset B$. Nesse sentido, o seguinte resultado é uma generalização do critério de igualdade entre conjuntos.

Teorema 11.3 — Cantor-Bernstein-Schröder. Sejam A e B dois conjuntos. Se existem funções injetoras $f : A \to B$ e $g : B \to A$ então A e B existe uma função bijetora $h : A \to B$.

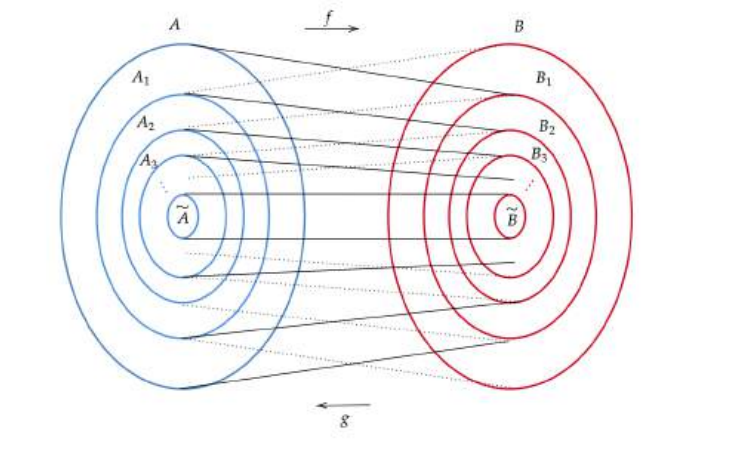
Demonstração. Seguimos o trabalho de "D. Tonien, *A simple visual proof of the Schröder-Bernstein theorem*. Elemente der Mathematik 62 (2007)".

Definimos as familias de conjuntos $\mathscr{F}_1 = \{A_i,\ i \in \mathbb{N}\}$ e $\mathscr{F}_1 = \{B_i,\ i \in \mathbb{N}\}$ em que

- $A_0 = A$ e $B_0 = B$
- se $i > 0$ então

$$A_i = g(B_{i-1}) \quad \text{e} \quad B_i = f(A_{i-1})$$

Graficamente



Observamos que, da injetividade de f e g, temos que existem bijeções

$$A \leftrightarrow B_1 \leftrightarrow A_2 \leftrightarrow B_3 \leftrightarrow A_4 \leftrightarrow \cdots$$

$$B \leftrightarrow A_1 \leftrightarrow B_2 \leftrightarrow A_3 \leftrightarrow B_4 \leftrightarrow \cdots$$

Por contrução

$$f(A_n) \subset B_n$$

e que

$$A_{i+1} \subset A_i \quad \text{e} \quad B_{i+1} \subset B_i \quad \forall\, i \in \mathbb{N},$$

de fato, para $i = 1$ temos

$$A_1 = g(B) \subset A \quad \text{e} \quad B_1 = f(A) \subset B.$$

Assuma que vale para n então $A_n \subset A_{n-1}$ e $B_n \subset B_{n-1}$ então

$$A_{n+1} = g(B_n) \subset g(B_{n-1}) = A_n$$

e

$$B_{n+1} = f(A_n) \subset f(A_{n-1} = B_n$$

de onde segue que vale para todo $n \in \mathbb{N}$.

Definimos agora as familias $\mathscr{F}_3 = \{C_i,\ i \in \mathbb{N}\}$ e $\mathscr{F}_4 = \{D_i,\ i \in \mathbb{N}\}$ em que

$$C_j = A_j \backslash A_{j+1} \quad D_j = B_j \backslash B_{j+1}.$$

Desta forma, $\mathscr{F}_3$ é uma partição de A e $\mathscr{F}_4$ é uma partição de B. Mais ainda os mapas

$$f|_{C_i} : C_i \to D_{i+1} \quad \text{e} \quad g|_{D_i} : D_i \to C_{i+1},$$

são bijetores para todo $i \in \mathbb{N}$, pois por um lado são injetores, e por outro lado são injetores e

$$\begin{aligned} f(C_i) &= f(A_i \backslash A_{i+1}) \\ &= f(A_i) \backslash f(A_{i+1}) \quad \text{(pois } f \text{ é injetor)} \\ &= B_{i+1} \backslash B_i = D_{i+1} \end{aligned}$$

$$\begin{aligned} g(D_i) &= g(B_i \backslash B_{i+1}) \\ &= f(B_i) \backslash f(B_{i+1}) \quad \text{(pois } g \text{ é injetor)} \\ &= A_{i+1} \backslash A_i = C_{i+1}. \end{aligned}$$

Sejam

$$\tilde{A} = \cap_{i\in\mathbb{N}} A_i \quad \text{e} \quad \tilde{B} = \cap_{i\in\mathbb{N}} B_i$$

Como $\tilde{B} \subset f(A)$ e

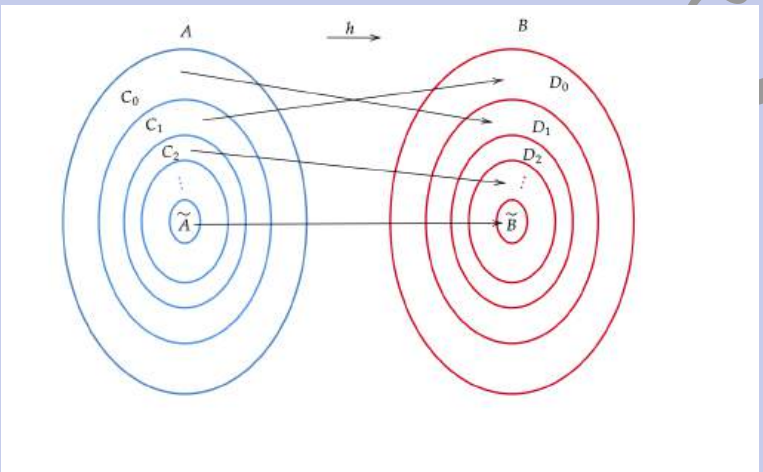
$$f^{-1}(\tilde{B}) = f^{-1}\left(\cap_{i\in\mathbb{N}} B_i\right) = \cap_{i\in\mathbb{N}} f^{-1}(B_i) = \cap_{i\in\mathbb{N}} A_i = \tilde{A},$$

temos que f é uma bijeção entre $\tilde{A}$ e $\tilde{B}$. De forma similar g é uma bijeção entre $\tilde{B}$ e $\tilde{A}$.

Construimos então $h : A \to B$ como

$$h(x) = \begin{cases} f(x) & \text{se} \quad x \in C_{2i} \\ g^{-1}(x) & \text{se} \quad x \in C_{2i+1} \\ f(x) = g^{-1}(x) & \text{se} \quad x \in \tilde{A}. \end{cases}$$

Como em cada elemento da partição h é bijetora, então h é bijetora de A em B.



■

As consequências deste resultado, para o caso dos conjuntos numéricos, é bem pouco intuitiva.

■ **Exemplo 11.8** Considere os conjuntos $A = (1,3)$ e $B = (1,3) \cup (4,5)$. Considere

$$f : A \to B, \quad f(x) = x,$$

e

$$g : B \to A, \quad g(x) = \begin{cases} \frac{3}{4} + \frac{1}{4}x & \text{se} \quad x \in (1,3) \\ x - 2 & \text{se} \quad x \in (4,5) \end{cases}.$$

Observamos as duas funções são injetoras. Para a primeira isto decorre trivialmente da definição pois

$$f(x_1) = f(x_2) \Rightarrow x_1 = x_2.$$

Mostrar a injetividade da função g requer um pouco de trabalho. Primeiramente observamos que se

$$1 < x < 3 \quad \to \quad 4 < 3 + x < 6 \quad \to \quad 1 < \frac{3+x}{4} < \frac{3}{2}$$

e se

$$4 < x < 5 \quad \to \quad 2 < x - 2 < 3.$$

De onde segue que $g(1,3) \cap g(4,5) = \emptyset$. Portanto se

$$g(x_1) = g(x_2) \quad \Rightarrow \quad [x_1 \in (1,3) \wedge x_2 \in (1,3)] \vee [x_1 \in (4,5) \wedge x_2 \in (4,5)]$$

Vemos cada caso por separado

- se $x_1 \in (1,3) \wedge x_2 \in (1,3)$ então

$$\frac{3+x_1}{4} = \frac{3+x_2}{4} \quad \Rightarrow \quad x_1 = x_2,$$

- se $x_1 \in (4,5) \wedge x_2 \in (4,5)$ então

$$x_1 - 2 = x_2 - 2 \quad \Rightarrow \quad x_1 = x_2.$$

Portanto, se $g(x_1) = g(x_2)$ temos que $x_1 = x_2$, de onde segue que g é injetora.

Agora, o teorema de Cantor-Bernstein-Schröder garante que existe uma função bijetora

$$h : (1,3) \to (1,3) \cup (4,5).$$

Veremos depois que isto implica que os dois conjuntos tem a mesma quantidade de elementos. ■

Um tipo particular de funções são as conhecidas como operações unárias e binárias.

Definição 11.6
- Dados dois conjuntos A e B uma operação unária é uma função $f : A \to B$.
- Dados três conjuntos A, B e C, uma operação binária é uma função $f : A \times B \to C$.

Obs.

- As operações unárias e binárias geralmente não são escritas na forma $f(a) = b$ (para a unária) ou $f(a,b) = c$ (para a binária) mas na forma
  - fa ou af para a unária, em que f é o símbolo da operação.
  - afb em que f é o símbolo utilizado para a operação binária.
- As operações binárias são a base do estudo de estruturas algébricas. Algumas delas veremos mais adiante no texto.

■ **Exemplo 11.9** Alguns exemplos de operações unárias são

- operação fatorial $! : \mathbb{N} \to \mathbb{N}$ dada por

  se $n = 0$ então $0! = 1$

  se $n > 0$ então $n! = n \cdot (n-1) \cdot (n-2) \cdots 2 \cdot 1$.
- o quadrado de um número $^2 : \mathbb{Z} \to \mathbb{N}$ definida por

$$n^2 = n \cdot n.$$

Alguns exemplos de operações binárias são

- Se $\mathscr{P}(A)$ o conjunto de partes de um conjunto A então a união

$$\cup : \mathscr{P}(A) \times \mathscr{P}(A) \to \mathscr{P}(A), \quad (U,V) \to U \cup V,$$

é uma operação binária.
- Se $\mathscr{P}$ é um conjunto formado por um número finito de proposições e de todas aquelas formadas a partir de conjunções de um número finitos delas, então a conjunção

$$\wedge : \mathscr{P} \times \mathscr{P} \to \mathscr{P}, \quad (p,q) \to p \wedge q,$$

é uma operação binária.

■

Dada uma familia de conjuntos $\mathscr{F} = \{A_i, i \in \mathbf{I}\}$ indexadas por um conjunto $\mathbf{I}$, consideramos o conjunto das funções

$$\mathscr{U} = \{f : \mathbf{I} \to \cup_{i \in \mathbf{I}} A_i,\ f(i) \in A_i\}$$

No caso em que $\mathbf{I} = \{1, \ldots, n\}$ este conjunto pode ser naturalmente identificado de forma bijetora com $A_1 \times \cdots A_n$ por meio da função

$$F : \mathscr{U} \to A_1 \times \cdots \times A_n, \quad F(f) = (f(1), \ldots, f(n))$$

Sua inversa é

$$F^{-1} : A_1 \times \cdots \times A_n \to \mathscr{U},$$

Neste caso $F^{-1}(a_1, \ldots, a_n) : \{1, \ldots, n\} \to \cup_{i=1}^{n} A_i$ é definida por

$$F^{-1}(f)(i) = a_i \quad \forall i = 1 \ldots n.$$

No caso de uma familia qualquer $\mathscr{F} = \{A_i, i \in \mathbf{I}\}$ o produto cartesiano é definido por

$$\prod_{i \in \mathbf{I}} A_i = \{f : \mathbf{I} \to \cup_{i \in \mathbf{I}} A_i, \ f(i) \in A_i\}.$$

Na definição de $\prod_{i \in \mathbf{I}} A_i$ cada $f \in \prod_{i \in \mathbf{I}} A_i$ é chamada de uma função escolha.

Nos seguintes casos temos garantida a função escolha:

- Para o caso em que $\mathbf{I}$ é finita, a existência de uma função escolha é garantida pois o produto cartesiano neste caso é não vazio como consequência dos axiomas de Zermelo-Fraenkel.
- Se $\mathbf{I} \neq \emptyset$ e todos os $A_i = A$ com A não vazio e, portanto existe $a \in A$ então a função constante $f(i) = a$ para todo $i \in \mathbf{I}$ existe e não precisamos do axioma da escolha.
- Se o conjuntos A_i são bem ordenados, então podemos definir $f(i)$ como sendo o menor elemento de A_i e não precisamos o axioma da escolha. De modo geral, se o conjunto tem alguma estrutura que permita diferenciar um elemento dele, podemos definir a função escolha utilizando esse elemento.
- Se temos um conjunto infinito de pares de bolinhas de gude brancas e queremos pegar uma de cada par, não temos como definir a função escolha e, portanto, não podemos garantir sua existência.

Desta forma para o caso infinito não podemos garantir que uma função dessas existe, ou equivalentemente, o produto cartesiano é não vazio. No entanto, isto é assumido como um axioma, que é o **Axioma da escoha:**

Para toda familia de conjuntos não vazios $\mathscr{F}$, seu produto cartesiano é não vazio.

Uma boa referência sobre o axioma da escolha e suas equivalências é: Jech T. J. - *The axiom of choice* - North Holland (1973).

É relevante também observar que o axioma da escolha é independente dos axiomas de Zermelo-Fraenkel. De fato, Godel mostrou que os axiomas de Zermelo-Fraenkel+(Axioma da escolha) são consistentes se os axiomas de Zermelo-Fraenkel são consistentes. Cohen mostrou que Zermelo-Fraenkel+ $\neg$(Axioma da escolha) são consistentes se os axiomas de Zermelo-Fraenkel são consistentes.

Nestas notas vamos assumir o axioma da escolha.

Em elaboração

II Conjuntos Numéricos

Em elaboração

12. Números Naturais

Começamos agora a estudar a construção dos conjuntos numéricos. Para responder à pergunta "o que é um número?" vamos mergulhar a resposta na teoria de conjuntos. Seguiremos assim a construção dos números naturais feita por von-Neuman (John von Neumann, matemático húngaro).

Vimos que,

- o axioma da existência garante a existência do conjunto vazio. Mais ainda, temos provado que o conjunto vazio é subconjunto de qualquer conjunto.
- o axioma do infinito, garante que para todo conjunto A existe o seu conjunto sucessor $s(A) = A \cup \{A\}$ que, junto ao axioma da regularidade e o axioma do par, é diferente $\{\emptyset, s(A)\}$.

Definição 12.1 Um conjunto A é dito indutivo se

- $\emptyset \in A$,
- $a \in A \rightarrow s(a) = a \cup \{a\} \in A$.

Obs. Observar que não fazemos distinção entre elemento e conjunto assim como foi dito nos axiomas de Zermelo-Fraenkel.

Assim,construimos um conjunto indutivo da seguinte forma começamos com o conjunto $\emptyset$, que denotamos por 0, e construímos os seus sucessores

- $0 = \emptyset$
- $1 = s(0) = \emptyset \cup \{\emptyset\} = \{\emptyset\} = \{0\}$
- $2 = s(1) = 1 \cup \{1\} = \{\{\emptyset\}, \{\{\emptyset\}\}\} = \{0,1\}$
- $3 = s(2) = 2 \cup \{2\} = \{\{\emptyset\},\ \{\{\emptyset\}\},\ \{\{\emptyset\},\ \{\{\emptyset\}\}\}\} = \{0,1,2\}$
- ...

O conjunto formado por todos estes elementos é naturalmente indutivo. Chamamos ao conjunto formado por todos estes elementos de $\mathcal{N}$.

Obs.

- Na verdade o conjunto $\mathcal{N}$ pode ser definido de forma mais precisa do que listando simplesmente os seus elementos. O mais correto seria dizer que $\mathcal{N}$ é o conjunto de elementos que satisfaz
  - para cada $a \in \mathcal{N}$ e $b, c \in a$ tais que $b \neq c$ temos que $b \in c$ ou $c \in b$. Mais ainda, se $c \in b \in a$ então $c \in a$.

  - O único $a \in \mathcal{N}$ elemento que não é sucessor de outro é 0.
  - todo elemento $a \neq 0$ tem um elemento, que chamamos de $a-1$, que não tem sucessor dentro de a, isto é

$$a = (a-1) \cup \{(a-1)\}$$

- Cada conjunto $n \in \mathcal{N}$ como construído acima tem precisamente "n" elementos. Mais ainda, cada sucessor $s(n)$ contém $0, 1, \ldots, n$.

Corolário 12.1 Se $s(n) = s(m)$ então $n = m$.

Demonstração. Provamos isto provanto a contrapositiva. Se $n \neq m$ então, por exemplo, existe k tal que $k \in n$ e $k \notin m$. Tal $k \neq 0$ pois $0 \in m$ e $0 \in n$. Temos então que $s(k) \in n$ mas $s(k) \notin m$. Portanto $s(n) \neq s(m)$. ■

A seguinte é a definição que caracteriza o conjunto dos números naturais. Veremos que esta caracterização vai ser utilizada para definir a soma, o produto e suas respectivas propriedades.

Definição 12.2 Um número natural é um conjunto que pertence a todo conjunto indutivo. O conjunto de todos estes elementos é chamado conjunto dos números naturais e o denotamos por $\mathbb{N}$.

O conjunto dos números naturais é indutivo pois

- $\emptyset \in \mathbb{N}$ já que $\emptyset$ está en todo conjunto indutivo
- se $A \in \mathbb{N}$ então $A \subset U$ para todo U indutivo. Portanto $S(A) \subset U$ para todo U indutivo. De onde $s(A) \in \mathbb{N}$

Obs. Pedir que os números naturais estejam em todo conjunto indutivo é uma condição de minimalidade. De fato podemos pensar num conjunto $\mathcal{M}$ que esteja construído a partir dos conjunto $\emptyset$ e A e todos seus sucessores. Claramente $\mathcal{M}$ é indutivo, no entanto seus elementos não vão estar em todos os conjuntos indutivos. Por exemplo A não está em $\mathcal{N}$.

Mostramos a seguir que existem os números naturais.

Teorema 12.1 Existe um conjunto cujos elementos são exatamente os números naturais

Demonstração. Temos construído o conjunto indutivo $\mathcal{N}$ utilizando o axioma da existência e do infinito. Claramente, todo conjunto indutivo U contém $\mathcal{N}$. De fato, $0 \in U$ pois $\emptyset \in U$ por U ser indutivo. Se existe $n \notin U$ então o conjunto

$$\{k \in n+1,\ k \notin U\}$$

é não vazio, portanto tem ao menos um elemento n^*. Claramente $n^* \neq 0$ pois $0 \in U$. Então $n^* = k+1$ para algum $k \in U$. Mas como U é indutivo $n^* = k+1$, contradizendo a definição de n^*.

Pelo axioma da especificação a função proposicional

$$x \in U \Leftrightarrow [x \in \mathcal{N} \wedge (\forall\ B \text{ conjunto indutivo},\ x \in B)]$$

tem um domínio que, por definição, deve ser $\mathbb{N}$. ■

Temos assim que o conjunto $\mathbb{N}$ é indutivo e é um subconjunto de todo conjunto indutivo.

Teorema 12.2 O conjunto $\mathcal{N}$ construído acima coincide com $\mathbb{N}$. Mais ainda, todo número natural diferente de 0 é sucessor de algúm número natural.

Demonstração. Sabemos que como $\mathbb{N}$ é indutivo $\mathcal{N} \subset \mathbb{N}$ e como $\mathbb{N}$ é indutivo e está contido em todo conjunto inductivo temos que $\mathbb{N} \subset \mathcal{N}$. De onde segue que $\mathcal{N} = \mathbb{N}$.

Para o restante do resultado observamos que a proposição

$$\exists\ a \in \mathbb{N},\ 0 = s(a)$$

é falsa pois não existe conjunto cujo sucessor seja $\emptyset$. Portanto, a negação da proposição é verdadeira de onde segue o resultado. ■

Teorema 12.3 — Princípio de indução ou Axioma indução. Todo subconjunto indutivo de $\mathbb{N}$ coincide com $\mathbb{N}$.

Demonstração. Assuma que $B \subset \mathbb{N}$. Como B é indutivo temos que $\mathbb{N} \subset B$ pelo teorema anterior. Portanto $B = \mathbb{N}$. ■

Portanto, para mostrar que um conjunto $M \subset \mathbb{N}$ é o conjunto dos número naturais mostramos o resultado do teorema, isto é:

Princípio de Indução: Se $M \subseteq \mathbb{N}$ tal que
i- $0 \in M$
ii- $k \in M \Rightarrow s(k) \in M,\ \forall\, k \in M$
então $M = \mathbb{N}$.

Definição 12.3 Dado $m,\ n \in \mathbb{N}$, definimos recursivamente
- $m + 0 = m$
- $m + s(n) = s(m+n)$

Obs. Observamos, da definição, que
- Como
$$m + s(0) = s(m+0) = s(m).$$
Se $s(0) = 1$ então faz sentido a definir $k+1 = s(k)$ pois
$$k + 1 = k + s(0) = s(k+0) = s(k).$$
- Se $n \neq 0$ então $n = s(p)$ para algum $p \in \mathbb{N}$, de onde
$$m + n = m + s(p) = s(m+p).$$

Utilizando a definição dos números naturais é possível mostrar que

Proposição 12.1 Para quaisquer $m,\ n,\ p \in \mathbb{N}$ temos
- $m+n$ está definido.
- O número 0 é o único natural tal que $m+0 = m = 0+m$ (existência de elemento neutro)
- $m + (n+p) = (m+n) + p$ (associatividade)
- $m+n = n+m$ (comutatividade)
- $m+p = n+p \Rightarrow m = n$ (cancelamento).
- $m+n = 0$ então $m = 0$ e $n = 0$.

Demonstração.
- Para cada $m \in \mathbb{N}$, considere o conjunto
$$M_m = \{n \in \mathbb{N},\ n+m \text{ está definido}\}.$$
Então $0 \in M_m$ pois $m+0$ está definido. Se $k \in M_m$ então $m+k$ está definido. Como
$$m + s(k) = s(m+k)$$
temos que $s(k) \in M_m$. Pelo princípio de indução temos que $\mathbb{N} \subset M_m$, de onde segue o pedido.
- Da definição $m+0 = m$. Seja
$$M = \{m \in \mathbb{N},\ 0+m = m\}$$
claramente $0 \in M$ pois $0+0 = 0$ da definição. Se $k \in \mathbb{N}$ então $0+k = k$, como
$$k+1 = s(k) = s(0+k) = 0 + s(k),$$

temos que $k+1 \in M$ de onde $M = \mathbb{N}$.
Por último se existe n tal que $m+n = m = n+m$ para todo natural m temos, em particular,

$$0 = 0+n = n+0 = n.$$

Portanto o 0 é único.

- Primeiramente observamos que $m+1 = 1+m$. Para isto, defina

$$M = \{n \in \mathbb{N},\ 1+m = m+1\}.$$

Claramente $0 \in M$ pois $1+0 = 1$ e $0+1 = s(0+0) = s(0) = 1$. Por outro lado se $k \in M$ então

$$s(m)+1 = (1+m)+1 = s(1+m) = s(s(m)) = 1+s(m),$$

de onde $M = \mathbb{N}$.
Seja $m \in \mathbb{N}$ e defina

$$M_m = \{n \in \mathbb{N},\ n+m = m+n\}.$$

Claramente $0 \in M_n$ pelo item anterior. Se $k \in M$ então $n+k = k+m$, como

$$\begin{aligned} m+(k+1) &= m+s(k) \\ &= s(m+k) \\ &= s(k+m) \\ &= k+m+1 \\ &= (k+1)+m \end{aligned}$$

de onde $s(k) \in M_n$ e portanto $M_n = \mathbb{N}$.

- Dados $m,\ n \in \mathbb{N}$ considere

$$M_{m,n} = \{p \in \mathbb{N},\ m+p = n+p \Rightarrow m = n\}.$$

Claramente $0 \in M_{n,m}$. Agora se $k \in M_{m,n}$ temos que $m+k = n+k \Rightarrow n = m$. Observamos que

$$\begin{aligned} m+s(k) = n+s(k) &\Rightarrow m+k+1 = n+k+1 \\ &\Rightarrow m+k = n+k, \end{aligned}$$

de onde $m = n$. Portanto $s(k) \in M_{m,n}$ e $M_{m,n} = \mathbb{N}$.

- Assuma que $m+n = 0$ então, se $n \neq 0$

$$m+n = m+s(n_1) = s(m+n_1) \neq 0.$$

Logo $n = 0$ de onde $m+0 = 0$ garante $m = 0$

■

De forma similar definimos o produto de números naturais.

Definição 12.4 Dados $m,\ n \in \mathbb{N}$, definimos recursivamente

- $m \cdot 0 = 0$
- $m \cdot (n+1) = m \cdot n + m$

Obs.

- Da definição, que

$$m \cdot 1 = m \cdot (0+1) = m \cdot 0 + m = 0 + m = m$$

- a partir do produto definimos a potenciação como segue, para $a,\ n \in \mathbb{N}$, definimos a^n como sendo

$$a^n = \overbrace{a \cdot a \cdots a}^{n \text{ vezes}}$$

se $n > 0$ e

$$a^0 = 1.$$

no caso em que $a \neq 0$. Observamos que 0^0 não está definido.

Utilizando a definição dos números naturais junto com as propriedades da soma é possível mostrar que

Proposição 12.2 Para quaisquer $m,\ n,\ p \in \mathbb{N}$ temos

- $0 \cdot m = 0$.
- $m \cdot n$ está definida.
- O número 1 é o único natural tal que $m \cdot 1 = m$ (existência de elemento neutro)..
- $m \cdot (n+p) = m \cdot n + m \cdot p$, e $(n+p) \cdot m = n \cdot m + p \cdot m$ (distributividade).
- $m \cdot n = n \cdot m$ (comutatividade).
- $m \cdot (n \cdot p) = (m \cdot n) \cdot p$ (associatividade)
- se $p \neq 0$ então $m \cdot p = n \cdot p \Rightarrow m = n$ (cancelamento).
- $m \cdot n = 0$ então $m = 0$ ou $n = 0$.

Demonstração.

- Seja

$$M = \{m \in \mathbb{M},\ 0 \cdot m = 0\}.$$

Claramente $0 \in M$. Se $k \in M$ então

$$0 \cdot s(k) = 0 \cdot k + 0 \cdot 1 = 0 + 0 = 0.$$

Pelo princípio de indução $M = \mathbb{N}$.

- Seja $m \in \mathbb{N}$ e defina

$$M = \{n \in \mathbb{N},\ m \cdot n \text{ está definida.}\}$$

Claramente $0 \in M$. Assuma que $k \in M$ então

$$m \cdot s(k) = m \cdot (k+1) = m \cdot k + m.$$

Como ambos termos estão definidos e a soma está definida, temos $s(k) \in M$ de onde $M = \mathbb{N}$.

- Seja

$$M = \{m \in \mathbb{N},\ 1 \cdot m = m\}.$$

Claramente $0 \in M$. Se $k \in M$ então

$$1 \cdot s(k) = 1 \cdot k + 1 \cdot 1 = k + 1 = s(k).$$

Portanto $s(k) \in M$ e $M = \mathbb{N}$. Para ver a unicidade observamos que se n é tal que $m \cdot n = m = n \cdot m$ para todo $m \in \mathbb{N}$ então

$$1 = 1 \cdot n = n \cdot 1 = n.$$

- Sejam $m,\ n \in \mathbb{N}$ e considere

$$M_{m,n} = \{p \in \mathbb{N},\ m \cdot (n+p) = m \cdot n + m \cdot p\}.$$

Claramente $0 \in M_{m,n}$. Assuma que $k \in M_{m,n}$ então

$$\begin{aligned} m\cdot(n+s(k)) &= m\cdot(n+k+1) \\ &= m\cdot(n+k)+m \\ &= m\cdot n+m\cdot k+m \\ &= m\cdot n+m\cdot(k+1) \\ &= m\cdot n+m\cdot s(k) \end{aligned}$$

de onde $s(k) \in M_{m,n}$ e, portanto, $\mathbb{N} = M_{m,n}$.
A outra identidade se prova de forma similar.

- Seja $m \in \mathbb{N}$ e defina o conjunto

$$M_m = \{n \in \mathbb{N},\ m\cdot n = n\cdot m\}.$$

Vejamos que $0 \in M$. para isto defina

$$N = \{m \in \mathbb{N},\ 0\cdot n = 0 = n\cdot 0\}$$

então $0 \in N$. Se $k \in N$ então $0\cdot k = 0 = k\cdot 0$. Como

$$0\cdot s(k) = 0\cdot(k+1) = 0\cdot k+0 = 0 = s(k)\cdot 0$$

temos que $s(k) \in N$ e, portanto, $N = \mathbb{N}$. De onde $0 \in M_m$.
Se $p \in M_m$ então $m\cdot p = p\cdot m$. Como

$$m\cdot s(p) = m\cdot p+m = p\cdot m+m = (p+1)\cdot m$$

temos que $s(p) \in M_m$ de onde $M_m = \mathbb{N}$.

- Sejam $m,\ n \in \mathbb{N}$ e considere

$$M_{m,n} = \{p \in \mathbb{N},\ m\cdot(n\cdot p) = (m\cdot n)\cdot p\}.$$

Claramente $0 \in M_{m,n}$. Assuma que $k \in M_{m,n}$, então

$$\begin{aligned} m\cdot(n\cdot s(k)) &= m\cdot(n\cdot(k+1)) \\ &= m\cdot(n\cdot k)+m\cdot n \\ &= (m\cdot n)\cdot k+(m\cdot n) \\ &= (m\cdot n)\cdot(k+1) \\ &= (m\cdot n)\cdot s(k). \end{aligned}$$

Portanto $s(k) \in M_{m,n}$ e $\mathbb{N} = M_{m,n}$.

- Se $m = n = 0$ não ha nada que provar. Claramente se $m = 0$ então $n = 0$ pois caso contrário a identidade não vale. Assuma $m \neq 0$, $n \neq 0$, que $m = n+k$ com $k \neq 0$, isto é $k = s(k_1)$. Se

$$m\cdot p = n\cdot p,$$

temos

$$\begin{aligned} m\cdot p &= n\cdot p+n\cdot k \\ &= n\cdot p+n\cdot s(k_1) \\ &= n\cdot p+n\cdot k_1+n \end{aligned}$$

então $0 = n\cdot k_1+n$ de onde $n = 0$ o que é uma contradição. Portanto $k = 0$ e $m = n$.

- Assuma que $m\cdot n = 0$ e assuma que $n \neq 0$ então $n = s(n_1)$ de onde

$$0 = m\cdot n = m\cdot s(n_1) = m\cdot n_1+m$$

então $m\cdot n_1 = 0$ e $m = 0$.

■

Definição 12.5 Sejam $k, m \in \mathbb{N}$ números naturais. Dizemos que $m > k$ (ou $k < m$) se existem um número $l \in \mathbb{N}$ tal que $l \neq 0$ e

$$m = k + l.$$

Dizemos que uma função proposicional $P(n)$ vale para todo $n \geq k$ se ela for verdadeira para $n = k$ e para todo m tal que $m > k$.

Obs.

- Dados $m,\ n \in \mathbb{N}$, denotamos
  - $m \geq n$ se, e somente se, $n \leq m$.
  - $m > n$ se, e somente se, $n < m$.
- Não é necessário definir a soma para definir $a < b$. De fato, utilizando a construção dos naturais feita acima podemos dizer que dados $a,\ b \in \mathbb{N}$ dizemos que

$$a < b \quad \Leftrightarrow \quad a \in b.$$

- Voltaremos mais tarde sobre isto e veremos que ">"induz o que chamamos uma "relação de ordem total"

O princípio de indução fornece uma técnica muito útil para provar que uma proposição é verdadeira a partir de um certo número natural. Éste é o conteúdo do seguinte teorema.

Teorema 12.4 — Princípio de Indução generalizada. Seja $k \in \mathbb{N}$ um número natural fixo e $P(n)$ uma função propocicional com domínio em $\mathbb{N}$. Se

- $P(k)$ é verdadeira e
- se, para todo $r > k$, $P(r)$ verdadeira garante que $P(r+1)$ é verdadeira,

então, $P(n)$ é verdadeira para todo $n \geq k$.

Demonstração. Para demonstrar o teorema utilizamos o princípio de indução. Definimos a função proposicional

$$Q(n) = P(n+k) \quad M = \{n \in \mathbb{N},\ Q(n) \text{ é verdadeira}\}$$

Observamos que

- $Q(0) = P(k)$ é verdadeira, então $0 \in M$
- se $r \in M, \Rightarrow Q(r) = P(k+r)$ é verdadeira então $Q(r+1) = P(k+r+1)$ é verdadeira e, portanto, $r+1 \in M$.

De onde segue que M satisfaz $i-$ e $ii-$ do princípio de indução, de onde segue que $M = \mathbb{N}$.

Isto garante que $Q(n)$ é verdadeira para todo $n \geq 0$, que é equivalente a dizer que $P(n)$ é verdadeira para todo $n \geq k$. ■

■ **Exemplo 12.1** 1. Provar que $10^n - 1$ é divisível por 3 para todo $n \geq 1$.

Para isto construímos a função proposicional

$$P(n) = 10^n - 1 \text{ é divisível por } 3$$

e seja M o seu domínio de verdade. Observamos que

- $1 \in M$ pois

$$10^1 - 1 = 9 = 3 \cdot 3$$

- Assuma que $k \in M$ então existe $K \in \mathbb{N}$ tal que $3 \cdot K = 10^k - 1$. Vemos que $k+1 \in M$, de fato

$$\begin{aligned} 10^{k+1} - 1 &= 10 \cdot 10^k - 1 \\ &= 9 \cdot 10^k + 10^k - 1 \\ &= 9 \cdot 10^k + 3 \cdot K \\ &= 3 \cdot (3 \cdot 10^k + K) \end{aligned}$$

Agora, pelo princício de indução, $M = \mathbb{N}$ e temos que $P(n)$ vale para todo $n \geq 1$.

2. Provar que, para todo $n \geq 1$, temos

$$\sum_{i=1}^{n} i^3 = 1^3 + 2^3 + \cdots + n^3 = \frac{n^2(n+1)^2}{4}.$$

Para isto construímos a função proposicional

$$P(n) = 1^3 + 2^3 + \cdots + n^3 = \frac{n^2(n+1)^2}{4}.$$

e seja M o seu domínio de verdade. Observamos que

- observamos que $1 \in M$ pois

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

- Assuma que $k \in M$ então

$$1^3 + 2^3 + \cdots + k^3 = \frac{k^2(k+1)^2}{4}.$$

Vemos que $k+1 \in M$, de fato

$$\begin{aligned} 1^3 + 2^3 + \cdots + k^3 + (k+1)^3 &= \frac{k^2(k+1)^2}{4} + (k+1)^3 \\ &= \frac{(k+1)^2}{4}(k^2 + 4k + 4) \\ &= \frac{(k+1)^2}{4}(k+2)^2 \\ &= \frac{(k+1)^2(k+2)^2}{4} \end{aligned}$$

Agora, pelo princício de indução, $M = \mathbb{N}$ e temos que $P(n)$ vale para todo $n \geq 1$.

3. Provar que $4^n - 1$ é divisível por 3 para todo $n \geq 1$.
Para isto construímos a função proposicional

$$P(n) = 4^n - 1 \text{ é divisível por } 3$$

e seja M o seu domínio de verdade. Observamos que

- $1 \in M$ pois

$$4^1 - 1 = 9 = 3.$$

- Assuma que $k \in M$ então existe $K \in \mathbb{N}$ tal que $3 \cdot K = 4^k - 1$. Vemos que $k+1 \in M$, de fato

$$\begin{aligned} 4^{k+1} - 1 &= 4 \cdot 4^k - 1 \\ &= 3 \cdot 4^k + 4^k - 1 \\ &= 3 \cdot 4^k + 3 \cdot K \\ &= 3 \cdot (4^k + K) \end{aligned}$$

Agora, pelo princício de indução, $M = \mathbb{N}$ e temos que $P(n)$ vale para todo $n \geq 1$.

4. Sejam Q, P_1, $P_2, \cdots$ proposições. Provar que

$$Q \wedge (P_1 \vee P_2 \vee \cdots \vee P_n) = (Q \wedge P_1) \vee (Q \wedge P_2) \vee \cdots \wedge (Q \wedge P_n)$$

para todo $n \in \mathbb{N}$.
Para isto construímos a função proposicional

$$R(n) = Q \wedge (P_1 \vee P_2 \vee \cdots \vee P_n) = (Q \wedge P_1) \vee (Q \wedge P_2) \vee \cdots \wedge (Q \wedge P_n)$$

e seja M o seu domínio de verdade. Observamos que

- observamos que $1 \in M$ pois

$$Q \wedge (P_1) = (Q \wedge P_1).$$

- Assuma que $k \in M$ então

$$Q \wedge (P_1 \vee P_2 \vee \cdots \vee P_k) = (Q \wedge P_1) \vee (Q \wedge P_2) \vee \cdots \wedge (Q \wedge P_k).$$

Vemos que $k+1 \in M$, de fato

$$\begin{aligned} Q \wedge (P_1 \vee P_2 \vee \cdots \vee P_{k+1}) &= Q \wedge [(P_1 \vee P_2 \vee \cdots \vee P_k) \vee P_{k+1}] \\ &= Q \wedge (P_1 \vee P_2 \vee \cdots \vee P_k) \vee (Q \wedge P_{k+1}) \\ &= (Q \wedge P_1) \vee (Q \wedge P_2) \vee \cdots \wedge (Q \wedge P_k) \vee (Q \wedge P_{k+1}) \end{aligned}$$

Agora, pelo princício de indução, $M = \mathbb{N}$ e temos que $R(n)$ vale para todo $n \geq 1$.

5. Para mostrar que uma proposição $P(n)$ com nomínio nos naturais é válida para todos os naturais $n \geq k$ temos que ver sempre que $P(k)$ é verdadeira não bastando mostrar que $P(n)$ verdadeira implica $P(n+1)$ verdadeira. De fato, observe que se

$$P(n) = \text{"}4^n = 4^{n+1} \quad \forall\, n \in \mathbb{N}\text{"}$$

Claramente se $P(n)$ é verdadeira temos

$$4^n = 4^{n+1} \Rightarrow 4 \cdot (4^n) = 4 \cdot 4^{n+1} \Rightarrow 4^{n+1} = 4^{n+2}$$

de onde $P(n+1)$ é verdadeira. No entanto sabemos que $P(0)$ é falsa e, portanto, o axioma de indução não nos permite concluir nada.

■

Em elaboração

13. Cardinalidade de conjuntos

Procuramos mensurar de alguma forma o tamanho dos conjuntos. Quando o conjunto tem um número natural de elementos isso pode ser feito simplesmente ao contar seus elementos. No entanto, se esse não for o caso, como mensuramos o conjunto? o que significa neste caso que dois conjuntos tem a mesma quantidade de elementos? É sobre isso que trata o conteúdo deste capítulo.

Começamos com algumas definições.

Definição 13.1

- A cardinalidade de um conjunto A é quantidade elementos de um conjunto. Denotamos a cardinalidade de A pelo símbolo $\sharp A$.
- Um número cardinal é o símbolo utilizado para designar a cardinalidade de um conjunto.
- Dados dois conjuntos A e B dizemos que $\sharp A \leq \sharp B$, se existe uma função injetora $f : A \to B$.
- Dois conjuntos A e B tem a mesma cardinalidade, é denotamos $\sharp A = \sharp B$, se existe uma função bijetora $f : A \to B$.

Obs. Dados dois conjuntos A, B tais que $\sharp A \leq \sharp B$ e assuma que não existe uma função bijetora $f : A \to B$ então dizemos que $\sharp A \neq \sharp B$ e, neste caso, denotamos

$$\sharp A < \sharp B.$$

Corolário 13.1 Se $A \subset B$ então $\sharp A \leq \sharp B$

Demonstração. Segue da injetividade da função $f : A \to B$ dada por $f(a) = a$. ■

Teorema 13.1 Seja A um conjunto, então $\sharp A < \sharp \mathscr{P}(A)$.

Demonstração. Dado A conjunto defina $f : A \to \mathscr{P}(A)$ como $f(a) = \{a\}$. Então f é injetora e $\sharp A \leq \sharp \mathscr{P}(A)$.

Seja $g : A \to \mathscr{P}(A)$ e considere o conjunto

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

Claramente, se existe $a \in A$ tal que $g(a) = B$ então temos que

$$a \in B \quad \text{se, e somente se} \quad a \notin B,$$

o que é uma contradição. De onde $B \notin \text{Img}(g)$.

Como para toda função podemos construir um tal conjunto B temos que nunca existe uma função sobrejetora de $A \to \mathscr{P}(A)$ e, portanto, não pode existir uma função bijetora. De onde segue que a cardinalidade dos conjuntos é diferente. ■

Corolário 13.2 Não existe um conjunto com cardinalidade maior do que todos os outros conjuntos.

Lema 13.1 Sejam A e B dois conjuntos. Assuma que existe uma função sobrejetora $f : A \to B$. Então $\sharp B \leq \sharp A$.

Demonstração. Para a prova utilizamos o axioma da escolha. Dado $b \in B$ escolhemos $a_b \in A$ tal que $f(a_b) = b$. Observamos que para cada b temos um único a_b. Seja $\tilde{A} = \cup_{b\in B} a_b \subset A$ e defina

$$h : \tilde{A} \to B, \quad h(a_b) = b$$

Claramente, h é bijetora por construção. Então temos

$$\sharp B = \sharp \tilde{A} \leq \sharp A.$$

■

Lema 13.2 Sejam A e B dois conjuntos. Assuma que $\sharp A \leq \sharp B$ e que $a \in A$ e $b \in B$ são dois elementos. Então

$$\sharp(A\backslash\{a\}) \leq \sharp(B\backslash b)$$

Demonstração. Seja $f : A \to B$ injetora. Seja $\tilde{A} = A\backslash\{a\}$, $\tilde{B} = B\backslash\{b\}$ e $a_0 \in A$ tal que $f(a_0) = b$. Definimos $h : \tilde{A} \to \tilde{B}$ por

$$h(x) = \begin{cases} f(x) & \text{se} \quad x \neq a_0 \\ f(a) & \text{se} \quad x = a_0 \end{cases}$$

Então h é injetora de onde segue o resultado. ■

Dada uma familia de conjuntos $\mathscr{F} = \{A_i,\ i \in \mathbf{I}\}$ podemos introduzir a relação

$A_i \sim A_j$ se tem a mesma cardinalidade.

A relação assim definida é de equivalência, de fato

- $A \sim A$ pois a função identidade $I(x) = x$ é bijetora.
- para todo $A,\ B \in \mathscr{F}$, se $A \sim B$ então existe $f : A \to B$ bijetora, de onde $f^{-1} : B \to A$ bijetora e, portanto, $B \sim A$.
- para todo $A,\ B,\ C \in \mathscr{F}$ se $A \sim B$ e $B \sim C$ então, como composição de funções bijetoras é bijetora, temos existe uma bijeção de $f : A \to C$. Portanto $A \sim C$

Lembramos que cada número natural n é um subconjunto de um conjunto indutivo, isto é

$$n + 1 = \{0, 1, 2, \ldots, n\}.$$

Definição 13.2 Um conjunto A é dito finito se ele tem a mesma cardinalidade que o conjunto correspondente um $n \in \mathbb{N}$. Neste caso, o cardinal de A será representado pelo número natural que tem a mesma cardinalidade que A.

Caso o conjunto não seja finito, ele será dito infinito.

Com a definição acima, se A um conjunto finito, o cardinal de A, que denotamos por $\sharp A$, é

- $\sharp A = 0$ se $A = \emptyset$.
- $\sharp A = n$ se A tem a mesma cardinalidade que $\{0, 1, 2, \ldots, n-1\}$ ou $\{1, 2, \ldots, n\}$.

■ **Exemplo 13.1**

- Da definição, todo conjunto A que tem a mesma cardinalidade com algúm conjunto da forma

$$\{0,1,2,3,\ldots,n\}$$

para algum $n \in \mathbb{N}$ é finito.

- Considere $P \subset \mathbb{N}$ dado por

$$P = \{3 \cdot k,\ k \in \mathbb{N}\}$$

Claramente a função $f : P \to \mathbb{N}$ dada por $f(x) = x$ é injetora. Por outro lado a função $g : \mathbb{N} \to P$ é também injetora. Agora o Teorema de Cantor-Bernestein Schröder garante a existência de uma bijeção. De onde segue que $\mathbb{N}$ não é finito.

■

Teorema 13.2 Seja A um conjunto. Então A é um conjunto finito se, e somente se, para todo subconjunto próprio $B \subset A$ temos $\sharp B \neq \sharp A$.

Demonstração. Assuma que A é finito e de cardinalidade n. Se $B \subset A$ própriamente, então B contém, pelo menos, um elemento menos que A e portanto terá cardinalidade $\sharp B \leq n-1 < n = \sharp B$. de onde $\sharp A \neq \sharp B$.

Por outro lado, se A é infinito, utilizando o axioma da escolha podemos escolher para cada $n \in \mathbb{N}$ um conjunto $B_n \subset A$ de cardinalidade n e de forma tal que $B_n \subset B_{n+1}$ (isto é, na verdade, consequência do princípio da boa ordem). Desta forma, se A é infinito existe $f : \mathbb{N} \to A$ injetora. Seja $g : A \backslash \{f(0)\} \to A$ definida por

$$g(a) = \begin{cases} a & \text{se} \quad a \notin \text{Img}(f) \\ g(a) = f(n-1) & \text{se} \quad a = f(n) \end{cases}.$$

Claramente g é injetora e sobrejetora. De onde $\sharp A = \sharp A \backslash \{f(0)\}$. Então A é infinito e existe um subconjunto próprio de A com a mesma cardinalidade que A. De onde provamos que A finito implica que todo subconjunto próprio tem caridalidade menor do que A. ■

■ **Exemplo 13.2**

- $A = \{a,b,c,d,e\}$ e $B = \{1,2,3,4,5\}$ são finitos e tem a mesma cardinalidade. Mais ainda $A \sim B$ pela correspondência

$$a \leftrightarrow 1 \quad b \leftrightarrow 2 \quad c \leftrightarrow 3 \quad d \leftrightarrow 4 \quad 5 \leftrightarrow e$$

- $A = \mathbb{N}$ e $B = \{2n,\ n \in \mathbb{N}\}$ tem a mesma cardinalidade e não são finitos. Mais ainda $A \simeq B$ pela correspondência

$$n \leftrightarrow 2n.$$

■

Assim como no conjunto dos números naturais é possível definir um operação soma e produto entre números cardinais, básicamente, a ideia é que se $\alpha = \sharp A$ e $\beta = \sharp B$ são dois números cardinais com $A \cap B = \emptyset$, então

$$\alpha + \beta = \sharp(A \cup B) \quad \text{e} \quad \alpha \cdot \beta = \sharp(A \times B).$$

No caso $0 = \sharp\emptyset$ é o elemento neutro da soma e 1 é o neutro do produto.

Mais ainda, $\alpha = \sharp A$ e $\beta = \sharp B$, podemos definir

$$\beta^{\alpha} = \sharp\{f : A \to B,\ \text{função}\}.$$

No caso, $0^0 = 1$ para números cardinais pois a única função que satisfaz é a que corresponde a relação nula $\emptyset = \emptyset \times \emptyset$.

Com isto temos os seguintes resultados para conjuntos finitos.

Proposição 13.1 Sejam A e B dois conjuntos finitos de um universo U. Então

$$\sharp(A\cup B)+\sharp(A\cap B)=\sharp A+\sharp B.$$

Demonstração. Assuma que

$$A=\{a_1,\ldots,a_k,a_{k+1}\ldots,a_n\}\qquad B=\{a_1,\ldots,a_k,b_1,\ldots b_m\}.$$

Então

$$A\cup B=\{a_1,\ldots,a_n,b_1,\ldots,b_m\}\qquad A\cap B=\{a_1,\ldots,a_k\}.$$

Temos assim as seguintes bijeções

$$\begin{aligned} A &\leftrightarrow \tilde{A}=\{1,2,\ldots,n\}\\ B &\leftrightarrow \tilde{B}=\{n+1,n+2,\ldots,n+m+k\}\\ A\cup B &\leftrightarrow \tilde{C}=\{1,2,\ldots,n+m\}\\ A\cap B &\leftrightarrow \tilde{D}=\{n+m+1,\ldots,n+m+k\} \end{aligned}$$

Observamos que $\tilde{A}\cap\tilde{B}=\emptyset$ e que $\tilde{C}\cap\tilde{D}=\emptyset$. Portanto

$$\begin{aligned} \sharp(A\cup B)+\sharp(A\cap B) &= \sharp\{1,2,\ldots,n+m\}+\sharp\{n+m+1,\ldots,n+m+k\}\\ &= \sharp\{1,\ldots,n+m+k\}\\ &= n+m+k\\ &= n+(m+k)\\ &= \sharp\{1,2,\ldots,n\}+\sharp\{n+1,n+2,\ldots,n+m+k\}\\ &= \sharp A+\sharp B. \end{aligned}$$

■

Corolário 13.3 Sejam α e β números cardinais finitos, então a soma entre eles tem como resultado o valor da soma como números naturais $\alpha\cdot\beta$.

Teorema 13.3 Para todo $n\in\mathbb{N}$ temos que se A é um conjunto tal que $\sharp A=n$ então $\sharp\mathscr{P}(A)=2^n$.

Demonstração. Vamos a mostrar o resultado pelo princípio de indução e assumindo a bijeção com conjuntos disjuntos para poder fazer a soma. Para isto construimos a função proposicional,

$$P(n)=\text{"}A\text{ é um conjunto tal que }\sharp A=n\text{ então }\sharp\mathscr{P}(A)=2^n.\text{"}$$

Seja $M\subset\mathbb{N}$ o domínio de verdade de $P(n)$.

Observamos que para $0\in M$ pois, neste caso, $A=\emptyset$ de onde $\mathscr{P}(A)=\{\emptyset\}$ que contém $1=2^0$ elementos.

Assuma que $k\in M$ vamos ver que $k+1$ em M também. De fato se

$$A=\{a_1,\ldots,a_k,a_{k+1}\}$$

escrevemos $A=A_1\cup A_k$ em que

$$A_1=\{a_1,\ldots,a_k\},\quad A_2=\{a_{k+1}\}$$

Então um elemento B do conjunto de partes de A satisfaz somente uma das seguintes afirmações

- $B\in\mathscr{P}(A_1)$ (temos $\sharp\mathscr{P}(A_1)$ elementos deste tipo)
- $B=C\cup A_2$ com $C\in\mathscr{P}(A_1)$ (temos $\sharp\mathscr{P}(A_1)$ elementos deste tipo).

portanto

$$\sharp\mathscr{P}(A) = \sharp\mathscr{P}(A_1) + \sharp\mathscr{P}(A_1) = 2^k + 2^k = 2^{k+1}.$$

de onde $k+1 \in M$ e, pelo princípio de indução, $M = \mathbb{N}$.

■

Obs. Quando A é não finito temos também que $\mathscr{P}(A) = 2^{\sharp A}$. Mas esse número cardinal tem a seguinte descrição: Dado A um conjunto, considere o conjunto F de todas as funções $f : A \to \{0,1\}$, então definimos

$$\chi : \mathscr{P}(A) \to F,$$

como sendo

$$\chi(B)(x) = \begin{cases} 1 & \text{se} \quad a \in B \\ 0 & \text{se} \quad a \notin B \end{cases}$$

Clamente, toda função f assume valor 1 em $B = f^{-1}(1)$, então $f = \chi_{f^{-1}(1)}$. Portanto χ é sobrejetora e naturalmente injetora. De onde se define

$$\sharp\mathscr{P}(A) := 2^{\sharp A}.$$

Teorema 13.4 Se $\sharp A = m$ e $\sharp B = n$ então existem $2^{n \cdot m}$ relações de A em B.

Demonstração. O resultado segue de observar que cada relação se corresponde biunívocamente com um elemento do conjunto de partes e, neste caso, o conjunto de partes tem 2^{nm} elementos. ■

Corolário 13.4 Se $\sharp A = m$ então existem 2^{m^2} relações em A.

Demonstração. Aplicando o teorema anterior para $B = A$ temos que $n = m$ de onde existem $2^{m \times m}$ relações, isto é 2^{m^2} relações em A. ■

De forma similar mostramos que

Teorema 13.5 Sejam n, $m \in \mathbb{N}$. Se A é um conjunto tal que $\sharp A = n$ e B é um conjunto tal que $\sharp B = m$ então $\sharp(A \times B) = n \cdot m$.

Demonstração. Seja B um conjunto com m elementos. Vamos mostrar que para todo conjunto A tal que $\sharp A = n$ temos que $\sharp(A \times B) = n \cdot m$. Para isto construimos a função proposicional

$$P(n) = \text{"Se } A \text{ é um conjunto tal que } \sharp A = n \text{ então } \sharp(A \times B) = n \cdot m.\text{"}$$

Seja M o domínio de verdade desta função. Observamos que se $0 \in M$, pois

$$\emptyset \times B = \emptyset \quad \text{e} \quad \sharp\emptyset \times B = 0 \cdot m = 0.$$

Assuma que $k \in M$, vamos ver que $k+1 \in N$. De fato se

$$A = \{a_1, \ldots, a_k, a_{k+1}\}$$

escrevemos $A = A_1 \cup A_k$ em que

$$A_1 = \{a_1, \ldots, a_k\}, \quad A_2 = \{a_{k+1}\}$$

Então um elemento u do conjunto $A \times B$ satisfaz somente uma das seguintes afirmações

- $u = (a_l, b)$ com $l \leq k$ e $b \in B$. Denotamos por $\tilde{A}$ aao conjuntos constituído por estes elementos. Temos $\sharp(A_1 \times B) = k \cdot m$ por hipótese indutiva.
- $u = (a_{k+1}, b)$ com $b \in B$. Denotamos por $\tilde{B}$ ao conjuntos constituído por estes elementos. Temos $\sharp\tilde{B} = \sharp B = m$, por construção.

Observamos que $\tilde{A} \cap \tilde{B} = \emptyset$,portanto

$$\begin{aligned} \sharp(A \times B) &= \sharp\tilde{A} + \sharp\tilde{B} \\ &= \sharp(A_1 \times B) + \sharp B \\ &= k \cdot m + m \\ &= (k+1) \cdot m. \end{aligned}$$

de onde $k+1 \in M$ e, pelo princípio de indução, $M = \mathbb{N}$. ■

Corolário 13.5 Sejam α e β números cardinais finitos, então o produto entre eles tem como resultado o valor do produto como números naturais $\alpha \cdot \beta$.

De maneira análoga a demonstração para o caso de dois conjuntos, podemos mostrar o seguinte resultado

Teorema 13.6 Sejam $\{A_1, \ldots, A_k\}$ uma familia de conjuntos tais que $\sharp A_i = n_i$ para todo $i = 1 \ldots k$ então $\sharp(A_1 \times \cdots \times A_k) = n_1 \cdot n_2 \cdot \cdots \cdot n_k$.

Demonstração. Provamos o resultado por indução em k. Primeiramente lembramos que se A é um conjunto tal que $\sharp A = n$ e B é um conjunto tal que $\sharp B = m$ então $\sharp(A \times B) = n \cdot m$.

Considere agora a função proposicional

$$P(k) = \text{"Se } \{A_1, \ldots, A_k\} \text{ é uma familia de conjuntos tais que } \sharp A_i = n_i$$

$$\text{para todo } i = 1 \ldots k \text{ então } \sharp(A_1 \times \cdots \times A_k) = n_1 \cdot n_2 \cdots n_k. \text{"}$$

Seja M o seu domínio de verdade. Observamos que $0 \in M$ da definição de cardinalidade do conjunto.

Assuma que $k \in M$, isto é que se $\{A_1, \ldots, A_k\}$ uma familia de conjuntos tais que $\sharp A_i = n_i$ então $\sharp(A_1 \times \cdots \times A_k) = n_1 \cdot n_2 \cdots n_k$.

Vejamos que $k+1 \in M$. De fato se $\{A_1, \ldots, A_k, A_{k+1}\}$ uma familia de conjuntos tais que $\sharp A_i = n_i$ para todo i temos

$$\begin{aligned} \sharp(A_1 \times \cdots \times A_k \times A_{k+1}) &= \sharp((A_1 \times \cdots \times A_k) \times A_{k+1}) \\ &= \sharp(A_1 \times \cdots \times A_k) \times \sharp(A_{k+1}) \\ &= (n_1 \cdot n_2 \cdot \cdots \cdot n_k) \cdot n_{k+1} \\ &= n_1 \cdot n_2 \cdot \cdots \cdot n_k \cdot n_{k+1}. \end{aligned}$$

Pelo princípio de indução temos que $P(k)$ vale para todo $k \in \mathbb{N}$.

■

Teorema 13.7 Sejam n, $m \in \mathbb{N}$. Se A é um conjunto tal que $\sharp A = n$ e B é um conjunto tal que $\sharp B = m$ então $\sharp(B)^{\sharp(A)} = m^n$.

Demonstração. Sejam A e B conjuntos e assuma que $\sharp A = n$ e $\sharp B = m$ e que

$$A = \{a_1, \ldots, a_n\} \quad \text{e} \quad B = \{b_1, b_2, \ldots, b_n\}.$$

Denotamos por

$$F(A,B) = \{f : A \to B, \text{ função}\}.$$

Observamos que uma função $f : A \to B$ é construída associar por uma única seta um elemento de A com um elemento de B, portanto para cada $a_i \in A$ temos m possibilidades para $f(a_i)$. Assim temos m^n possibilidades diferentes de escolher a função f.

■

Corolário 13.6 Sejam α e β números cardinais finitos, então o número cardinal β^α é o mesmo número que o número natural que é resultado de fazer β^α.

Temos dividido os conjuntos em finitos e infinitos. No entanto, para distinguir um pouco melhor entre a cardinalidade dos conjuntos que são infinitos introduzimos o conceito de enumerabilidade.

Definição 13.3 Um conjunto A é dito enumerável se existe uma função injetora $f : A \to \mathbb{N}$. Em particular

- se a função for sobrejetora sobre um conjunto finito de $\mathbb{N}$ então A é dito enumerável finito.
- se a função for sobrejetora sobre um subconjunto de $\mathbb{N}$ com a mesma cardinalidade que $\mathbb{N}$ então A é dito enumerável infinito.

Os conjuntos que não admitem uma tal função são chamados de não enumeráveis.

Proposição 13.2 Seja A um conjunto infinito, então existe $g : \mathbb{N} \to A$ injetora.

Demonstração. Assuma exista uma função escolha $f : \mathscr{P}(A) \to A$, então definimos

$$\begin{aligned} f(A) &= a_0 \\ f(A\backslash\{a_0\}) &= a_1 \\ \vdots &\quad \vdots \\ f(A\backslash\{a_0,\ldots,a_n\}) &= a_{n+1} \\ \vdots &\quad \vdots \end{aligned}$$

Como A é infinito temos que cada

$$A\backslash\{a_0,\ldots,a_n\} \neq \emptyset$$

e como f é uma função escolha $a_n \notin \{a_0,\ldots,a_{n-1}\}$. O conjunto $B = \{a_i, i \in \mathbb{N}\}$ é então enumerável. Agora seja $g : \mathbb{N} \to B$ definida por $g(n) = a_n$. ■

De forma similar, assumindo o axioma da escolha, podemos provar o seguinte resultado.

Teorema 13.8 — Princípio da Partição. Sejam A e B dois conjuntos. Se existe $f : A \to B$ sobrejetora então existe $g : B \to A$ injetora.

Demonstração. Utilizamos o axioma da escolha. Construimos uma partição de A dada pelos conjuntos

$$f^{-1}(b) \quad \forall\, b \in B.$$

Escolhemos um único elemento $a_b \in f^{-1}(b)$ e definimos

$$g(b) = a_b \in f^{-1}(b).$$

A função assim definida é injetora pois

$$\begin{aligned} g(b) = g(b') &\Leftrightarrow a_b = a'_b \\ &\Rightarrow f(a_b) = f(a'_b) \\ &\Rightarrow b = b'. \end{aligned}$$

■

■ **Exemplo 13.3** • O conjunto dos números naturais é enumerável infinito de forma natural.

- Todo conjunto finito é, em particular enumerável.
- O conjunto $\mathbb{N}\times\mathbb{N}$ é enumerável. Para isto considere $f:\mathbb{N}\times\mathbb{N}\to\mathbb{N}$ dada por

$$f(n,m)=2^n3^m.$$

Observamos que $2^{n_1}3^{m_1}=2^{n_2}3^{m_2}$ se, e somente se, $n_1=n_2$ e $m_1=m_2$. De onde segue que f é injetora. Por outro lado $g:\mathbb{N}\to\mathbb{N}\times\mathbb{N}$ dada por $g(n)=(n,n)$ é naturalmente injetora. O teorema de Cantor Bernstein e Schröder nos garante que os dois conjuntos tem a mesma cardinalidade.

- Veremos depois que o conjunto dos números reais não são enumeráveis. ■

Proposição 13.3 O conjunto $\mathbb{Z}$ dos números inteiros é enumerável.

Demonstração. De fato, considere a função

$$f(z)=\begin{cases}2^n & \text{se} \quad 0\le n\\ 3^{-n} & \text{se} \quad n<0\end{cases}$$

Como 2 e 3 são coprimos temos que

$$2^a\neq 3^b \quad \forall\, a,b\in\mathbb{N}\backslash\{0\}.$$

Da mesma forma, se prova que $2^a=2^b$ se, e somente se, $a=b$ e que $3^a=3^b$ se, e somente se $a=b$. Portanto f é injetora. ■

Proposição 13.4 Sejam A, B conjuntos enumeráveis. Então

- Todo subconjunto $C\subset A$ é enumerável.
- Se existe $f:U\to A$ injetora, então U é enumerável.
- Se existe $f:A\to V$ sobrejetora, então V é enumerável.
- $A\times B$ é enumerável.
- $A\cup B$ é enumerável.

Demonstração.

- Seja $C\subset A$ subconjunto. Como A é enumerável temos que existe uma função injetora $f:A\to\mathbb{N}$. Em particular, $f|_A:A\to\mathbb{N}$ é injetora. De onde segue que C é enumerável.
- Como A é enumerável existe $g:A\to\mathbb{N}$ tal que g é injetora. Então $g\circ f:U\to\mathbb{N}$ é injetora. Portanto U é enumerável.
- Seja $f:A\to V$ é sobrejetora e considere a função injetora $g:A\to\mathbb{N}$ dada pela enumerabilidade de A. Então, da sobrejetividade de f temos que para cada $v\in V$ existe $a_v\in A$. Definimos $F:V\to\mathbb{N}$ por

$$F(v)=g(a_v).$$

observamos que se $F(v_1)=F(v_2)$ se, e somente se $a_{v_1}=a_{v_2}$ mas, pelo fato de f ser função, isto ocorre se $v_1=v_2$. Portanto F é injetora.
- Como A e B são enumeráveis, existem $f:A\to\mathbb{N}$ e $g:B\to\mathbb{N}$ funções injetoras. Considere $F:A\times B\to\mathbb{N}\times\mathbb{N}$ dada por

$$F(a,b)=(f(a),g(b)),$$

é injetora pois f e g são. Como $F(A\times B)\subset\mathbb{N}\times\mathbb{N}$ é enumerável, então $A\times B$ é enumerável.
- Como A e B são enumeráveis, existem $f:A\to\mathbb{N}$ e $g:B\to\mathbb{N}$ funções injetoras. Definimos $F:A\cup B\to\mathbb{N}$ por

$$F(z)=\begin{cases}2\cdot f(z) & \text{se} \quad z\in A\\ 2\cdot g(z)+1 & \text{se} \quad z\in B\backslash A\end{cases}$$

que é claramente injetora. Por outro lado $g:\mathbb{N}\to\mathbb{Z}$ dada por $g(n)=n$ é naturalmente injetora. O teorema de Cantor Bernstein e Schröder nos garante que os dois conjuntos tem a mesma cardinalidade.

■

Corolário 13.7 Sejam $\{A_i,\ i \in \mathbb{N}\}$ uma coleção de conjuntos enumeráveis. Então

$$\bigcup_{i\in\mathbb{N}} A_i$$

é enumerável.

Demonstração. Considere as funções injetoras $f_n : A_n \to \mathbb{N}$ dadas pela enumerabilidade de A_n para todo $n \in \mathbb{N}$ então

$$F : \mathbb{N}\times\mathbb{N} \to \bigcup_{i\in\mathbb{N}} A_i,$$

definida por

$$F(n,m) = f_n(m),$$

é claramente sobrejetora. De onde segue que $\bigcup_{i\in\mathbb{N}} A_i$ é enumerável. ■

Proposição 13.5 O conjunto

$$\mathbb{Q}_+^* = \left\{\frac{a}{b},\ (a,b) \in (\mathbb{Z}\backslash\{0\})\times(\mathbb{Z}\backslash\{0\}),\ a>0,\ b>0\right\}$$

é enumerável

Demonstração. Considere os números racionais escritos na forma irredutível, isto é na forma

$$\frac{p}{q} \quad \text{onde } p,\ q \in \mathbb{Z}, \text{ tais que } (p,q) = 1.$$

Seja $f : \mathbb{Q}_+^* \to \mathbb{N}$ dada por

$$f\left(\frac{p}{q}\right) = 2^p 3^q.$$

Observamos que se

$$f\left(\frac{p}{q}\right) = f\left(\frac{p_1}{q_1}\right)$$

então $2^p 3^q = 2^{p_1} 3^{q_1}$ e, pelo teorema fundamental da aritmética, temos que $p_1 = p$ e $q_1 = q$ e, portanto

$$\frac{p}{q} = \frac{p_1}{q_1}.$$

Logo, f é injetora e, portanto $\mathbb{Q}_+^*$ é enumerável.

■

Corolário 13.8 O conjunto dos racionais é enumerável.

Demonstração. Observamos que $\mathbb{Q} = \mathbb{Q}_+^* \cup \{0\} \cup \mathbb{Q}_-^*$ onde

$$\mathbb{Q}_+^* = \left\{\frac{a}{b},\ (a,b) \in (\mathbb{Z}\backslash\{0\})\times(\mathbb{Z}\backslash\{0\}),\ a>0,\ b>0\right\}$$

$$\mathbb{Q}_-^* = \left\{\frac{a}{b},\ (a,b) \in (\mathbb{Z}\backslash\{0\})\times(\mathbb{Z}\backslash\{0\}),\ a<0,\ b>0\right\}$$

e que existe uma bijeção $F : \mathbb{Q}_+^* \to \mathbb{Q}_-^*$ dada por $F(x) = -x$. Portanto, os três conjuntos são enumeráveis, de onde segue que $\mathbb{Q}$ é enumerável. ■

■ **Exemplo 13.4** Para ilustrar um pouco o contra-intuitivo dos conjuntos infinitos temos o experimento mental chamado de "Hotel de Hilbert". Neste experimento considera-se um hotel com infinitos quartos (tantos quartos como números naturais), no qual todos os quartos contêm um hóspede. Desta forma o hotel está lotado. Ao chegar um novo hóspede que deseja se hospedar no hotel, o recepcionista consegue acomoda-lo pedindo a cada hospede do quarto n ir para o quarto $n+1$, ficando assim o quarto 1 livre. Mais ainda, se cada hóspede ir do quarto n ao quarto $2n$ podemos deixar livre um número infinito de hóspedes.

Claramente isto só pode acontecer pois o conjunto de quartos é infinito, pois se fosse finito a pessoa que ocupa o último quarto não teria como se movimentar. ■

Pelo que vimos acima, para conjuntos infinitos, a noção de cardinalidade é um pouco delicada e pode ser pouco intuitiva. A definição diz que para mostrar que dois conjuntos tem a mesma cardinalidade devemos construir uma função bijetora. No entanto, construir a tal função bijetora pode ser una tarefa um tanto complicada. Nesse sentido o teorema de Cantor-Bernstein-Schröder simplifica o problema.

■ **Exemplo 13.5** Considere os conjuntos $A=(0,1]$ e $B=(1,2)\cup(3,4]$. Considere

$$f:A\to B \quad f(x)=x+3$$

$$g:B\to A \quad g(x)=\begin{cases}\frac{x-1}{2} & \text{se} \quad x\in(1,2)\\ \frac{x-2}{2} & \text{se} \quad x\in(3,4)\end{cases}$$

Observamos as duas funções são injetoras, mais ainda, que

$$g(1,2)=(0,1/2) \quad g(3,4]=(1/2,1].$$

Portanto A e B tem a mesma quantidade de elementos. ■

Como vimos os conjuntos finitos tem associado um número cardinal que é igual ao número $n\in\mathbb{N}$ com a mesma cardinalidade embora "número cardinal" e "número natural" sejam dois conceitos diferentes, não ha problema em denotar os dois números da mesma forma. Neste caso o número cardinal é chamado de número cardinal finito. Os números cardinais dos conjuntos infinitos são camados de infinitos ou números cardinais transfinitos. Como vimos o conjunto dos números cardinais formam um conjunto ordenado (utilizando funções injetoras e bijetoras) e, mais ainda há um resultado de tricotomia, isto é, dados dois números cardinais a e b se cumple uma das seguintes

$$a<b, \quad a=b, \quad a>b.$$

A cardinalidade dos naturais é denotada por $\aleph_0$ (Aleph 0). Os conjuntos enumeráveis infinitos tem cardinalidade $\aleph_0$ pelo teorema de Cantor-Bernstein-Schröder. De fato, por um lado sabemos que $f:A\to\mathbb{N}$ é injetora. Como A é infinito, então a função é sobrejetora sobre um conjunto com a mesma cardinalidade de $\mathbb{N}$, de onde construímos uma função injetora $g:\mathbb{N}\to A$.

Vimos que tanto os números inteiros como os racionais tem a mesma cardinalidade e igual a $\aleph_0$ e, portanto, são enumeráveis. Sempre é possível construir conjuntos de cardinalidade maior. Desta forma temos os sucessores de $\aleph_0$ são denotados por $\aleph_1=s(\aleph_0)$, $\aleph_2=s(\aleph_1)\ldots$.

Por outro lado, veremos depois que os reais terão cardinalidade $\mathfrak{c}$, que é chamada de cardinalidade do contínuo, e que satisfaz $\aleph_0<\mathfrak{c}=2^{\aleph_0}$.

Existe uma hipótese, chamada de *Hipótese do contínuo* que diz que não há número cardinal, isto é número que indique a quantidade de elementos do conjunto, entre as cardinalidades $\aleph_0$ e $2^{\aleph_0}$, isto é $\aleph_1=\mathfrak{c}$. Observamos também que foi mostrado que essa hipótese não pode ser demonstrada nem refutada dentro da teoria de conjuntos de Zermelo-Fraenkel.

Também é sabido que há conjuntos com cardinalidade maior que o contínuo, por exemplo, o conjunto $\mathscr{P}(\mathbb{R})$ tem cardinalidade $2^{\mathfrak{c}}>\mathfrak{c}$.

De modo geral temos as seguintes relações entre as cardinalidades

- $\aleph_0^{\aleph_0}=\mathfrak{c}$
- $\mathfrak{c}^n=\left(2^{\aleph_0}\right)^n=2^{n\times\aleph_0}=2^{\aleph_0}$
- $\mathfrak{c}_0^{\aleph}=\left(2^{\aleph_0}\right)_0^{\aleph}=2^{\aleph_0\times\aleph_0}=2^{\aleph_0}$

- $\mathfrak{c}^{\mathfrak{c}} = \left(2^{\aleph_0}\right)^{\mathfrak{c}} = 2^{\aleph_0 \times \mathfrak{c}} = 2^{\mathfrak{c}}$.

Para mais detalhes sobre número cardinais, sua aritmética e demais pode ser conjultado o trabalho W. Sierpinski, *Cardinal and ordinal numbers*-PWN, Warsaw (1965).

■ **Exemplo 13.6**

- O conjunto P dos números naturais pares com o 0 e o conjunto I dos naturais ímpares tem a mesma cardinalidade. De fato $f : P \to I$ dada por $f(p) = p+1$ é injetora e $g : I \to P$ dada por $g(p) = p+1$ também é injetora, agora pelo teorema de Cantor-Bernstein-Schröder existe um bijeção entre I e P.
- O intervalo $A = (-1,1)$ e o conjunto dos números reais tem a mesma cardinalidade. Podemos argumentar pelo teorema de Cantor-Bernstein-Schröder. No entanto vamos construir a bijeção. De fato, considere $f : A \to \mathbb{R}$ dada por

$$f(x) = \frac{x}{1-x^2}$$

Observamos que

$$f^{-1}(a) = \begin{cases} 0 & \text{se} \quad a = 0 \\ \frac{-1+\sqrt{1+4\cdot a^2}}{2\cdot a} & \text{se} \quad a \neq 0. \end{cases}$$

pois, se $a = 0$ então $f \circ f^{-1}(0) = f(0) = 0$ e se $a \neq 0$ então

$$f \circ f^{-1}(a) = \frac{-1+\sqrt{1+4\cdot a^2}}{2\cdot a} \cdot \frac{1}{1-\left(1+\frac{1-\sqrt{1+4\cdot a^2}}{2\cdot a^2}\right)} = a.$$

De forma similar,

$$f^{-1} \circ f(a) = \frac{-1+\sqrt{1+4\cdot \frac{a^2}{(1-a^2)^2}}}{2\cdot \frac{a}{1-a^2}} = a.$$

se mostra que $f^{-1} \circ f(x) = x$.

- O intervalos $I_1 = (0,1)$, $I_2 = [0,1)$ e $I_3 = [0,1]$ tem a mesma cardinalidade. De fato, utilizando o teorema de Schröder-Bernstein, e as funções injetoras

$$f_1 : (0,1) \to [0,1], \quad f(x) = x \quad \text{e} \quad g_1 : [0,1] \to (0,1), \quad g(x) = x/2$$

e

$$f_2 : (0,1) \to [0,1), \quad f(x) = x \quad \text{e} \quad g_2 : [0,1) \to (0,1), \quad g(x) = x/2$$

temos o resultado.

- Podemos mostrar que $(0,1) \times (0,1)$ tem a mesma cardinalidade de $\mathbb{R}^2$. Utilizando o teorema de Cantor-Bernstein-Schröder e as funções injetoras $f : (0,1) \times (0,1) \to \mathbb{R}^2$ e $g : \mathbb{R}^2 \to (0,1) \times (0,1)$ dadas por

$$f(x,y) = (x,y) \quad \text{e} \quad g(x,y) = \left(\frac{2\cdot x - 1 + \sqrt{1+4\cdot x^2}}{4\cdot x}, \frac{2\cdot y - 1 + \sqrt{1+4\cdot y^2}}{4\cdot y}\right)$$

- O conjunto $(0,1) \times (0,1)$ tem a mesma cardinalidade que $(0,1)$. Por um lado temos função injetora $f : (0,1) \to (0,1) \times (0,1)$ dada por

$$f(0, a_1a_2a_3a_4\ldots) = (0, a_1a_3a_5\ldots,\ 0, a_2a_4a_6\ldots),$$

e por outro lado $g : (0,1) \times (0,1) \to (0,1)$ definida por

$$g(0, a_1a_2a_3\ldots,\ 0, b_1b_2b_3\ldots) = 0, a_1b_1a_2b_2a_3b_3\ldots,$$

é também injetora.

- Da mesma forma podemos mostrar que para $\mathbb{R}^n$ a cardinalidade é $\mathfrak{c}$.

■

Fechamos o capítulo com uuma consequência do axioma daregularidade. Para isto precisamos de uma definição prévia.

Definição 13.4 Considere uma familia de conjuntos $\{A_i,\ i \in \mathbf{I}\}$ com $\mathbf{I} \subset \mathbb{N}$. Dizemos que A_i é uma cadeia descendente se

$$A_i \subset A_j \quad \forall\ j < i$$

para todo $i \in \mathbf{I}$.

Outra consequência do axioma da regularidade é o seguinte resultado.

Teorema 13.9 Não existe uma cadeia infinita e descendente de conjuntos.

Demonstração. Se existe uma tal cadeia. Então defina $f : \mathbb{N} \to A = \cup A_i$ dada por $f(i) = A_i$. Considere $\text{Img}(f)$ e $F = \{f(n),\ n \in \mathbb{N}\}$.

Pelo axioma da regularidade existe $B \in F$ tal que $B \cap F = \emptyset$. No entanto $B = f(k)$ pois é um elemento de B e $B \subset f(k-1)$ de onde $B = f(k) \cap F$, de onde B não pode ser disjunto de F, o que é uma contradição. Portanto não existe tal cadeia. ■

14. Números Inteiros

Temos construído até agora os número naturais. No entanto o conjunto dos naturais, como conjunto numérico, não é completo o suficiente no seguinte sentido: De forma geral, procuramos um conjunto de números $\mathbb{A}$ munido de operações soma $(+)$ e produto $(\cdot)$ tal que se $a_0, a_1, \ldots a_n,\ b \in \mathbb{A}$ então a função proposicional do tipo polinomial, isto é, da forma

$$P(x) = "x \in \mathbb{A},\ a_0 + a_1 \cdot x + \cdots + a_n \cdot x^n = b."$$

tenha domínio de verdade não vazio em $\mathbb{A}$.

Porém, para os naturais é fácil chegar em funções proposicionais deste tipo com domínio vazio. Por exemplo

$$P(x) = "x \in \mathbb{N},\ x+5 = 3." \quad \text{ou} \quad Q(x) = "x \in \mathbb{N},\ 4 \cdot x = 5."$$

tem por domínio de verdade o conjunto vazio em $\mathbb{N}$.

É por isso que se faz necessário ampliar o universo de números no qual podemos descrever estas funções. O objetivo então é achar um conjunto numérico de forma tal que as funções propocisionais polinomiais sobre os naturais estejam contempladas e que tenham seu domínio de verdade não vazio nele. Claramente, este novo conjunto numérico deve ser construído de forma tal que contenha o conjunto de números naturais.

Nesse sentido, o primeiro passo é a construção dos números inteiros. Damos uma ideia rápida da construção deste conjunto numérico.

Começamos definindo em $\mathbb{N} \times \mathbb{N}$ a relação de equivalência

$$(a,b) \sim (c,d) \ \Leftrightarrow\ a+d = b+c$$

- A relação é reflexiva pois para todo $(a,b) \in \mathbb{N} \times \mathbb{N}$ temos

$$a+b = b+a \quad \Rightarrow (a,b) \sim (a,b).$$

- A relação é simétrica pois

$$\begin{aligned} (a,b) \sim (c,d) &\Leftrightarrow a+d = b+c \\ &\Leftrightarrow c+b = d+a \\ &\Leftrightarrow (c,d) \sim (a,b). \end{aligned}$$

- A relação é transitiva pois

$$\begin{aligned}[(a,b)\sim(c,d)]\wedge[(c,d)\sim(e,f)] &\Leftrightarrow (a+d=b+c)\wedge(c+f=d+e)\\ &\Rightarrow (a+d=b+c)\wedge(c+f=b+e)\\ &\Rightarrow a+f+c+d=b+e+d+a=b+e+b+c\\ &\Rightarrow a+f=b+e \quad \text{(cancelamentento em } \mathbb{N})\\ &\Leftrightarrow (a,b)\sim(e,f).\end{aligned}$$

O espaço quociente por esta relação é

$$\mathbb{Z}=\mathbb{N}\times\mathbb{N}/\sim$$

Se $(a,b)\in\mathbb{N}\times\mathbb{N}$ temos três casos possíveis

$$\begin{aligned}a>b &\Rightarrow a=b+n\in\mathbb{N} \Rightarrow (a,b)\in[(a,b)]=[(n,0)].\\ a=b &\Rightarrow (a,b)\in[(a,b)]=[(0,0)]\\ b>a &\Rightarrow b=a+n\in\mathbb{N} \Rightarrow (a,b)\in[(a,b)]=[(0,n)].\end{aligned}$$

Definimos então, para cada $n\in\mathbb{N}$ tal que $n>0$, as classes

$$\mathbf{n}=[(n,0)]=\{(n+k,k),\ k\in\mathbb{N}\}$$

também será denotada por **+n**, a classe

$$\text{-}\mathbf{n}=[(0,n)]=\{(k,n+k),\ k\in\mathbb{N}\}.$$

e se $n=0$ a classe

$$\mathbf{0}=[(0,0)]=\{(k,k),\ k\in\mathbb{N}\}.$$

Com esta notação, podemos escrever

$$\mathbb{Z}=\{\ldots,\text{-}\mathbf{3},\text{-}\mathbf{2},\text{-}\mathbf{1},\mathbf{0},\mathbf{1},\mathbf{2},\mathbf{3},\ldots\}$$

Passamos agora a definir as operações de soma e produto entre números inteiros. A soma de números inteiros é a operação $+:\mathbb{Z}\times\mathbb{Z}\to\mathbb{Z}$ definida por

$$[(a,b)]+[(c,d)]=[(a+c,b+d)]$$

Obs. A operação soma nos números inteiros não é igual a operação soma nos números naturais. A notação correta teria um simbolo para cada operação, então seria $+_{\mathbb{Z}}:\mathbb{Z}\times\mathbb{Z}\to\mathbb{Z}$ definida por

$$[(a,b)]+_{\mathbb{Z}}[(c,d)]=[(a+_{\mathbb{N}}c,b+_{\mathbb{N}}d)].$$

Como a notação fica muito sobrecarregada, deixamos a interpretação a cargo do leitor e subentendida ao contexto.

É fácil ver que a soma, está bem definida, isto é não depende da escolha dos representantes. De fato se

$$[(a,b)]=[(a',b')] \qquad [(c,d)]=[(c',d')]$$

então,

$$(a+c)+(b'+d') \quad = \quad (b+d)+(a'+c')$$

e portanto,

$$[(a+c,b+d)]=[(a'+c',b'+d')]$$

Mais ainda, temos que a soma nos Inteiros generaliza a soma nos naturais. De fato, observamos que se $m \leq n$ são números naturais, e $a = n+m$ e $b+m = n$ então

$$\begin{aligned}
\mathbf{n}+\mathbf{m} &= [(n,0)]+[(m,0)] = [(n+m,0)] = \mathbf{a} \\
\mathbf{n}+(\mathbf{\text{-}m}) &= [(n,0)]+[(0,m)] = [(n,m)] = [(b,0)] = \mathbf{b} \\
(\mathbf{\text{-}n})+\mathbf{m} &= [(0,n)]+[(m,0)] = [(m,n)] = [(0,b)] = \mathbf{\text{-}b} \\
(\mathbf{\text{-}n})+(\mathbf{\text{-}m}) &= [(0,n)]+[(0,m)] = [(0,n+m)] = \mathbf{\text{-}a}.
\end{aligned}$$

Utilizando as definições acima podemos mostrar as seguintes propriedades da soma.

Proposição 14.1 Sejam $\mathbf{a}$, $\mathbf{b}$, $\mathbf{c}$ números em $\mathbb{Z}$. Então

- $\mathbf{a}+\mathbf{b} = \mathbf{b}+\mathbf{a}$ (comutatividade).
- $\mathbf{a}+(\mathbf{b}+\mathbf{c}) = (\mathbf{a}+\mathbf{b})+\mathbf{c}$ (associatividade).
- Existe um único elemento $\mathbf{0} = [(0,0)] \in \mathbb{Z}$ tal que $\mathbf{a}+\mathbf{0} = \mathbf{a}$ para todo $\mathbf{a} \in \mathbb{Z}$ (existência de elemento neutro).
- Para todo $\mathbf{a} \in \mathbb{Z}$ existe $-\mathbf{a} \in \mathbb{Z}$ tal que $\mathbf{a}+(-\mathbf{a}) = \mathbf{0}$ (existência de elemento inverso).
- Se $\mathbf{a}+\mathbf{b} = \mathbf{a}+\mathbf{c}$ Então $\mathbf{b} = \mathbf{c}$. (cancelamento na adição).

Demonstração. Sejam

$$\mathbf{a} = [(a_1,a_2)] \quad \mathbf{b} = [(b_1,b_2)] \quad \text{e} \quad \mathbf{c} = [(c_1,c_2)]$$

- $$\begin{aligned}
\mathbf{a}+\mathbf{b} &= [(a_1,a_2)]+[(b_1,b_2)] \\
&= [(a_1+b_1,a_2+b_2)] \\
&= [(b_1+a_1,b_2+a_2)] \\
&= \mathbf{b}+\mathbf{a}.
\end{aligned}$$
- $$\begin{aligned}
\mathbf{a}+(\mathbf{b}+\mathbf{c}) &= ([(a_1,a_2)]+[(b_1,b_2)])+[(c_1,c_2)] \\
&= [(a_1+b_1,a_2+b_2)]+[(c_1,c_2)] \\
&= [(a_1+b_1+c_1,a_2+b_2+c_2)] \\
&= [(a_1,a_2)]+[(b_1+c_1,b_2+c_2)] \\
&= [(a_1,a_2)]+([(b_1,b_2)]+[(c_1,c_2)] \\
&= (\mathbf{a}+\mathbf{b})+\mathbf{c}.
\end{aligned}$$
- Provamos somente a unicidade pois a existência e a propriedade foi mostrada acima. Assuma que existe um outro $\mathbf{k} \in \mathbb{Z}$ que satisfaz $\mathbf{a}+\mathbf{k} = \mathbf{a}$ para todo $\mathbf{a} \in \mathbb{Z}$ então,

  $$\mathbf{0} = \mathbf{0}+\mathbf{k} = \mathbf{k}$$

  de onde segue a unicidade.
- Definimos $-\mathbf{a}$ da seguinte forma

  $$\begin{aligned}
&\text{se} \quad (n,0) \in \mathbf{a} \quad \Rightarrow \quad -\mathbf{a} = [(0,n)] \quad \text{e} \quad \mathbf{a}+(-\mathbf{a}) = [(n,n)] = \mathbf{0}, \\
&\text{se} \quad (0,n) \in \mathbf{a} \quad \Rightarrow \quad -\mathbf{a} = [(n,0)] \quad \text{e} \quad \mathbf{a}+(-\mathbf{a}) = [(n,n)] = \mathbf{0}.
\end{aligned}$$
- $$\begin{aligned}
\mathbf{a}+\mathbf{b} = \mathbf{a}+\mathbf{c} \quad &\Rightarrow \quad [(a_1+b_1,a_2+b_2)] = [(a_1+c_1,a_2+c_2)] \\
&\Rightarrow \quad a_1+b_1+a_2+c_2 = a_1+c_1+a_2+b_2 \\
&\Rightarrow \quad b_1+c_2 = c_1+b_2 \quad \text{(cancelamento em } \mathbb{N}) \\
&\Rightarrow \quad \mathbf{b} = \mathbf{c}.
\end{aligned}$$

■

Definição 14.1 Dados $\mathbf{a}, \mathbf{b} \in \mathbb{Z}$ definimos

$$\mathbf{a} - \mathbf{b} = \mathbf{a} + (-\mathbf{b})$$

Os inteiros munidos da operação soma formam uma estrutura algébrica particular que passamos a descrever.

Definição 14.2 Seja G um conjunto e $\star : G \times G \to G$ uma operação binária definida sobre G. O par ordenado $(G, \star)$ é um grupo se são satisfeitas os seguintes axiomas:

- Associatividade: Quaisquer elementos $a,\ b,\ c \in G$ temos $(a \star b) \star c = a \star (b \star c)$
- Existência do elemento neutro: Existe um elemento $e \in G$ tal que $e \star a = a \star e = a$
- Existência do elemento simétrico: Para qualquer elemento $a \in G$, existe outro elemento $a' \in G$, tal que, $a \star a' = a' \star a = e$, onde e é o elemento neutro previamente mencionado.

Mais ainda, se para todos $a,\ b \in G$ temos a comutatividade, isto é, que $a \star b = b \star a$ o grupo é dito abeliano.

Corolário 14.1 O conjunto dos números inteiros munidos da operação soma, isto é $(\mathbb{Z}, +)$, é um grupo abeliano.

Demonstração. Inmediato da definição de grupo abeliano e as propriedades listadas acima. ■

Assim como acontece com a soma, podemos fazer com o produto. O produto de números inteiros $\cdot : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$ está definida em função da soma e da multiplicação nos números naturais da seguinte forma: se

$$\mathbf{n} = [(a,b)] \quad \text{e} \quad \mathbf{m} = [(c,d)]$$

então

$$\mathbf{n} \cdot \mathbf{m} = [(a \cdot c + b \cdot d, a \cdot d + b \cdot c)].$$

Obs. Novamente, aqui a operação produto nos números inteiros não é igual a operação produto nos números naturais. A notação correta teria um simbolo para cada operação, então seria seria $\cdot_{\mathbb{Z}} : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$ definida por

$$\mathbf{n} \cdot_{\mathbb{Z}} \mathbf{m} = [(a \cdot_{\mathbb{N}} c +_{\mathbb{N}} b \cdot_{\mathbb{N}} d, a \cdot_{\mathbb{N}} d +_{\mathbb{N}} b \cdot_{\mathbb{N}} c)].$$

Como a notação fica muito sobrecarregada, deixamos a interpretação a cargo do leitor e subentendida ao contexto.

É fácil ver que a multiplicação está bem definida, isto é se

$$\mathbf{n} = [(a,b)] = [(a',b')] \quad \text{e} \quad \mathbf{m} = [(c,d)] = [(c',d')]$$

então

$$\begin{aligned} a + b' = b + a' &\Rightarrow ca + cb' = cb + ca' \\ a + b' = b + a' &\Rightarrow db + da' = da + db'. \end{aligned}$$

Somando as equações temos

$$\begin{aligned} ca + cb' + db + da' &= cb + ca' + da + db' \Rightarrow \\ [(ac + db, cb + da)] &= [(a'c + b'd, a'd + b'c)] \Rightarrow \\ [(a,b)] \cdot [(c,d)] &= [(a',b')] \cdot [(c,d)]. \end{aligned}$$

De forma similar se mostra que

$$[(a',b')] \cdot [(c,d)] = [(a',b')] \cdot [(c',d')].$$

Em particular observamos que se $\mathbf{a} = [(a,b)]$ então

$$\begin{aligned} [(a,b)]\cdot[(0,0)] &= [(0,0)] \quad \Rightarrow \quad \mathbf{a}\cdot\mathbf{0} = \mathbf{0}, \\ [(a,b)]\cdot[(1,0)] &= [(a,b)] \quad \Rightarrow \quad \mathbf{a}\cdot\mathbf{1} = \mathbf{a}. \end{aligned}$$

Mais ainda se $n,\ m \in \mathbb{N}$ tais que $a = n\cdot m$ então

$$\begin{aligned} \mathbf{n}\cdot\mathbf{m} &= [(n,0)]\cdot[(m,0)] = [(n\cdot m,0)] = \mathbf{a} \\ \mathbf{n}\cdot(\mathbf{\text{-}m}) &= [(n,0)]+[(0,m)] = [(0,n\cdot m)] = [(0,a)] = \mathbf{\text{-}a} \\ (\mathbf{\text{-}n})\cdot\mathbf{m} &= [(0,n)]\cdot[(m,0)] = [(0,n\cdot m)] = [(0,a)] = \mathbf{\text{-}a} \\ (\mathbf{\text{-}n})\cdot(\mathbf{\text{-}m}) &= [(0,n)]\cdot[(0,m)] = [(n+m,0)] = \mathbf{a}. \end{aligned}$$

Em particular vemos que se $n,\ m \in \mathbb{N}$ então

$$\mathbf{n}\cdot(\mathbf{\text{-}m}) = (\mathbf{\text{-}n})\cdot\mathbf{m} = \mathbf{\text{-}a}.$$

Utilizando as definições acima podemos mostrar as seguintes propriedades do produto.

Proposição 14.2 Sejam $\mathbf{a}$, $\mathbf{b}$, $\mathbf{c}$ numeros em $\mathbb{Z}$. Então

- $\mathbf{a}\cdot\mathbf{b} = \mathbf{b}\cdot\mathbf{a}$ (comutatividade).
- $\mathbf{a}\cdot(\mathbf{b}\cdot\mathbf{c}) = (\mathbf{a}\cdot\mathbf{b})\cdot\mathbf{c}$ (associatividade).
- Existe $\mathbf{1} = [(1,0)] \in \mathbb{Z}$ tal que $\mathbf{a}\cdot\mathbf{1} = \mathbf{a}$ (existência de elemento neutro).
- $\mathbf{a}\cdot(\mathbf{b}+\mathbf{c}) = (\mathbf{a}\cdot\mathbf{b})+(\mathbf{a}\cdot\mathbf{c})$ (distributividade).
- Se $\mathbf{a}\cdot\mathbf{b} = \mathbf{a}\cdot\mathbf{c}$ Então $\mathbf{b} = \mathbf{c}$. (cancelamento no produto).

Demonstração. Sejam

$$\mathbf{a} = [(a_1,a_2)] \quad \mathbf{b} = [(b_1,b_2)] \quad \text{e} \quad \mathbf{c} = [(c_1,c_2)]$$

- $$\begin{aligned} \mathbf{a}\cdot\mathbf{b} &= [(a_1\cdot b_1+a_2\cdot b_2, a_1\cdot b_2+b_1\cdot a_2)] \\ &= [(b_1\cdot a_1+b_2\cdot a_2, b_1\cdot a_2+a_1\cdot b_2)] \\ &= \mathbf{b}\cdot\mathbf{a}. \end{aligned}$$
- $$\begin{aligned} \mathbf{a}\cdot(\mathbf{b}\cdot\mathbf{c}) &= [(a_1,a_2)]\cdot[(b_1\cdot c_1+b_2\cdot c_2, b_1\cdot c_2+b_2\cdot c_1)] \\ &= [(a_1\cdot(b_1\cdot c_1+b_2\cdot c_2)+a_2\cdot(b_1\cdot c_2+b_2\cdot c_1), a_1\cdot(b_1\cdot c_2+b_2\cdot c_1)+a_2\cdot(b_1\cdot c_1+b_2\cdot c_2))] \\ &= [(a_1\cdot b_1+a_2\cdot b_2, a_1\cdot b_2+b_1\cdot a_2)]\cdot[(c_1,c_2)] \\ &= (\mathbf{a}\cdot\mathbf{b})\cdot\mathbf{c}. \end{aligned}$$
- Existe $\mathbf{1} = [(1,0)] \in \mathbb{Z}$ tal que
$$\begin{aligned} \mathbf{a}\cdot\mathbf{1} &= [(a\cdot 1+0\cdot b, a\cdot 0+1\cdot b)] \\ &= [(a,b)] \\ &= \mathbf{a}. \end{aligned}$$
- $$\begin{aligned} \mathbf{a}\cdot(\mathbf{b}+\mathbf{c}) &= [(a_1,a_2)]\cdot[(b_1+c_1,b_2+c_2)] \\ &= [(a_1\cdot(b_1+c_1)+a_2\cdot(b_2+c_2), a_2\cdot(b_1+c_1)+a_1\cdot(b_2+c_2))] \\ &= [(a_1\cdot b_1+a_1\cdot c_1+a_2\cdot b_2+a_2\cdot c_2, a_2\cdot b_1+a_2\cdot c_1+a_1\cdot b_2+a_1\cdot c_2)] \\ &= [(a_1\cdot b_1+a_2\cdot b_2, a_1\cdot b_2+a_2\cdot b_1)] \\ &\quad +[(a_1\cdot c_1+a_2\cdot c_2, a_2\cdot c_1+a_1\cdot c_2)] \\ &= (\mathbf{a}\cdot\mathbf{b})+(\mathbf{a}\cdot\mathbf{c}). \end{aligned}$$

•

$$\begin{aligned}
\mathbf{a}\cdot\mathbf{b}=\mathbf{a}\cdot\mathbf{c} &\Rightarrow [(a_1\cdot b_1+a_2\cdot b_2, a_1\cdot b_2+b_1\cdot a_2)]\\
&= [(a_1\cdot c_1+a_2\cdot c_2, a_1\cdot c_2+c_1\cdot a_2)]\\
&\Rightarrow ((a_1\cdot b_1+a_2\cdot b_2)\cdot(a_1\cdot c_1+a_2\cdot c_2)\\
&\quad +(a_1\cdot b_2+b_1\cdot a_2)\cdot(a_1\cdot c_2+c_1\cdot a_2)\\
&= (a_1\cdot b_1+a_2\cdot b_2)\cdot(a_1\cdot c_2+c_1\cdot a_2)\\
&\quad +(a_1\cdot b_2+b_1\cdot a_2)\cdot(a_1\cdot c_1+a_2\cdot c_2)\\
&\Rightarrow (b_1\cdot c_1+b_2\cdot c_2)=(b_2\cdot c_1+b_1\cdot c_2) \quad \text{(cancelamento nos naturais)}\\
&\Rightarrow \mathbf{b}=\mathbf{c}.
\end{aligned}$$

■

O conjunto dos números inteiros munidos com a soma e o produto tem uma estrutura algébrica que passamos a descrever de forma geral.

Definição 14.3 Considere um conjunto A com um elemento $0\in A$ e duas operações binárias

$$+ : A\times A\to A \qquad \cdot : A\times A\to A$$

que satisfazem as seguintes condições:

- $(A,+)$ é grupo abeliano com elemento neutro igual a 0.
- Associatividade de $\cdot$: para todo $a,b,c\in A$ temos $(a\cdot b)\cdot c=a\cdot(b\cdot c)$
- Distributividade de $\cdot$ em relação a $+$: $a\cdot(b+c)=a\cdot b+a\cdot c$ e $(a+b)\cdot c=a\cdot c+b\cdot c$
- Existência de elemento neutro 1 de $\cdot$: existe $1\in A$ tal que $1\neq 0$ tal que para todo $a\in A$, temos $1\cdot a=a\cdot 1=a$.

Corolário 14.2 O conjunto dos números inteiros munidos das operações soma e produto, isto é $(\mathbb{Z},+,\cdot)$, é um Anel.

Demonstração. Inmediato da definição de anel e das propriedades listadas acima. ■

Teorema 14.1 Sejam $\mathbf{a}$, $\mathbf{b}\in\mathbb{Z}$. Toda função proposicional da forma

$$P(x)=\text{"}x\in\mathbb{Z},\ x+\mathbf{a}=\mathbf{b}\text{"},$$

tem por domínio de verdade $M=\{\mathbf{b}+(\mathbf{-a})\}$.

Demonstração. Imediato das propriedades da soma em $\mathbb{Z}$. ■

Nos inteiros temos uma relação de ordem dada por

$$[(a,b)]\leq[(c,d)] \quad\Leftrightarrow\quad a+d\leq b+c$$

Observamos que a relação está bem definida, de fato assuma que

$$[(a,b)]=[(a',b')],\quad [(c,d)]=[(c',d')] \quad \text{e que} [(a,b)]\leq[(c,d)],$$

então

$$\begin{aligned}
a+d\leq b+c &\Rightarrow a+b'+d\leq b+b'+c\\
&\Rightarrow a+b'+d+d'\leq b+b'+c+d'\\
&\Rightarrow a'+b+d+d'\leq b+b'+c'+d\\
&\Rightarrow a'+d'\leq b'+c' \quad \text{(cancelamento em } \mathbb{N})
\end{aligned}$$

De onde segue que a relação está bem definida.

- $\leq$ é reflexiva: seja $[(a,b)] \in \mathbb{Z}$ então $a+b \leq a+b$ de onde $[(a,b)] \leq [(a,b)]$
- $\leq$ é antisimétrica: sejam $[(a,b)],\ [(c,d)] \in \mathbb{Z}$ tais que $[(a,b)] \leq [(c,d)]$ e $[(c,d)] \leq [(a,b)]$, então

  $$a+d \leq b+c \leq a+d$$

  de onde $a+c = b+c$ e, portanto, $[(a,b)] = [(c,d)]$
- $\leq$ é transitiva: sejam $[(a,b)],\ [(c,d)],\ [(e,f)] \in \mathbb{Z}$ tais que $[(a,b)] \leq [(c,d)]$ e $[(c,d)] \leq [(e,f)]$ então, existem $p,\ q \in \mathbb{N}$ tais que

  $$a+d+p = b+c \quad \text{e} \quad c+f+q = e+d$$

  $$\begin{aligned}(a+f+p+q)+d+c &= (a+d+p)+(f+c+q)\\ &= b+c+e+d\\ &= (b+e)+(c+d) \quad \rightarrow \quad a+f \leq b+e.\end{aligned}$$

  e, portanto $[(a,b)] \leq [(e,f)]$.

Vejamos que esta relação é compatível com a que conhecemos usualmente para $\mathbb{Z}$. Sejam $m,\ n \in \mathbb{N}$. Então

$$\begin{aligned} & & \mathbf{-n \leq m} & \text{ pois } & [(0,n)] \leq [(m,0)],\\ \text{se } & m \leq n \Rightarrow & \mathbf{m \leq n} & \text{ pois } & [(n,0)] \leq [(m,0)],\\ \text{se } & m \leq n \Rightarrow & \mathbf{-n \leq -m} & \text{ pois } & [(0,n)] \leq [(0,m)].\end{aligned}$$

Mais ainda podemos mostrar que

$$\begin{aligned} \mathbf{a \leq b} &\Rightarrow \mathbf{a+c \leq b+c}\\ \mathbf{a \leq b} \text{ e } \mathbf{0 \leq c} &\Rightarrow \mathbf{a \cdot c \leq b \cdot c}.\end{aligned}$$

Em particular dizemos que

$$\mathbf{a < b} \quad \Leftrightarrow \quad (\mathbf{a \leq b}) \wedge (\mathbf{a \neq b}).$$

Com isto podemos anunciar o seguinte teorema

Teorema 14.2 — Tricotomia dos Inteiros. Sejam $\mathbf{a},\ \mathbf{b}$ números em $\mathbb{Z}$ então ocorre uma das seguintes situações $\mathbf{a} = \mathbf{b}$ ou $\mathbf{a} < \mathbf{b}$ ou $\mathbf{b} < \mathbf{a}$.

Demonstração. Provamos por contradição. Para isto assuma que $\mathbf{a} \neq \mathbf{b}$ e que $\mathbf{a} < \mathbf{b}$ e $\mathbf{b} < \mathbf{a}$ simultáneamente. Então, se $\mathbf{a} = [(a,b)]$ e $\mathbf{b} = [(c,d)]$, temos

$$\begin{aligned} a+d &< b+c\\ c+b &< d+a \quad \Rightarrow \quad c+b < a+d < c+b\end{aligned}$$

o que é uma contradição.

Por outro lado se $\mathbf{a} = \mathbf{b}$ e $\mathbf{a} < \mathbf{b}$ temos

$$\begin{aligned} a+d &< b+c\\ a+d &= b+c \quad \Rightarrow \quad a+d < c+b = a+d\end{aligned}$$

o que é também uma contradição. De forma similar mostramos que o caso $\mathbf{a} = \mathbf{b}$ e $\mathbf{b} < \mathbf{a}$ gera uma contradição. ■

Definição 14.4 Seja $\mathbf{a} \in \mathbb{Z}$. Dizemos que

- $\mathbf{a}$ é não negativo se $\mathbf{0} \leq \mathbf{a}$
- $\mathbf{a}$ é não positivo se $\mathbf{a} \leq \mathbf{0}$
- $\mathbf{a}$ é positivo se $\mathbf{0} < \mathbf{a}$
- $\mathbf{a}$ é negativo se $\mathbf{a} < \mathbf{0}$

A seguir listamos as regras de sinais para o produto.

Teorema 14.3 Sejam $\mathbf{a},\ \mathbf{b} \in \mathbb{Z}$, mostrar que
a) Se $\mathbf{a} > 0$ e $\mathbf{b} > 0$ então $\mathbf{a} \cdot \mathbf{b} > 0$
b) Se $\mathbf{a} < 0$ e $\mathbf{b} < 0$ então $\mathbf{a} \cdot \mathbf{b} > 0$
c) Se $\mathbf{a} > 0$ e $\mathbf{b} < 0$ então $\mathbf{a} \cdot \mathbf{b} < 0$

Demonstração. Utilizamos o fato de que, para todo $\mathbf{a} \in \mathbb{Z}$ sempre existe $n \in \mathbb{N}$ tal que se

$$\mathbf{a} > 0 \ \Rightarrow\ \mathbf{a} = [(n,0)]$$

$$\mathbf{a} < 0 \ \Rightarrow\ \mathbf{a} = [(0,n)]$$

a) Se $\mathbf{a} > 0$ e $\mathbf{b} > 0$ então
$$\begin{aligned} \mathbf{a} \cdot \mathbf{b} &= [(n,0)] \cdot [(m,0)] \\ &= [(n \cdot m, 0)] > 0 \end{aligned}$$
b) Se $\mathbf{a} < 0$ e $\mathbf{b} < 0$
$$\begin{aligned} \mathbf{a} \cdot \mathbf{b} &= [(0,n)] \cdot [(0,m)] \\ &= [(n \cdot m, 0)] > 0 \end{aligned}$$
c) Se $\mathbf{a} > 0$ e $\mathbf{b} < 0$
$$\begin{aligned} \mathbf{a} \cdot \mathbf{b} &= [(n,0)] \cdot [(0,m)] \\ &= [(0, n \cdot m)] > 0 \end{aligned}$$

■

Idetificamos naturalmente os Naturais como um subconjunto dos inteiros pela seguinte função injetora

$$f : \mathbb{N} \to \mathbb{Z}, \qquad f(n) = [(n,0)] \in \mathbb{Z}$$

Em particular, observamos que

$$\begin{aligned} f(n \cdot p + q) &= [(n \cdot p + q, 0)] \\ &= [(n \cdot p, 0)] + [(q,0)] \\ &= [(n,0)] \cdot [(p,0)] + [(q,0)] \\ &= f(n) \cdot f(p) + f(q). \end{aligned}$$

É por meio desta função (e identificação) que dizemos $\mathbb{N} \subset \mathbb{Z}$.

Definição 14.5 Seja A um subconjunto não vazio de $\mathbb{Z}$.
- Dizemos que A é limitado inferiormente se existe $\alpha \in \mathbb{Z}$ tal que $\alpha \leq a$ para todo $a \in A$. Neste caso α é chamado de cota inferior de A. A maior das cotas inferiores é chamado de ínfimos. No caso em que o ínfimo seja um elemento de A, dizemos que ele é o mínimo de A.
- Dizemos que A é limitado superiormente se existe $\beta \in \mathbb{Z}$ tal que $a \leq \beta$ para todo $a \in A$. Neste caso β é chamado de cota superior de A. A menor das cotas superiores é chamado de supremo. No caso em que o supremo seja um elemento de A, dizemos que ele é o máximo de A.

■ **Exemplo 14.1**
- $\mathbb{N}$ é limitado inferiormente em $\mathbb{Z}$. De fato $\alpha = 0$ é a cota inferior (e mínimo).
- $A = \{-4,-3,-2,-1,0,1,2,3,4,5\}$ é limitado superiormente e inferiormente. Neste caso -4 cota inferior (que é mínimo) e 5 é conta superior (que é máximo).

■

Embora os Naturais admitam cota inferior, eles não admitem cota superior em $\mathbb{Z}$ como mostra o seguinte resultado.

Teorema 14.4 O conjunto $\mathbb{N}$ não admite cota superior em $\mathbb{Z}$.

Demonstração. Observamos que $\mathbb{N}$ admite conta superior se

$$\exists\, z \in \mathbb{Z},\ \forall\, n \in \mathbb{N},\ n \leq z$$

Vamos mostrar que a negação disto é verdadeira, isto é, que

$$\forall\, z \in \mathbb{Z},\ \exists\, n \in \mathbb{N},\ z < n.$$

Portanto, mostramos que para todo $z \in \mathbb{Z}$ temos que existe um natural n tal que $z < n$ de onde segue que $\mathbb{N}$ não pode admitir cota superior.

Claramente, se $z \leq 0$ então existe $1 \in \mathbb{N}$ tal que $z < 1$. Se $z > 0$ então $z \in \mathbb{N}$ e, portanto o seu sucessor, $s(z) \in \mathbb{N}$ de onde segue que existe o natural $s(z)$ tal que $z < s(z)$. ■

Teorema 14.5 — Princípio da boa ordem.
- Seja $A \subset \mathbb{N}$ um conjunto não vazio então A possui elemento mínimo.
- Seja $A \subset \mathbb{Z}$ um conjunto não vazio e limitado inferiormente, então A possui elemento mínimo.

Demonstração. Provamos cada caso por separado.

- Para os Naturais considere o conjunto

$$B = \{n \in \mathbb{N},\ n \leq a,\ \forall\, a \in A\}.$$

Claramente $0 \in B$. Seja $a \in A$, então $a+1 \notin B$ pois $a \in A$ e $a \leq a+1$. Então $B \neq \mathbb{N}$. Portanto $0 \in B$ e $B \neq \mathbb{N}$ portanto existe um $k \in B$ tal que $k+1 \notin B$ pois, caso contrário, o princípio de indução garante que $B = \mathbb{N}$.
Vamos mostrar que k ao mínimo de A. De fato $k \in B$, portanto $k \leq a, \forall a \in A$ e portanto é cota inferior. Se mostrarmos que k em A teremos que é a maior das cotas inferiores de A e portanto o mínimo de A.
Vamos mostrar que $k \in A$ por contradição. Para isto, supomos que $k \notin A$ e, portanto $k < a$ para todo $a \in A$. De onde $k+1 \leq a$ para todo $a \in A$ e, consequêntemente $k+1 \in B$ o que contradiz a escolha do k. Logo $k \in A$ é um mínimo para A.

- Seja $A \in \mathbb{Z}$ limitado inferiormente. Seja α uma cota inferior de A. Seja

$$A' = \{a - \alpha, a \in A\} \subset \mathbb{N}.$$

Pelo princípio da boa ordem de $\mathbb{N}$ (item anterior) temos que A' possui elemento mínimo $\alpha' \in A'$. Então existe $a' \in A$ tal que $\alpha' = a' - \alpha$ de onde $m = \alpha' + \alpha \in A$ e, mais ainda, é um mínimo de A. De fato se $a \in A$ então $\alpha \leq < a - \alpha$ e $\alpha + \alpha' \in A$, de onde $\alpha + \alpha' \leq a$.

■

Corolário 14.3
- Sejam $\mathbf{a} \in \mathbb{Z}$ tais que $\mathbf{0} < \mathbf{a} \leq \mathbf{1}$ então $a = 1$.
- Sejam $\mathbf{a}$, $\mathbf{b} \in \mathbb{Z}$ tais que $\mathbf{a} < \mathbf{b} \leq \mathbf{a}+\mathbf{1}$ então $\mathbf{b} = \mathbf{a}+\mathbf{1}$.

Demonstração.
- Seja $A = \{x \in \mathbb{Z},\ 0 < x \leq \mathbf{1}/\}$. Claramente $\mathbf{1} \in A$ e A é limitado inferiormente por $\mathbf{0}$. Pelo princípio da boa ordem, A possui elemento mínimo, $\mathbf{m}$. Se $\mathbf{m} < 1$ temos que

$$0 < \mathbf{m}^2 < \mathbf{m} < \mathbf{1},$$

e, portanto $\mathbf{m}^2 \in A$ e é menor do que $\mathbf{m}$ portanto $\mathbf{m}$ não pode ser mínimo. Então $\mathbf{m} = \mathbf{1}$ e é o mínimo e máximo elemento de A, portanto $A = \{\mathbf{1}\}$.

- Seja $A = \{x \in \mathbb{Z},\ \mathbf{a} < x \leq \mathbf{a}+\mathbf{1}/\}$. Aqui $\mathbf{a}+1 \in A$ de onde segue que $A \neq \emptyset$. Também temos que A está limitado inferiormente por $\mathbf{a}$. Pelo princípio da boa ordem, A possui elemento mínimo $\mathbf{m} \in A$ e, portanto,

$$0 < \mathbf{m} - \mathbf{a} \leq 1.$$

Agora, pelo item anterior, $\mathbf{m} - \mathbf{a} = \mathbf{1}$, de onde $\mathbf{m} = \mathbf{a}+\mathbf{1}$.

‘

■

Em elaboração

15. Divisibilidade

O objetivo desta seção é dar uma ideia rápida sobre o algoritmo da divisão nos números inteiros e suas aplicações. Começamos com a definição.

Definição 15.1 Dados $a,\ b \in \mathbb{Z}$ com $a \neq 0$. Dizemos que $a|b$ (a divide a b) se existe $c \in \mathbb{Z}$ tal que $b = a \cdot c$. Mais ainda, neste caso, dizemos que b é um múltiplo de a.

Proposição 15.1 Sejam $a, b \in \mathbb{Z}\backslash\{0\}$. Então

- $1|a$, $a|a$ e $a|0$
- se $a|b$ e $b|c$ então $a|c$.
- se $a|c$ e $b|d$ então $a \cdot b|c \cdot d$.
- se $a|(c+d)$ então $a|c$ se, e somente se $a|d$.
- se $a > 0$ e $b > 0$ e $a|b$ então $a \leq b$

Demonstração.

- Observamos que

  $$a = 1 \cdot a, \quad a = 1 \cdot a \quad \text{e} \quad 0 = a \cdot 0.$$

  o que mostra o resultado.
- Da hipótese temos que existem inteiros $p,\ q$ tais que

  $$a = p \cdot b \quad \text{e} \quad b = q \cdot c$$

  então

  $$a = p \cdot b = p \cdot q \cdot c = (p \cdot q) \cdot c.$$

  Portanto $c|a$.
- Sabemos que existem inteiros $p,\ q$ tais que

  $$c = p \cdot a \quad \text{e} \quad d = q \cdot b$$

  então

  $$c \cdot d = (p \cdot a) \cdot (q \cdot b) = (a \cdot b) \cdot (q \cdot p)$$

  portanto $a \cdot b|c \cdot d$.

- Provamos uma implicação pois a outra é similar. Da hipótese temos que existem inteiros $p,\ q$ tais que

  $$c+d=a\cdot p \quad \text{e} \quad c=a\cdot q$$

  então

  $$d=a\cdot p-a\cdot q=a\cdot(p-q).$$

  de onde segue que $a|d$.
- Sejam $a,\ b\in\mathbb{N}$. Se $b\neq 0$ e $a|b$ então existe $p\in\mathbb{Z}$ tal que $a=p\cdot b$. Como $a,\ b>0$ temos que $p>0$ portanto, $p\geq 1$ de onde

  $$a=a\cdot 1\leq p\cdot a=b.$$

■

■ **Exemplo 15.1** Sejam $a,\ b\in\mathbb{Z}$ e $n\in\mathbb{N}$ então

- $(a-b)|(a^n-b^n)$.
  Provamos o resultado por indução. Seja

  $$P(n)=\text{"}(a-b)|(a^n-b^n)\text{"}$$

  e M o domínio de verdade de P. Observamos que $0\in M$ pois $a^0-b^0=0$ e $(a-b)|0$.
  Assuma que $k\in M$, isto é

  $$a^k-b^k=p\cdot(a-b)$$

  . Como

  $$\begin{aligned} a^{k+1}-b^{k+1} &= (a-b)\cdot a^k+b\cdot(a^k-b^k) \\ &= (a^k+p\cdot b)\cdot(a-b). \end{aligned}$$

  Portanto $k+1\in M$ e, pelo princípio de indução, $M=\mathbb{N}$.
- $(a+b)|(a^{2\cdot n+1}+b^{2\cdot n+1})$.
  Provamos o resultado por indução. Seja

  $$P(n)=\text{"}(a+b)|(a^{2\cdot n+1}+b^{2\cdot n+1})\text{"}$$

  e M o domínio de verdade de P. Observamos que $0\in M$ pois $a^1+b^1=a+b$.
  Assuma que $k\in M$, isto é

  $$a^{2\cdot k+1}+b^{2\cdot k+1}=p\cdot(a+b)$$

  . Como

  $$\begin{aligned} a^{2\cdot k+3}-b^{2\cdot k+3} &= (a^2-b^2)a^{2\cdot k+1}+b^2\cdot(a^{2\cdot k+1}+b^{2\cdot k+1}) \\ &= (a^{2\cdot k}+p\cdot b^2)\cdot(a+b). \end{aligned}$$

  Portanto $k+1\in M$ e, pelo princípio de indução, $M=\mathbb{N}$.
- $a+b|a^{2\cdot n}-b^{2\cdot n}$.
  Provamos o resultado por indução. Seja

  $$P(n)=\text{"}(a+b)|(a^{2\cdot n}-b^{2\cdot n})\text{"}$$

  e M o domínio de verdade de P. Observamos que $0\in M$ pois $a^0-b^0=0$ e $a+b|0$.
  Assuma que $k\in M$, isto é

  $$a^{2\cdot k}+b^{2\cdot k}=p\cdot(a-b)$$

  . Como

  $$\begin{aligned} a^{2\cdot k+2}-b^{2\cdot k+2} &= (a^2-b^2)a^{2\cdot k}+b^2\cdot(a^{2\cdot k}-b^{2\cdot k+1}) \\ &= [(a^{2\cdot k}\cdot(a-b))+p\cdot b^2]\cdot(a+b). \end{aligned}$$

  Portanto $k+1\in M$ e, pelo princípio de indução, $M=\mathbb{N}$.

■

Definição 15.2 Um número $p \in \mathbb{N}\backslash\{0,1\}$ é dito primo se sus únicos divisores são 1 e ele mesmo.

A importância dos números primos está no seguinte resultado.

Teorema 15.1 — Fudamental da Aritmética. Todo número natural maior do que 1 é primo ou se escreve de modo único, a menos de uma ordem nos seus fatores, como um produto de primos.

Demonstração. Utilizamos o princípio de indução. Seja $P(n)$ a função proposicional sobre $\mathbb{N}$ definida por

$$P(n) \quad = \quad \text{"}n+2 \text{ é primo ou se escreve de modo único, a menos de uma ordem nos seus fatores, como um produto de primos"}$$

Seja M o seu domínio de verdade, então $0 \in M$ pois 2 é primo.

Assuma que $k \in M$ e vejamos o que acontece com $k+1$. Se $k+1$ for primo, não temos nada a provar. Se $k+1$ não for primo então existem $p,\ q \in \mathbb{N}$ tais que $1 < p,\ q < k+1$ satisfazendo $k+1 = p \cdot q$. Como sabemos que $q,\ p \in M$ podemos escrever, de forma única,

$$p = p_1 \cdots p_r \quad q = q_1 \cdots q_l.$$

Então $k+1 = p_1 \cdots p_r \cdot q_1 \cdots q_l$. Vejamos agora que a escrita é única. Para assuma que existem duas escritas de primos

$$k+1 = \tilde{p}_1 \cdots \tilde{p}_t = \tilde{q}_1 \cdots \tilde{q}_s$$

onde os $\tilde{p}_j$'s e $\tilde{q}_i$'s são primos. Como $\tilde{p}_1 | \tilde{q}_1 \cdots \tilde{q}_s$ temos que $\tilde{p}_1 = \tilde{q}_j$ para algum j. Podemos supor, depois de reordenamento que é $\tilde{q}_1$. Então

$$m = \tilde{p}_2 \cdots \tilde{p}_t = \tilde{q}_2 \cdots \tilde{q}_s < k+1.a$$

Agora, como $m \in M$ temos que $t = s$ e que os $\tilde{p}_i$ e $\tilde{q}_j$ são iguais a pares. ■

É fácil ver que a quantidade de números primos é infinita

Teorema 15.2 — Euclides. O conjunto formado pelos números primos não é finito.

Demonstração. Mostramos pelo método do absurdo ou contradição. Assuma que se A é o conjunto formado por todos os números primos, então $\sharp A = k \in \mathbb{N}$, denotamos por

$$A = \{p_1, \ldots, p_k\}$$

aos elementos de A de forma tal que $p_i < p_{i+1}$ para todo i. Considere o número

$$a = (p_1 \cdot p_2 \cdots p_k) + 1$$

Claramente $a > p_k$ e $p_i \not| a$ para todo $i \leq k$ pois $p_i \not| 1$ então a so tem como divisor a 1 e a, portanto é primo o que é uma contradição. ■

Agora mostramos o resultado principal desta seção

Teorema 15.3 Sejam $a,\ b$ dois números naturais com $0 < a < b$. Existem dois únicos naturais $q,\ r$ tais que

$$b = a \cdot q + r \quad \text{e} \quad 0 \leq r < a.$$

Demonstração. Considere o conjunto

$$A = \{b - a \cdot k,\ k \in \mathbb{N}\} \cap \mathbb{N}$$

Pelo princípio da boa ordem em $\mathbb{N}$ existe um elemento mínimo $r = b - a \cdot q$ para algum $q \in \mathbb{N}$.

Se $a|b$ então $r = 0$ não temos nada a provar. Se $a \not| b$ então $r \neq a$. Assuma que $r > a$ então existe $c \in \mathbb{N}$ tal que $c + a = r$ e, consequêntemente,

$$c = b - (q+1) \cdot a$$

com $c < r$, contradizendo o fato de r ser mínimo. Portanto $r < a$.

Agora, só resta provar a unicidade, assuma que

$$a \cdot q + r = b = a \cdot q' + r'$$

para naturais $q,\ q', r,\ r'$ tais que $0 \leq r \leq r' < a$ Então

$$a \cdot (q - q') = r' - r.$$

Se $q - q' \neq 0$ então $a < r' - r$ o que é uma contradição. Portanto $q = q'$ de onde $r = r'$ provando a unicidade. ■

Corolário 15.1 Dados dois números naturais $a,\ b$ com $1 < a < b$, existe um natural n tal que

$$n \cdot a \leq b \leq (n+1) \cdot b$$

Demonstração. Do algoritmo da divisão, temos que existe $n \in \mathbb{N}$ tal que

$$b = n \cdot a + r$$

com $0 \leq r < a$. Portanto

$$n \cdot a \leq b \leq n \cdot a + r \leq n \cdot a + a = (n+1) \cdot a.$$

■

Definição 15.3 Sejam $a,\ b \in \mathbb{N}\backslash\{0\}$. Um número $d \in \mathbb{N}$ é um divisor comum de a e b se $d|a$ e $d|b$.

Um divisor comum de a e b será dito o máximo divisor comum, e será denotado por $d = (a,b)$, se para todo c divisor comum de a e b temos que $c|d$.

■ **Exemplo 15.2** Sejam $a,\ b \in \mathbb{N}$. Então

- $(0,a) = a$
- $(1,a) = 1$
- $(a,a) = a$
- $a|b$ se, e somente se, $a = (a,b)$.

De fato se $d = (a,b)$ então $d|a$, de onde $a = (a,b)$. A outra implicação é imediata da definição.

■

Definição 15.4 Dois números $a,\ b \in \mathbb{N}\backslash\{0\}$ são ditos primos entre si se $(a,b) = 1$.

Teorema 15.4 Sejam $a,\ b \in \mathbb{Z}$ números diferentes de 0 e seja $d = (a,b)$. Os conjuntos

$$A = \{s = d \cdot n,\ n \in \mathbb{Z}\} \quad \text{e} \quad B = \{s = m \cdot a + n \cdot b,\ m,\ n \in \mathbb{Z}\},$$

são iguais.

Demonstração. Observamos que todo elemento de $x \in B$ é divisível por d, portanto $x = d \cdot p$ para algum $p \in \mathbb{Z}$. Então $B \subset A$.

Por outro lado seja

$$c = \min(B \cap \mathbb{N}),$$

então

$$c = n \cdot a + m \cdot b.$$

Portanto $d|c$.

Por outro lado, se $c|z$ para todo $z \in B$. De fato, se

$$z = n_1 \cdot a + m_1 \cdot b,$$

e

$$z = p \cdot c + r \quad \text{com} \quad 0 \leq r < c,$$

temos que

$$0 \leq r = (n_1 - n) \cdot a + (m_1 - m) \cdot b < c.$$

De onde segue que $r = 0$ pela minimalidade de c. Então $c|a$ e $c|b$ de onde $c|d$. Portanto $c = d$ e $d \in B$ e $A \subset B$. ■

■ **Exemplo 15.3** Sejam $a,\ b \in \mathbb{N}\backslash\{0\}$. e assuma que existe $m,\ n \in \mathbb{Z}$ tais que

$$(a,b) = d = m \cdot a + n \cdot b$$

então, se $k = p \cdot d$, toda equação sobre $\mathbb{Z}$ da forma

$$a \cdot x + b \cdot y = k$$

tem solução dada por

$$x = p \cdot m \quad \text{e} \quad y = p \cdot n.$$

Estas equações são conhecidas como equações diofantinas, pode ser mostrado que todo par da forma

$$x = p \cdot m + l \cdot b \quad \text{e} \quad y = p \cdot n - l \cdot a \qquad l \in \mathbb{Z}$$

também é solução de

$$a \cdot x + b \cdot y = k.$$

Mais ainda, o teorema anterior garante que a equação diofantina

$$a \cdot x + b \cdot y = k$$

tem solução se, e somente se $d|k$. ■

Proposição 15.2 Sejam $a,\ b \in \mathbb{Z}$, então $(a,b) = 1$ se, e somente se, $1 = m \cdot a + n \cdot b$ para $m,\ n \in \mathbb{Z}$.

Demonstração. Como $(a,b) = 1$ temos, pelo resultado anterior que $1 = m \cdot a + n \cdot b$ para $m,\ n \in \mathbb{Z}$.

Por outro lado, se $1 = m \cdot a + n \cdot b$ para $m,\ n \in \mathbb{Z}$ então, $d = (a,b)$ divide a 1, de onde $d = 1$. ■

Lema 15.1 Sejam $a,\ b,\ n \in \mathbb{N}$ com $a < n \cdot a < b$. Se existe $(a, b - n \cdot a)$ então (a,b) existe e

$$(a, b - n \cdot a) = (a,b).$$

Demonstração. Seja $d = (a, b - n \cdot a)$, como $d|a$ e $d|b - n \cdot a$ e $b = b - n \cdot a + n \cdot a$ segue que d é divisor comum de a e b então $c|(a,b)$. Se $c = (a,b)$ então $c|b - n \cdot a$ portanto $c|d$. Decorre disto que $c = d$. ■

A seguir apresentamos uma técnica para determinar o máximo divisor comúm de dois números naturais a e b. Assuma, sem perder generalidade que $a < b$.

Se $a|b$ então $(a,b) = a$. Caso $a \not| b$ então existe $q_1,\ r_1 \in \mathbb{N}$ tais que

$$b = a \cdot q_1 + r_1.$$

Então

- se $r_1|a$ então

$$r_1 = (a, r_1) = (a, b - q_1 \cdot a) = (a,b)$$

- se $r_1 \not| a$ então existem $q_2,\ r_2 \in \mathbb{N}$

$$a = r_1 \cdot q_2 + r_2 \quad r_2 < r_1.$$

Novamente temos duas posibilidades

  - se $r_2|r_1$ então

$$r_2 = (r_1, r_2) = (r_1, a - q_2 \cdot r_1) = (r_1, a) = (b,a)$$

  - se $r_2 \not| r_1$ então existem $q_3,\ r_3 \in \mathbb{N}$

$$r_1 = r_2 \cdot q_3 + r_3 \quad r_3 < r_2.$$

Novamente temos duas posibilidades e o procedimento pode continuar um número finito de vezes pois o conjunto dos $= \{r_1, r_2, r_3, \cdots\} \subset \mathbb{N}$ com $r_i < r_{i+1}$ e portanto possui um mínimo, pelo princípio da boa ordem. Logo, existe um k tal que $r_k \in R$ e $r_k|r_{k-1}$. De onde segue que

$$(a,b) = r_k.$$

Lema 15.2 Se $(a,b) = d$ e $a = p \cdot d$ e $b = q \cdot d$ então $(p,q) = 1$.

Demonstração. Se $(p,q) = c > 1$ então $p = p_1 \cdot c$ e $q = q_1 \cdot c$ então $(a,b) = c \cdot d$ o que contradiz a definição de d. Portanto $c = 1$. ■

■ **Exemplo 15.4** Seja $a \in \mathbb{Z}$ e $n \in \mathbb{N}$.

- $(a+1, a^{2\cdot n+1} - 1) = (a+1, a-1)$.
  De fato, utilizando que $(a+1)|(a^{2\cdot n} - 1)$ temos
$$\begin{aligned}(a+1, a^{2\cdot n+1} - 1) &= (a+1, a \cdot (a^{2\cdot n} - 1) + (a-1)\\ &= (a+1, a-1).\end{aligned}$$
- $(a+1, a^{2\cdot n} + 1) = (a+1, 2)$.
  De fato, utilizando que $(a+1)|(a^{2\cdot n} + 1)$ temos
$$\begin{aligned}(a+1, a^{2\cdot n} + 1) &= (a+1, (a^{2\cdot n} - 1) + 2)\\ &= (a+1, 2).\end{aligned}$$
- $\left(a+1, \frac{a^{2\cdot n}-1}{a+1}\right) = (a+1, 2\cdot n)$.
  Escrevemos
$$\begin{aligned}\frac{a^{2\cdot n} - 1}{a+1} &= a^{2\cdot n-1} - a^{2\cdot n-2} + a^{2\cdot n-3} + \cdots - a^2 + a - 1\\ &= (a^{2\cdot n-1} + 1) - (a^{2\cdot n-2} - 1) + (a^{2\cdot n-3} + 1) + \cdots - (a^2 - 1) + (a+1) - 2\cdot n\end{aligned}$$

  e utilizamos que

$$a+1|(a^{2\cdot k} - 1) \quad \text{e} \quad a+1|(a^{2\cdot k+1} + 1),$$

  para obter o resultado.

- $\left(a+1, \frac{a^{2\cdot n+1}+1}{a+1}\right) = (a+1, 2\cdot n+1)$. Escrevemos

$$\begin{aligned}\frac{a^{2\cdot n+1}-1}{a+1} &= a^{2\cdot n} - a^{2\cdot n-1} + a^{2\cdot n-2} + \cdots + a^2 - a + 1 \\ &= (a^{2\cdot n}-1) - (a^{2\cdot n-1}+1) + (a^{2\cdot n-2}-1) + \cdots + (a^2-1) - (a+1) + (2\cdot n+1)\end{aligned}$$

e utilizamos que

$$a+1 | (a^{2\cdot k}-1) \quad \text{e} \quad a+1 | (a^{2\cdot k+1}+1),$$

para obter o resultado.

■

■ **Exemplo 15.5** Sejam $a \neq b$, $(a,b) = 1$ e $n \in \mathbb{N}$. Observamos que

$$(a-b, b^k) = 1 \quad \text{e} \quad (a+b, b^k) = 1$$

de fato, como $(a,b) = 1$ temos que existe s, $t \in \mathbb{R}$ tal que

$$s\cdot a + t\cdot b = 1 \quad \Rightarrow \quad \begin{array}{l} s\cdot(a-b) + (t+s)\cdot b = 1 \\ s\cdot(a+b) + (t-s)\cdot b = 1 \end{array}$$

de onde $(a-b, b) = 1$ e $(a+b, b) = 1$ de onde segue o resultado.

Com isto, podemos ver que

- $\left(a-b, \frac{a^n-b^n}{a-b}\right) = (a-b, n)$.

De fato, observamos que

$$\begin{aligned}\frac{a^n-b^n}{a-b} &= a^{n-1} + a^{n-2}\cdot b + \cdots + a\cdot b^{n-2} + b^{n-1} \\ &= (a^{n-1} - b^{n-1} + (a^{n-2}\cdot b - b^{n-1}) + \cdots + (a\cdot b^{n-2} - b^{n-1} + n\cdot b^{n-1}.\end{aligned}$$

E utilizamos que

$$a-b | (a^k - b^k),$$

junto a $(a-b, b^k) = 1$ para obter

$$\left(a-b, \frac{a^n-b^n}{a-b}\right) = (a-b, n\cdot b^{n-1}) = (a-b, n).$$

- se $a+b \neq 0$ então $\left(a+b, \frac{a^{2\cdot n+1}+b^{2\cdot n+1}}{a+b}\right) = (a+b, 2\cdot n+1)$.

De fato, observamos que

$$\begin{aligned}\frac{a^{2\cdot n+1}+b^{2\cdot n+1}}{a+b} &= a^{2\cdot n} - a^{2\cdot n-1}\cdot b + \cdots - a\cdot b^{2\cdot n-1} + b^{2\cdot n} \\ &= (a^{2\cdot n} - b^{2\cdot n}) - (a^{2\cdot n-1}\cdot b + b^{2\cdot n}) + \cdots - (a\cdot b^{2\cdot n-1} + b^{2\cdot n-1}) + (2\cdot n+1)\cdot b^{2\cdot n}.\end{aligned}$$

E utilizamos que

$$a+b | (a^{2\cdot k} - b^{2\cdot k}) \quad \text{e} \quad a+b | (a^{2\cdot k+1} + b^{2\cdot k+1}),$$

junto a $(a+b, b^k) = 1$ para obter

$$\left(a+b, \frac{a^{2\cdot n+1}+b^{2\cdot n+1}}{a+b}\right) = (a+b, (2\cdot n+1)\cdot b^{2\cdot n}) = (a+b, 2\cdot n+1).$$

■

Em elaboração

16. Números Racionais

Com o conjunto dos números inteiros, garantimos que todas as funções proposicionais da forma

$$P(x) = \text{"}x \in \mathbb{Z},\ x + a = b.\text{"}$$

para $a,\ b \in \mathbb{Z}$, tem domínio de verdade não vazio. No entanto, por exemplo, a função proposicional

$$P(x) = \text{"}x \in \mathbb{N},\ 2 \cdot x = 7.\text{"}$$

tem domínio de verdade vazio em $\mathbb{Z}$.

Continuamos então a ampliar o universo de números de forma tal que toda função proposicional do tipo polinomial sobre os inteiros esteja contemplada no novo conjunto e com o intuito de que seu domínio de verdade seja não vazio. O próximo passo é a construção dos números racionais.

Consideramos o conjunto $\mathbb{Z}^* = \mathbb{Z} \backslash \{0\}$.

Teorema 16.1 A relação $\sim$ sobre $\mathbb{Z} \times \mathbb{Z}^*$ definida por

$$(a,b) \sim (c,d) \quad \Leftrightarrow \quad a \cdot d = b \cdot c$$

é de equivalênca.

Demonstração.

- Reflexiva: De fato, como $a \cdot b = a \cdot b$ temos que $(a,b) \sim (a,b)$.
- Simétrica: Se $(a,b) \sim (c,d)$ então $a \cdot d = b \cdot c$ e, portanto $b \cdot c = a \cdot d$. Então $(c,d) = (a,b)$.
- Transitiva: Se $(a,b) \sim (c,d)$ então $a \cdot d = b \cdot c$ e se $(c,d) \sim (e,f)$ então $c \cdot f = d \cdot e$. Portanto

$$a \cdot d \cdot f = b \cdot c \cdot f \quad \text{e} \quad b \cdot c \cdot f = b \cdot d \cdot e.$$

como $d \neq 0$ temos, por cancelamento nos inteiros, que $a \cdot f = b \cdot e$.

■

Definição 16.1 Dado $(a,b) \in \mathbb{Z} \times \mathbb{Z}^*$, denotamos por

$$\frac{a}{b} = \{(c,d) \in \mathbb{Z} \times \mathbb{Z}^*,\ (a,b) \sim (c,d)\}$$

Obs. Observamos que $(a,b) \sim (c,d)$ se, e somente se $\frac{a}{b} = \frac{c}{d}$, isto é $a \cdot d = b \cdot c$. De fato, como a relação $\sim$ é de equivalência temos que se $(a,b) \sim (c,d)$ então a classe $\frac{a}{b}$ é igual à clase $\frac{c}{d}$.

Por outro lado, se as classes são iguais, temos que por exemplo $(c,d) \in \frac{c}{d} - \frac{a}{b}$ e, portanto, $(c,d) \sim (a,b)$ ou, equivalentemente, $a \cdot d = b \cdot c$.

Definição 16.2 Denotamos por $\mathbb{Q}$ ao conjunto de todas as classes de equivalência

$$\mathbb{Q} = \mathbb{Z} \times \mathbb{Z}^* / \sim = \left\{ \frac{a}{b},\ (a,b) \in \mathbb{Z} \times \mathbb{Z}^* \right\}.$$

Este conjunto recebe o nome de conjunto dos números racionais.

Assim como fizemos com os naturais e inteiros, definimos as operações soma e produto.

Definição 16.3 Sejam $\frac{a}{b}$ e $\frac{c}{d}$ dois números racionais. Definimos a soma $+ : \mathbb{Q} \times \mathbb{Q} \to \mathbb{Q}$ por

$$\frac{a}{b} + \frac{c}{d} = \frac{a \cdot d + b \cdot c}{b \cdot d}.$$

e o produto $\cdot : \mathbb{Q} \times \mathbb{Q} \to \mathbb{Q}$ por

$$\frac{a}{c} \cdot \frac{c}{d} = \frac{a \cdot c}{b \cdot d}$$

Obs. As operações soma e produto nos números racionais não são as mesmas que as operações soma e produto nos números inteiros. A notação correta teria um simbolo para cada operação, então seria algo da forma $+_{\mathbb{Q}} : \mathbb{Q} \times \mathbb{Q} \to \mathbb{Q}$ dada por

$$\frac{a}{b} +_{\mathbb{Q}} \frac{c}{d} = \frac{a \cdot_{\mathbb{Z}} d +_{\mathbb{Z}} b \cdot_{\mathbb{Z}} c}{b \cdot_{\mathbb{Z}} d}.$$

e $\cdot_{\mathbb{Q}} : \mathbb{Q} \times \mathbb{Q} \to \mathbb{Q}$

$$\frac{a}{c} \cdot_{\mathbb{Q}} \frac{c}{d} = \frac{a \cdot_{\mathbb{Z}} c}{b \cdot_{\mathbb{Z}} d}$$

Como a notação fica muito sobrecarregada, deixamos a interpretação a cargo do leitor e subentendida ao contexto.

Mostramos agora que as definições de soma e produto são boas e não dependem do representante da classe escolhido para computá-las. De fato, assuma que

$$\frac{a}{c} = \frac{a'}{c'} \quad \text{isto é} \quad a \cdot c' = c \cdot a',$$

e

$$\frac{b}{d} = \frac{b'}{d'} \quad \text{isto é} \quad b \cdot d' = d \cdot b'.$$

Calculamos

$$\frac{a'}{b'} + \frac{c'}{d'} = \frac{a' \cdot d' + b' \cdot c'}{b' \cdot d'} \qquad \frac{a'}{c'} \cdot \frac{c'}{d'} = \frac{a' \cdot c'}{b' \cdot d'}.$$

Como

$$\begin{aligned} (a \cdot d + b \cdot c) \cdot b' \cdot d' &= a \cdot d \cdot b' \cdot d' + b \cdot c \cdot b' \cdot d' \\ &= a' \cdot b \cdot d \cdot d' + c' \cdot d \cdot b \cdot b' \\ &= (a' \cdot d' + c' \cdot b') \cdot b \cdot d. \end{aligned}$$

Temos

$$\frac{a'\cdot d'+b'\cdot c'}{b'\cdot d'}=\frac{a\cdot d+b\cdot c}{b\cdot d}.$$

De forma similar, como

$$\begin{aligned} a'\cdot c'\cdot b\cdot d &= a'\cdot b\cdot c'\cdot d \\ &= a\cdot b'\cdot c\cdot d' \\ &= a\cdot c\cdot b'\cdot d'. \end{aligned}$$

Temos

$$\frac{a\cdot c}{b\cdot d}=\frac{a'\cdot c'}{b'\cdot d'}.$$

O fato de ter mostrado que o resultado é independente do representante da classe escolhido para fazer a conta nos permite fazer qualquer operação utilizando convenientemente qualquer representante da classe de equivalência que define o número.

Obs.

- A classe $\frac{0}{1}$ satisfaz

$$\frac{0}{1}+\frac{a}{b}=\frac{a}{b} \quad \text{e} \quad \frac{0}{1}\cdot\frac{a}{b}=\frac{0}{b}=\frac{0}{1}.$$

- a classe $\frac{1}{1}$ satisfaz

$$\frac{1}{1}\cdot\frac{a}{b}=\frac{a}{b}.$$

- Se $\frac{a}{b}\in\mathbb{Q}$ então $\frac{-a}{b}\in\mathbb{Q}$ satisfaz

$$\frac{a}{b}+\frac{-a}{b}=\frac{0}{b}=\frac{0}{1}.$$

- Se $\frac{a}{b}\in\mathbb{Q}$ tal que $\frac{a}{b}\neq\frac{0}{1}$ então $a\neq 0$ e, portanto, está definido $\frac{b}{a}\in\mathbb{Q}$. Observamos que

$$\frac{a}{b}\cdot\frac{b}{a}=\frac{1}{1}.$$

dizemos neste caso que

$$\left(\frac{a}{b}\right)^{-1}=\frac{b}{a}.$$

Mais ainda definimos, para $\frac{a}{b}\neq\frac{0}{1}$ e $\frac{p}{q}\in\mathbb{Q}$

$$\frac{p}{q}\div\frac{a}{b}=\frac{p}{q}\cdot\left(\frac{a}{b}\right)^{-1}=\frac{p}{q}\cdot\frac{b}{a}.$$

Proposição 16.1 Sejam $\mathbf{a}$, $\mathbf{b}$, $\mathbf{c}$ numeros em $\mathbb{Q}$. Então

- $\mathbf{a}+\mathbf{b}=\mathbf{b}+\mathbf{a}$ (comutatividade).
- $\mathbf{a}+(\mathbf{b}+\mathbf{c})=(\mathbf{a}+\mathbf{b})+\mathbf{c}$ (associatividade).
- Existe um único elemento $\mathbf{0}=\frac{0}{1}\in\mathbb{Q}$ tal que $\mathbf{a}+\mathbf{0}=\mathbf{a}$ (existência de elemento neutro).
- Para todo $\mathbf{a}\in\mathbb{Q}$ existe $-\mathbf{a}\in\mathbb{Q}$ tal que $\mathbf{a}+(-\mathbf{a})=\mathbf{0}$ (existência de elemento inverso).
- Se $\mathbf{a}+\mathbf{b}=\mathbf{a}+\mathbf{c}$ Então $\mathbf{b}=\mathbf{c}$. (cancelamento na adição).
- $\mathbf{a}\cdot\mathbf{b}=\mathbf{b}\cdot\mathbf{a}$ (comutatividade).
- $\mathbf{a}\cdot(\mathbf{b}\cdot\mathbf{c})=(\mathbf{a}\cdot\mathbf{b})\cdot\mathbf{c}$ (associatividade).
- Para todo $\mathbf{a}\in\mathbb{Q}$ tal que $\mathbf{a}\neq\mathbf{0}$ existe um único $\mathbf{a}^{-1}\in\mathbb{Q}$ tal que $\mathbf{a}\cdot\mathbf{a}^{-1}=\mathbf{1}$.

- Existe um único $\mathbf{1} = \frac{1}{1} \in \mathbb{Q}$ tal que $\mathbf{a} \cdot \mathbf{1} = \mathbf{a}$ (existência de elemento neutro).
- $\mathbf{a} \cdot (\mathbf{b} + \mathbf{c}) = (\mathbf{a} \cdot \mathbf{b}) + (\mathbf{a} \cdot \mathbf{c})$ (distributividade).
- Se $\mathbf{a} \neq \mathbf{0}$ e $\mathbf{a} \cdot \mathbf{b} = \mathbf{a} \cdot \mathbf{c}$ então $\mathbf{b} = \mathbf{c}$ (cancelamento no produto).

Demonstração. Sejam

$$\mathbf{a} = \frac{a_1}{a_2}, \quad \mathbf{b} = \frac{b_1}{b_2} \quad \text{e} \quad \mathbf{c} = \frac{c_1}{c_2}.$$

- $$\begin{aligned} \mathbf{a} + \mathbf{b} &= \frac{a_1 \cdot b_2 + b_1 \cdot a_2}{a_2 \cdot b_2} \\ &= \frac{b_1 \cdot a_2 + a_1 \cdot b_2}{b_2 \cdot a_2} \\ &= \mathbf{b} + \mathbf{a}. \end{aligned}$$
- $$\begin{aligned} \mathbf{a} + (\mathbf{b} + \mathbf{c}) &= \frac{a_1}{a_2} + \frac{b_1 \cdot c_2 + c_1 \cdot b_2}{b_2 \cdot c_2} \\ &= \frac{a_1 \cdot (b_2 \cdot c_2) + (b_1 \cdot c_2 + c_1 \cdot b_2) \cdot a_2}{a_2 \cdot c_2 \cdot b_2} \\ &= \frac{(a_1 \cdot b_2 + b_1 \cdot a_2) \cdot c_2 + (b_2 \cdot a_2) \cdot c_1}{a_2 \cdot c_2 \cdot b_2} \\ &= \frac{a_1 \cdot b_2 + b_1 \cdot a_2}{a_2 \cdot b_2} + \frac{c_1}{c_2} = (\mathbf{a} + \mathbf{b}) + \mathbf{c}. \end{aligned}$$
- Seja $\mathbf{0} = \frac{0}{1} \in \mathbb{Q}$, então
  $$\begin{aligned} \mathbf{0} + \mathbf{a} &= \frac{0}{1} + \frac{a_1}{a_2} \\ &= \frac{0 \cdot a_2 + a_1 \cdot 1}{1 \cdot a_2} \\ &= \frac{a_1}{a_2}. \end{aligned}$$
  Assuma que existe outro elemento $\mathbf{d}$ com a mesma propriedade, então
  $$\mathbf{d} = \mathbf{d} + \mathbf{0} = \mathbf{0}.$$
  Portanto $\mathbf{0}$ é o único elemento com esta propriedade.
- Considere $\mathbf{a} \in \mathbb{Q}$ e defina
  $$-\mathbf{a} = \frac{-a_1}{a_2},$$
  então
  $$\mathbf{a} + (-\mathbf{a}) = \frac{a_1 \cdot a_2 + (-a_1) \cdot a_2}{a_2 \cdot a_2} = \frac{0}{a_2 \cdot a_2} = \mathbf{0}.$$
- $$\begin{aligned} \mathbf{a} + \mathbf{b} = \mathbf{a} + \mathbf{c} &\Rightarrow \frac{a_1 \cdot b_2 + b_1 \cdot a_2}{a_2 \cdot b_2} = \frac{a_1 \cdot c_2 + c_1 \cdot a_2}{a_2 \cdot c_2} \\ &\Rightarrow (a_1 \cdot b_2 + b_1 \cdot a_2) \cdot (a_2 \cdot c_2) = (a_2 \cdot b_2) \cdot (a_1 \cdot c_2 + c_1 \cdot a_2) \\ &\Rightarrow (b_1 \cdot a_2) \cdot (a_2 \cdot c_2) = (a_2 \cdot b_2) \cdot (c_1 \cdot a_2) \quad \text{(Cancelamento em } \mathbb{Z}) \\ &\Rightarrow b_1 \cdot c_2 = b_2 \cdot c_1 \quad \text{(Cancelamento em } \mathbb{Z}) \\ &\Rightarrow \mathbf{b} = \mathbf{c}. \end{aligned}$$
- $$\begin{aligned} \mathbf{a} \cdot \mathbf{b} &= \frac{a_1 \cdot b_1}{a_2 \cdot b_2} \\ &= \frac{b_1 \cdot a_1}{b_2 \cdot a_2} \\ &= \mathbf{b} \cdot \mathbf{a} \end{aligned}$$

- $$\begin{aligned}\mathbf{a}\cdot(\mathbf{b}\cdot\mathbf{c}) &= \frac{a_1}{a_2}\cdot\frac{b_1\cdot c_1}{b_2\cdot c_2}\\ &= \frac{a_1\cdot b_1\cdot c_1}{a_2\cdot b_2\cdot c_2}\\ &= \frac{a_1\cdot b_1}{a_2\cdot b_2}\cdot\frac{c_1}{c_2}\\ &= (\mathbf{a}\cdot\mathbf{b})\cdot\mathbf{c}\end{aligned}$$
- Seja $\mathbf{a}\in\mathbb{Q}$ tal que $\mathbf{a}\neq\mathbf{0}$ então $a_1\neq 0$ portanto defina

  $$\mathbf{a}^{-1}=\frac{a_2}{a_1}$$

  então

  $$\mathbf{a}\cdot\mathbf{a}^{-1}=\frac{a_1\cdot a_2}{a_2\cdot a_1}=\mathbf{1}.$$
- Claramente se $\mathbf{1}=\frac{1}{1}$ então, para todo $\mathbf{a}\in\mathbb{Q}$ temos

  $$\mathbf{1}\cdot\mathbf{a}=\frac{1\cdot a_1}{1\cdot a_2}=\frac{a_1}{a_2}=\mathbf{a}.$$

  Se $\mathbf{d}$ é outro elemento de $\mathbb{Q}$ com a propriedade $\mathbf{d}\cdot\mathbf{a}=\mathbf{a}$ para todo $\mathbf{a}\in\mathbb{Q}$ temos

  $$\mathbf{d}=\mathbf{d}\cdot\mathbf{1}=\mathbf{1}.$$

  Portanto o $\mathbf{1}$ é único.
- $$\begin{aligned}\mathbf{a}\cdot(\mathbf{b}+\mathbf{c}) &= \frac{a_1}{a_2}\cdot\frac{b_1\cdot c_2+c_1\cdot b_2}{b_2\cdot c_2}\\ &= \cdot\frac{a_1\cdot(b_1\cdot c_2+c_1\cdot b_2)}{a_2\cdot b_2\cdot c_2}\\ &= \cdot\frac{a_1\cdot b_1\cdot c_2+a_1\cdot c_1\cdot b_2)}{a_2\cdot b_2\cdot c_2}\\ &= \cdot\frac{a_1\cdot b_1}{a_2\cdot b_2}+\frac{a_1\cdot c_1}{a_2\cdot c_2}\\ &= (\mathbf{a}\cdot\mathbf{b})+(\mathbf{a}\cdot\mathbf{c})\end{aligned}$$
- Se $\mathbf{a}\neq\mathbf{0}$ então

  $$\begin{aligned}\mathbf{a}\cdot\mathbf{b}=\mathbf{a}\cdot\mathbf{c} &\Rightarrow \frac{a_1\cdot b_1}{a_2\cdot b_2}=\frac{a_1\cdot c_1}{a_2\cdot c_2}\\ &\Rightarrow (a_1\cdot b_1)\cdot(a_2\cdot c_2)=(a_1\cdot c_1)\cdot(a_2\cdot c_2)\\ &\Rightarrow (b_1\cdot c_2)=(c_1\cdot b_2)\quad(\text{cancelamento em }\mathbb{Z})\\ &\Rightarrow \mathbf{b}=\mathbf{c}.\end{aligned}$$

■

Os números racionais munidos com a soma e o produto tem uma estrutura algébrica que passamos a descrever de forma geral.

Definição 16.4 Considere um conjunto A com elementos 0 e 1 em A e duas operações binárias

$$+:A\times A\to A\qquad\cdot:A\times A\to A$$

que satisfazem as seguintes condições:

- $(A,+,\cdot,0,1)$ é anel com elemento neutro igual a 0 e unidade.
- Para todo $a\in A$ tal que $a\neq 0$ existe $b\in A$ tal que $a\cdot b=1$

Então $(A,+,\cdot)$ é um corpo.

Uma propriedade importante dos corpos é a seguinte.

Corolário 16.1 Seja $(A,+,\cdot)$ um corpo. Considere $a \neq 0$ e $b \neq 0$ então $a \cdot b \neq 0$.

Demonstração. Assuma que $a \cdot b = 0$ então, como $a \neq 0$ e $b \neq 0$ existem a' e b' tais que $a \cdot a' = 1$ e $b \cdot b' = 1$ de onde

$$0 = 0 \cdot b' \cdot a' = a \cdot b \cdot b' \cdot a' = 1.$$

o que é uma contradição. Portanto $a \cdot b \neq 0$. ■

Em particular, temos o seguinte resultado.

Corolário 16.2 O conjunto dos números racionais munidos das operações soma e produto, isto é $(\mathbb{Q},+,\cdot)$, é um Corpo.

Demonstração. Inmediato da definição de anel e das propriedades listadas acima. ■

Obs. Se $a,\ b \in \mathbb{Z}$ tal que $a \neq 0$ e $b \neq 0$ temos definido

$$\left(\frac{a}{b}\right)^{-1} = \frac{b}{a}.$$

Observamos que, para $r \in \mathbb{N}\backslash\{0\}$ temos

$$\begin{aligned}\left[\left(\frac{a}{b}\right)^{-1}\right]^r &= \left[\frac{b}{a}\right]^r \\ &= \frac{b^r}{a^r} \\ &= \left[\left(\frac{a}{b}\right)^r\right]^{-1}.\end{aligned}$$

Definimos então

$$\left(\frac{a}{b}\right)^{-r} = \left[\left(\frac{a}{b}\right)^{-1}\right]^r.$$

Com esta definição se cumple

$$\left(\frac{a}{b}\right)^r \left(\frac{a}{b}\right)^s = \left(\frac{a}{b}\right)^{r+s},$$

para $r,\ s \in \mathbb{Z}$.

Definição 16.5 Sejam $\frac{a}{b}$ e $\frac{c}{d}$ dois números racionais. Dizemos que $\frac{a}{b}$ é menor e igual a $\frac{c}{d}$ e denotamos por

$$\frac{a}{b} \leq \frac{c}{d} \quad \text{se} \quad a \cdot d \leq b \cdot c.$$

Mais ainda, dizemos que

$$\frac{a}{b} < \frac{c}{d} \quad \Leftrightarrow \quad \left(\frac{a}{b} \leq \frac{c}{d}\right) \wedge \left(\frac{a}{b} \neq \frac{c}{d}\right).$$

Vejamos que, de fato, a relação definida acima é uma relação de ordem.

- Refexividade: Seja $\frac{a}{b} \in \mathbb{Q}$ então $a \cdot b \leq a \cdot b$ temos que $\frac{a}{b} \leq \frac{a}{b}$.

- Antisimetria: Sejam $\frac{a}{b},\ \frac{c}{d} \in \mathbb{Q}$ e assuma que

$$\left(\frac{a}{b} \leq \frac{c}{d}\right) \wedge \left(\frac{c}{d} \leq \frac{a}{b}\right).$$

Então

$$(a \cdot d \leq b \cdot c) \wedge (b \cdot c \leq a \cdot d) \quad \Rightarrow a \cdot d = b \cdot c.$$

Portanto

$$\frac{a}{b} \leq \frac{c}{d}.$$

- Sejam $\frac{a}{b},\ \frac{c}{d}, \frac{e}{f} \in \mathbb{Q}$ e assuma que

$$\left(\frac{a}{b} \leq \frac{c}{d}\right) \wedge \left(\frac{c}{d} \leq \frac{e}{f}\right).$$

Então

$$(a \cdot d \leq b \cdot c) \wedge (c \cdot f \leq e \cdot d),$$

para $d,\ c,\ f$ inteiros positivos. Portanto,

$$\begin{aligned} a \cdot f \cdot d &\leq b \cdot c \cdot f \\ &\leq b \cdot e \cdot d \quad \Rightarrow \quad a \cdot f \leq b \cdot e. \end{aligned}$$

De onde segue que

$$\frac{a}{b} \leq \frac{e}{f}.$$

Obs.

Dados $\mathbf{a},\ \mathbf{b} \in \mathbb{Q}$, denotamos

- $\mathbf{a} \geq \mathbf{b}$ se, e somente se, $\mathbf{b} \leq \mathbf{a}$.
- $\mathbf{a} > \mathbf{b}$ se, e somente se, $\mathbf{b} < \mathbf{a}$.

Definição 16.6 Seja $(A, \leq)$ um conjunto munido de uma ordem total. Se $a \leq b$ e $a \neq b$ então dizemos que a é menor que b e denotamos por $a < b$.

Definição 16.7 Um corpo ordenado é um corpo A munido de uma relação de ordem total $\leq$ que satisfaz

- Para todo $a,\ b,\ c \in A$ se $a < b$ então $a + c < b + c$.
- Para todo $a,\ b \in A$ se $0 < a$ e $0 < b$ então $0 < a \cdot b$.

A seguir mostramos uma propriedade importante para corpos ordenados.

Corolário 16.3 Seja $(A, +, \cdot, 0, 1, <)$ um corpo ordenado e $a \in A$ tal que $a \neq 0$ então $0 < a^2$.

Demonstração. Observamos que temos duas situações:

- se $0 < a$ então $0 = 0 \cdot a < a \cdot a = a^2$.
- se $a < 0$ temos que $0 = a + (-a) < 0 + (-a)$ de onde $0 < (-a)$. Pelo item anterior $0 < (-a)^2$. Como

$$(-a)^2 + (-a) \cdot a = (-a) \cdot ((-a) + a) = 0,$$

e

$$(-a) \cdot a + a^2 = ((-a) + a) \cdot a = 0,$$

temos

$$(-a)^2 = -((-a) \cdot a) = -(-a^2) = a^2.$$

Portanto $0 < a \cdot a = a^2$.

■

Vamos mostrar que os números racionais formam um corpo ordenado.

Proposição 16.2 Sejam $a,\ b$, e c números racionais

- $a \leq b$ se, e somente se, $a+c \leq b+c$ para todo $c \in \mathbb{Q}$.
- Se $a \leq b$ e $0 \leq c$ então $a \cdot c \leq b \cdot c$
- Se $a \leq b$ e $c \leq 0$ então $b \cdot c \leq a \cdot c$.

Demonstração. Sejam

$$a = \frac{p_1}{q_1} \quad b = \frac{p_2}{q_2} \quad \text{e} \quad c = \frac{p_3}{q_3}$$

com $q_3 > 0$ (sempre é possível pedir isso)

- Observamos que

$$\begin{aligned}
a \leq b &\Leftrightarrow p_1 \cdot q_2 \leq p_2 \cdot q_1 \\
&\Leftrightarrow p_1 \cdot q_2 \cdot q_3 \leq p_2 \cdot q_1 \cdot q_3 \\
&\Leftrightarrow p_1 \cdot q_2 \cdot q_3 + q_1 \cdot q_2 \cdot p_3 \leq p_2 \cdot q_1 \cdot q_3 + q_1 \cdot q_2 \cdot p_3 \quad \text{(propieddade dos inteiros)} \\
&\Leftrightarrow (p_1 \cdot q_3 + q_1 \cdot p_3) \cdot q_2 \leq (p_2 \cdot q_3 + q_2 \cdot p_3) \cdot q_1 \\
&\Leftrightarrow (p_1 \cdot q_3 + q_1 \cdot p_3) \cdot q_2 \cdot q_3 \leq (p_2 \cdot q_3 + q_2 \cdot p_3) \cdot q_1 \cdot q_3 \\
&\Leftrightarrow \frac{p_1 \cdot q_3 + q_1 \cdot p_3}{q_1 \cdot q_3} \leq \frac{p_2 \cdot q_3 + q_2 \cdot p_3}{q_2 \cdot q_3} \\
&\Leftrightarrow \frac{p_1}{q_1} + \frac{p_3}{q_3} \leq \frac{p_2}{q_2} + \frac{p_3}{q_3}.
\end{aligned}$$

- Como $c \geq 0$ temos que $p_3 \geq 0$. Então

$$\begin{aligned}
a \leq b &\Rightarrow p_1 \cdot q_2 \leq p_2 \cdot q_1 \\
&\Rightarrow p_1 \cdot q_2 \cdot p_3 \cdot q_3 \leq p_2 \cdot q_1 \cdot p_3 \cdot q_3 \quad \text{(pois } p_3 \geq 0 \text{ e } q_3 \geq 0\text{)} \\
&\Rightarrow \frac{p_1 \cdot p_3}{q_1 \cdot q_3} \leq \frac{p_2 \cdot p_3}{q_2 \cdot q_3} \\
&\Rightarrow \frac{p_1}{q_1} \cdot \frac{p_3}{q_3} \leq \frac{p_2}{q_2} \cdot \frac{p_3}{q_3}.
\end{aligned}$$

- Como $c \leq 0$ temos que $p_3 \leq 0$. Então

$$\begin{aligned}
a \leq b &\Rightarrow p_1 \cdot q_2 \leq p_2 \cdot q_1 \\
&\Rightarrow p_2 \cdot q_1 \cdot p_3 \cdot q_3 \leq p_1 \cdot q_2 \cdot p_3 \cdot q_3 \quad \text{(pois } p_3 \leq 0 \text{ e } q_3 \geq 0\text{)} \\
&\Rightarrow \frac{p_2 \cdot p_3}{q_2 \cdot q_3} \leq \frac{p_1 \cdot p_3}{q_1 \cdot q_3} \\
&\Rightarrow \frac{p_2}{q_2} \cdot \frac{p_3}{q_3} \leq \frac{p_1}{q_1} \cdot \frac{p_3}{q_3}.
\end{aligned}$$

■

Teorema 16.2 — Tricotonomia em $\mathbb{Q}$. Dados $a,\ b \in \mathbb{Q}$ temos que $a < b$ ou $a = b$ ou $b < a$.

Demonstração. Sejam

$$a = \frac{p_1}{q_1} \quad \text{e} \quad b = \frac{p_2}{q_2},$$

com $0 < q_1$ e $0 < q_2$. Da tricotomia em $\mathbb{Z}$ temos que $p_1 \cdot q_2 = p_2 \cdot q_1$ se $a = b$ ou $p_1 q_2 < p_2 q_1$ que é quando $a < b$ ou $p_2 q_1 < p_1 q_2$ que é quando $b < a$. ■

Corolário 16.4 Os racionais formam um corpo ordenado.

Demonstração. Mostramos cada uma das propriedades:

- Se $a < b$ então $a \leq b$ e portanto $a+c \leq b+c$.Porém se $a+c = b+c$ então teríamos que $a = b$ o que não acontece. Portanto $a+c < b+c$.
- Se $0 < a$ e $a < b$ então $0 \leq a \cdot b$ no entanto $a \cdot b \neq 0$ pois $a \neq 0$ e $b \neq 0$. De onde $0 < a \cdot b$.

■

Teorema 16.3 Sejam $\mathbf{a}$, $\mathbf{b}$, $\mathbf{c} \in \mathbb{Q}$. Toda função proposicional da forma

$$P(x) = \text{"}x \in \mathbb{Q},\ \mathbf{a} \cdot x + \mathbf{b} = \mathbf{c}\text{"}.$$

tem por domínio de verdade $M = \{[\mathbf{c} + (\text{-}\mathbf{b})] \cdot \mathbf{a}^{-1}.\}$.

Demonstração. Imediato das propriedades da soma em $\mathbb{Q}$. ■

Obs. Os números inteiros podem ser vistos como um subconjunto dos números racionais da seguinte forma: defina $f : \mathbb{Z} \to \mathbb{Q}$ por

$$f(a) = \frac{a}{1}.$$

é fácil ver que

$$f(a+b) = f(a) + f(b) \quad \text{e} \quad f(a \cdot b) = f(a) \cdot f(b).$$

desta forma dizemos que $\mathbb{Z} \subset \mathbb{Q}$. Mais ainda, temos que se $a \leq b$ em $\mathbb{Z}$ então $f(a) \leq f(b)$.

Lema 16.1 Todo número racional positivo pode ser escrito, de forma única, como $a = \frac{m}{n}$ com $(m,n) = 1$.

Demonstração. Seja $a = \frac{p}{q}$ para $0 \leq p,\ 0 < q$ e assuma que $d = (p,q)$ então $p = p_1 \cdot d$ e $q = q_1 \cdot d$. Observamos que, como $p \cdot q_1 \cdot d = p_1 \cdot q \cdot d$ temos que

$$a = \frac{p}{q} = \frac{p_1}{q_1}$$

com $(p_1, q_1) = 1$. Se

$$\frac{p_1}{q_1} = \frac{p_2}{q_2} \quad \Rightarrow \quad p_1 \cdot q_2 = p_2 \cdot q_1.$$

com $(p_1, q_1) = 1$ e $(p_2, q_2) = 1$ Como $(p_1, q_1) = 1$ temos que $p_1 | p_2$ e $p_2 = c_1 \cdot p_1$. Da misma forma $q_2 = c_2 \cdot q_1$. Mas então $\frac{c_1}{c_2} = 1$ de onde segue que $c_1 = c_2 = 1$. ■

Obs. Vamos dizer que um número racional $0 \leq a$ está escrito na forma irredutível quando escrito na forma $\frac{p}{q}$ em que $(p,q) = 1$.

Lema 16.2 — densidade dos racionais. Sejam a e b dois números racionais tais que $a < b$, então existe um número racional c tal que $a < c < b$.

Demonstração. Escrevemos

$$a = \frac{p_1}{q_1} \quad \text{e} \quad b = \frac{p_2}{q_2}.$$

Então $a < b$ garante que

$$p_1 \cdot q_2 < p_2 \cdot q_1.$$

Definimos

$$c = \frac{p_2 \cdot q_1 + p_1 \cdot q_2}{2 \cdot q_1 \cdot q_2}.$$

claramente $c \in \mathbb{Q}$. Observamos que

$$\begin{aligned} 2 \cdot q_1 \cdot q_2 \cdot p_1 &= q_1 \cdot q_2 \cdot p_1 + q_1 \cdot q_2 \cdot p_1 \\ &< q_1 \cdot p_2 \cdot q_1 + q_1 \cdot q_2 \cdot p_1 \\ &= (p_2 \cdot q_1 + p_1 \cdot q_2) \cdot q_1 \quad \Rightarrow \quad a < c, \end{aligned}$$

e

$$\begin{aligned} (p_2 \cdot q_1 + p_1 \cdot q_2) \cdot q_2 &= p_2 \cdot q_1 \cdot q_2 + p_1 \cdot q_2 \cdot q_2 \\ &< p_2 \cdot q_1 \cdot q_2 + q_1 \cdot p_2 \cdot q_2 \\ &= (2 \cdot q_1 \cdot q_2) \quad \Rightarrow \quad c < b, \end{aligned}$$

obtendo assim o pedido. ■

Os racionais não formam um conjunto bem ordenado com a ordem acima.

Teorema 16.4 O conjunto dos números racionais, com a ordem definida acima, não é um conjunto bem ordenado.

Demonstração. Vamos mostrar que existem subconjuntos não vazios de $\mathbb{Q}$, limitados inferiormente e sem elemento mínimo. Para isto considere

$$A = \{a \in \mathbb{Q}, 1 < 2 \cdot a\}$$

Claramente

- $A \neq \emptyset$ pois, por exemplo, $a = 1 \in A$.
- para todo $a \in A$ temos que $0 < a$.
- $a = \frac{1}{2}$ é limite inferior de A.

Assuma A admite elemento mínimo $m \in A$ e assuma que

$$m = \frac{p}{q} \quad (p,q) = 1.$$

Então, como $\frac{1}{2}$ é limite inferior, temos que temos que

$$\frac{1}{2} < \frac{p}{q} \Rightarrow \frac{1}{2} < \frac{1}{2}\left(\frac{1}{2} + \frac{p}{q}\right) < \frac{p}{q}.$$

Portanto

$$\frac{1}{2}\left(\frac{1}{2} + \frac{p}{q}\right) \in A \quad \text{e} \quad \frac{1}{2}\left(\frac{1}{2} + \frac{p}{q}\right) < \frac{p}{q},$$

o que é uma contradição. ■

Teorema 16.5 O conjunto $\mathbb{Q}$, com a ordem acima, não possui elemento máximo nem mínimo.

Demonstração. Assuma que existe um elemento mínimo m em $\mathbb{Q}$. Então $m = \frac{p}{q}$ com $p < 0$ e $q > 0$. Como $0 < \frac{2}{1}$ temos que $\frac{2}{1} \cdot \frac{p}{q} \in \mathbb{Q}$ e

$$\frac{2}{1} \cdot \frac{p}{q} < \frac{p}{q}$$

o que é uma contradição. De forma similar se mostra que não tem máximo. ■

17. Números Reais

Temos visto na seção anterior a construção dos número racionais. Com os números racionais temos que o domínio de verdade as proposições da forma

$$P(x) = \text{"}x \in \mathbb{N},\ a \cdot x + b = c.\text{"}$$

para $a,\ b,\ c \in \mathbb{Q}$ tem domínio de verdade vazio em $\mathbb{Q}$. No entanto, sobre os racionais ainda temos funções proposicionais do tipo polinomial com domínio de verdade vazio como mostra o seguinte exemplo.

■ **Exemplo 17.1** A função proposicional em $\mathbb{Q}$

$$P(x) = \text{"}x \in \mathbb{R},\ x^2 = 2.\text{"}$$

tem domínio de verdade vazio. De fato, se $\frac{a}{b} \in \mathbb{Q}$ está no domínio, então temos que

$$a^2 = 2 \cdot b^2.$$

Como, pelo teorema fundamental da aritmética, $a = p_1 \cdots p_k$ e $b = q_1 \cdots q_l$ para $p_i,\ q_j$ primos, temos que

$$a^2 = p_1^2 \cdots p_k^2 = 2 \cdot q_1^2 \cdots q_l^2.$$

Do lado esquerdo o 2 deve aparecer um numero par de vezes e, no entanto, do lado direito deve aparecer um número impar de vezes. O que é uma contradição pois teríamos duas decomposições diferentes em primos de a^2.

Mais ainda, o conjunto $A = \{x \in \mathbb{Q},\ x^2 < 2\}$ é um conjunto limitado, pois é fácil ver que $-2 < x < 2$ para todo $x \in A$ e não admite supremo. De fato se existir um supremo $m \in \mathbb{Q}$ então $m > 1$, pois por exemplo

$$1 < (5/4)^2 < 2, \quad \text{de onde} \quad m > (5/4) > 1.$$

Portanto

$$2 < m^2 + 2 \cdot m + 1.$$

Também $m^2 < 2$. De fato, se $m^2 \geq 2$ temos que, como $m \in \mathbb{Q}$ sabemos, pelo visto acima, que $m^2 \neq 2$. Se $m^2 > 2$ temos que $m \notin A$. Defina

$$\delta = (2 - m^2) \cdot 2^{-1} \cdot m^{-1}$$

Temos que $\delta < 0$. Seja

$$n = m + \delta,$$

então $n < m$ e

$$\begin{aligned} n^2 &= m^2 + 2\cdot\delta\cdot m + \delta^2 \\ &= m^2 + (2 - m^2) + \delta^2 \\ &= 2 + \delta^2 \\ &> 2 \end{aligned}$$

De onde n também é cota superior, o que contradiz o fato de m ser supremo.

Assuma então $m^2 < 2$. Seja

$$\varepsilon = (2 - m^2)\cdot(2\cdot m + 1)^{-1} \quad \Rightarrow \quad 0 < \varepsilon < 1.$$

Defina

$$r = m + \varepsilon$$

satisfaz $m < r$ e

$$\begin{aligned} r^2 &= m^2 + 2\cdot\varepsilon\cdot m + \varepsilon^2 \\ &= m^2 + (\varepsilon + 2\cdot m)\cdot\varepsilon \\ &< m^2 + (1 + 2\cdot m)\cdot\varepsilon \\ &= m^2 + (2 - m^2) = 2. \end{aligned}$$

Então, $r \in A$ e $r \leq m$ o que é também uma contradição. De onde seque que A não admite supremo. Observe que o supremo, no caso, seria $\sqrt{2}$ que não pertence a $\mathbb{Q}$. ∎

É por este tipo de situações que continuamos ampliar nosso conjunto numérico de forma tal que, neste novo conjunto numérico, as funções proposicionais sobre os racionais estejam contempladas e o seu domínio de verdade seja não vazio.

Para definir os números reais vamos a proceder de uma forma diferente ao que foi feito anteriormente. Tanto para definir os números inteiros quanto os racionais considerávamos subconjuntos de um produto cartesiano de dois conjuntos. Para a construção dos números reais vamos a considerar classes de equivalência de funções.

Começamos com a função valor absoluto $|\ |_{\mathbb{Q}} : \mathbb{Q} \to \mathbb{Q}$ que é definida por

$$|a|_{\mathbb{Q}} = \begin{cases} a & \text{se} \quad 0 \leq a \\ -a & \text{se} \quad a < 0. \end{cases}$$

Obs. Tiramos o subíndice $|\ |_{\mathbb{Q}}$ da função para não carregar a notação e a passamos a denotar por $|\ |$.

Algumas propriedades desta função são

- $|a| = |-a|$.
- $a \leq |a|$ e $-a \leq |a|$.
- $|a\cdot b| = |a|\cdot|b|$
- $|a + b| \leq |a| + |b|$

Demonstração. A prova da primeira e da segunda propriedade são inmediatas da definição.

Para mostrar a terceira temos três casos

- $0 \leq a$ e $0 \leq b$. Neste caso $|a\cdot b| = a\cdot b = |a|\cdot|b|$.
- $0 \leq a$ e $b < 0$. Neste caso $|a\cdot b| = a\cdot(-b) = |a|\cdot|b|$.

- $a<0$ e $b<0$. Neste caso $|a\cdot b| = (-a)\cdot(-b) = |a|\cdot|b|$.

Para a quarta temos dois casos.

- Se $a+b<0$ então

$$|a+b| = -(a+b) = -a+-b \leq |a|+|b|.$$

- Se $0 \leq a+b$

$$|a+b| = a+b \leq |a|+|b|.$$

■

Definição 17.1 Uma sequência de números racionais é uma função $x : \mathbb{N} \to \mathbb{Q}$. Denotamos à sequência por $(x_n)_{n\in\mathbb{N}}$ e por $x_n = x(n)$.

Definição 17.2 Seja $(x_n)_{n\in\mathbb{N}}$ uma sequência de números racionais. Dizemos que:

- A sequência $(x_n)_{n\in\mathbb{N}}$ é de Cauchy se: para todo $\varepsilon \in \mathbb{Q}$ com $\varepsilon > 0$ existe um $n_0 \in \mathbb{N}$ tal que se $n_0 < n,\ m$ então $|x_m - x_n| \leq \varepsilon$.
  Denotamos por $\mathscr{C}_{\mathbb{Q}}$ ao conjunto das sequências de números racionais que são de Cauchy.
- A sequência $(x_n)_{n\in\mathbb{N}}$ converge a um número $a \in \mathbb{Q}$ se: para todo $\varepsilon \in \mathbb{Q}$ com $0 < \varepsilon$ existe um $n_0 \in \mathbb{N}$ tal que se $n_0 < n$ então $|a - x_n| \leq \varepsilon$.

Obs. Seja $(x_n)_{n\in\mathbb{N}}$ uma sequência então, como vimos antes é uma função $x : \mathbb{N} \to \mathbb{Q}$. Assim uma sequência pode ser vista como um processo que vai assumindo valores a medida que aumenta n.

- Se a sequência é de Cauchy significa que seus termos ficam arbitrariamente próximos uns dos outros a medida que n é maior. Isto, em matemática, é descrito dizendo que para qualquer $\varepsilon > 0$, podendo ser arbitrariamente pequeno, temos que a distância entre os seus elementos $x(n)$ e $x(m)$ para $n,\ m$ suficientemente grandes, será menor que ε. Mais ainda, para cada $\varepsilon > 0$ podemos achar um n_0 tal que

$$|x_{n_0} - x_m| < \varepsilon$$

  para todo $m > n_0$.
- Se a sequência é convergente a q então os seus termos ficam arbitrariamente perto de um ponto fixo q. Isto, em matemática, é descrito dizendo que para qualquer $\varepsilon > 0$, podendo ser arbitrariamente pequeno, temos que a distância entre q e $x(n)$, para n suficientemente grandes, será menor que ε. Mais anda, para cada $\varepsilon > 0$ podemos achar um n_0 tal que

$$|q - x_m| < \varepsilon$$

  para todo $m > n_0$. Ou seja, todos os termos sucessivos estão, no máximo a uma distância menor que $\varepsilon < 0$.

Se um processo físico é descrito por uma sequência (por exemplo a variação de temperatura $T(n)$ no instante $t = n$), o fato que a sequência de eventos seja de Cauchy permite ver que o processo tem uma certa previsibilidade pois a partir do valor que assume em um ponto, os outros vão estar perto deste. O fato da sequência ser convergente, permite dizer que os valores vão estar muito perto do valor ao qual converge (por exemplo T_0).

O seguinte resultado relaciona os dois conceitos.

Teorema 17.1 Seja $(x_n)_{n\in\mathbb{N}}$ uma sequência convergente a um número $a \in \mathbb{Q}$. Então ela é de Cauchy.

Demonstração. Seja $0 < \varepsilon$ um número racional. Como a sequência $(x_n)_{n\in\mathbb{N}}$ converge a a temos que, para $\frac{1}{2}\cdot\varepsilon$ existe um n_0 tal que se $n_0 < n$ então $|a - x_n| \leq \frac{1}{2}\cdot\varepsilon$. Sejam $n_0 < m,\ n$ então observamos que

$$\begin{aligned} |x_n - x_m| &= |x_n - a + a - x_m| \\ &\leq |x_n - a| + |x_m - a| \leq \\ &\leq \frac{1}{2}\cdot\varepsilon + \frac{1}{2}\cdot\varepsilon = \varepsilon. \end{aligned}$$

Portanto para todo $\varepsilon \in \mathbb{Q}$ tal que $\varepsilon > 0$ existe um $n_0 \in \mathbb{N}$ tal que se $n_0 < n,\ m$ então $|x_m - x_n| \leq \varepsilon$. ■

■ **Exemplo 17.2** • Considere a sequência $(x_n)_{n\in\mathbb{N}}$ em que

$$x_n = (-1)^n$$

Esta sequência não é de Cauchy nem convergente. De fato,

$$|x_n - x_{n+(2m+1)}| = |(-1)^n + (-1)^n| = 2$$

portanto existe $1 = \varepsilon > 0$ tal que para todo n_0 temos $n, m > n_0$ e

$$|x_n - x_{n+(2m+1)}| \geq 1.$$

Como não é uma sequência de Cauchy, ela não pode ser convergente.

- Dado $q \in \mathbb{Q}$, considere a sequência $(x_n)_{n\in\mathbb{N}}$ em que

$$x_n = q \quad \forall\, n \in \mathbb{N},$$

Ou seja x é a função constante. Claramente para todo $\varepsilon > 0$ existe $n_0 = 1$ tal que $m, n > 1$ temos

$$|x_n - x_m| = 0 < \varepsilon,$$

portanto, é uma sequência de Cauchy e, mais ainda convergente pois para todo $\varepsilon > 0$ existe $n_0 = 1$ tal que se $n > n_0$ então

$$|x_n - q| = 0 < \varepsilon.$$

- Uma sequência de Cauchy que não é convergente em $\mathbb{Q}$ pode ser construída como segue: Seja $a \in (0,1)$ um número irracional, então

$$a = 0, a_1 a_2 \ldots a_n a_{n+1} \ldots$$

Então

$$x_n = 0, a_1 \ldots a_n.$$

Então se $n > m$ temos

$$x_n - x_m = \frac{a_{n+1} \ldots a_m}{10^m} < \frac{1}{10^n}$$

Dado $\varepsilon > 0$ existe n_0 de forma tal que $\frac{1}{10^{n_0}} < \varepsilon$ e de forma tal que se $n,\ m > n_0$ então

$$|x_n - x_m| < \frac{1}{10^{\min\{n,m\}}} < \varepsilon.$$

Observamos que a sequência não converge em $\mathbb{Q}$. De fato, se o limite for $q \in \mathbb{Q}$ tem um número máximo n de cassas decimais ou é uma dízima periódica. Em qualquer dos dois casos haverá sempre um m suficientemente grande em que $x_m - q \neq 0$ pela construção do x_n é pelo fato de a ser irracional. Portanto chegamos a uma contradição. De onde segue que a sequência não é convergente.

- Considere a sequência $(x_n)_{n\in\mathbb{N}}$ em que

$$x_n = \left(1 + \frac{2}{n}\right)^2$$

Observamos que ela é de Cauchy e é convergente. Mostramos cara uma por separado embora, por causa do teorema acima, seja suficiente mostrar que é convergente para termos que é de Cauchy.

Para ver que é de Cauchy considere $n > m \geq 1$ e fazemos

$$\begin{aligned} x_m - x_n &= \left(2+\frac{2}{n}+\frac{2}{m}\right)\cdot\left(\frac{2}{m}-\frac{2}{n}\right) \\ &= 2\left(2+\frac{2}{n}+\frac{2}{m}\right)\cdot\left(\frac{1}{m}-\frac{1}{n}\right), \end{aligned}$$

Como $n > m > 1$ temos

$$\frac{1}{m}-\frac{1}{n} < \frac{1}{m}$$

e

$$2\left(2+\frac{2}{n}+\frac{2}{m}\right) < 12$$

Portanto

$$|x_m - x_n| < \frac{12}{m}$$

Seja $\varepsilon > 0$, então sempre existe um número natural n_0 tal que

$$n_0 > 12\cdot\varepsilon^{-1}.$$

Assim, dado $\varepsilon > 0$ existe um numero natural $n_0 > 10\cdot\varepsilon^{-1}$ tal que se $n,\ m > n_0$ temos

$$|x_n - x_m| \leq \frac{12}{\min\{n,\ m\}} < \frac{12}{n_0} < \varepsilon.$$

De onde a sequência é de Cauchy.
Vamos mostrar que a sequência é convergente. Observamos que, da forma de x_n quanto maior for n o termo $\frac{2}{n}$ está mais perto de 0, desta forma, quando n for a infinito este irá para 0 e x_n ficará mais perto de 1.
Vamos mostrar então que a sequência converge para 4.
Observamos que

$$|x_n - 1| = \left|\frac{4}{n}+\frac{4}{n^2}\right| < \frac{8}{n}.$$

Seja $\varepsilon > 0$, então existe um numero natural n_0 tal que $n_0 > 8\cdot\varepsilon^{-1}$.
Assim, dado $\varepsilon > 0$ existe um numero natural $n_0 > 8\cdot\varepsilon^{-1}$ tal que se $n > n_0$ então

$$|x_n - 1| < \frac{8}{n} < \frac{8}{n_0} < \varepsilon.$$

■

Proposição 17.1 Sejam $(x_n)_{n\in\mathbb{N}},\ (y_n)_{n\in\mathbb{N}} \in \mathscr{C}_{\mathbb{Q}}$ e $a \in \mathbb{Q}$.

- Existe M tal que, para todo $n \in \mathbb{N}$ temos $|x_n| < M$.
- Seja $a \in \mathbb{Q}$ tal que $a \neq 0$. A sequência $(z_n)_{n\in\mathbb{N}}$ definida por $z_n = a\cdot x_n + y_n$ para todo $n \in \mathbb{N}$ é de Cauchy.
- A sequência $(z_n)_{n\in\mathbb{N}}$ definida por $z_n = x_n \cdot y_n$ para todo $n \in \mathbb{N}$ é de Cauchy.

Demonstração. Sejam $(x_n)_{n\in\mathbb{N}},\ (y_n)_{n\in\mathbb{N}} \in \mathscr{C}_{\mathbb{Q}}$ e $a \in \mathbb{Q}$.

- Seja $(x_n)_{n\in\mathbb{N}}$ uma sequência de Cauchy e considere $\varepsilon = 1$ então existe n_0 tal que se $n,\ m > n_0$ temos que $|x_{n_0+1} - x_m| < 1$. Portanto

$$x_{n_0+1} - 1 < x_m < x_{n_0+1} + 1 \quad \forall\, m.$$

Como $A = \{|x_0|, \ldots, |x_{n_0}|, |x_{n_0+1} - 1|, |x_{n_0+1} + 1|\}$ é um conjunto finito temos que existe $N = \max A$. De onde segue o resultado.

- Seja $\varepsilon > 0$ então existe n_0 tal que

$$|x_n - x_m| < \frac{1}{2} \cdot |a|^{-1} \cdot \varepsilon \quad \text{e} \quad |y_n - y_m| < \frac{1}{2} \cdot \varepsilon,$$

para todo $n_0 < n,\ m$. Considere a sequência $(z_n)_{n\in\mathbb{N}}$ definida por $z_n = a \cdot x_n + y_n$ para todo $n \in \mathbb{N}$ então

$$|z_n - z_m| = |a| \cdot |x_n - x_m| + |y_n - y_m| < \varepsilon.$$

- Seja $\varepsilon > 0$ então existe n_0 tal que

$$|x_n - x_m| < \frac{1}{2} \cdot M_x^{-1} \cdot \varepsilon \quad |y_n - y_m| < \frac{1}{2} M_y^{-1} \cdot \varepsilon$$

para todo $n_0 < n,\ m$ e M_x e M_y como no primeiro item. Considere a sequência $(z_n)_{n\in\mathbb{N}}$ definida por $z_n = x_n \cdot y_n$ então

$$\begin{aligned} |z_n - z_m| &= |x_n \cdot y_n - x_m \cdot y_n + x_m \cdot y_n - x_m \cdot y_m| \\ &= |x_n - x_m| \cdot |y_n| + |x_m| \cdot |y_n - y_m| \\ &\leq |x_n - x_m| \cdot M_y + M_x \cdot |y_n - y_m| < \varepsilon. \end{aligned}$$

para todo $n,\ m \in \mathbb{N}$ e portanto, é de Cauchy.

■

Estabelecemos no conjunto $\mathscr{C}_{\mathbb{Q}}$ a seguinte relação

$$(x_n)_{n\in\mathbb{N}} \sim (y_n)_{n\in\mathbb{N}} \quad \text{se, e somente se} \quad (x_n - y_n)_{n\in\mathbb{N}} \quad \text{converge a 0.}$$

Vejamos que a relação é de equivalência:

- Reflexiva: Claramente $(x_n)_{n\in\mathbb{N}} \sim (x_n)_{n\in\mathbb{N}}$ pois $x_n - x_n = 0$ para todo $n \in \mathbb{N}$
- Simétrica: Se $(x_n)_{n\in\mathbb{N}} \sim (y_n)_{n\in\mathbb{N}}$ então $(x_n - y_n)_{n\in\mathbb{N}}$ converge a 0. Como $|y_n - x_n| = |x_n - y_n|$ temos que $(y_n - x_n)_{n\in\mathbb{N}}$ também converge a 0.
- Transitiva: Se Se $(x_n)_{n\in\mathbb{N}} \sim (y_n)_{n\in\mathbb{N}}$ e $(y_n)_{n\in\mathbb{N}} \sim (z_n)_{n\in\mathbb{N}}$ então, da definição da relação de equivalência temos que dado $\varepsilon > 0$ existe n_0 tal que

$$|x_n - y_n| < \frac{1}{2} \cdot \varepsilon \quad |y_n - z_n| < \frac{1}{2} \cdot \varepsilon$$

para todo $n_0 < n$. Portanto

$$|x_n - z_n| \leq |x_n - y_n| + |y_n - z_n| < \varepsilon.$$

e portanto $(x_n - z_n)_{n\in\mathbb{N}}$ converge a 0.

Definição 17.3 O conjunto dos números reais $\mathbb{R}$ é o conjunto

$$\mathbb{R} = \mathscr{C}_{\mathbb{Q}} / \sim .$$

Denotamos à clase de $(x_n)_{n\in\mathbb{N}}$ por $[x_n]_{n\in\mathbb{N}}$. Então um número real a é uma classe de equivalência

$$a = [x_n]_{n\in\mathbb{N}}$$

para alguma sequência de Cauchy $(x_n)_{n\in\mathbb{N}} \in \mathscr{C}_{\mathbb{Q}}$.

■ **Exemplo 17.3** Vimos anteriormente que a solução de $x^2 = 2$ não pode ser achada dentro dos racionais. O mesmo argumento pode ser feito para mostrar que para todo p primo o domínio de verdade da proposição

$$P(x) = "x^2 = p",$$

é vazio em $\mathbb{Q}$. De fato, se $\frac{a}{b} \in \mathbb{Q}$ está no domínio, então temos que

$$a^2 = p \cdot b^2.$$

Como, pelo teorema fundamental da aritmética, $a = p_1 \cdots p_k$ e $b = q_1 \cdots q_l$ para $p_i,\ q_j$ primos, temos que

$$a^2 = p_1^2 \cdots p_k^2 = p \cdot q_1^2 \cdots q_l^2.$$

Do lado esquerdo o p deve aparecer um numero par de vezes e, no entanto, do lado direito deve aparecer um número impar de vezes. O que é uma contradição pois teríamos duas decomposições diferentes em primos de a^2.

■

Passamos agora a definir as operações soma e produto.

Definição 17.4 Sejam $t = [x_n]_{n\in\mathbb{N}}$ e $s = [y_n]_{n\in\mathbb{N}}$ em $\mathbb{R}$. Definimos a soma $+ : \mathbb{R}\times\mathbb{R} \to \mathbb{R}$ por

$$t + s = [x_n + y_n]_{n\in\mathbb{N}}.$$

e o produto $\cdot : \mathbb{R}\times\mathbb{R} \to \mathbb{R}$ por

$$t \cdot s = [x_n \cdot y_n]_{n\in\mathbb{N}}$$

Obs. As operações soma e produto nos números reais não são as mesmas que as operações soma e produto nos números racionais. A notação correta teria um simbolo para cada operação, então seria algo da forma $+_{\mathbb{R}} : \mathbb{R}\times\mathbb{R} \to \mathbb{R}$ por

$$t +_{\mathbb{R}} s = [x_n +_{\mathbb{Q}} y_n]_{n\in\mathbb{N}}.$$

e $\cdot_{\mathbb{R}} : \mathbb{R}\times\mathbb{R} \to \mathbb{R}$ por

$$t \cdot_{\mathbb{R}} s = [x_n \cdot_{\mathbb{Q}} y_n]_{n\in\mathbb{N}}$$

Como a notação fica muito sobrecarregada, deixamos a interpretação a cargo do leitor e subentendida ao contexto.

Outra observação é que, a diferença dos número inteiros e racionais, a fórmula para computar as operações não é feito por uma equação simples envolvendo um número finito de elementos. Elas requerem um número infinito de passos e elementos.

Mostramos agora que as definições de soma e produto são boas e não dependem do representante da classe escolhido para computá-las. De fato, assuma que

$$[x_n]_{n\in\mathbb{N}} = [x'_n]_{n\in\mathbb{N}} \quad \text{e} \quad [y_n]_{n\in\mathbb{N}} = [y'_n]_{n\in\mathbb{N}}$$

isto é,

$$(x_n - x'_n)_{n\in\mathbb{N}} \quad \text{e} \quad (y_n - y'_n)_{n\in\mathbb{N}}$$

convergem a 0. Então, dada $\varepsilon \in \mathbb{Q}$ com $\varepsilon > 0$ existe um n_0 tal que se $n_0 < n$ então

$$|x_n - x'_n| < \frac{1}{2}\cdot\varepsilon \quad \text{e} \quad |y_n - y'_n| < \frac{1}{2}\cdot\varepsilon$$

Portanto

$$|(x_n + y_n) - (x'_n + y'_n)| < \frac{1}{2}\cdot\varepsilon + \frac{1}{2}\cdot\varepsilon = \varepsilon.$$

De onde segue que $[x_n + y_n]_{n\in\mathbb{N}} = [x'_n + y'_n]_{n\in\mathbb{N}}$.

De forma similar, temos que dado $\varepsilon > 0$ existe um n_0 tal que se $n_0 < n$ então

$$|x_n - x'_n| < \frac{1}{2}\cdot M_{y'}^{-1}\cdot\varepsilon \quad \text{e} \quad |y_n - y'_n| < \frac{1}{2}\cdot M_x^{-1}\cdot\varepsilon$$

Portanto

$$\begin{aligned} |x_n \cdot y_n - x'_n \cdot y'_n| &\leq |x_n \cdot y_n - x_n \cdot y'_n| + |x_n \cdot y'_n - x'_n \cdot y'_n| \\ &= |x_n| \cdot |y_n - y'_n| + |x_n - x'_n| \cdot |y'_n| \\ &= M_x \cdot |y_n - y'_n| + |x_n - x'_n| \cdot M_y. \end{aligned}$$

De onde segue que $[x_n \cdot y_n]_{n\in\mathbb{N}} = [x'_n \cdot y'_n]_{n\in\mathbb{N}}$.

■ **Exemplo 17.4** Considere as sequências

$$(x_n)_{n\in\mathbb{N}} \quad \text{e} \quad (y_n)_{n\in\mathbb{N}}$$

definidas por

$$x_n = \frac{1}{n} \quad y_n = 1 + \frac{2}{n+2}$$

Observamos que as duas sequências são de Cauchy. De fato, dado $\varepsilon > 0$ existe $n_0 \in \mathbb{N}$, $n_0 \cdot \varepsilon > 4$ tal que se $m,n > n_0$ temos

$$|x_n - x_m| < \frac{2}{\min\{n,m\}} < \varepsilon$$

e

$$|y_n - y_m| < \frac{4}{\min\{n+2,m+2\}} < \varepsilon.$$

Então, pelo resultado anterior, as sequências $(u_n)_{n\in\mathbb{N}}$ e $(v_n)_{n\in\mathbb{N}}$ definidas por

$$u_n = x_n + y_n = 1 + \frac{1}{n} + \frac{2}{n+2}$$

e

$$v_n = x_n \cdot y_n = \frac{1}{n} + \frac{2}{n\cdot(n+2)},$$

são de Cauchy.

■

Obs.

- A classe $0 = [x_n]_{n\in\mathbb{N}}$ tal que $x_n = 0$ para todo $n \in \mathbb{N}$ satisfaz
$$0 + t = 0 \quad \text{e} \quad 0 \cdot t = 0 \quad \forall t \in \mathbb{R}.$$
- a classe $1 = [x_n]_{n\in\mathbb{N}}$ tal que $x_n = 1$ para todo $n \in \mathbb{N}$
$$1 \cdot t = t \quad \forall t \in \mathbb{R}.$$
- Se $t = [x_n]_{n\in\mathbb{N}}$ então $-t = [-x_n]_{n\in\mathbb{N}}$ satisfaz
$$t + (-t) = 0.$$
- Se $t = [x_n]_{n\in\mathbb{N}}$ tal que $t \neq 0$ temos que existe $N \in \mathbb{N}$ tal que $x_n \neq 0$ para todo $n \in \mathbb{N}$ tal que $n > N$. De fato, como a sequência é de Cauchy temos que para cada $k \in \mathbb{N}$ existe n_k tal que $|x_n - x_m| < \frac{1}{k}$ e $x_{n_k} > \frac{1}{k}$. Como a sequência não converge para 0 existe um $K \in \mathbb{N}$ tal que $|x_n| > \frac{1}{K}$ para todo $n > n_K$ pois, caso contrário, teríamos que sempre existe $x_m < \frac{1}{k}$ para todo k de onde segue que a sequência converge para 0 o que é uma contradição.
Mais ainda temos que $x_m > 0$ ou $x_m < 0$ para todo $m > n_K$. De fato, se $x_{n_K} > 0$ então, como a sequência é de Cauchy temos que existe $\varepsilon = \frac{1}{2\cdot K}$ tal que
$$x_m = x_m - x_n + x_n > \frac{1}{K} + x_m - x_n > \frac{1}{K} - \frac{1}{2\cdot K} = \frac{1}{2\cdot K}.$$
De forma similar se mostra se $x_m < 0$.
- Se $t = [x_n]_{n\in\mathbb{N}}$ tal que $t \neq 0$, definimos $t^{-1} = [y_n^{-1}]_{n\in\mathbb{N}}$ onde $y_n = 0$ para $n \leq n_0$ e $y_n = x_n^{-1}$ para todo $n > n_0$ satisfaz
$$t \cdot t^{-1} = 1.$$

Podemos mostrar que $\mathbb{R}$ munido da soma e o produto definido acima satisfaz o seguinte resultado.

Proposição 17.2 Sejam $\mathbf{a}$, $\mathbf{b}$, $\mathbf{c}$ números em $\mathbb{R}$. Então

- $\mathbf{a}+\mathbf{b}=\mathbf{b}+\mathbf{a}$ (comutatividade).
- $\mathbf{a}+(\mathbf{b}+\mathbf{c})=(\mathbf{a}+\mathbf{b})+\mathbf{c}$ (associatividade).
- Existe $\mathbf{0}\in\mathbb{R}$ tal que $\mathbf{a}+\mathbf{0}=\mathbf{a}$ para todo $\mathbf{a}\in\mathbb{R}$ (existência de elemento neutro).
- Para todo $\mathbf{a}\in\mathbb{R}$ existe $-\mathbf{a}\in\mathbb{R}$ tal que $\mathbf{a}+(-\mathbf{a})=\mathbf{0}$ (existência de elemento inverso).
- Se $\mathbf{a}+\mathbf{b}=\mathbf{a}+\mathbf{c}$ Então $\mathbf{b}=\mathbf{c}$. (cancelamento na adição).
- $\mathbf{a}\cdot\mathbf{b}=\mathbf{b}\cdot\mathbf{a}$ (comutatividade).
- $\mathbf{a}\cdot(\mathbf{b}\cdot\mathbf{c})=(\mathbf{a}\cdot\mathbf{b})\cdot\mathbf{c}$ (associatividade).
- Existe $\mathbf{1}$ tal que $\mathbf{a}\cdot\mathbf{1}=\mathbf{a}$ (existência de elemento neutro).
- Para todo $\mathbf{a}\in\mathbb{R}$ tal que $\mathbf{a}\neq\mathbf{0}$ existe $\mathbf{a}^{-1}\in\mathbb{R}$ tal que $\mathbf{a}\cdot\mathbf{a}^{-1}=\mathbf{1}$.
- $\mathbf{a}\cdot(\mathbf{b}+\mathbf{c})=(\mathbf{a}\cdot\mathbf{b})+(\mathbf{a}\cdot\mathbf{c})$ (distributividade).
- Se $\mathbf{a}\neq\mathbf{0}$ e $\mathbf{a}\cdot\mathbf{b}=\mathbf{a}\cdot\mathbf{c}$. Então $\mathbf{b}=\mathbf{c}$ (cancelamento no produto).

Portanto os número reais formam um corpo.

Demonstração. Sejam

$$\mathbf{a}=[a_n]_{n\in\mathbb{N}},\quad \mathbf{b}=[b_n]_{n\in\mathbb{N}},\quad \text{e}\quad \mathbf{c}=[c_n]_{n\in\mathbb{N}}$$

números em $\mathbb{R}$. Então

- $$\begin{aligned}\mathbf{a}+\mathbf{b} &= [a_n+b_n]_{n\in\mathbb{N}}\\ &= [b_n+a_n]_{n\in\mathbb{N}}\\ &= \mathbf{b}+\mathbf{a}\end{aligned}$$
- $$\begin{aligned}\mathbf{a}+(\mathbf{b}+\mathbf{c}) &= [a_n]_{n\in\mathbb{N}}+[b_n+c_n]_{n\in\mathbb{N}}\\ &= [a_n+(b_n+c_n)]_{n\in\mathbb{N}}\\ &= [(a_n+b_n)+c_n]_{n\in\mathbb{N}}\\ &= [(a_n+b_n)]_{n\in\mathbb{N}}+[c_n]_{n\in\mathbb{N}}\\ &= (\mathbf{a}+\mathbf{b})+\mathbf{c}.\end{aligned}$$
- Seja

  $$\mathbf{0}=[y_n]_{n\in\mathbb{N}}\quad \text{em que}\quad y_n=0\quad \forall\, n\in\mathbb{N}.$$

  Observamos que $(0)_{n\in\mathbb{N}}$ é de Cauchy naturalmente. então
  $$\begin{aligned}\mathbf{a}+\mathbf{0} &= [a_n+0]_{n\in\mathbb{N}}\\ &= [a_n]_{n\in\mathbb{N}}\\ &= \mathbf{a}.\end{aligned}$$
- Seja $\mathbf{a}=[a_n]_{n\in\mathbb{N}}\in\mathbb{R}$ e considere

  $$-\mathbf{a}=[-a_n]_{n\in\mathbb{N}}$$

  Observamos que $(-a_n)_{n\in\mathbb{N}}$ é de Cauchy, pois

  $$|-a_n-(-a_m)|=|a_n-a_m|$$

  portanto, se $(a_n)_{n\in\mathbb{N}}$ é de Cauchy, então $(-a_n)_{n\in\mathbb{N}}$ também é de Cauchy. Agora
  $$\begin{aligned}\mathbf{a}+(-\mathbf{a}) &= [a_n+(-a_n)]_{n\in\mathbb{N}}\\ &= [0]_{n\in\mathbb{N}}=\mathbf{0}.\end{aligned}$$

- Como

$$\mathbf{a}+\mathbf{b}=[a_n+b_n]_{n\in\mathbb{N}} \quad \text{e} \quad \mathbf{a}+\mathbf{c}=[a_n+c_n]_{n\in\mathbb{N}},$$

então $\mathbf{a}+\mathbf{b}=\mathbf{a}+\mathbf{c}$ implica que

$$((a_n+b_n)-(a_n+c_n))_{n\in\mathbb{N}} \quad \text{converge a 0,}$$

isto é

$$(b_n-c_n)_{n\in\mathbb{N}} \quad \text{converge a 0.}$$

Portanto $\mathbf{b}=\mathbf{c}$. Então $\mathbf{b}=\mathbf{c}$.

-
$$\begin{aligned}\mathbf{a}\cdot\mathbf{b} &= [a_n\cdot b_n]_{n\in\mathbb{N}}\\ &= [b_n\cdot a_n]_{n\in\mathbb{N}}\\ &= \mathbf{b}\cdot\mathbf{a}\end{aligned}$$

-
$$\begin{aligned}\mathbf{a}\cdot(\mathbf{b}\cdot\mathbf{c}) &= [a_n]_{n\in\mathbb{N}}\cdot[b_n\cdot c_n]_{n\in\mathbb{N}}\\ &= [a_n\cdot(b_n\cdot c_n)]_{n\in\mathbb{N}}\\ &= [(a_n\cdot b_n)\cdot c_n]_{n\in\mathbb{N}}\\ &= [(a_n\cdot b_n)]_{n\in\mathbb{N}}\cdot[c_n]_{n\in\mathbb{N}}\\ &= (\mathbf{a}\cdot\mathbf{b})+\mathbf{c}.\end{aligned}$$

- Seja

$$\mathbf{1}=[y_n]_{n\in\mathbb{N}} \quad \text{em que} \quad y_n=1 \quad \forall\, n\in\mathbb{N}.$$

Observamos que $(y_n)_{n\in\mathbb{N}}$ é de Cauchy naturalmente. então

$$\begin{aligned}\mathbf{a}\cdot\mathbf{1} &= [a_n\cdot 1]_{n\in\mathbb{N}}\\ &= [a_n]_{n\in\mathbb{N}}\\ &= \mathbf{a}.\end{aligned}$$

- Se $\mathbf{a}\neq\mathbf{0}$ então existe ε_0 para todo $n_0\in\mathbb{N}$ tal que $n_0<n$ e $|a_n|\geq\varepsilon_0$. Portanto existe a_n^{-1} para todo $n>n_0$. Considere então a sequência $(\alpha_n)_{n\in\mathbb{N}}$ definida por

$$\alpha_n=\begin{cases}1 & \text{se} \quad n\leq n_0\\ a_n^{-1} & \text{se} \quad n_0\leq n\end{cases}$$

Se $n,m>n_0$ então

$$|\alpha_n-\alpha_m|=\frac{|a_n-a_m|}{|a_n\cdot a_m|}<\frac{1}{\varepsilon_0^2}|a_n-a_m|,$$

portanto $(\alpha_n)_{n\in\mathbb{N}}$ é de Cauchy. Mais ainda, para todo $n>n_0$ temos

$$a_n\cdot\alpha_n=1$$

portanto

$$[a_n\cdot\alpha_n]_{n\in\mathbb{N}}=[1]_{n\mathbb{N}}=\mathbf{1}.$$

Então definimos $\mathbf{a}^{-1}=[\alpha_n]_{n\in\mathbb{N}}$ e obtemos

$$\mathbf{a}\cdot\mathbf{a}^{-1}=\mathbf{1}.$$

- $$\begin{aligned}\mathbf{a}\cdot(\mathbf{b}+\mathbf{c}) &= [a_n\cdot(b_n+c_n)]_{n\in\mathbb{N}}\\ &= [(a_n\cdot b_n)+(a_n\cdot c_n)]_{n\in\mathbb{N}}\\ &= [(a_n\cdot b_n)]_{n\in\mathbb{N}}+[(a_n\cdot c_n)]_{n\in\mathbb{N}}\\ &= (\mathbf{a}\cdot\mathbf{b})+(\mathbf{a}\cdot\mathbf{c}).\end{aligned}$$
- Se $\mathbf{a}\cdot\mathbf{b}=\mathbf{a}\cdot\mathbf{c}$ então

  $$((a_n\cdot b_n)-(a_n\cdot c_n))_{n\in\mathbb{N}} \quad \text{converge a } 0.$$

  de onde

  $$(a_n\cdot(c_n-b_n))_{n\in\mathbb{N}} \quad \text{converge a } 0.$$

  Assuma que $\mathbf{a}\neq 0$ isto é (a_n) não converge a 0. Então existe ε_0 para todo $n\in\mathbb{N}$ tal que $n_0<n$ e $|a_n|\geq\varepsilon_0$. Portanto, para todo $n>n_0$ temos

  $$|a_n\cdot(c_n-b_n)|\geq\varepsilon_0|c_n-b_n|$$

  De onde seque que

  $$(a_n\cdot(c_n-b_n))_{n\in\mathbb{N}} \quad \text{converge a } 0$$

  se, somente se,

  $$((c_n-b_n))_{n\in\mathbb{N}} \quad \text{converge a } 0.$$

■

Obs. Os números racionais podem ser vistos como um subconjunto dos números reais da seguinte forma: defina $f:\mathbb{Q}\to\mathbb{R}$ por

$$f(a)=(x_n)_{n\in\mathbb{N}} \quad \text{em que } x_n=a \quad \forall n\in\mathbb{N}.$$

é fácil ver que

$$f(a+b)=f(a)+f(b) \quad \text{e} \quad f(a\cdot b)=f(a)\cdot f(b).$$

desta forma dizemos que $\mathbb{Q}\subset\mathbb{R}$. Mais ainda, temos que se $a\leq b$ em $\mathbb{Q}$ então $f(a)\leq f(b)$.

Obs. Assim como foi feito para os números racionais definimos para $a\in\mathbb{R}$ e $n\in\mathbb{N}$

$$a^n=\overbrace{a\cdot a\cdots a}^{n \text{ termos}},$$

e

$$a^{-n}=(a^n)^{-1}=(a^{-1})^n.$$

Com ésta definição vemos que se cumple

$$a^r\cdot a^s=a^{r+s},$$

para todo $r,\ s\in\mathbb{Z}$.

Definição 17.5 Dado $s \in \mathbb{R}$ dizemos que $0 \leq s$ se $s = [x_n]_{n\in\mathbb{N}}$ existe um $n_0 \in \mathbb{N}$ tal que se $n_0 < n$ então $0 \leq x_n$.

Dados dois números reais s e t dizemos que $s \leq t$ se

$$0 \leq t + (-s).$$

Mais ainda, dizemos que

$$s < t \quad \Leftrightarrow (s \leq t) \wedge (s \neq t).$$

Obs. Dados $t,\ s \in \mathbb{R}$, denotamos

- $t \geq s$ se, e somente se, $s \leq t$.
- $t > s$ se, e somente se, st.

Proposição 17.3 Sejam $a,\ b$, e c números reais

- $a \leq b$ se, e somente se, $a + c \leq b + c$ para todo $c \in \mathbb{R}$
- Se $a \leq b$ e $0 \leq c$ então $a \cdot c \leq b \cdot c$
- Se $a \leq b$ e $c \leq 0$ então $b \cdot c \leq a \cdot c$.

Demonstração. • Observamos que

$$\begin{aligned} a \leq b &\Leftrightarrow 0 \leq b + (-a) \\ &\Leftrightarrow 0 \leq b + (-a) + c + (-c) \\ &\Leftrightarrow 0 \leq (b+c) + (-a) + (-c) \\ &\Leftrightarrow 0 \leq (b+c) + [-(a+c)] \\ &\Leftrightarrow a + c \leq (b+c). \end{aligned}$$

Para os itens que seguem, sejam

$$a = [x_n]_{n\in\mathbb{N}}, \quad b = [y_n]_{n\in\mathbb{N}} \quad \text{e} \quad c = [z_n]_{n\in\mathbb{N}}$$

- Se $a \leq b$ e $0 \leq c$ então existem naturais n_0 e n_1 tal que se $n > n_2 = \max\{n_0, n_1\}$ temos

$$0 \leq (y_n - x_n) \quad \text{e} \quad 0 \leq z_n.$$

portanto

$$0 \leq (y_n - x_n) \cdot z_n = (y_n \cdot z_n) - (x_n \cdot z_n).$$

de onde segue que $a \cdot c \leq b \cdot c$.

- Se $a \leq b$ e $c \leq 0$ então existem naturais n_0 e n_1 tal que se $n > n_2 = \max\{n_0, n_1\}$ temos

$$0 \leq (y_n - x_n) \quad \text{e} \quad 0 \leq -z_n.$$

portanto

$$0 \leq (y_n - x_n) \cdot (-z_n) = -(y_n \cdot z_n) + (x_n \cdot z_n).$$

de onde segue que $b \cdot c \leq a \cdot c$.

Seguem inmediato da definição dos reais e das propriedades do $\leq$ em $\mathbb{Q}$. ■

Corolário 17.1 Os números reais formam um corpo ordenado.

Demonstração. Somente resta mostrar que se $a = [x_n]_{n\in\mathbb{N}}$ e $b = [y_n]_{n\in\mathbb{N}}$ são números reais, então $a \leq b$ ou $b \leq a$.

Para isto observamos que se $a \neq b$ então a sequência $(z_n)_{n\in\mathbb{N}}$ definida por

$$z_n = (x_n - y_n)$$

não converge para 0. Vamos mostrar que existe $n_0 \in \mathbb{N}$ tal que para todo $n > n_0$ temos

$$0 < x_n - y_n \quad \text{ou} \quad 0 < y_n - x_n.$$

Caso isto acontece, temos de forma natural, que $a < b$ ou $b < c$.

Como $(z_n)_{n\in\mathbb{N}}$ é de Cauchy e não converge para 0 temos que existe $\varepsilon_0 \in \mathbb{Q}$ tal que para todo $n_0 \in \mathbb{N}$ temos que $n > n_0$ e $|z_n| \geq \varepsilon_0$.

Seja $\varepsilon_1 < \varepsilon_0$ então existe um $n_1 \in \mathbb{N}$ tal que se n, m são maiores que n_1 temos $|z_n - z_m| < \varepsilon_1$. Assuma que $n_2 > n_1$ e que $z_{n_1} > 0$ então $z_{n_1} > \varepsilon_0 > \varepsilon_1$. Portanto

$$\begin{aligned} -\varepsilon_1 < z_m - z_n < \varepsilon_1 \quad &\Rightarrow \quad -\varepsilon_1 + z_n < z_m < \varepsilon_1 + z_n \\ &\Rightarrow \quad 0 < z_m. \end{aligned}$$

de onde $b \leq a$. Caso $z_{n_1} < 0$ então, por um argumento similar chegamos a

$$z_m < 0 \Rightarrow a \leq b,$$

provando o que queríamos. ■

Teorema 17.2 — Tricotonomia em $\mathbb{R}$. Dados $a,\ b \in \mathbb{R}$ temos que $a < b$ ou $a = b$ ou $b < a$.

Demonstração. Segue do fato de $\mathbb{R}$ ser um corpo bem ordenado. De fato se $a = [x_n]_{n\in\mathbb{N}}$ e $b = [y_n]_{n\in\mathbb{N}}$ tais que $a \neq b$ então $(x_n - y_n)_{n\in\mathbb{N}}$ não converge para 0. Portanto existe um $n_0 \in \mathbb{N}$ tal que

$$0 < x_n - y_n \quad \text{ou} \quad 0 < y_n - x_n,$$

para todo $n > n_0$. De onde segue que $a < b$ ou $b < a$. ■

Obs. Os números racionais podem ser vistos como um subconjunto dos números reais da seguinte forma: defina $f : \mathbb{Q} \to \mathbb{R}$ por

$$f(a) = (x_n)_{n\in\mathbb{N}} \quad \text{em que } x_n = a\ \forall n \in \mathbb{N}.$$

é fácil ver que

$$f(a+b) = f(a) + f(b) \quad \text{e} \quad f(a\cdot b) = f(a)\cdot f(b).$$

desta forma dizemos que $\mathbb{Q} \subset \mathbb{R}$. Mais ainda, temos que se $a \leq b$ em $\mathbb{Q}$ então $f(a) \leq f(b)$.

Temos assim as seguintes cadeias de inclussões

$$\mathbb{N} \subset \mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R}.$$

O conjunto $\mathbb{I} = \mathbb{R}\backslash\mathbb{Q}$ é o conjunto dos números chamados irracionais.

Lema 17.1 O conjunto dos números reais não é enumerável.

Obs. Daremos aqui uma demonstração eurística do resultado de Cantor. Para mais detalhes consultar o livro: Robert Roth Stoll - Set theory and logic. Dover. (1979)

Demonstração. Vamos mostrar qua a cardinalidade de $\mathscr{P}(\mathbb{N})$ é igual a cardinalidade de $\mathbb{R}$ e portanto $\mathbb{R}$ não pode ser enumerável pois isso garante a existência de uma função sobrejetora de $\mathbb{N} \to \mathscr{P}(\mathbb{N})$ o que, pelo que vimos no teorema 13.1, não pode acontecer.

Primeiramente considere $f : \mathbb{R} \to \mathscr{P}(\mathbb{Q})$ a função definida por

$$f(x) = \{q \in \mathbb{Q},\ q \leq x\}$$

Observamos que se $x \neq y$ então, por exemplo $x < y$. Da densidade dos racionais, temos que existe um racional q_1 tal que

$$x < q_1 < y \quad \Rightarrow f(x) \neq f(y).$$

Portanto f é injetora. De onde segue que a cardinalidade de $\sharp\mathbb{R}$ é menor ou igual que a cardinalidade de $\sharp\mathscr{P}(\mathbb{Q})$

Como os racionais são enumeráveis, temos que $\sharp\mathscr{P}(\mathbb{Q})$ é menor ou igual que $\sharp\mathscr{P}(\mathbb{N})$.

Definimos a função injetora $g : \mathscr{P}(\mathbb{N}) \to \mathbb{R}$ da seguinte forma: Para $A \subset \mathbb{N}$ definimos $\chi_A : \mathbb{N} \to \{0,1\}$ por

$$\chi_A(n) = \begin{cases} 1 & \text{se} \quad n \in A \\ 0 & \text{se} \quad n \notin A \end{cases}$$

e definimos

$$g(A) = \frac{\chi_A(0)}{10} + \cdots + \frac{\chi_A(n)}{10^n} + \cdots$$

Claramente se $A \neq B$ então $g(A) \neq g(B)$ e portanto a função é injetora. De onde segue que $\sharp\mathscr{P}(\mathbb{N})$ é menor igual que $\sharp\mathbb{R}$. De onde segue que todas as cardinalidades são iguais. ■

Vamos a provar agora uma propriedade dos números reais que, basicamente, diz que um número real não pode ser infinitamente grande ou infinitamente pequeno.

Teorema 17.3 — Propriedade arquimediana. Dados a e b número positivos em $\mathbb{R}$ existe $n \in \mathbb{N}$ tal que $b < n \cdot a$

Demonstração. Sejam $a = [x_n]_{n\in\mathbb{N}}$ e $b = [y_n]_{n\in\mathbb{N}}$ números positivos. Então existe $n_0 \in \mathbb{N}$ tal que

$$0 < x_n \quad \text{e} \quad 0 < y_n,$$

para todo $n > n_0$. Observamos que o que temos que mostrar é o seguinte:

$$\text{Existem } m,\ n \in \mathbb{N} \text{ tal que se } k > n \text{ então } y_k < m \cdot x_k.$$

Assuma que isto não acontece, então para todo $m,\ n$ temos $k > n$ e $y_k \geq m \cdot x_k$.

Seja $\varepsilon \in \mathbb{Q}$ tal que $\varepsilon > 0$.

- Como $(y_n)_{n\in\mathbb{N}}$ é de Cauchy, temos que existe $R \in \mathbb{Q}$, $R = \frac{p}{q}$ com $(p,q) = 1$, tal que

$$0 < y_n < R$$

- Como $(x_n)_{n\in\mathbb{N}}$ é de Cauchy, existe $n_1 > n_0$ tal que se $n,\ m > 0$ então

$$|x_n - x_m| < \frac{1}{2}\varepsilon$$

Como $\varepsilon = \frac{q_1}{q_2}$, o algoritmo da divisão garante a existência de um $l \in \mathbb{N}$ tal que

$$2 \cdot p \cdot q_2 < l \cdot q \cdot q_1 \quad \Rightarrow \quad \frac{1}{l} \cdot R < \frac{1}{2} \cdot \varepsilon.$$

Agora, dado $m = l$ e $n \in \mathbb{N}$ com $n > n_1$ temos que $k > n_1$ e

$$0 < l \cdot x_k < y_k < R \quad \Rightarrow 0 < x_k < \frac{1}{l} \cdot R < \frac{1}{2} \cdot \varepsilon$$

Então, se $m > k$ temos

$$\begin{aligned} |x_m| &\leq |x_m - x_k| + |x_k| \\ &< \frac{1}{2}\cdot\varepsilon + \frac{1}{2}\cdot\varepsilon \\ &= \varepsilon. \end{aligned}$$

E isto vale para todo $\varepsilon > 0$. Então $(x_n)_{n\in\mathbb{N}}$ converge a 0 o que contradiz o fato de a ser positivo. Portanto existem $m,\ n \in \mathbb{N}$ tal que se $k > n$ então $y_n < m \cdot x_n$. ■

Estendemos a função valor absoluto aos número reais, isto é definimos $|\ |_{\mathbb{R}} : \mathbb{R} \to \mathbb{R}$ por

$$|a|_{\mathbb{R}} = \begin{cases} a & \text{se} \quad 0 \leq a \\ -a & \text{se} \quad a < 0. \end{cases}$$

É fácil verificar que possui as mesmas propriedades que para o caso dos racionais e que $|a| < b$ se, e somente se $-b < a < b$. Mais ainda, se $q_1,\ q_2$ são números racionais, então

$$|q_1 - q_2|_{\mathbb{R}} = |q_1 - q_2|_{\mathbb{Q}},$$

via a identificação $\mathbb{Q} \subset \mathbb{R}$. De fato, temos que se $q_i = [q_i]_{n\in\mathbb{N}}$ para $i = 1, 2$ e

$$\begin{aligned} q_1 - q_2 \geq 0 \quad &\Rightarrow \quad |q_1 - q_2|_{\mathbb{Q}} = q_1 - q_2 \geq 0 \ \Rightarrow \ [q_1]_{n\in\mathbb{N}} - [q_2]_{n\in\mathbb{N}} \geq 0 \\ q_1 - q_2 < 0 \quad &\Rightarrow \quad |q_1 - q_2|_{\mathbb{Q}} = q_2 - q_1 > 0 \ \Rightarrow \ [q_2]_{n\in\mathbb{N}} - [q_1]_{n\in\mathbb{N}} > 0. \end{aligned}$$

É por isto que tiramos o subíndice $|\ |_{\mathbb{R}}$ da notação e denotamos a função valor absoluto por $|\ |$ indistintamente se for sobre os reais ou racionais, deixando ao leitor a interpretação do contexto.

Com esta definição e o resultado anterior podemos mostrar que os numeros racionais são densos no conjunto dos números reais.

Teorema 17.4 Dados um número real a e um número racional q, $0 < q$, existe um número racional r tal que

$$|a - r| < q.$$

Demonstração. Seja $a = [x_n]_{n\in\mathbb{N}}$. Como $(x_n)_{n\in\mathbb{N}}$ é de Cauchy, dado $q \in \mathbb{Q}$, $0 < q$, existe $n_0 \in \mathbb{N}$ tal que se $n > n_0$ então $|x_n - x_{n_0}| < q$. Defina agora $r = (y_n)_{n\in\mathbb{N}}$ tal que

$$y_n = x_{n_0} \quad \forall\, n \in \mathbb{N}.$$

Então $r \in \mathbb{Q}$. Como

$$-q + y_n < x_n < q + y_n \quad \forall\, n > n_0$$

temos

$$-q < x_n - y_n < q \quad \forall\, n > n_0 \quad \Rightarrow \quad |x_n - r| < q \quad \forall\, n > n_0.$$

De onde segue que $|a - r| < q$. ■

O seguinte resultado é a propriedade geométrica masi importante dos números reais e que é de grande utilidade na análise matemática. Básicamente, o resultado garante que os números reais, como conjunto, não tem "furos".

Teorema 17.5 Todo conjunto não vazio de $\mathbb{R}$ que é limitado superiormente admite elemento supremo.

Demonstração. Seja $A \subset \mathbb{R}$ um conjunto não vazio e seja M uma cota superior de A. Seja $a \in A$ definimos as sequências $(u_n)_{n\in\mathbb{N}}$ e $(v_n)_{n\in\mathbb{N}}$ pelo seguinte processo recursivo ou jogo (veremos recorrências mais adiante no texto):

- $u_0 = M$ e $v_0 = a$
- Assuma conhecido u_n e v_n, calculamos

$$M_n = \frac{1}{2} \cdot (u_n + v_n)$$

então
  - se M_n é conta superior, então $u_{n+1} = M_n$ e $v_{n+1} = v_n$.
  - se M_n não é cota superior, então $u_{n+1} = u_n$ e $v_{n+1} = M_n$.

Observamos que

a) para cada n v_n não é cota superior.

b)
$$\begin{aligned} u_{n+1} - v_{n+1} &= M_n - v_n \\ &= = \frac{1}{2} \cdot (u_n + v_n) - v_n \\ &= \frac{1}{2} \cdot (u_n - v_n) \\ &\leq \frac{1}{2^n} |M - a|. \end{aligned}$$

c) por definição,

$$|u_n - u_{n+1}| \leq \frac{1}{2} |u_{n-1} - u_n|$$

d)
$$\begin{aligned} |u_n - u_{n+k}| &\leq (|u_n - u_{n+1}| + |u_{n+1} - u_{n+2}| + \cdots + |u_{n+k-1} - u_{n+k}|) \\ &= \left(|u_n - u_{n+1}| + \frac{1}{2} \cdot |u_n - u_{n+1}| + \cdots + \frac{1}{2^{k-1}} |u_n - u_{n+1}| \right) \\ &< 2|u_n - u_{n+1}| \\ &\leq \frac{2}{2^n} |M - a|. \end{aligned}$$

Para cada n consideramos $q_n \in \mathbb{Q}$ tal que $|u_n - q_n| < \frac{1}{n}$ e consideramos a sequência $(q_n)_{n \in \mathbb{N}}$. Seja $\varepsilon > 0$ e $m \in \mathbb{N}$ tal que $1 < \frac{m}{3} \varepsilon$ e $\frac{2}{2^m} |M - a| < \frac{1}{3} \cdot \varepsilon$ (tal m existe pela propiedade arquimediana) então

$$|q_n - q_m| \leq |q_n - u_n| + |u_n - u_m| + |u_m - q_m| < \varepsilon.$$

portanto $(q_n)_{n \in \mathbb{N}}$ é de Cauchy e representa um real que chamamos de b. Mais ainda, da construção, temos que $(u_n)_{n \in \mathbb{N}}$ converge para b. Por outro lado

$$|v_n - q_n| \leq |v_n - u_n| + |q_n - u_n| \leq \frac{1}{2^n} |M - a| + \frac{1}{n}$$

de onde segue que $(v_n)_{n \in \mathbb{N}}$ converge para b.
Assuma que existe $a' \in A$ tal que $b < a'$, escolhemos $\varepsilon = a' - b$, e como $(u_n)_{n \in \mathbb{N}}$ converge para b existe um n tal que $u_n - b < \varepsilon$, portanto

$$u_n < b + \varepsilon = b + (a' - b) = a',$$

o que é uma contradição pois u_n é uma cota superior de A. Portanto b é a cota superior.
Assuma agora que $b' < b$ é cota superior de A, então seja $\varepsilon = b - b'$. Como $(v_n)_{n \in \mathbb{N}}$ converge para b temos que existe um $n_0 \in \mathbb{N}$ tal que para todo $n_0 < n$ vale $b' < v_n$ mas v_n não é cota superior o que contradiz o fato de b' ser cota superior.

■

Obs. Com este resultado podemos ver que se $b \in \mathbb{R}$ e $b > 0$ então a função proposicional

$$P(x) = "x \in \mathbb{R},\ x^2 = b."$$

tem domínio de verdade não vazio em $\mathbb{R}$ e é dado pelo

$$s = \sup\{x \in \mathbb{R},\ x^2 < b\}.$$

De fato se $s^2 < b$, para todo $n \in \mathbb{N}$ tal que $n > \frac{2 \cdot s + 1}{b - s^2}$ temos que $s_n = s + \frac{1}{n}$ é tal que $s < s_n$ e $s_n^2 < b$ portanto s não pode ser supremo. De forma similar, se $s^2 > b$ entao escolhemos $m = \frac{2 \cdot s}{s^2 - b}$ e obtemos que $\tilde{s}_m = s - \frac{1}{m}$ é tal que $s > \tilde{s}_m$ e $\tilde{s}_m^2 > b^2$ contradizendo novamente o fato de s se supremo.

Podemos ver que toda função proposicional polinomial em $\mathbb{R}$

$$P(x) = "x \in \mathbb{R},\ a_{2k+1} \cdot x^{2k+1} + \cdots + a_1 \cdot x + a_0 = 0",$$

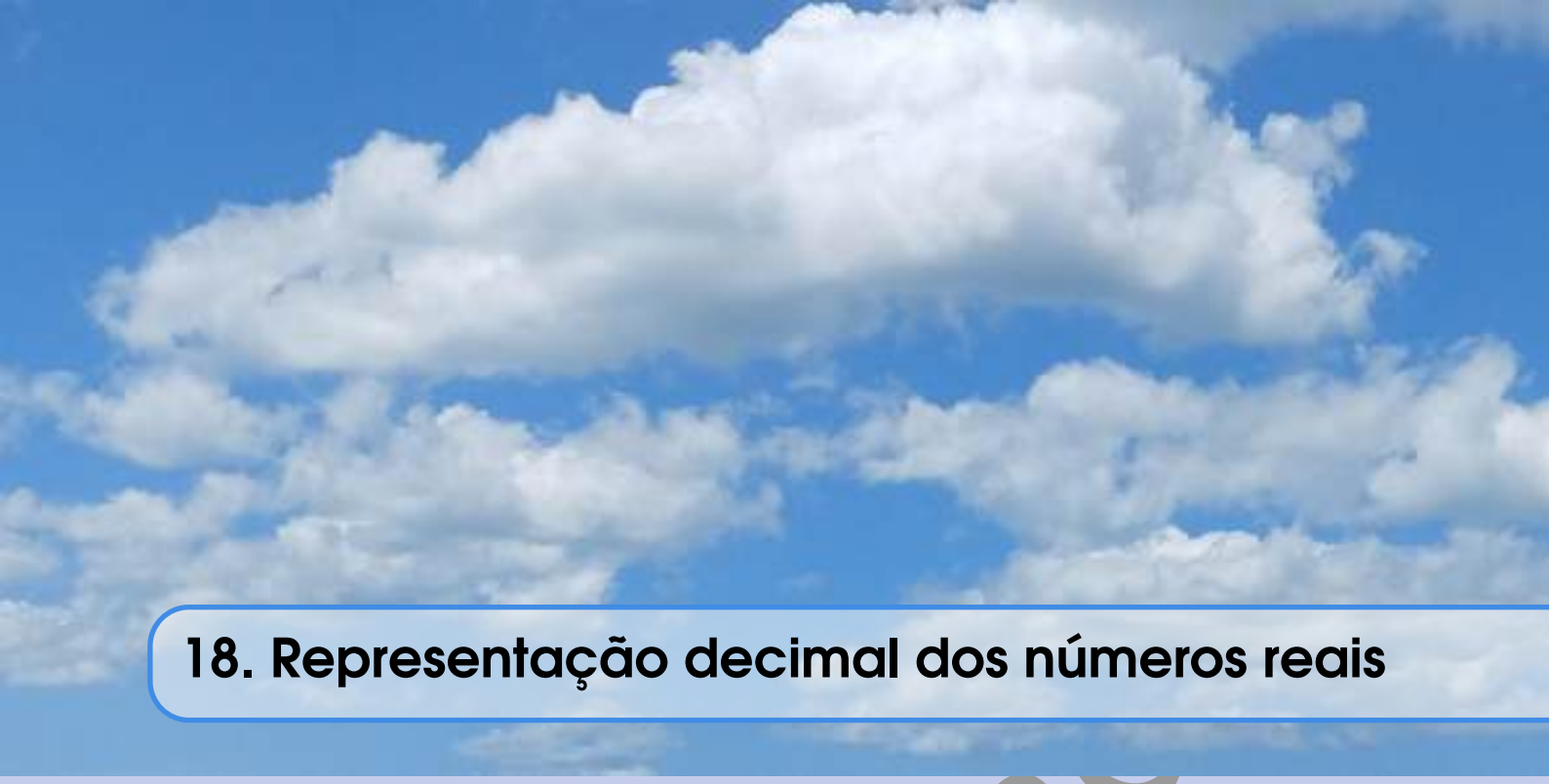
para $k \in \mathbb{N}$ e $a_{2k+1} \neq 0$, tem domínio de verdade não vazio em $\mathbb{R}$. Para demonstrar isto se utiliza a continuidade do a função polinomial junto ao Teorema do valor intermediário (Cálculo I). Para esses dois conceitos é utilizado fortemente a propriedade da existência de supremo.

É fácil ver que, no entanto, ainda há funções proposicionais polinomiais sobre os números reais com comínio de verdade vazio. De fato, por exemplo, a função proposicional

$$Q(x) = "x \in \mathbb{R},\ x^2 + 1 = 0"$$

Tem domínio de verdade vazio em $\mathbb{R}$. Para resolver finalmente o problema do domínio de verdade não vazio para funções proposicionais do tipo polinomial, é construído um outro conjunto numérico que é o conjunto dos números complexos.

Em elaboração



18. Representação decimal dos números reais

Vimos, na seção anterior, que um número real pode ser representado por uma sequência $(x_n)_{n\in\mathbb{N}}$ de números racionais. No entanto, esta representação é pouco conveniente para efeitos práticos, visto que temos que temos que especificar um conjunto enumerável de números. Para simplificar a notação surge a bem conhecida representação decimal dos números reais.

Vamos a estudar a representação decimal dos reais não negativos, pois para os negativos basta considerar a representação decimal do valor absoluto do número e acrecentar um sinal $-$ na frente.

Números inteiros: Primeiramente representamos o 0 e depois o restante dos números.

- O número 0 terá por representação decimal

  $$0 = \text{"}0{,}00\ldots\text{"} \quad \text{ou, simplesmente por} \quad 0.$$

- No caso dos inteiros positivos observamos que, o algoritmo da divisão, nos permite escrever todo número inteiro a como somas

  $$a = a_0 + a_1 \cdot 10 + a_2 \cdot 10^2 + \cdots + a_n \cdot 10^n$$

  Assim, representamos o numero a por

  $$a = \text{"}a_n \ldots a_2 a_1 a_0, 0000\ldots\text{"} \quad \text{ou, simplesmente por} \quad a = \text{"}a_n \ldots a_2 a_1 a_0\text{"}.$$

■ **Exemplo 18.1** A representação do número

$$2 + 3 \cdot 10 + 5 \cdot 10^2 + 1 \cdot 10^3 = \text{"1532"}.$$

■

Números racionais: No caso em que a é um número racional, sempre podemos escrever

$$a = \frac{p}{q},$$

para $p,\ q \in \mathbb{N}$ tais que $(p,q) = 1$. Primeiramente vamos representar cada número da forma

$$\frac{a_0}{1} + \frac{a_1}{10} + \frac{a_2}{10^2} + \cdots + \frac{a_n}{10^n},$$

com

$$a_0 \in \mathbb{N} \quad \text{e} \quad a_i \in \{0,1,2,3,4,5,6,7,8,9\}.$$

Se a_0 tem representação decimal

$$a_0 = "a_{0m} \ldots a_{00}"$$

então a será representado pela expressão

$$a = "a_{0m} \ldots a_{00}, a_1 a_2 \ldots a_n"$$

e agora dividimos em dois casos:

- Existe $k \in \mathbb{N}$ tal que q divide a $10^k \cdot p$. Neste caso temos que

  $$10^k \cdot p = b \cdot q$$

  onde

  $$b = b_0 + b_1 \cdot 10 + \cdots + b_r \cdot 10^r.$$

  Então

  $$\begin{aligned} \frac{p}{q} &= \frac{1}{10^k} \cdot \frac{10^k \cdot p}{q} \\ &= \frac{1}{10^k} \cdot \frac{b}{1} \\ &= \frac{a}{10^k} \\ &= b_r \cdot \frac{1}{10^{k-r}} + b_{r-1} \cdot \frac{1}{10^{k-r+1}} + \cdots + b_1 \cdot \frac{1}{10^{k-1}} + b_0 \cdot \frac{1}{10^k}. \end{aligned}$$

  e representamos como acima.
- Não existe $k \in \mathbb{N}$ tal que q divide a $10^k \cdot p$. Claramente, neste caso, $q \neq 10^l$ para todo $l \in \mathbb{N}$. Do algoritmo da divisão temos que

  $$p = q \cdot a_0 + r,$$

  com $0 < r < q$. Considere o menor $m \in \mathbb{N}$ tal que

  $$r < q < 10^m \cdot r$$

  Agora aplicamos o algoritmo da divisão a

  $$10^{m+k} \cdot r = d_k \cdot q + r_k \quad k \geq 0$$

  como temos no máximo q restos possíveis. Escolhemos os menores $k_1 < k_2$ tais que $r_{k_1} = r_{k_2}$. Temos então que

  $$10^m \cdot r \cdot (10^{k_2} - 10^{k_1}) = q \cdot b \quad \Rightarrow \quad 10^{k_1} \cdot (10^{k_2-k_1} - 1) < b < 10^{m+k_1} \cdot (10^{k_2-k_1} - 1).$$

  Novamente, pelo algoritmo da divisão, temos que

  $$\begin{aligned} b &= c + 10^{k_1} \cdot (10^{k_2-k_1} - 1) \cdot d \\ &= c + d \cdot (10^{k_2} - 10^{k_1}) \end{aligned}$$

  com

  $$c < (10^{k_2} - 10^{k_1}) \quad \text{e} \quad d < 10^{m+k_1}$$

  Portanto, escrevemos

  $$c = c_0 + c_1 \cdot 10 + \ldots + c_{k_2} \cdot 10^{k_2-1}$$

$$d = d_0 + d_1 \cdot 10 + \cdots + d_{m+k_1-1} \cdot 10^{m+k_1-1}$$

Então

$$\frac{10^m \cdot r}{q} = \frac{b}{(10^{k_2} - 10^{k_1})} = \frac{d}{1} + \frac{c}{(10^{k_2} - 10^{k_1})}.$$

Observamos que

$$\frac{c}{(10^{k_2} - 10^{k_1})} = \frac{1}{10^{k_1}} \cdot \frac{c}{10^{k_2-k_1} - 1}.$$

Agora, utilizamos a identidade

$$\frac{1}{10^n - 1} = \frac{1}{10^n} + \frac{1}{10^{2 \cdot n}} + \cdots + \frac{1}{10^{n \cdot k}} + \cdots$$

que será mostrada quando estudemos recorrências. Com esta identidade, vemos que se

$$e = e_0 + e_1 \cdot 10 + \cdots + e_{n-1} \cdot 10^{n-1}$$

$$\frac{e}{10^n - 1} = \frac{e}{10^n} + \frac{e}{10^{2 \cdot n}} + \cdots + \frac{e}{10^{n \cdot k}} + \cdots$$

que é escrita como dízima periódica

$$\frac{e}{10^n - 1} = \text{"}0, \overline{e_{n-1} e_{n-2} \ldots e_1 e_0}\text{"}.$$

Com esta notação, temos

$$\frac{r}{q} = \frac{d}{10^m} + \frac{c}{10^m \cdot (10^{k_2} - 10^{k_1})}$$

se escreve

$$\frac{r}{q} = \text{"}0, d_{m+k_1-1} \ldots d_1 d_0 \overline{c_{k_2-1} c_{k_2-2} \ldots c_1 c_0}\text{"}.$$

Portanto

$$\frac{p}{q} = \text{"}a_0, d_{m+k_1-1} \ldots d_1 d_0 \overline{c_{k_2-1} c_{k_2-2} \ldots c_1 c_0}\text{"}.$$

Da notação acima, temos

Obs.

$$\frac{r}{q} = \frac{b}{10^m \cdot (10^{k_2} - 10^{k_1})} = \frac{c + d \cdot (10^{k_2} - 10^{k_1})}{10^m \cdot (10^{k_2} - 10^{k_1})} = \frac{(c + d \cdot 10^{k_2}) - d \cdot 10^{k_1}}{10^m \cdot (10^{k_2} - 10^{k_1})}$$

Então se temos uma dizima periódica da forma

$$0, d_m \cdots d_0 \overline{c_k \cdots c_0}$$

podemos representála como número racional calculando

$$d = d_0 + \cdots + d_m \cdot 10^m \quad \text{e} \quad c = c_0 + \cdots + c_k \cdot 10^k$$

e fazendo

$$\frac{(c + 10^{k+1} \cdot d) - d}{10^m (10^{k+1} - 1)}.$$

■ **Exemplo 18.2** Considere o número $\frac{19}{99}$: observamos que

$$19 < 99 < 10 \cdot 19$$

Então

$$10 \cdot 19 \cdot (10^2 - 1) = 99 \cdot 190$$

Então, na notação acima, temos $m = 1$, $k_1 = 0$, $k_2 = 2$ e $b = 190$. Mais ainda,

$$190 = 99 \cdot 1 + 91$$

de onde $c = 91$ e $d = 1$. Escrevemos então

$$\frac{19}{99} = 0,1\overline{91}.$$

Observamos que, pelo formato do número e a notação, também poderiamos ter escrito

$$0,1\overline{91} = 0,\overline{19}.$$

Por outro lado, transformando de dízimas periódicas a número racional temos duas expressões equivalentes:

- Para o caso: $0,1\overline{91}$ temos

  $$d = 1 \quad c = 91$$

  de onde o número fica

  $$\frac{(91 + 10^2 \cdot 1) - 1}{10 \cdot (10^2 - 1)} = \frac{190}{990}.$$

- Para o caso: $0,\overline{19}$ temos

  $$d = 0 \quad c = 19$$

  de onde o número fica

  $$\frac{(19 + 10^2 \cdot 0) - 0}{(10^2 - 1)} = \frac{19}{99}.$$

■

Números Irracionais: Tamos visto como escrever os números inteiros e racionais na forma decimal. Já com os irracionais isto nunca poderá ser concluido. O número irracional não, por definição é um número que não é racional, então sua representação decimal nunca poderá ser feita pois é o trabalho de escrever um número com infinitas casas decimais depois do 0, o máximo que podemos fazer é uma aproximação racional e escrevé-los como

$$a = "a_0, a_1 \ldots a_n \ldots"$$

onde cada

$$a_j \in \{0,1,2,3,4,5,6,7,8,9\} \quad \forall\, j \in \mathbb{N}\backslash\{0\}$$

Observamos, pelo fato de não ser racional, nunca vamos ter um a $n-$upla da forma

$$a_{k+1} \ldots a_{k+n}$$

que se repete na forma de dízimas periódicas depois da vírgula. Então não temos como simplificar de alguma forma a notação. Em geral, a menos dos casos de raizes quadradas de números primos, ou otros racionais

similares) os números irracionais são nomeados por alguma letra como é o caso do número π, número e etc. Tambem observamos que há constantes que se conhecem com um número grande de casas decimais e das quais não se sabe se são racionais ou irracionais, por exemplo $\pi + e$ ou $\pi \cdot e$.

Se a é um irracional, com

$$a = "a_0, a_1 \dots a_n \dots",$$

a sequência que define a é

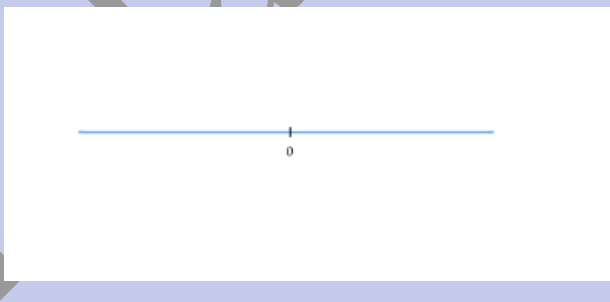
$$a = [q_j]_{j\in\mathbb{N}} \quad \text{onde} \quad q_j = \frac{a_0}{1} + \frac{a_1}{10} + \cdots + \frac{a_j}{10^j}.$$

■ **Exemplo 18.3** Por exemplo, para o número π sabemos que

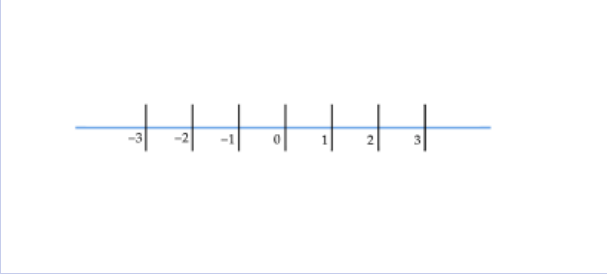
$$\begin{aligned}\pi \;=\; & 3,14159265358979323846264338327950288419716939937510\\ & 58209749445923078164062862089986280348253421170679821 48\\ & 08651328230664709384460955058223172535940812848111745 02\\ & 84102701938521105559644622948954930381964428810975665 93\\ & 34461284756482337867831652712019091456485669234603486 10\\ & 45432664821339360726024914127 3\cdots\end{aligned}$$

Consulte em *http://www.geom.uiuc.edu/ huberty/math5337/groupe/digits.html* para mais detalhes. ■

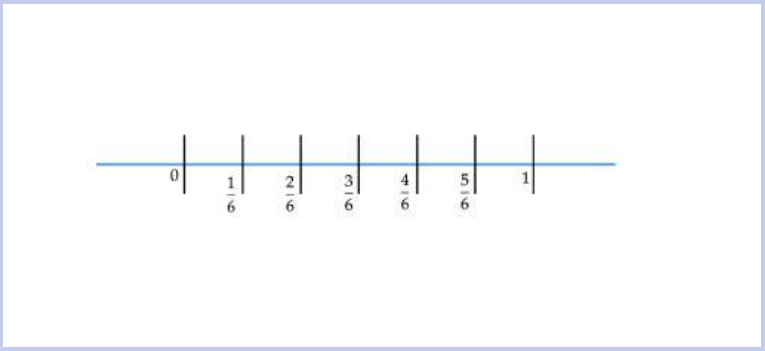
Para representar gráficamente os números reais vamos a utilizar uma reta, que será chamada de reta real, sobre a qual vamos distinguir um ponto 0, que corresponde ao número 0.



Com uma unidade de comprimento marcamos os inteiros do lado esquerdo os negativos e do lado direito os positivos. As marcas são a múltiplos de este comprimento.



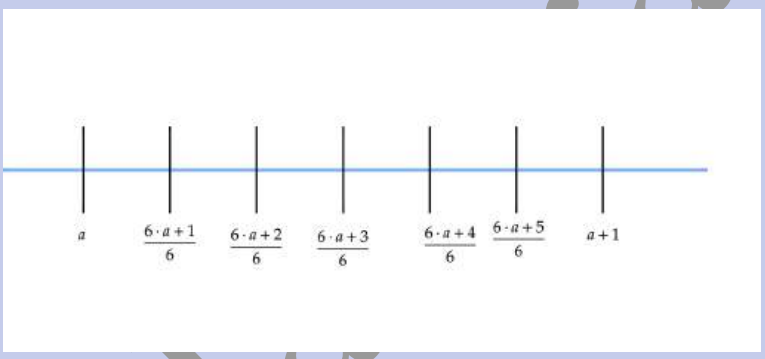
Para representar os racionais primeiramente observamos que para representar um racional $\frac{p}{q} < 1$ particionamos o segmento da reta entre 0 e 1 em q partes iguais e marcamos a prosição p. Por exemplo, representamos os racionais $\frac{1}{6}$, $\frac{2}{6}$, $\frac{3}{6}$, $\frac{4}{6}$ e $\frac{5}{6}$ como segue:



Agora, todo racional da forma $\frac{p}{q}$ pode ser escrito como

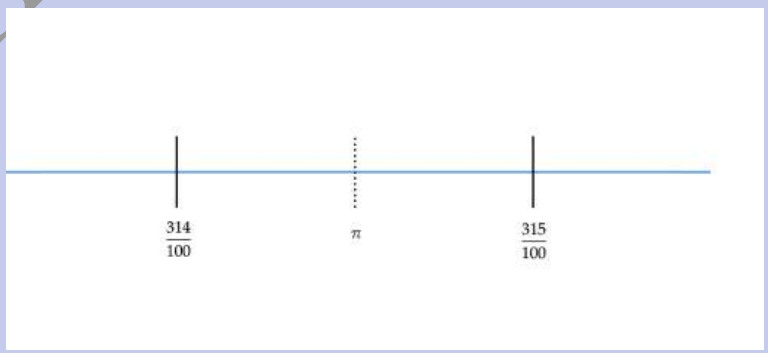
$$\frac{p}{q} = \frac{a}{1} + \frac{p'}{q}$$

com $p' > 0$. Então para representar $\frac{p}{q}$ particionamos o segmento da reta entre a e $a+1$ em q partes e marcamos o correspondente a marca p'. Por exemplo os racionais $\frac{6\cdot a+1}{6}$, $\frac{6\cdot a+2}{6}$, $\frac{6\cdot a+3}{6}$, $\frac{6\cdot a+4}{6}$ e $\frac{6\cdot a+5}{6}$ como segue:



Os números reais que não são racionais podem ser também representados exatamente por um ponto na reta. Porém pode ser um trabalho delicado, dada a definição dos irracionais. Embora alguns casos particulares possam ser representados utilizando argumentos de trigonometria e demais, podemos fazer uma repressentação informal da seguinte forma: sabemos que o número irracional vai estar entre dois racionais. Então, por abuso gráfico escolhemos dois racionais que estejam arbitráriamente próximos (tanto quanto a definição do nosso gráfico permitir) e marcamos o ponto do meio.

Por exemplo o número π: pelo visto acima ele satisfaz $\frac{314}{100} < \pi < \frac{315}{100}$ e o representamos marcando um ponto neste intervalo, por exemplo:



19. Sequências e Recorrências

Neste capítulo estudaremos com um pouco mais de detalhes as sequências de números e sua definição por meio de recursões ou processos recursivos do tipo que utilizamos nas demonstrações de alguns dos tópicos já vistos.

Começamos o capítulo generalizando as definições sobre sequências para o caso em que os números da sequência são números reais.

Definição 19.1

- Uma sequência de números reais é uma função $x : \mathbb{N} \to \mathbb{R}$. Denotamos à sequência por $(x_n)_{n\in\mathbb{N}}$ e por $x_n = x(n)$.
- Seja $(x_n)_{n\in\mathbb{N}}$ uma sequência de números reais, uma subsequência é uma aplicação $y : \mathbb{N} \to \mathbb{R}$ obtida de compor x com uma função $m : \mathbb{N} \to \mathbb{N}$ em que $m(i) \leq m_{i+1}$, isto é $y = x \circ m$. Denotamos a subsequência por $(x_{m_k})_{k\in\mathbb{N}}$ em que $m_{n_k} = (x \circ m)(k)$.
- Seja $(x_n)_{n\in\mathbb{N}}$ uma sequência de números reais. Dizemos que:
  - A sequência $(x_n)_{n\in\mathbb{N}}$ é de Cauchy se para todo $\varepsilon \in \mathbb{R}$ tal que $\varepsilon > 0$ existe um $n_0 \in \mathbb{N}$ tal que se $n_0 < n,\ m$ então $|x_m - x_n| \leq \varepsilon$.
  - A sequência $(x_n)_{n\in\mathbb{N}}$ converge a um número $a \in \mathbb{R}$ se para todo $\varepsilon \in \mathbb{R}$ tal que $0 < \varepsilon$ existe um $n_0 \in \mathbb{N}$ tal que se $n_0 < n$ então $|a - x_n| \leq \varepsilon$.
    Neste último caso denotamos

$$\lim_{n\to\infty} x_n = a.$$

Corolário 19.1 Seja x um número real, $x = [x_n]_n$ para $(x_n)_{n\in\mathbb{N}}$ uma sequência de Cauchy de números racionais. Então, como $x_n \in \mathbb{Q} \subset \mathbb{R}$ pela identificação vista, temos que $(x_n)_{n\in\mathbb{N}}$ é uma sequência de Cauchy de números reais que converge a x.

Demonstração. O baso de ser sequência de Cauchy segue da densidade dos racionais nos reais. De fato, para todo $\varepsilon > 0$ existe um número racional $\tilde{\varepsilon} > 0$ tal que $\varepsilon > \tilde{\varepsilon} > 0$. Portanto, há um n_0 tal que se $n,\ m > n_0$ então $|x_n - x_m| < \varepsilon$. Agora da inclusão canônica de $\mathbb{Q} \subset \mathbb{R}$ temos que a sequência é de Cauchy.

Para cada n seja, pela densidade de $\mathbb{Q}$ em $\mathbb{R}$ o número racional y_n tal que

$$|x - y_n| < \frac{1}{2^n},$$

então, se $n > m$ temos

$$\begin{aligned} |y_m - y_n| &< |y_m - x| + |x - y_n| \\ &< \frac{1}{2^m} + \frac{1}{2^n} \\ &\leq \frac{1}{2^{n-1}} \end{aligned}$$

Portanto $(y_n)_{n\in\mathbb{N}}$ é uma sequência de Cauchy, pois dado $\varepsilon > 0$ existe um n_0 de forma tal que $2^{n_0-1} \cdot \varepsilon > 1$ e se $m, n > n_0$ então

$$|y_m - y_n| < \varepsilon.$$

Observamos que

$$|x_n - y_n| \leq |x_n - x_m| + |x_m - y_m| + |y_m - y_n|$$

de onde segue que

$$||x_n - y_n| + (-|x_m - y_m|)| \leq |x_n - x_m| + |y_m - y_n|$$

Portanto a sequência $(z_n)_{n\in\mathbb{N}}$ definida por

$$z_n = |x_n - y_n| \quad \forall\, n \in \mathbb{N},$$

é de Cauchy e converge para 0 pois, caso contrário, existe em $\delta > 0$ tal que para todo $n \in \mathbb{N}$ temos $m > n$

$$\delta < |x_m - y_m|$$

de onde $\delta < |x - y_m|$ o que é um absurdo pela construção de $(y_n)_{n\in\mathbb{N}}$. ■

Se $(x_n)_{n\in\mathbb{N}}$ é uma sequência convergente de números reais, então utilizando o mesmo argumento que para sequências convergentes de números racionais, podemos mostrar que ela é de Cauchy. No conjunto dos números reais podemos ver que a volta deste resultado, isto é, se é de Cacuhcy então é convergente, também vale. Esse é o conteúdo do proximo resultado.

Teorema 19.1 Seja $(x_n)_{n\in\mathbb{N}}$ uma sequência reais então ela é de Cauchy se, e somente se, é convergente .

Demonstração. A prova de que se é convergente é de Cauchy é idéntica ao caso de sequência convergente de números racionais.

Assuma que $(x_n)_{n\in\mathbb{N}}$ é de Cauchy. Como cada $x_n \in \mathbb{R}$ temos que existem sequências de Cauchy $(y_k^n)_{k\in\mathbb{N}}$ tais que

$$x_n = [y_k^n]_{k\in\mathbb{N}}$$

Dado $k \in \mathbb{N}$ fixo definimos a sequência $(z_n)_{n\in\mathbb{N}}$ por

$$z_n = y_k^n, \quad \forall\, n \in \mathbb{N}.$$

Observamos que $(z_n)_{n\in\mathbb{N}}$ é uma sequência de Cauchy. De fato, se $\varepsilon > 0$ existe um $n_0 \in \mathbb{N}$ tal que se $n, m > n_0$ temos

$$|x_n - y_k^n| < \frac{1}{3} \cdot \varepsilon$$
$$|x_m - y_k^m| < \frac{1}{3} \cdot \varepsilon$$
$$|x_n - x_m| < \frac{1}{3} \cdot \varepsilon$$

De onde segue que

$$\begin{aligned} |z_n - z_m| &= |y_k^n - y_k^m| \\ &= |y_k^n - x_n| + |x_n - x_m| + |x_m - y_k^m| < \varepsilon. \end{aligned}$$

Portanto, $(z_n)_{n\in\mathbb{N}}$ é de Cauchy. Seja $x = [z_n]_{n\in\mathbb{N}}$. Observamos que dado $\varepsilon > 0$ existe um $n_0 \in \mathbb{N}$ tal que se $n, m > n_0$ temos

$$\begin{aligned} |x - z_m| &< \frac{1}{3}\cdot\varepsilon \\ |y_k^m - x_m| &< \frac{1}{3}\cdot\varepsilon \\ |x_n - x_m| &< \frac{1}{3}\cdot\varepsilon \end{aligned}$$

e, portanto

$$\begin{aligned} |x - x_n| &= |x - z_m| + |z_m - x_n| \\ &= |x - z_m| + |y_k^m - x_m| + |x_n - x_m| < \varepsilon. \end{aligned}$$

Portanto $(x_n)_{n\in\mathbb{N}}$ converge a x. ■

■ **Exemplo 19.1** • Seja $(x_n)_{n\in\mathbb{N}}$ uma sequência reais em que

$$x_n = \frac{2\cdot n}{n+1} \quad \forall\, n \in \mathbb{N}.$$

Dado $\varepsilon > 0$ existe n_0 satisfazendo $n_0 > 2\cdot\varepsilon^{-1}$ tal que se $n > n_0$ temos

$$\begin{aligned} |x_n - 2| &= \frac{2\cdot n}{n+1} \\ &= \frac{2}{n+1} \\ &< \frac{2}{n_0+1} < \varepsilon \end{aligned}$$

Portanto a sequência $(x_n)_{n\in\mathbb{N}}$ converge a 2, de onde

$$\lim_{n\to\infty} x_n = 2.$$

Como a sequência é convergente é de Cauchy. Seja $m : \mathbb{N} \to \mathbb{N}$ definida por $m(n) = 3\cdot n + 1$ então $(x_{m_n})_{n\in\mathbb{N}}$ e uma subsequência de $(x_n)_{n\in\mathbb{N}}$ e está definida por

$$\begin{aligned} x_{m_n} &= \frac{2\cdot m(n)}{m(n)+1} \\ &= \frac{2\cdot(3\cdot n+1)}{(3\cdot n+1)+1} \\ &= \frac{6\cdot n+2}{3\cdot m+2}, \qquad \forall\, n \in \mathbb{N}. \end{aligned}$$

• Seja $(x_n)_{n\in\mathbb{N}}$ uma sequência reais em que

$$x_n = \frac{2}{n+3}\cdot\cos\left(\frac{n}{2}\cdot\pi\right), \quad \forall\, n \in \mathbb{N}.$$

Dado $\varepsilon > 0$ existe n_0 satisfazendo $n_0 > 2\cdot\varepsilon^{-1}$ tal que se $n > n_0$ temos

$$\begin{aligned} |x_n - 0| &= \frac{2}{n+3}\cdot\left|\cos\left(\frac{n}{2}\cdot\pi\right)\right| \\ &\leq \frac{2}{n+3} \\ &< \frac{2}{n_0} < \varepsilon \end{aligned}$$

Portanto a sequência $(x_n)_{n\in\mathbb{N}}$ converge a 0, de onde

$$\lim_{n\to\infty} x_n = 0.$$

Como a sequência é convergente é de Cauchy. Seja $m:\mathbb{N}\to\mathbb{N}$ definida por $m(n)=4\cdot n$ então $(x_{m_n})_{n\in\mathbb{N}}$ e uma subsequência de $(x_n)_{n\in\mathbb{N}}$ e está definida por

$$\begin{aligned} x_{m_n} &= \frac{2}{m(n)+3}\cdot\cos\left(\frac{m(n)}{2}\cdot\pi\right) \\ &= \frac{2}{4\cdot n+3}\cdot\cos(2\cdot\pi) \\ &= \frac{2}{4\cdot n+3} \quad \forall\, n\in\mathbb{N}. \end{aligned}$$

Por outro lado se $k:\mathbb{N}\to\mathbb{N}$ definida por $k(n)=2\cdot n+1$ então $(x_{k_n})_{n\in\mathbb{N}}$ e uma subsequência de $(x_n)_{n\in\mathbb{N}}$ e está definida por

$$\begin{aligned} x_{k_n} &= \frac{2}{k(n)+3}\cdot\cos\left(\frac{k(n)}{2}\cdot\pi\right) \\ &= \frac{2}{n+3}\cos\left(\frac{2\cdot n+1}{2}\cdot\pi\right)=0, \qquad \forall\, n\in\mathbb{N}. \end{aligned}$$

Portanto a subsequência $(x_{k_n})_{n\in\mathbb{N}}$ tem todos seus termos iguais a 0.

■

A existência de uma ordem e a tricotomia nos números reais nos permite dar a seguinte definição.

Definição 19.2 Seja $(x_n)_{n\in\mathbb{N}}$ uma sequência reais. Dizemos que ela é

- crecente: se para todo $n\in\mathbb{N}$ temos $x_n < x_{n+1}$.
- não decrecente:se para todo $n\in\mathbb{N}$ temos $x_n \le x_{n+1}$.
- decrecente:se para todo $n\in\mathbb{N}$ temos $x_{n+1} < x_n$.
- não crecente:se para todo $n\in\mathbb{N}$ temos $x_{n+1} \le x_n$.
- monótona se ela for não crescente ou não decrescente.
- limitada superiormente: se existe $M\in\mathbb{R}$ tal que $x_n \le M$ para todo $n\in\mathbb{N}$.
- limitada inferiormente: se existe $M\in\mathbb{R}$ tal que $M \le x_n$ para todo $n\in\mathbb{N}$.
- limitada: se a sequência for limitada inferiormente e superiormente.
- ilimitada: se não for limitada.

O fato de uma sequência $(x_n)_{n\in\mathbb{N}}$ monótona e/ou limitada da informações sobre a convergencia da mesma ou, pelo menos de uma subsequência da própria sequência. Isso é o que veremos nos resultados a seguir.

Teorema 19.2 — da Convergência Monótona. Toda sequência monónota e limitada converge.

Demonstração. Seja $(x_n)_{n\in\mathbb{N}}$ uma sequência monótona limitada. Assuma que é não decrescente (o caso não crescente é similar)

Considere o conjunto $A=\{x_i,\ i\in\mathbb{N}\}$. Como a sequência é limitada temos que A é limitado. Portanto, pela existência de supremo em subconjuntos limitados de $\mathbb{R}$ temos que existe

$$s=\sup A.$$

Seja $\varepsilon>0$, da definição de supremos exist eum $n_0\in\mathbb{N}$ tal que

$$s-\varepsilon < x_{n_0} \le x_n \le s < s+\varepsilon$$

de onde

$$-\varepsilon < x_n - s < \varepsilon \quad \Rightarrow |x_n - s| < \varepsilon$$

Portanto $(x_n)_{n\in\mathbb{N}}$ converge para s.

■

■ **Exemplo 19.2** • Seja $(x_n)_{n\in\mathbb{N}}$ uma sequência reais em que

$$x_n = (-1)^n \quad \forall\, n \in \mathbb{N}.$$

Claramente é uma sequência que é limitada. Não é crescente nem decrescente pois

$$x_{2n} > x_{2n+1} > x_{2n+2} \quad \forall\, n \in \mathbb{N}.$$

Seja $m_1,\ m_2 : \mathbb{N} \to \mathbb{N}$ dada por $m_1(j) = 2\cdot j$ e $m_2(j) = 2\cdot j + 1$ então as subsequênciasy, $z : \mathbb{N} \to \mathbb{R}$ dadas por

$$y(j) = x \circ m_1(j) = 1 \quad \text{e} \quad z(j) = x \circ m_2(j) = -1 \quad \forall\, j \in \mathbb{N}$$

são monótonas (de fato são constantes) e convergentes a 1 e -1 respectivamente.

- Seja $(x_n)_{n\in\mathbb{N}}$ uma sequência reais em que

$$x_n = \sqrt{1+n^2} \quad \forall\, n \in \mathbb{N}.$$

Observamos que, para todo $n \in \mathbb{N}$ temos

$$x_n \geq 1 \quad \text{e} \quad x_n < x_{n+1}.$$

De fato, para $n = 0$ temos que $x_0 = 1 \geq 1$ e $x_1 = \sqrt{2} > 1 = x_0$. Assuma que o que está acima vale para n vemos que vale para $n+1$. Como

$$x_n^2 = 1 + n^2 < 1 + (n+1)^2 = x_{n+1}^2 \quad \Rightarrow \quad 1 \leq x_n < x_{n+1}$$

de onde segue que

$$x_n \geq 1 \quad \text{e} \quad x_n < x_{n+1} \quad \forall n \in \mathbb{N}.$$

Portanto x_n é crescente, limitada inferiormente. Mais ainda, para todo $M \in \mathbb{R}$ existe um número natural $n_0 > \sqrt{|M^2 - 1|}$ tal que se $m > n_0$ então

$$x_m^2 = 1 + m^2 > 1 + n_0^2 > M^2 \quad \Rightarrow x_n > M.$$

Então, x_m não é limitada superiormente e portanto não é limitada.

- Seja $(x_n)_{n\in\mathbb{N}}$ uma sequência reais em que

$$x_n = \frac{n}{1+n^2}$$

Observamos que, como $0 \leq n \leq 1 + n^2$ para todo $n \in \mathbb{N}$temos que $0 \leq x_n \leq 1$. De onde segue que a sequência é limitada superiormente e inferiormente, portanto é limitada. Mais ainda, como

$$x_0 = 0 < \frac{1}{2} = x_1 \quad \text{e} \quad x_1 = \frac{1}{2} > \frac{2}{5} = x_2$$

a sequência não é crescente nem decrescente.
Se $m : \mathbb{N} \to \mathbb{N}$ tal que $m(j) = j+1$ então a subsequência $x \circ m : \mathbb{N} \to \mathbb{R}$ que denotamos por $(x_{n_j})_{j\in\mathbb{N}}$ para $n_j = m(j)$ é crescente. De fato, se $j \geq 1$ temos

$$\begin{aligned} j\cdot((j+1)^2+1) &= j^3 + 2\cdot j^2 + 2\cdot j \\ &> j^3 + j \\ &= j\cdot(j^2+1) \quad \Rightarrow \frac{j}{j^2+1} > \frac{(j+1)}{(j+1)^2+1}. \end{aligned}$$

de onde segue que

$$x_{n_j} > x_{n_{j+1}} \quad \forall\, j \in \mathbb{N}.$$

Veremos que esta subsequência é convergente, mais ainda, veremos que a sequência original é convergente a 0. De fato, dado $\varepsilon > 0$ existe um número natural $n_0 > \frac{1}{\varepsilon}$ tal que se $n > n_0$ então

$$\begin{aligned} |x_n - 0| &= \frac{n}{1+n^2} \\ &\leq \frac{1}{n} \\ &< \frac{1}{n_0} < \varepsilon. \end{aligned}$$

De onde

$$\lim_{n\to\infty} x_n = 0.$$

- Seja $(x_n)_{n\in\mathbb{N}}$ uma sequência reais em que

$$x_n = \frac{n}{n+1}$$

Observamos que, como $0 \leq n \leq 1+n$ para todo $n \in \mathbb{N}$temos que $0 \leq x_n \leq 1$. De onde segue que a sequência é limitada superiormente e inferiormente, portanto é limitada. Mais ainda, como

$$n^2 + 2\cdot n < n^2 + 2\cdot n + 1$$

temos que

$$x_n < x_{n+1}$$

de onde seque que a sequência é crescente.
A sequência converge a 1. De fato, dado $\varepsilon > 0$ existe um número natural n_0 satisfazendo $n_0 + 1 > \frac{1}{\varepsilon}$ tal que se $n > n_0$ então

$$\begin{aligned} |x_n - 1| &= \frac{1}{1+n} \\ &< \frac{1}{1+n_0} < \varepsilon. \end{aligned}$$

De onde

$$\lim_{n\to\infty} x_n = 1.$$

■

Lema 19.1 Toda sequência $(x_n)_{n\in\mathbb{N}}$ admite uma subsequência que pode ser não decrescente ou não crescente.

Demonstração. Dada a sequência $(x_n)_{n\in\mathbb{N}}$, considere a função proposicional

$$P(n) = "x_n > x_m \quad \forall m > n"$$

e seja $M \subset \mathbb{N}$ o seu domínio de verdade.

Se M é um conjunto infinito então, como $\mathbb{N}$ é bem ordenado, podemos escrever $M = \{n_i,\ i \in \mathbb{N}\}$ de forma tal que se $i < j$ então $n_i < n_j$. Seja $m : \mathbb{N} \to \mathbb{N}$ definida por $m(i) = n_i$, então $(x_{n_j})_{j\in\mathbb{N}}$ é uma subsequência de $(x_n)_{n\in\mathbb{N}}$ e

$$x_{n_i} > x_{n_j} \quad \forall\, i < j.$$

portanto a subsequência é decrescente.

Se M é um conjunto finito e seja $k = \max M$. Então $n_1 = k+1 \notin M$, portanto existe $n_2 > n_1$ tal que $x_{n_1} \geq x_{n_2}$. Como $n_2 \notin M$ então existe n_3 tal que $x_{n_2} \geq x_{n_3}$. Podemos repetir este processo indefinidamente e achar um conjunto $\tilde{M} = \{n_i,\ i \in \mathbb{N}\}$ que organizamos de forma tal que $n_i < n_j$ sempre que $i < j$. Considere a função $m : \mathbb{N} \to \mathbb{N}$ dada por $m(j) = n_j$. Então $(x_{n_j})_{j\in\mathbb{N}}$ é uma subsequência de $(x_n)_{n\in\mathbb{N}}$ e

$$x_{n_i} \leq x_{n_j} \quad \forall\, i < j.$$

portanto a subsequência é não decrescente. ■

Teorema 19.3 — Bolzano-Weierstrass. Toda sequência limitada tem uma subsequência convergente.

Demonstração. Seja $(x_n)_{n\in\mathbb{N}}$ uma sequência limitada. Pelo lema anterior existe uma subsequência monótona que é limitada. O teorema da convergencia monótona garante que esta subsequência deve converger. ■

Seja $(x_n)_{n\in\mathbb{N}}$ uma sequência. Sabemos que x_n é o valor de uma função $x:\mathbb{N}\to\mathbb{R}$. No entanto existem diferentes formas de definir os valores $x(n)=x_n$ da função. Listamos aqui alguns.

- Direta: a partir do valor de $x(n)=x_n$.
  Por exemplos a sequência $(x_n)_{n\in\mathbb{N}}$ dada por
  $$x(n)=\frac{1}{n+1}.$$
- por recursão: A partir dos valores de x em $\{0,1,\ldots,n\}$ obtemos o valor de $x(n+1)$ por uma fórmula sobre os valores conhecidos $\{x(0),x(1),\ldots,x(n)\}$.
  Por exemplos a sequência $(x_n)_{n\in\mathbb{N}}$ dada por
  $$x(0)=1 \quad x(1)=1 \qquad x(n+1)=x(n)+x(n-1)$$

Olhamos com um pouco mais de detalhe o último caso.

Definição 19.3 Uma relação de recorrência é uma equação que expressa os termos de uma sequência de numeros reais $(x_n)_{n\in\mathbb{N}}$ como função dos valores anteriores, isto é

$$x(n+1)=f(n+1,x(n),\ldots,x(0)).$$

■ **Exemplo 19.3** No conjunto dos números reais, a solução de $x^2=p$ é o número que costumamos denotar como $\sqrt{p}$ é que, por exemplo, é irracional quando p primo (foi visto antes que neste caso não é racional).

Construímos agora uma sequência de Cauchy que descreve este número como número real utilizando o conhecido como "Método de Babilónia"para cálculo da raiz quadrada de qualquer número p. O método consiste em construir uma sequência $(x_n)_{n\in\mathbb{N}}$ por meio de uma recorrência. O algoritmo é o seguinte

1- Escolha $x_0\in\mathbb{Q}$ tal que
$$x_0^2<p<(x_0+1)^2.$$

2- Para $n\geq 1$ calcule
$$x_n=\frac{1}{2}\cdot\left(x_{n-1}+p\cdot x_{n-1}^{-1}\right).$$

Observamos que

$$\begin{aligned} x_n^2-p &= x_n\cdot x_n-p \\ &= x_n(x_n-p\cdot x_n^{-1}) \\ &= 2\cdot x_n\cdot\left(x_n-\frac{1}{2}(x_n+p\cdot x_n^{-1})\right) \\ &= 2\cdot x_n\cdot(x_n-x_{n+1}) \end{aligned}$$

Tambem temos que $x_n^2\geq p$ para todo $n\geq 1$. De fato, vemos que

$$\begin{aligned} x_{n+1}^2 &= \frac{1}{4}\cdot(x_n^2+2\cdot p+p^2\cdot x_n^{-2}) \\ &\geq \frac{1}{4}\cdot x_n^{-2}\cdot(x_n^4+2\cdot p\cdot x_n^2+p^2) \\ &\leq \frac{1}{4}\cdot x_n^{-2}\cdot 4\cdot p\cdot x_n^2=p, \end{aligned}$$

onde a última linea segue do fato que para $a,\ b \in \mathbb{Q}$ temos

$$(a^2+b^2) > 2\cdot a\cdot b.$$

Juntanto estas duas estimativas temos que

$$2\cdot x_n\cdot(x_n - x_{n+1}) = x_n^2 - p \geq 0 \quad \Rightarrow \quad x_n \geq x_{n+1} \quad \forall\, n \geq 1.$$

com isto, temos que

$$p\cdot x_n^{-1} \geq p\cdot x_{n-1}^{-1} \quad \Rightarrow \quad -p\cdot x_{n-1}^{-1} \geq -p\cdot x_n^{-1}.$$

$$\begin{aligned} |x_n - x_{n+1}| &= \frac{1}{2}x_n^{-1}\cdot(x_n^2 - p) \\ &= \frac{1}{2}\cdot(x_n - p\cdot x_n^{-1}) \\ &\leq \frac{1}{2}\cdot(x_n - p\cdot x_{n-1}^{-1}) \\ &= \frac{1}{2}\cdot(x_n + x_{n-1} - 2x_n) \\ &\leq \frac{1}{2}\cdot|x_{n-1} - x_n|. \end{aligned}$$

Como consequência disto temos que se para algum m temos que

$$x_m = x_{m+1} \quad \Rightarrow \quad x_n = x_m \quad \forall\, n \geq m.$$

Agora, utilizando indução é fácil mostrar que

$$|x_{n+1} - x_n| < \frac{1}{2^n}|x_1 - x_0| = \frac{1}{2^{n+1}}\cdot x_0^{-1}(p - x_0^2)$$

e que

$$|x_n^2 - p| = 2\cdot x_n\cdot(x_n - x_{n+1}) < \frac{1}{2^{n+1}}\cdot x_1\cdot x_0^{-1}(p - x_0^2)$$

De onde segue que, se $m > n$ temos

$$|x_n - x_m| < |x_n - x_{n+1}| + \cdots + |x_{m-1} - x_m| < \frac{1}{2^n}\cdot x_0^{-1}(p - x_0^2)$$

Portanto, dado $\varepsilon > 0$ existe um $n_0 \in \mathbb{N}$ de forma tal que

$$\sup\{x_1, 1\}\cdot\frac{1}{2^{n_0}}\cdot x_0^{-1}(p - x_0^2) < \varepsilon.$$

Se $m, n > n_0$ temos, pelo visto acima, que

$$|x_m - x_n| < \varepsilon.$$

e

$$|x_n^2 - p| < \varepsilon$$

Então $(x_n)_{n\in\mathbb{N}}$ é de Cauchy e que $(x_n^2)_{n\in\mathbb{N}}$ converge a p. Mais ainda, como

$$|x_n - \sqrt{p}|\cdot|x_n + \sqrt{p}| = |x_n^2 - p| < \varepsilon$$

temos

$$|x_n - \sqrt{p}| < \varepsilon\cdot(x_n + \sqrt{p}) < \varepsilon\cdot(x_1 + \sqrt{p})^{-1},$$

de onde segue que $(x_n)_{n\in\mathbb{N}}$ converge a $\sqrt{p}$. Mais ainda, $[x_n]_{n\in\mathbb{N}}$ é o que denotamos por $\sqrt{p}$.

Por exemplo, utilizamos o método para calcular a raiz quadrada de dois números. Aqui observamos que temos um erro inherente ao uso da calculadora! Outra coisa, escrevemos os número em notação decimal embora falaremos disto depois.

- $\sqrt{4}$

$$x_0 = 1 \quad x_1 = 2,5 \quad x_2 = 2,05 \quad x_3 = 2,00060975609756$$

$$x_4 = 2,00000009292229 \quad x_5 = 2 \quad x_6 = 2.$$

Então $\sqrt{4} = 2$

- $\sqrt{3}$

$$x_0 = 1, \quad x_1 = 2, \quad x_3 = 1,75 \quad x_3 = 1,73214285714286$$

$$x_4 = 1,73205081001473 \quad x_5 = 1,73205080756888 \quad x_6 = 1,73205080756888 \quad x_7 = \cdots$$

Aqui o erro da calculadora não permite distinguir os membros seguintes da sequência. Observar que os membros da sequência são aproximações racionais melhores para o número real $\sqrt{3}$.

■

Um caso particular, sobre definição de sequências por recursão está no seguinte resultado.

Teorema 19.4 — Princípio de Recursão. Seja A um conjunto não vazio e $f : A^n \times \mathbb{N} \to A$ uma função. Então existe uma única sequência $x : \mathbb{N} \to A$ tal que

- $x_0 = a_0, \ldots, x_{n-1} = a_{n-1}$
- $x_m = f(m, x_{m-1}, \ldots, x_{m-n})$ para $m \geq n$

Demonstração. Para fazer a demonstração utilizamos o princício de indução. Considere a função proposicional

$$P(n) = \text{"}x(n) \text{ está definida para } n\text{"}$$

Seja M o domínio de verdade de P. Observamos que $\{0, \ldots, n-1\} \subset M$ pois $x_0 = a_0, \ldots, x_{n-1} = a_{n-1}$ estão definidos. Se $m \in M$, isto é, x_k está definida para todo $k \leq m$, então

$$x_{m+1} = f(m+1, x_m, \ldots, x_{m-n+1})$$

está definida. Portanto $m+1 \in M$ e, pelo princípio de indução x_n está definida para todo $n \in \mathbb{N}$.

Para mostrar a unicidade onsidere a função proposicional

$$Q(n) = \text{"Se } y(n) \text{ está definida pela recursão do enunciado então } y(n) = x(n)\text{"}$$

Seja N o domínio de verdade de Q. Observamos que $\{0, \ldots, n-1\} \subset N$ pois

$$x_0 = a_0 = y_0, \ldots, x_{n-1} = a_{n-1} = y_{n-1}.$$

Se $y_m = x_m$ então

$$y_{m+1} = f(m+1, y_{m-n+1}, \ldots, y_m) = f(m+1, x_{m-n+1}, \ldots, x_m) = x_{m+1}$$

e, portanto $m+1 \in N$. Pelo princípio de indução $x_n = y_n$ para todo $n \in \mathbb{N}$. ■

■ **Exemplo 19.4** A sequência de Fibonacci $(x_n)_{n \in \mathbb{N}}$ é definida como a única sequência de números naturais tal que

- $x_0 = 1$ e $x_1 = 1$.
- $x_{n+2} = x_{n+1} + x_n$ para $n \geq 3$..

■

A seguir listamos algumas recorrências bem conhecidas

- **Progressão aritmética**. É a sequência $(x_n)_{n\in\mathbb{N}}$ de números reais definida pela seguinte recorrência: Dados $a,\ r \in \mathbb{R}$ temos

$$x_0 = a \qquad x_n = x_{n-1} + r \quad \forall n \geq 1.$$

  De forma geral, podemos ver que

$$x_n = a + n \cdot r.$$

- **Progressão geométrica**. É a sequência $(x_n)_{n\in\mathbb{N}}$ de números reais definida pela seguinte recorrência: Dados $a,\ r \in \mathbb{R}$ temos

$$x_0 = a \qquad x_n = r \cdot x_{n-1} \quad \forall n \geq 1.$$

  De forma geral, podemos ver que

$$x_n = a \cdot r^n.$$

- Seja $(x_n)_{n\in\mathbb{N}}$ de números reais. Construimos de forma recursiva duas recorrências que são importantes de forma geral.
  - **O somatório:** É a sequência de números reais

$$\left(a_n = \sum_{i=0}^{n} x_i\right)_{n\in\mathbb{N}}$$

  definida da seguinte forma

$$a_0 = \sum_{i=0}^{0} x_i = x_0 \qquad a_n = \sum_{i=0}^{n} x_i = a_{n-1} + x_n.$$

  É fácil ver que

$$\sum_{i=0}^{n} x_i = x_0 + x_1 + \cdots + x_n.$$

  De fato, seja

$$P(n) = \text{"} \sum_{i=0}^{n} x_i = x_0 + x_1 + \cdots + x_n \text{"},$$

  e considere M o seu domínio de verdade. Então $0 \in M$ pois

$$\sum_{i=0}^{0} x_i = x_0.$$

  Assuma que $n \in M$ então

$$\begin{aligned} \sum_{i=0}^{n+1} x_i &= x_{n+1} + \sum_{i=0}^{n} x_i \\ &= x_{n+1} + x_0 + x_1 + \cdots + x_n \\ &= x_0 + x_1 + \cdots + x_n + x_{n+1} \end{aligned}$$

  De onde $n+1 \in M$ e, pelo princípio de indução, $M = \mathbb{N}$.
  Sejam $(x_n)_{n\in\mathbb{N}}$ e $(y_n)_{n\in\mathbb{N}}$ duas sequências. Então

i-

$$\sum_{i=0}^{n} c \cdot x_i = c \cdot \sum_{i=0}^{n} x_i.$$

De fato seja

$$P(n) = \text{"} \sum_{i=0}^{n} c \cdot x_i = c \cdot \sum_{i=k}^{n} x_i \text{"}$$

e considere M o seu domínio de verdade. Então $0 \in M$, pois

$$\sum_{i=0}^{0} c \cdot x_i = c \cdot x_0 = \cdot \sum_{i=0}^{0} x_i.$$

Se $n \in M$ então como

$$\begin{aligned} \sum_{i=0}^{n+1} c \cdot x_i &= c \cdot x_{n+1} + \sum_{i=0}^{n} c \cdot x_i \\ &= c \cdot x_{n+1} + c \cdot \sum_{i=k}^{n} x_i \\ &= c \cdot \left(x_{n+1} + \sum_{i=k}^{n} x_i \right) = c \cdot \sum_{i=0}^{n+1} x_i. \end{aligned}$$

Portanto $n+1 \in M$ e, pelo princípio de indução $N = \mathbb{N}$.

ii-

$$\sum_{i=0}^{n} (x_i + y_i) = \sum_{i=0}^{n} x_i + \sum_{i=0}^{n} y_i.$$

De fato seja

$$P(n) = \text{"} \sum_{i=0}^{n} (x_i + y_i) = \sum_{i=0}^{n} x_i + \sum_{i=0}^{n} y_i \text{"}$$

e considere M o seu domínio de verdade. Então $0 \in M$, pois

$$\sum_{i=0}^{0} (x_i + y_i) = x_0 + y_0 = \sum_{i=0}^{0} x_i + \sum_{i=0}^{0} y_i.$$

Se $n \in M$ então como

$$\begin{aligned} \sum_{i=0}^{n+1} (x_i + y_i) &= x_{n+1} + y_{n+1} + \sum_{i=0}^{n} (x_i + y_i) \\ &= x_{n+1} + y_{n+1} + \sum_{i=0}^{n} x_i + \sum_{i=0}^{n} y_i \\ &= \sum_{i=0}^{n+1} x_i + \sum_{i=0}^{n+1} y_i. \end{aligned}$$

Portanto $n+1 \in M$ e, pelo princípio de indução $N = \mathbb{N}$.

iii-

$$\sum_{i=0}^{n} c = (n+1) \cdot c.$$

De fato seja

$$P(n) = \text{"} \sum_{i=0}^{n} c = (n+1) \cdot c \text{"}$$

e considere M o seu domínio de verdade. Então $0 \in M$, pois

$$\sum_{i=0}^{0} c = c = 1 \cdot c.$$

Se $n \in M$ então como

$$\begin{aligned}\sum_{i=0}^{n+1} c &= c + \sum_{i=0}^{n} c \\ &= c + (n+1)\cdot c = (n+2)\cdot c.\end{aligned}$$

Portanto $n+1 \in M$ e, pelo princípio de indução $N = \mathbb{N}$.

iv- Propiedad Telescópica

$$\sum_{i=0}^{n} (x_{i+1} - x_i) = x_{n+1} - x_0.$$

De fato seja

$$P(n) = \text{"} \sum_{i=0}^{n} (x_{i+1} - x_i) = x_{n+1} - x_0 \text{"}$$

e considere M o seu domínio de verdade. Então $0 \in M$, pois

$$\sum_{i=0}^{0} (x_{i+1} - x_i) = x_1 + x_0.$$

Se $n \in M$ então como

$$\begin{aligned}\sum_{i=0}^{n+1} (x_{i+1} - x_i) &= x_{n+2} - x_{n+1} + \sum_{i=0}^{n} (x_{i+1} - x_i) \\ &= x_{n+2} - x_{n+1} + (x_{n+1} - x_0) = x_{n+2} - x_0.\end{aligned}$$

Portanto $n+1 \in M$ e, pelo princípio de indução $N = \mathbb{N}$.

– **A somatoria generalizada:** É a sequência de números reais

$$\left(a_n = \sum_{i=k}^{n+k} x_i \right)_{n \in \mathbb{N}}$$

definida da seguinte forma

$$a_n = \left(\sum_{i=0}^{n+k} x_i \right) - \left(\sum_{i=0}^{k-1} x_i \right).$$

– **A produtória:** É a sequência de números reais

$$\left(a_n = \prod_{i=0}^{n} x_i \right)_{n \in \mathbb{N}}$$

definida da seguinte forma

$$a_0 = \prod_{i=0}^{0} x_i = x_0 \qquad a_n = \prod_{i=0}^{n} x_i = a_{n-1} \cdot x_n.$$

É fácil ver que

$$\prod_{i=0}^{n} x_i = x_0 \cdot x_1 \cdots x_n.$$

De fato, seja

$$P(n) = "\prod_{i=0}^{n} x_i = x_0 \cdot x_1 \cdots x_n",$$

e considere M o seu domínio de verdade. Então $0 \in M$ pois

$$\prod_{i=0}^{0} x_i = x_0.$$

Assuma que $n \in M$ então

$$\begin{aligned} \prod_{i=0}^{n+1} x_i &= x_{n+1} \cdot \prod_{i=0}^{n} x_i \\ &= x_{n+1} \cdot (x_0 \cdot x_1 \cdots x_n) \\ &= x_0 \cdot x_1 \cdots x_n \cdot x_{n+1}. \end{aligned}$$

De onde $n+1 \in M$ e, pelo princípio de indução, $M = \mathbb{N}$.

Sejam $(x_n)_{n\in\mathbb{N}}$ e $(y_n)_{n\in\mathbb{N}}$ duas sequências. Então

i-

$$\prod_{i=0}^{n} c \cdot x_i = c^n \cdot \prod_{i=0}^{n} x_i.$$

De fato seja

$$P(n) = "\prod_{i=0}^{n} c \cdot x_i = c^n \cdot \prod_{i=k}^{n} x_i"$$

e considere M o seu domínio de verdade. Então $0 \in M$, pois

$$\prod_{i=0}^{0} c \cdot x_i = c \cdot x_0 = c \cdot \prod_{i=0}^{0} x_i.$$

Se $n \in M$ então como

$$\begin{aligned} \prod_{i=0}^{n+1} c \cdot x_i &= c \cdot x_{n+1} \cdot \prod_{i=0}^{n} c \cdot x_i \\ &= c \cdot x_{n+1} \cdot c \cdot \prod_{i=k}^{n} x_i \\ &= c^{n+1} \cdot \left(x_{n+1} \cdot \prod_{i=k}^{n} x_i \right) = c^{n+1} \cdot \prod_{i=0}^{n+1} x_i. \end{aligned}$$

Portanto $n+1 \in M$ e, pelo princípio de indução $N = \mathbb{N}$.

ii-

$$\prod_{i=0}^{n} (x_i \cdot y_i) = \prod_{i=0}^{n} x_i \cdot \prod_{i=0}^{n} y_i.$$

De fato seja

$$P(n) = "\prod_{i=0}^{n} (x_i \cdot y_i) = \prod_{i=0}^{n} x_i \cdot \prod_{i=0}^{n} y_i"$$

e considere M o seu domínio de verdade. Então $0 \in M$, pois

$$\prod_{i=0}^{0} (x_i \cdot y_i) = x_0 \cdot y_0 = \prod_{i=0}^{0} x_i \cdot \prod_{i=0}^{0} y_i.$$

Se $n \in M$ então como

$$\begin{aligned}\prod_{i=0}^{n+1}(x_i \cdot y_i) &= x_{n+1} \cdot y_{n+1} + \prod_{i=0}^{n}(x_i \cdot y_i) \\ &= x_{n+1} \cdot y_{n+1} \cdot \prod_{i=0}^{n} x_i \cdot \prod_{i=0}^{n} y_i \\ &= \prod_{i=0}^{n+1} x_i \cdot \prod_{i=0}^{n+1} y_i.\end{aligned}$$

Portanto $n+1 \in M$ e, pelo princípio de indução $N = \mathbb{N}$.

iii-

$$\prod_{i=0}^{n} c = c^{n+1}.$$

De fato seja

$$P(n) = \text{"}\prod_{i=0}^{n} c = c^{n+1}\text{"}$$

e considere M o seu domínio de verdade. Então $0 \in M$, pois

$$\prod_{i=0}^{0} c = c = c^1.$$

Se $n \in M$ então como

$$\begin{aligned}\prod_{i=0}^{n+1} c &= c \cdot \prod_{i=0}^{n} c \\ &= c \cdot c^{n+1} = c^{n+2}.\end{aligned}$$

Portanto $n+1 \in M$ e, pelo princípio de indução $N = \mathbb{N}$.

– **A Produtória generalizada:** É a sequência de números reais

$$\left(a_n = \prod_{i=k}^{n+k} x_i\right)_{n \in \mathbb{N}}$$

definida da seguinte forma

$$a_n = \left(\prod_{i=0}^{n+k} x_i\right) \cdot \left(\prod_{i=0}^{k-1} x_i\right)^{-1}.$$

■ **Exemplo 19.5** Para alguns casos particulares, podemos calcular os termos genéricos do somatorio e a produtoria dos termos de uma sequência.

- Se sequência $(x_n)_{n \in \mathbb{N}}$ definida pela progressão aritmética para $a,\ r \in \mathbb{R}$ temos

$$x_n = a + n \cdot r.$$

Portanto se

$$S_n = \sum_{i=0}^{n} x_n$$

temos que

$$2S_n = (x_n + x_0) + (x_{n-1} + x_1) + \cdots + (x_0 + x_n) = (n+1)(a + x_n)$$

de onde segue que

$$S_n = \frac{1}{2} \cdot (n+1) \cdot (a + x_n).$$

- Se sequência $(x_n)_{n\in\mathbb{N}}$ definida pela progressão geométrica para $a,\ r \in \mathbb{R}$ temos

$$x_n = a \cdot n^r$$

Portanto se

$$S_n = \sum_{i=0}^{n} x_n$$

temos que

$$S_n - qS^n = x_0 - x_{n+1} = a(1-q^{n+1})$$

de onde segue que

$$S_n = a \cdot \frac{1-q^{n+1}}{1-q}.$$

■

Achar o termo genérico da recorrência em função dos dados iniciais pode ser uma tarefa difícil, no entanto existem alguns casos em que isto é possível.

■ **Exemplo 19.6** • Considere a sequência $(x_n)_{n\in\mathbb{N}}$ de números reais definida por uma expressão da forma

$$x_0 = a \quad x_n = n \cdot x_{n-1} \quad \forall\, n \geq 1$$

Observamos que

$$x_2 = 2 \cdot a,\ x_3 = 3 \cdot 2 \cdot a,\ \ldots, x_n = n \cdots 3 \cdot 2 \cdot a = n! \cdot a.$$

- Considere a sequência $(x_n)_{n\in\mathbb{N}}$ de números reais definida por uma expressão da forma

$$x_0 = a \quad x_n = x_{n-1} + f(n) \quad \forall\, n \geq 1$$

para $f : \mathbb{N} \to \mathbb{R}$.
Observamos que

$$x_n = a + \sum_{j=1}^{n} f(n)$$

■

Definição 19.4 Uma sequência $(x_n)_{n\in\mathbb{N}}$ de números reais definida por uma expressão da forma

$$x_n = c_d \cdot x_{n-d} + \cdots + c_1 \cdot x_{n-1} + f(n) \qquad x_0 = a_0,\ \ldots,\ x_{d-1} = a_{d-1}$$

é dita uma recorrência linear de ordem d.
Caso $f(n) = 0$ para todo $n \in \mathbb{N}$ então chamamos a recorrência de linear homogênea de ordem d.

■ **Exemplo 19.7** • A sequência de Fibonacci é uma recorrência linear homogênea.

- A sequência $(x_n)_{n\in\mathbb{N}}$ em que $x_0 = 1$ e $x_1 = 2$ e

$$x_{n+2} = 2 \cdot x_{n+1} + x_n \quad \forall\, n \in \mathbb{N}.$$

■

Teorema 19.5 Considere uma sequência $(x_n)_{n\in\mathbb{N}}$ de números reais definida por uma expressão da forma

$$\begin{aligned} x_0 &= a \\ x_{n+1} &= r\cdot x_n \quad \forall\, n \geq 1, \end{aligned}$$

Então, o termo genérico da sequência é,

$$x_n = r^n \cdot a$$

Demonstração. Foi feita acima quando vimos o termo genérigo da progressão geométrica. ■

Teorema 19.6 Considere uma sequência $(x_n)_{n\in\mathbb{N}}$ de números reais definida por uma expressão da forma

$$\begin{aligned} x_0 &= a \\ x_{n+1} &= g(n)\cdot x_n + f(n) \quad \forall\, n \geq 1, \end{aligned}$$

para $f,\ g : \mathbb{N} \to \mathbb{R}$ duas funções. Então, o termo genérico da recorrência pode ser escrito como produto

$$x_n = z_n \cdot y_n$$

em que

$$z_n = g(n-1)\cdot z_{n-1}$$

$$y_n = y_{n-1} + f(n-1)[g(n-1)\cdot z_{n-1}]^{-1}$$

Demonstração. Substituindo $x_n = y_n \cdot z_n$ temos,

$$\begin{aligned} x_n &= z_n \cdot y_n \\ &= g(n-1)\cdot z_{n-1}\cdot (y_{n-1} + f(n-1)[g(n-1)\cdot z_{n-1}]^{-1}) \\ &= g(n-1)\cdot z_{n-1}\cdot y_{n-1} + f(n-1) \\ &= g(n-1)\cdot x_{n-1} + f(n-1). \end{aligned}$$

■

■ **Exemplo 19.8** Considere a recorrência

$$\begin{aligned} x_0 &= a \\ x_{n+1} &= r\cdot x_n + r^n \quad \forall\, n \geq 1, \end{aligned}$$

Então resolvemos

$$z_n = r\cdot z_{n-1} \Rightarrow z_n = r^n \cdot z_0$$

e

$$y_n = y_{n-1} + r^{n-1}[r\cdot r^{n-1}\cdot z_0]^{-1} = y_{n-1} + \frac{1}{z_0\cdot r} + y_0.$$

que tem por solução

$$y_n = \frac{n+1}{z_0\cdot r} + y_0$$

portanto a solução de x_n é

$$x_n = z_0\cdot r^n \cdot \left(\frac{n+1}{z_0\cdot r} + y_0\right) = z_0\cdot y_0\cdot r^n + (n+1)r^{n-1}$$

$$\begin{aligned} x_n &= r(z_0 \cdot y_0 \cdot r^{n-1} + n \cdot r^{n-2}) + r^{n-1} \\ &= x_{n-1} + r^{n-1}. \end{aligned}$$

■

A seguir mostramos um reultado geral para resolução de recorrências lineares de segunda ordem.

Teorema 19.7 Considere uma sequência $(x_n)_{n\in\mathbb{N}}$ de números reais definida por uma expressão da forma

$$\begin{aligned} x_0 &= a \\ x_1 &= b \\ x_{n+1} &= c_1 \cdot x_n + c_2 \cdot x_{n-1} \quad \forall\, n \geq 1, \end{aligned}$$

e a equação de segundo grau $R:\ x^2 - c_1 \cdot x - c_2 = 0$, que chamamos de equação característica da recorrência.

- Se R tem duas raizes reais iguais $r = r_1 = r_2$ então

  $$x_n = \alpha \cdot r^n + n \cdot \beta \cdot r^n$$

  para α e β constantes que depende dem a e b.
- Se R tem duas raizes reais distintas $r_1 \neq r_2$ então

  $$x_n = \alpha \cdot r_1^n + \beta \cdot r_2^n$$

  para α e β números reais que são determinados em função de a e b.

Demonstração. Primeiramnte observamos que $c_1 \neq 0$ pois a recorrência é de segunda ordem.

- Se r é a única raiz de r temos

  $$r^2 = c_1 \cdot r + c_2 \quad r = -\frac{1}{2} \cdot c_1 \quad \text{e} \quad c_1^2 = 4 \cdot c_2$$

  de onde

  $$c_1 \cdot r - 2 \cdot c_2 = -\frac{1}{2} \cdot (c_1^2 - 4 \cdot c_2) = 0.$$

  Com isto, para $n \geq 2$ temos

  $$\begin{aligned} x_n &= \alpha \cdot r^n + \beta \cdot n \cdot r^n \\ &= \alpha \cdot r^{n-2} \cdot r^2 + n \cdot \beta r^n \cdot r^2 \\ &= \alpha \cdot r^{n-2} \cdot (c_1 \cdot r + c_2) + n \cdot \beta \cdot r^{n-2} \cdot (c_1 \cdot r + c_2) \\ &= c_1 \cdot (\alpha \cdot r^{n-1} + (n-1) \cdot \beta \cdot r^{n-1}) + c_2 \cdot (\alpha \cdot r^{n-2} + (n-2) \cdot \beta \cdot r^{n-2}) \\ &\quad + (c_1 \cdot r - 2 \cdot c_2) \cdot \beta \cdot r^{n-2} \\ &= c_1 \cdot x_{n-1} + c_2 \cdot x_{n-2}. \end{aligned}$$

  Agora, o resultado segue da unicidade da solução. Mais ainda, para achar α e β temos um sistema

  $$\begin{cases} \alpha &= a \\ \alpha \cdot r + \beta \cdot r &= b \end{cases}$$

  que tem por solução

  $$\alpha = a \quad \text{e} \quad \beta = b \cdot r^{-1} + (-a).$$

- Primeiramente observamos que se r_1 e r_2 são raizes distintas de R temos que $r_1 + (-r_2) \neq 0$ e

  $$r_1^2 = c_1 \cdot r_1 + c_2 \quad \text{e} \quad r_1^2 = c_1 \cdot r_1 + c_2.$$

Com isto, para $n \geq 2$ temos

$$\begin{aligned} x_n &= \alpha \cdot r_1^n + \beta \cdot r_2^n \\ &= \alpha \cdot r_1^{n-2} \cdot r_1^2 + \beta \cdot r_2^{n-2} \cdot r_2^2 \\ &= \alpha \cdot r_1^{n-2} \cdot (c_1 \cdot r_1 + c_2) + \beta \cdot r_2^{n-2} \cdot (c_1 \cdot r_2 + c_2) \\ &= c_1 \cdot (\alpha \cdot r_1^{n-1} + \beta r_2^{n-1}) + c_2 \cdot (\alpha \cdot r_1^{n-2} + \beta \cdot r_2^{n-2}) \\ &= c_1 \cdot x_{n-1} + c_2 \cdot x_{n-2}. \end{aligned}$$

Agora, o resultado segue da unicidade da solução. Mais ainda, para achar α e β temos um sistema

$$\begin{cases} \alpha + \beta &= a \\ \alpha \cdot r_1 + \beta \cdot r_2 &= b \end{cases}$$

que tem por solução

$$\alpha = (b + (-a \cdot r_2) \cdot (r_1 + (-r_2))^{-1} \quad \text{e} \quad \beta = (a \cdot r_1 + (-b)) \cdot (r_1 + (-r_2))^{-1}.$$

■

Obs. A resolução de recorrências de segunda ordem cuja equação característica não tem raizes no conjunto dos números reais será vista quando estudemos números complexos.

■ **Exemplo 19.9** • A sequência de Fibonacci é dada por

$$\begin{aligned} x_0 &= 1 \\ x_1 &= 1 \\ x_{n+1} &= x_n + x_{n-1} \quad \forall\, n \geq 1, \end{aligned}$$

então a equação

$$x^2 - x - 1 = 0$$

tem por raizes

$$r_1 = \frac{1-\sqrt{5}}{2} \quad \text{e} \quad r_2 = \frac{1+\sqrt{5}}{2}.$$

portanto

$$x_n = \alpha \left(\frac{1-\sqrt{5}}{2}\right)^n + \beta \left(\frac{1+\sqrt{5}}{2}\right)^n$$

Como $x_0 = 1 = x_1$ temos que

$$\alpha = -\frac{1}{\sqrt{5}}\left(\frac{1-\sqrt{5}}{2}\right) \quad \text{e} \quad \beta = \frac{1}{\sqrt{5}}\left(\frac{1-\sqrt{5}}{2}\right).$$

Portanto

$$x_n = \frac{1}{\sqrt{5}}\left[\left(\frac{1+\sqrt{5}}{2}\right)^n - \left(\frac{1+\sqrt{5}}{2}\right)^n\right].$$

- A sequência dada por

$$\begin{aligned} x_0 &= 1 \\ x_1 &= 1 \\ x_{n+1} &= 4 \cdot x_n - 4 \cdot x_{n-1} \quad \forall\, n \geq 1, \end{aligned}$$

então a equação

$$x^2 - 4 \cdot x + 4 = 0$$

tem por raizes

$$r_1 = r_2 = 2.$$

portanto o termo genérico é

$$x_n = \alpha \cdot 2^n + \beta \cdot n \cdot 2^n$$

Como $x_0 = 1 = x_1$ temos que

$$\alpha = 1 \quad \text{e} \quad 2 \cdot \alpha + 2 \cdot \beta = 1$$

de onde

$$\beta = -\frac{1}{2}$$

e

$$x_n = (2 - n) \cdot 2^{n-1} \quad \forall n \in \mathbb{N}.$$

■

Teorema 19.8 Considere uma sequência $(x_n)_{n\in\mathbb{N}}$ de números reais definida por uma expressão da forma

$$\begin{aligned} x_0 &= a \\ x_1 &= b \\ x_{n+1} &= c_1 \cdot x_n + c_2 \cdot x_{n-1} + f(n) \quad \forall\, n \geq 1, \end{aligned}$$

para $f : \mathbb{N} \to \mathbb{R}$ uma função, e y_n uma sequência que satisfaz

$$y_{n+1} = c_1 \cdot y_n + c_2 \cdot y_{n-1}$$

então se $z_n = x_n + y_n$ temos que

$$z_{n+1} = c_1 \cdot z_n + c_2 \cdot z_{n-1} + f(n).$$

Demonstração. Fazemos a conta com z_n como definido acima e obtemos

$$\begin{aligned} z_{n+1} &= x_{n+1} + y_{n+1} \\ &= c_1 \cdot (x_n + y_n) + c_2 \cdot (x_{n-1} + y_{n-1}) + f(n) \\ &= c_1 \cdot z_n + c_2 \cdot z_{n-1} + f(n) \end{aligned}$$

■

■ **Exemplo 19.10** Considere uma sequência $(x_n)_{n\in\mathbb{N}}$ de números reais definida por uma expressão da forma

$$\begin{aligned} x_0 &= 1 \\ x_1 &= 1 \\ x_{n+1} &= -x_n + 2 \cdot x_{n-1} + 12 \cdot n - 2 \quad \forall\, n \geq 1, \end{aligned}$$

Para achar a solução desta recorrência vamos primeiramente estudar a solução da recorrência homogênea

$$y_{n+1} = -y_n + 2 \cdot y_{n-1}.$$

e depois procuramos uma solução particular da recorrência

$$z_{n+1} = -z_n + 2 \cdot z_{n-1} + 12 \cdot n - 2$$

Logo, a x_n terá por expressão $x_n = z_n + y_n$. Finalmente estudamos o caso x_0 e x_1 para determinar a forma precisa de x_n.

- Estudamos a recorrência

  $$y_{n+1} = -y_n + 2 \cdot y_{n-1}.$$

  A equação característica é

  $$x^2 + x - 2 = 0$$

  que tem raizes

  $$r_1 = 1 \quad \text{e} \quad r_2 = -2.$$

  Então a solução da recorrência

  $$y_{n+1} = -y_n + 2 \cdot y_{n-1},$$

  é da forma

  $$y_n = \alpha \cdot (1)^n + \beta(-2)^n = \alpha + \beta \cdot 2^n.$$

- Para z_n temos que propor uma solução. Aqui o estudo é intuitivo. Propomos uma solução da forma

  $$z_n = a \cdot n^2.$$

  Então

  $$a \cdot (n+1)^2 = -a \cdot n^2 + 2 \cdot a \cdot (n-1)^2 + 12 \cdot n - 2.$$

  Simplificando temos

  $$12 \cdot n - 2 = 6 \cdot a \cdot n - a$$

  portanto $a = 2$. De onde

  $$z_n = 2 \cdot n^2$$

- Utilizando o visto acima temos que

  $$x_n = \alpha + \beta \cdot 2^n + 2 \cdot n^2.$$

  Como $x_0 = 1 = x_1$ temos

  $$\alpha + \beta = 1 \quad \text{e} \quad 1 = \alpha - 2 \cdot \beta + 2.$$

  de onde segue que

  $$\alpha = \frac{1}{3} \quad \text{e} \quad \beta = \frac{2}{3}.$$

Então, a o termo genérico será

$$x_n = \frac{1}{3} + \frac{(-2)^{n+1}}{3} + 2 \cdot n^2.$$

■

20. Números Complexos

Vimos que com os números reais, toda função proposicional em $\mathbb{R}$ da forma

$$P(x) = "x \in \mathbb{R},\ a_{2k+1} \cdot x^{2k+1} + \cdots + a_1 \cdot x + a_0 = 0",$$

para $k \in \mathbb{N}$ e $a_{2k+1} \neq 0$, tem domínio de verdade não vazio. Também vimos que a função proposicional

$$Q(x) = "x \in \mathbb{R},\ x^2 + 1 = 0".$$

Tem domínio de verdade vazio em $\mathbb{R}$. Novamente procuramos ampliar o conjunto numérico de forma tal que as funções proposicionais sobre os números reais estejam contempladas no novo conjunto numérico e de forma tal que, no novo conjunto numérico, seu domínio de verdade seja não vazio. Nesse sentido introduzimos os números complexos.

Para construir o conjunto dos números complexos vamos primeiramente construir seus elementos. Para isto utilizamos um simbolo **i**, então dados $a,\ b \in \mathbb{R}$ construimos os elementos

$$a + b\mathbf{i},$$

e dizemos que dois elementos $z_1 = (a + b\mathbf{i})$ e $z_2 = (c + d\mathbf{i})$ são iguais se $(a = c) \wedge (b = d)$.

Obs. Aqui o sinal $+$ é uma notação e, em princípio, nada tem a ver com a notação. Mais adiante, no texto, veremos que podemos relacionar esse $+$ com a operação soma entre números complexos.

Definição 20.1 O conjunto dos números complexos, que denotamos por $\mathbb{C}$,é o conjunto

$$\mathbb{C} = \{z = a + b\mathbf{i},\ a,\ b \in \mathbb{R}\}.$$

Em particular se $z = a + b\mathbf{i}$ então

- a é chamada de parte real de z e a denotamos por $\mathbf{Re}(z)$
- b é chamada de parte real de z e a denotamos por $\mathbf{Im}(z)$

Sobre o conjunto dos números complexos definimos duas operações.

- Soma: $+ : \mathbb{C} \times \mathbb{C} \to \mathbb{C}$ dada por

$$(a + b\mathbf{i}) + (c + d\mathbf{i}) = (a + c) + (b + d)\mathbf{i}.$$

- Produto: $\cdot : \mathbb{C} \times \mathbb{C} \to \mathbb{C}$ dada por

$$(a+b\mathbf{i}) \cdot (c+d\mathbf{i}) = (a \cdot c + (-(b \cdot d)) + (a \cdot d + b \cdot c)\mathbf{i}.$$

Obs. Na definição de soma acima utilizamos indistintamente a soma de números reais e de complexos, junto com a simbologia de "$+$" utilizada na construção do número complexo. Algo similar ocorre com o produto, a notação correta seria utilizar as operações $+_{\mathbb{R}}$ e $\cdot_{\mathbb{R}}$ para as operações sobre os números reais e $+_{\mathbb{C}}$ e $\mathbb{R}$ e definir:

- Soma: $+_{\mathbb{C}} : \mathbb{C} \times \mathbb{C} \to \mathbb{C}$ dada por

$$(a+b\mathbf{i}) +_{\mathbb{C}} (c+d\mathbf{i}) = (a +_{\mathbb{R}} c) + (b +_{\mathbb{R}} d)\mathbf{i}.$$

- Produto: $\cdot_{\mathbb{C}} : \mathbb{C} \times \mathbb{C} \to \mathbb{C}$ dada por

$$(a+b\mathbf{i}) \cdot_{\mathbb{C}} (c+d\mathbf{i}) = [a \cdot_{\mathbb{R}} c +_{\mathbb{R}} (-(b \cdot_{\mathbb{R}} d)] + (a \cdot_{\mathbb{R}} d +_{\mathbb{R}} b \cdot_{\mathbb{R}} c)\mathbf{i}.$$

Claramente, a definição fica sobrecarregada, portanto a omitiremos e deixamos a interpretação ao contexto.

Seja $a+b\mathbf{i} \in \mathbb{C}$ um número complexo qualquer.

- O elemento $\mathbf{0} = 0+0\mathbf{i}$ satisfaz

$$(a+b\mathbf{i}) + (0+0\mathbf{i}) = a+b\mathbf{i},$$

$$(a+b\mathbf{i}) + (-a+(-b)\mathbf{i}) = 0+0\mathbf{i} = \mathbf{0},$$

e

$$(a+b\mathbf{i}) \cdot (0+0\mathbf{i}) = 0+0\mathbf{i} = \mathbf{0}.$$

- O elemento $\mathbf{1} = 1+0\mathbf{i}$ satisfaz

$$(a+b\mathbf{i}) \cdot (1+0\mathbf{i}) = a+b\mathbf{i}.$$

- o elemento $0+a\mathbf{i}$, que denotamos por $a\mathbf{i}$ satisfaz

$$(0+a\mathbf{i})^2 = (0-a^2)+0\mathbf{i} = -a^2+0\mathbf{i}$$

em particular $(0+1\mathbf{i})^2 = -1+0\mathbf{i}$.

- O produto

$$(a+b\mathbf{i}) \cdot (a-b\mathbf{i}) = (a^2+b^2)+0\mathbf{i}.$$

Em particular vemos que $a+b\mathbf{i} \neq \mathbf{0}$ se, e somente se, $a^2+b^2 \neq 0$.

- Se $a+b\mathbf{i} \neq \mathbf{0}$ então

$$(a+b\mathbf{i}) \cdot \left(\frac{a}{a^2+b^2} + \left(\frac{-b}{a^2+b^2} \right) \mathbf{i} \right) = 1+0\mathbf{i} = \mathbf{1}.$$

Teorema 20.1 Os números complexos com a soma e o produto formam um corpo.

Demonstração. Temos que mostrar as propriedades de corpo. Para isto considere

$$z_1 = a+b\mathbf{i}, \quad z_2 = c+d\mathbf{i} \quad \text{e} \quad z_3 = e+f\mathbf{i}.$$

-

$$\begin{aligned} z_1+z_2 &= (a+c)+(b+d)\mathbf{i} \\ &= (c+a)+(d+b)\mathbf{i} \\ &= z_2+z_1. \end{aligned}$$

- $$\begin{aligned} z_1+(z_2+z_3) &= (a+b\mathbf{i})+(c+e)+(d+f)\mathbf{i} \\ &= (a+c+e)+(b+d+f)\mathbf{i} \\ &= (a+c)+(b+d)\mathbf{i}+(e+f\mathbf{i}) \\ &= (z_1+z_2)+z_3. \end{aligned}$$
- Existe o elemento $\mathbf{0}=0+0\mathbf{i}$

  $$\mathbf{0}+z_1=(a+0)+(b+0)\mathbf{i}=z_1.$$

  Observamos que é único. De fato se w possui a mesma propriedade, temos

  $$\mathbf{0}=w+\mathbf{0}=w.$$

- Dado z_1 definimos $-z_1=-a+(-b)\mathbf{i}$, então

  $$z_1+(-z_1)=(a+(-a))+(b+(-b))\mathbf{i}=0+0\mathbf{i}=\mathbf{0}.$$

- $$\begin{aligned} z_1+z_2=z_1+z_3 &\Leftrightarrow (a+c)+(b+d)\mathbf{i}=(a+e)+(b+f)\mathbf{i} \\ &\Leftrightarrow [(a+c)=(a+e)]\wedge[(b+d)=(b+f)] \\ &\Leftrightarrow (c=e)\wedge(d=f) \quad \text{(cancelamente em } \mathbb{R}) \\ &\Leftrightarrow c+d\mathbf{i}=e+f\mathbf{i} \quad \Rightarrow \quad z_2=z_3. \end{aligned}$$

- $$\begin{aligned} z_1\cdot z_2 &= (a\cdot c-b\cdot d)+(a\cdot b+b\cdot c)\mathbf{i} \\ &= (c\cdot a-d\cdot b)+(b\cdot a+c\cdot b)\mathbf{i} \\ &= z_1+z_2. \end{aligned}$$
- Provamos o cancelamento da soma por completitude.
  $$\begin{aligned} z_1\cdot(z_2\cdot z_3) &= (a+b\mathbf{i})\cdot[(c\cdot e-d\cdot f)+(c\cdot f+d\cdot e)\mathbf{i}] \\ &= [a\cdot(c\cdot e-d\cdot f)-b\cdot(c\cdot f+d\cdot e)][(c\cdot e-d\cdot f)\cdot b+(c\cdot f+d\cdot e)\cdot a]\mathbf{i} \\ &= [(a\cdot c-b\cdot d)+(a\cdot b+b\cdot c)\mathbf{i}]\cdot(e+f\mathbf{i}) \\ &= (z_1\cdot z_2)\cdot z_3. \end{aligned}$$
- Vimos acima que existe $\mathbf{1}=1+0\mathbf{i}\in\mathbb{C}$ tal que $z_1\cdot\mathbf{1}=z_1$.
- Para todo $z_1\in\mathbb{C}$ tal que $z_1\neq\mathbf{0}$ vimos acima que existe um único $z_1^{-1}\in\mathbb{C}$ definido por

  $$z_1^{-1}=\frac{a}{a^2+b^2}+\frac{b}{a^2+b^2}\mathbf{i},$$

  tal que

  $$z_1^{-1}\cdot z_1=\mathbf{1}.$$

- $$\begin{aligned} z_3\cdot(z_1+z_2) &= (e+f\mathbf{i})[(a+c)+(b+d)\mathbf{i}] \\ &= [e\cdot(a+c)-f\cdot(b+d)]+[e\cdot(b+d)+(a+c)\cdot f]\mathbf{i} \\ &= [e\cdot a+e\cdot c-f\cdot b+f\cdot d]+[e\cdot b+e\cdot d+a\cdot f+c\cdot f]\mathbf{i} \\ &= z_3\cdot z_1+z_3\cdot z_2. \end{aligned}$$
- Provamos o cancelamento do produto por completitude.
  $$\begin{aligned} z_1\cdot z_2=z_1\cdot z_3 &\Rightarrow z_1^{-1}\cdot z_1\cdot z_2=z_1^{-1}\cdot z_1\cdot z_3 \\ &\Rightarrow z_2=z_3. \end{aligned}$$

■

Teorema 20.2 Seja $j : \mathbb{R} \to \mathbb{C}$ definida por

$$j(a) = a + 0\mathbf{i},$$

então

- j é injetora,
- $j(a+b) = j(a) + j(b)$
- $j(a \cdot b) = j(a) \cdot j(b)$.

Demonstração.

- Assuma que $j(a) = j(b)$ então $a + 0\mathbf{i} = b + 0\mathbf{i}$ de onde $a = b$ e portanto j é injetora.
- da definição
$$\begin{aligned} j(a+b) &= (a+b) + 0\mathbf{i} \\ &= (a+0\mathbf{i}) + (b+0\mathbf{i}) \\ &= j(a) + j(b). \end{aligned}$$
- da definição
$$\begin{aligned} j(a \cdot b) &= (a \cdot b) + 0\mathbf{i} \\ &= (a+0\mathbf{i}) \cdot (b+0\mathbf{i}) \\ &= j(a) \cdot j(b). \end{aligned}$$

■

Obs. É por meio desta função injetora que identificamos $\mathbb{R}$ como um subconjunto de $\mathbb{C}$. Temos assim uma torre de inclussões:

$$\mathbb{N} \subset \mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}.$$

Em função desta identificação temos

$$a \in \mathbb{R} \equiv a + 0\mathbf{i}$$

e da regra

$$(a+0\mathbf{i}) \cdot (b+c\mathbf{i}) = (a \cdot c) + (a \cdot b)\mathbf{i}$$

que escrevemos

$$a \cdot (b+c\mathbf{i}) = (a \cdot b) + (a \cdot c)\mathbf{i}.$$

Corolário 20.1 O conjunto dos números complexos não é enumerável

Demonstração. Como $\mathbb{R} \subset \mathbb{C}$, se $\mathbb{C}$ for enumerável então $\mathbb{R}$ também deveria ser, o que é uma contradição. ■

Definição 20.2 Dado $z = a + b\mathbf{i}$ um número complexo, denotamos por $\bar{z}$ ao número

$$\bar{z} = a + (-b)\mathbf{i} := a - b\mathbf{i}.$$

O produto

$$z \cdot \bar{z} = a^2 + b^2 + 0\mathbf{i}$$

pode ser identificado com o número real $a^2 + b^2$. Definimos o módulo do número complexo $z = a + b\mathbf{i}$ por

$$|z| = \sqrt{z \cdot \bar{z}} = \sqrt{a^2 + b^2}.$$

Corolário 20.2 Sejam $z_1,\ z_2 \in \mathbb{C}$ então
- $\overline{z_1+z_2} = \overline{z_1}+\overline{z_2}$
- $\overline{z_1 \cdot z_2} = \overline{z_1} \cdot \overline{z_2}$

Demonstração. Sejam $z_1 = a+b\mathbf{i}$ e $z_2 = c+d\mathbf{i}$. Então.

$$\begin{aligned}\overline{z_1+z_2} &= a+c-(b+d)\mathbf{i}\\ &= a-b\mathbf{i}+c-d\mathbf{i}\\ &= \overline{z_1}+\overline{z_2}\end{aligned}$$

e

$$\begin{aligned}\overline{z_1 \cdot z_2} &= (a\cdot c-b\cdot d)+(ad+bc)\mathbf{i}\\ &= (a-b\mathbf{i})\cdot(c-d\mathbf{i})\\ &= \overline{z_1}\cdot\overline{z_2}.\end{aligned}$$

■

Teorema 20.3 O conjuntos dos números complexos não é um corpo ordenado.

Demonstração. Assuma que $\mathbb{C}$ é um corpo ordenado. Então, como $0+\mathbf{i} \neq 0+0\mathbf{i}$ temos duas posibilidades:
- $0+\mathbf{i} < 0+0\mathbf{i}$ então, como

  $$0+0\mathbf{i} < (0+\mathbf{i})^2 = -1+0\mathbf{i}$$

  de onde

  $$0+0\mathbf{i} < (-1+0\mathbf{i})^2 = 1+0\mathbf{i}$$

  portanto

  $$1+0\mathbf{i} = (1+0\mathbf{i})+(0+0\mathbf{i}) < (1+0\mathbf{i})+(-1+0\mathbf{i}) = 0+0\mathbf{i} < (-1+0\mathbf{i})^2 = 1+0\mathbf{i}.$$

  o que é uma contradição.
- $0+0\mathbf{i} < 0+\mathbf{i}$ então, como

  $$0+0\mathbf{i} < (0+\mathbf{i})^2 = -1+0\mathbf{i} \quad \Rightarrow 0+0\mathbf{i} < (-1+0\mathbf{i})^2 = 1+\mathbf{i}.$$

  Temos então que

  $$1+0\mathbf{i} = (1+0\mathbf{i})+(0+0\mathbf{i}) < (1+0\mathbf{i})+(-1+0\mathbf{i}) = 0+0\mathbf{i} < (1+0\mathbf{i})^2 = 1+0\mathbf{i}.$$

  o que é uma contradição

■

Por fim observamos que nos complexos toda função proposicional da forma

$$P(x) = \text{"}x \in \mathbb{R},\ a_k \cdot x^k + \cdots + a_1 \cdot x + a_0 = 0\text{"},$$

como $a_0, \ldots, a_k \in \mathbb{C}$ e $a_k \neq 0$ tem domínio de verdade não vazio. Mais ainda, pode ser mostrado que o domínio de verdade contém, no máximo, k elementos. A prova deste resultado é conhecido como o **Teorema fundamental da Álgebra**.

Para representar gráficamente os número complexos consideramos a função $\phi : \mathbb{C} \to \mathbb{R}^2$ dada por

$$\phi(a+b\mathbf{i}) = (a,b).$$

Observamos que a função é, de fato, bijetora. Para isto, observamos que

$$\begin{aligned}\phi(a+b\mathbf{i}) = \phi(c+d\mathbf{i}) &\Leftrightarrow (a,b) = (c,d)\\ &\Leftrightarrow a = c \wedge b = d.\end{aligned}$$

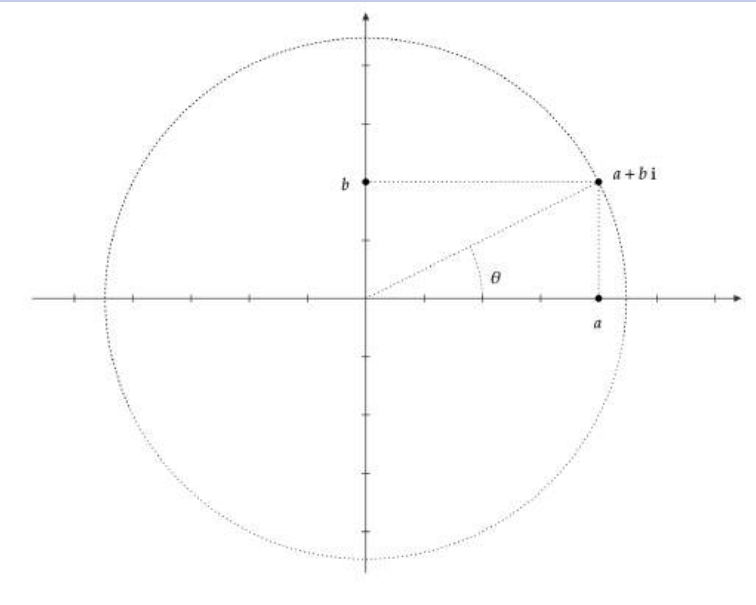
E, todo $(a,b) \in \mathbb{R}^2$ pode ser visto como

$$\phi(a+b\mathbf{i}) = (a,b).$$

Então representamos os numeros complexo no plano $\mathbb{R}^2$, identificando

$$(a,b) \equiv a+b\mathbf{i}.$$

como segue:



Assumindo que conhecemos um pouco de trigonometria elementar, vemos que

$$a = \sqrt{a^2+b^2}\cos(\theta) \quad \text{e} \quad b = \sqrt{a^2+b^2}\sin(\theta)$$

Observamos então que, para todo número complexo $z = a+b\mathbf{i}$ podemos escreber

$$z = |z|(\cos(\theta)+\sin(\theta)\mathbf{i}).$$

para $\theta \in [0,2\pi)$ tal que

$$\cos(\theta) = \frac{a}{\sqrt{a^2+b^2}} \quad \text{e} \quad \sin(\theta) = \frac{b}{\sqrt{a^2+b^2}}$$

O ângulo θ assim obtido é chamado de argumento de z é será denotado por

$$\theta = \mathbf{Arg}(z).$$

Teorema 20.4 Sejam $z_1,\ldots,z_m \in \mathbb{C}$. Considere

$$\rho_i = |z_i| \quad \text{e} \quad \theta_i = \mathbf{Arg}(z_i),$$

então $z = z_1 \cdot z_n$ é o número complexo

$$z = \rho\cos(\phi)+\rho\sin(\phi)\mathbf{i}$$

em que

$$\rho = \rho_1 \cdot \rho_2 \cdots \rho_n$$

e $\phi \in [0, 2\pi)$ tal que existe $k \in \mathbb{N}$ satisfazendo

$$\phi + 2 \cdot k \cdot \pi = \theta_1 + \theta_2 + \cdots + \theta_n.$$

Demonstração. Porvamos por indução no número n. Se $n = 2$ temos Se

$$z_1 = \rho_1(\cos(\theta_1) + \sin(\theta_1)\mathbf{i}) \quad \text{e} \quad z_2 = \rho_2 \cos(\theta_2) + \sin(\theta_2)\mathbf{i})$$

então

$$\begin{aligned} z_1 \cdot z_2 &= \rho_1\rho_2[(\cos(\theta_1) \cdot \cos(\theta_2) - \sin(\theta_1) \cdot \sin(\theta_2)) + (\cos(\theta_1) \cdot \sin(\theta_1) + \cos(\theta_2) \cdot \sin(\theta_2))\mathbf{i}] \\ &= \rho_1\rho_2[\cos(\theta_1 + \theta_2) + \sin(\theta_1 + \theta_2)\mathbf{i}] \end{aligned}$$

Então

$$|z_1 \cdot z_2| = \rho_2 \cdot \rho_2 = |z_1| \cdot |z_2|.$$

e

$$\mathbf{Arg}(z_1 \cdot z_2) = \mathbf{Arg}(z_1) + \mathbf{Arg}(z_2) + 2 \cdot k \cdot 2\pi.$$

para algum $k \in \mathbb{N}$.

Assuma que vale para n números, vejamos que acontece para $n+1$. Como vale para n temos que $z = z_1 \cdot z_n$ é o número complexo

$$z = \rho \cos(\phi) + \rho \sin(\phi)\mathbf{i}$$

em que

$$\rho = \rho_1 \cdot \rho_2 \cdots \rho_n$$

e $\phi \in [0, 2\pi)$ tal que existe $k \in \mathbb{N}$ satisfazendo

$$\phi + 2 \cdot k \cdot \pi = \theta_1 + \theta_2 + \cdots + \theta_n.$$

Calculamos

$$\begin{aligned} z_1 \cdots z_n \cdot z_{n+1} &= (\rho \cdot \cos(\theta) + \rho \cdot \sin(\theta)\mathbf{i}) \cdot (\rho_{n+1} \cdot \cos(\theta_{n+1}) + \rho_{n+1} \cdot \sin(\theta_{n+1})\mathbf{i} \\ &= [(\rho \cdot \rho_{n+1}) \cdot \cos(\theta + \theta_{n+1})] + [(\rho \cdot \rho_{n+1}) \cdot \sin(\theta + \theta_{n+1})]\mathbf{i} \end{aligned}$$

$$z_1 \cdots z_n \cdot z_{n+1} = \tilde{\rho} \cos(\phi) + \tilde{\rho} \sin(\phi)\mathbf{i}$$

em que

$$\tilde{\rho} = \rho_1 \cdot \rho_2 \cdots \rho_n \cdot \rho_{n+1}$$

e $\phi \in [0, 2\pi)$ tal que existe $k \in \mathbb{N}$ satisfazendo

$$\phi + 2 \cdot k \cdot \pi = \theta_1 + \theta_2 + \cdots + \theta_n + \theta_{n+1}.$$

Portanto, a identidade também vale para $n+1$ números. O axioma de indução garante que vale para um número $n \geq 2$ de elementos. ■

O visto acima fornece uma forma de resolver equações do tipo

$$z^m = a + b\mathbf{i}.$$

De fato, se

$$a + b\mathbf{i} = \rho\cos(\theta) + \rho\sin(\theta)\mathbf{i},$$

temos que

$$z_k = \sqrt[m]{\rho}\cos(\theta_k) + \sqrt[m]{\rho}\sin(\theta_k)\mathbf{i}.$$

com $\tilde{\theta}_k \in [0, 2\pi)$ congruente com

$$\frac{1}{m}\cdot(\theta + 2\cdot k\cdot\pi) \quad 0 \leq k < m,$$

satisfaz

$$z_k^m = a + b\mathbf{i}.$$

Observamos que para $k \geq m$ temos que $k = i + l\cdot m$ então

$$\theta_k = \frac{1}{m}\cdot(\theta + 2\cdot k\cdot\pi) = \theta_i + 2\cdot l\cdot\pi,$$

e os números complexos z_k que obtemos coincidem com os primeiros m obtidos.

Corolário 20.3 Para todo $z \in \mathbb{C}$ existem duas soluçções da equação $x^2 = z$ que denotamos por z_1 e z_2 e que são tais que $z_1 = -z_2$.

Demonstração. A existência de duas soluções é resultados da discussão acima. O fato de que as soluções $z_1 = -z_2$ satisfazem essa relação é consequência do fato

$$\mathbf{Arg}(z_2) = \mathbf{Arg}(z_1) + \pi.$$

■

■ **Exemplo 20.1** Procuramos as soluções da equação

$$z^5 = 1 + 1\mathbf{i}.$$

Observamos que

$$1 + 1\mathbf{i} = \sqrt{2}\cos\left(\frac{1}{4}\cdot\pi\right) + \sqrt{2}\sin\left(\frac{1}{4}\cdot\pi\right),$$

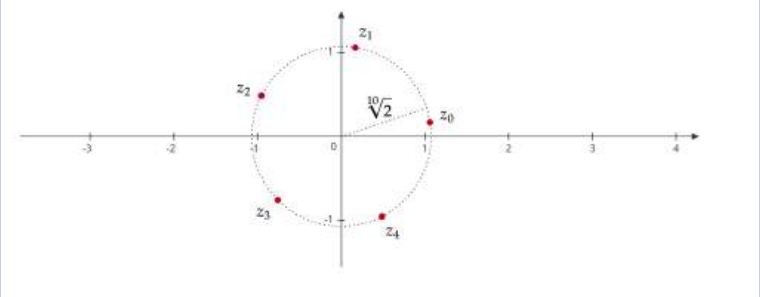
de onde seguem que os argumentos possíveis para z são

$$\begin{aligned}
\theta_0 &= \frac{1}{20}\cdot\pi, \\
\theta_1 &= \frac{1}{20}\cdot\pi + \frac{1}{5}\cdot\pi = \frac{9}{20}\cdot\pi, \\
\theta_2 &= \frac{1}{20}\cdot\pi + \frac{2}{5}\cdot\pi = \frac{17}{20}\cdot\pi, \\
\theta_3 &= \frac{1}{20}\cdot\pi + \frac{3}{5}\cdot\pi = \frac{27}{20}\cdot\pi, \\
\theta_4 &= \frac{1}{20}\cdot\pi + \frac{4}{5}\cdot\pi = \frac{33}{20}\cdot\pi,
\end{aligned}$$

portanto, as soluções são

$$z_i = \sqrt[10]{2}\cos(\theta_i) + \sqrt[10]{2}\sin(\theta_i)\mathbf{i}, \quad i = 0, 1, 2, 3, 4.$$

No plano complexo, estas soluções estão nos pontos indicados.



■

Vamos estudar agora a solução da equação

$$x^2 + z_1 \cdot x + z_2 = 0.$$

Para achar a solução vamos a derivar a bem conhecida fórmula de resolução da equação quadrática (conhecida no Brasil como fórmula de Bhaskara).

Teorema 20.5 — Fórmula quadrática. Considere a função proposicional sobre $\mathbb{C}$ dada por

$$P(x) = \text{"}x^2 + z_1 \cdot x + z_2 = 0\text{"}.$$

Se

$$z_1^2 - 4 \cdot z_2 = \rho \cdot \cos(\theta) + \rho \cdot \sin(\theta)\mathbf{i},$$

Então, seu domínio de verdade é $M = \{x_1, x_2\}$ em que

$$x_1 = \frac{1}{2}[-z_1 + w] \quad \text{e} \quad x_2 = \frac{1}{2}[-z_1 + (-w)],$$

para

$$w = \sqrt{\rho} \cdot \cos\left(\frac{1}{2} \cdot \theta\right) + \sqrt{\rho} \cdot \sin\left(\frac{1}{2} \cdot \theta\right)\mathbf{i}.$$

Demonstração. Comenzamos observando que, pelo corolário 20.3 existe um $w \in \mathbb{C}$ tal que w e $-w$ são solução de

$$y^2 = z_1^2 - 4 \cdot z_2.$$

Mais ainda, observamos que se

$$z_1^2 - 4 \cdot z_2 = \rho \cdot \cos(\theta) + \rho \cdot \sin(\theta)\mathbf{i},$$

então, pelo visto acima, temos que

$$w = \sqrt{\rho} \cdot \cos\left(\frac{1}{2} \cdot \theta\right) + \sqrt{\rho} \cdot \sin\left(\frac{1}{2} \cdot \theta\right)\mathbf{i}$$

Agora, manipulando a equação temos

$$\begin{aligned} x^2 + z_1 \cdot x + z_2 = 0 &\Leftrightarrow x^2 + z_1 \cdot x + \frac{1}{4} \cdot z_1^2 = -z_2 + \frac{1}{4} \cdot z_1^2 \\ &\Leftrightarrow 4 \cdot x^2 + 4z_1 \cdot x + z_1^2 = z_1^2 - 4 \cdot z_2 \\ &\Leftrightarrow (2 \cdot x + z_1)^2 = z_1^2 - 4 \cdot z_2. \end{aligned}$$

portanto

$$2\cdot x+z_1=w \quad \text{ou} \quad 2\cdot x+z_1=-w$$

de onde, as soluções x_1, x_2 da equação

$$x^2+z_1\cdot x+z_2=0.$$

são

$$x_1=\frac{1}{2}[-z_1+w] \quad \text{e} \quad x_2=\frac{1}{2}[-z_1+(-w)].$$

■

■ **Exemplo 20.2** Considere a equação

$$x^2+x+1=0$$

calculamos a solução de

$$y^2=1-4\cdot 1=-3$$

que são

$$w=0+\sqrt{3}\mathbf{i} \quad -w=0+(-\sqrt{3})\mathbf{i}$$

Então,

$$x_1=\frac{1}{2}+\frac{1}{2}\cdot\sqrt{3}\mathbf{i} \quad \text{e} \quad x_2=\frac{1}{2}+\frac{1}{2}\cdot(-\sqrt{3})\mathbf{i}$$

são as soluções procuradas. ■

Já vimos como resolver recorrências lineares de ordem 2 no caso em que a equação característica tem raizes reais. Agora, para completar o estudo vemos o caso de recorrências sobre os números reais no caso em que as raizes da equação característica são complexas.

Teorema 20.6 Considere uma sequência $(x_n)_{n\in\mathbb{N}}$ de números reais definida por uma expressão da forma

$$\begin{aligned} x_0 &= a \\ x_1 &= b \\ x_{n+1} &= c_1\cdot x_n+c_2\cdot x_{n-1} \quad \forall\, n\geq 1, \end{aligned}$$

e a equação de segundo grau $R:\ x^2-c_1\cdot x-c_2=0$, que chamamos de equação característica da recorrência. Se R tem duas raizes complexas r_1 e r_2 temos

$$x_n=\alpha\cdot r_1^n+\beta\cdot r_2^n$$

para α, β números complexos que são determinados em função de a e b.

Demonstração. A demonstração é idéntica ao caso real. Primeiramente observamos que se r_1 e r_2 são raizes de R temos que

$$r_1^2=c_1\cdot r_1+c_2 \quad \text{e} \quad r_1^2=c_1\cdot r_1+c_2.$$

Com isto, para $n \geq 2$ temos

$$\begin{aligned} x_n &= \alpha \cdot r_1^n + \beta \cdot r_2^n \\ &= \alpha \cdot r_1^{n-2} \cdot r_1^2 + \beta \cdot r_2^{n-2} \cdot r_2^2 \\ &= \alpha \cdot r_1^{n-2} \cdot (c_1 \cdot r_1 + c_2) + \beta \cdot r_2^{n-2} \cdot (c_1 \cdot r_2 + c_2) \\ &= c_1 \cdot (\alpha \cdot r_1^{n-1} + \beta r_2^{n-1}) + c_2 \cdot (\alpha \cdot r_1^{n-2} + \beta \cdot r_2^{n-2}) \\ &= c_1 \cdot x_{n-1} + c_2 \cdot x_{n-2}. \end{aligned}$$

Agora, o resultado segue da unicidade da solução. Mais ainda

$$a = x_0 = \alpha + \beta \quad \text{e} \quad b = x_1 = \alpha \cdot r_1 + \beta \cdot r_2$$

de onde seque que α e β determinados em função de a e b.

■

Considere uma sequência $(x_n)_{n\in\mathbb{N}}$ de números reais definida por uma expressão da forma

$$\begin{aligned} x_0 &= a \\ x_1 &= b \\ x_{n+1} &= c_1 \cdot x_n + c_2 \cdot x_{n-1} \quad \forall\, n \geq 1, \end{aligned}$$

tal que a equação caracteríctca $R:\ x^2 - c_1 \cdot x - c_2 = 0$, tem duas raizes complexas r_1 e r_2. Então $r_1 \neq r_2$ e

$$x_n = \alpha \cdot r_1^n + \beta \cdot r_2^n.$$

Mais ainda, para achar α e β temos um sistema

$$\left\{ \begin{array}{rcl} \alpha + \beta & = & a \\ \alpha \cdot r_1 + \beta \cdot r_2 & = & b \end{array} \right.$$

que tem por solução

$$\alpha = (b + (-a \cdot r_2) \cdot (r_1 + (-r_2))^{-1} \quad \text{e} \quad \beta = (a \cdot r_1 + (-b)) \cdot (r_1 + (-r_2))^{-1}.$$

Observamos que as raizes devem satisfazer $r_1 = \bar{r_2}$. De fato, como $c_1^2 - 4 \cdot c_1 \in \mathbb{R}$ e $c_1^2 - 4 \cdot c_1 < 0$ para que as raizes sejam complexas, temos que se $w \in \mathbb{C}$ é solução de

$$y^2 = c_1^2 - 4 \cdot c_2 \quad \Rightarrow \quad w = 0 + \sqrt{4 \cdot c_2 - c_1^2}\,\mathbf{i}.$$

de onde

$$r_1 = \frac{1}{2} \cdot \left(c_1 + \sqrt{4 \cdot c_2 - c_1^2}\,\mathbf{i} \right) \quad \text{e} \quad \frac{1}{2} \cdot \left(c_1 - \sqrt{4 \cdot c_2 - c_1^2}\,\mathbf{i} \right)$$

e $r_1 = \overline{r_2}$. Então, podemos escrever

$$r_1 = \rho \cdot \cos(\theta) + \rho \cdot \sin(\theta)\mathbf{i}$$

$$r_2 = \rho \cdot \cos(\theta) - \rho \cdot \sin(\theta)\mathbf{i}$$

e

$$\begin{aligned} x_n &= \alpha \cdot r_1^n + \beta \cdot r_2^n \\ &= (\alpha + \beta) \cdot \rho^n \cdot \cos(n \cdot \theta) + (\alpha - \beta) \cdot \rho^n \cdot \sin(n \cdot \theta)\mathbf{i}. \end{aligned}$$

para α e β números complexos que dependem de a e b.

■ **Exemplo 20.3** Considere a sequência $(x_n)_{n\in\mathbb{N}}$ de números reais definida pela expressão

$$\begin{aligned} x_0 &= 1 \\ x_1 &= 2 \\ x_{n+1} &= x_n - x_{n-1} \quad \forall\, n \geq 1, \end{aligned}$$

então, a equação característica é $x^2 - x + 1 = 0$ que tem por raizes

$$r_1 = \frac{1}{2} + \frac{1}{2}\sqrt{3}\mathbf{i},$$

$$r_2 = \frac{1}{2} - \frac{1}{2}\sqrt{3}\mathbf{i}.$$

Então

$$x_n = \alpha \cdot r_1^n + \beta \cdot r_2^n$$

Como

$$1 = x_0 = \alpha + \beta \quad e \quad 2 = x_1 = \alpha \cdot r_1 + \beta \cdot r_2$$

temos

$$\alpha = r_2 \quad \text{e} \quad \beta = r_1.$$

Utilizando que

$$r_1 \cdot r_2 = \left(\frac{1}{4} + \frac{3}{4}\right) + 0\mathbf{i} = 1 + 0\mathbf{i},$$

e que

$$r_1 = \cos\left(\frac{1}{3}\cdot\pi\right) + \sin\left(\frac{1}{3}\cdot\pi\right)\mathbf{i},$$

$$r_2 = \cos\left(\frac{1}{3}\cdot\pi\right) - \sin\left(\frac{1}{3}\cdot\pi\right)\mathbf{i},$$

temos

$$\begin{aligned} x_n &= r_1^{n-1} + r_2^{n-1} \\ &= \left(\cos\left(\frac{n-1}{3}\cdot\pi\right) + \sin\left(\frac{n-1}{3}\cdot\pi\right)\mathbf{i} + \cos\left(\frac{n-1}{3}\cdot\pi\right) - \sin\left(\frac{n-1}{3}\cdot\pi\right)\mathbf{i}\right) \\ &= 2\cdot\cos\left(\frac{n-1}{3}\cdot\pi\right) + 0\mathbf{i}. \end{aligned}$$

De onde segue que

$$x_n = 2\cdot\cos\left(\frac{n-1}{3}\cdot\pi\right) \quad \forall\, n \in \mathbb{N}.$$

■

III

Introdução à Análise combinatória

Em elaboração

21. Introdução à Análise combinatória

Neste capítulo vamos estudar a contagem de elementos de um conjuntos sob alguma hipótese ou condição. Em particular, daremos atenção ao problema do número de formas de alocar objetos em compartimentos sob hipóteses nos mesmos.

O primeiro resultado que estudamos e como contar o número de elementos que pertencem a união de vários conjuntos que não são necessariamente disjuntos. Esse é o conteúdo do seguinte teorema.

Teorema 21.1 — Princípio de inclusão-exclusão. Seja $\{A_1,\ldots,A_n\}$ uma familia de conjuntos finitos. Então

$$\sharp(\cup_{i=1}^n A_i)) = \sum_{i=1}^n \sharp A_i - \sum_{1\le i<j\le n} \sharp(A_i\cap A_j) + \sum_{1\le i<j<k\le n} \sharp(A_i\cap A_j\cap A_k) - \cdots + (-1)^n \sharp(\cap_{i=1}^n A_i)\,.$$

Demonstração. Construimos a função proposicional

$$P(n) = \text{"Dada uma familia de } n \text{ conjuntos finitos } A_1,\ldots,A_n \text{ temos}$$

$$\sharp(\cup_{i=1}^n A_i)) = \sum_{i=1}^n \sharp A_i - \sum_{1\le i<j\le n} \sharp(A_i\cap A_j) + \sum_{1\le i<j<k\le n} \sharp(A_i\cap A_j\cap A_k) - \cdots + (-1)^n \sharp(\cap_{i=1}^n A_i)\,."$$

Seja M o seu domínio de verdade. Observamos que $2\in M$ por causa da identidade

$$\sharp(A\cup B) = \sharp A + \sharp B - \sharp(A\cap B),$$

que vimos quando estudamos cardinalidade de conjuntos.

Assuma que $k\in M$ vejamos que $k+1\in M$. Para isto, consideramos

$$\tilde{A} = \cup_{i=1}^k A_i \quad \text{e} \quad \tilde{B} = A_{k+1}.$$

Então, como

$$\tilde{A}\cap\tilde{B} = \cup_{i=1}^k (A_i\cap A_k)$$

Temos

$$\begin{aligned}
\sharp\tilde{A} &= \sum_{i=1}^{k}\sharp A_i - \sum_{1\le i<j\le k}\sharp(A_i\cap A_j) + \sum_{1\le i<j<l\le k}\sharp(A_i\cap A_j\cap A_l) - \cdots + (-1)^k\sharp\left(\cap_{i=1}^{k}A_i\right)\\
\sharp\tilde{B} &= \sharp A_{k+1}\\
\sharp(\tilde{A}\cap\tilde{B}) &= \sum_{i=1}^{k}\sharp(A_i\cap A_{k+1}) - \sum_{1\le i<j\le k}\sharp(A_i\cap A_j\cap A_{k+1})\\
&\quad + \sum_{1\le i<j<l\le k}\sharp(A_i\cap A_j\cap A_l\cap A_{k+1}) - \cdots + (-1)^k\sharp\left(\cap_{i=1}^{k+1}A_i\right)
\end{aligned}$$

Agora o resultado segue se aplicar identidades acima em

$$\sharp(\tilde{A}\cup\tilde{B}) = \sharp\tilde{A} + \sharp\tilde{B} - \sharp(\tilde{A}\cap\tilde{B}).$$

Portanto $k+1\in M$. De onde $M=\{n\in\mathbb{N},\ n\ge 2\}$. ■

■ **Exemplo 21.1** Sobre um grupo de 70 pessoas sabemos que

- 40 jogam futebol
- 35 jogam tênis
- 15 jogam os dois esportes.

Queremos saber

- Quantas pessoas jogam somente um esporte?.
- Quantas pessoas jogam somente futebol?.
- Quantas pessoas jogam somente tênis?
- Quantas pessoas não jogam nenhum esporte ?.

Sabemos que

$$\sharp F = 40 \quad \sharp T = 35 \quad \sharp(F\cap T) = 15$$

Então o conjunto universo U satisfaz $\sharp U = 70$. Mais ainda

$$\begin{aligned}
\sharp(F\backslash(F\cap T)) &= 40-15=25\\
\sharp(T\backslash(F\cap T)) &= 35-15=20\\
\sharp(F\cup T) &= \sharp F+\sharp T-\sharp(F\cap T) = 40+35-15=60\\
\sharp(U\backslash(F\cup T)) &= 70-60=10.
\end{aligned}$$

- 45 pessoas jogam somente um esporte.
- 25 pessoas jogam somente futebol.
- 20 pessoas jogam somente tênis.
- 10 pessoas não jogam nenhum esporte.

■

Vimos anteriormente que se $A_1,\ldots,A_k$ são conjuntos de cardinalidades $n_1,\ldots,n_k$ respectivamente, então temos que

$$\sharp(A_1\times\cdots\times A_k) = n_1\cdots n_k.$$

então, o número de elementos da forma $(a_1,\ldots,a_k)$ em que $a_i\in A_i$ é $n_1\cdots n_k$.

■ **Exemplo 21.2** De quantas formas podemos formar uma placa de carro sabendo que 4 casas devem ser letras e 3 números?

Se $\mathscr{A}=\{a,b,\ \ldots,z\}$ e $\mathscr{N}=\{0,1,\ldots,9\}$ temos que uma placa de carro será um elemento de

$$\mathscr{N}^3\times\mathscr{A}^4$$

então, como

$$\sharp(\mathscr{N}^3 \times \mathscr{A}^4) = 10^3 \cdot 26^4 = 456.976.000,$$

temos 456.976.000 possibilidades de placas diferentes. ■

■ **Exemplo 21.3** Se queremos acomodar n pessoas ao redor de uma mesa redonda, temos que:

- Como a mesa é redonda então não há uma ordem linear, escolhida uma ordem temos n rotações da mesma que também são possíveis e se identificam com a original. Uma vez escolhida onde se senta a primeira pessoa, temos

  $$(n-1)!$$

  possibilidades de distruibuir as pessoas restantes nos 5 lugares que restam.
- Se, por exemplo, temos 3 homens e 3 mulheres e queremos que eles se sentem intercalados, esolhido o lugar da primeira pessoa, uma mulher, automáticamente temos 2! lugares para as outras mulheres e 3! possibilidades para os homens. Então temos

  $$3! \cdot 2!$$

  possibilidades diferentes.

■

Lembramos que o fatorial é a operação unária que associa a cada número natural $n \in \mathbb{N}$ o número $n!$ da seguinte forma

$$\begin{array}{lll} \text{se } n = 0 & \text{então} & 0! = 1 \\ \text{se } n > 0 & \text{então} & n! = n \cdot (n-1) \cdot (n-2) \cdots 2 \cdot 1. \end{array}$$

Consideremos agora um conjunto A com n elementos, isto é

$$A = \{a_1, \ldots, a_n\}.$$

Definição 21.1 Um arranjo de $r \leq n$ elementos de A é um elemento

$$(a_1, \ldots, a_r) \in A^r$$

de forma tal que $a_i \neq a_j$ sempre que $i \neq j$.

■ **Exemplo 21.4** Se $A = \{a,b,c,d\}$ então

$$(a,a,b) \quad (b,c,b) \quad (c,d,d)$$

não são arranjos de 3 elementos de A. No entanto

$$(a,b,c) \quad (b,a,c) \quad (c,d,a)$$

são arranjos de 3 elementos de A. ■

Teorema 21.2 Seja A um conjunto de n elementos. O número de arranjos de r elementos de A é dado por

$$\frac{n!}{(n-r)!} = n \cdot (n-1) \cdots (n-r+1)$$

Demonstração. Provamos contando as possibilidades. Observamos que se o arranjo for

$$(a_1, \ldots, a_r)$$

temos que a_1 é um elemento qualquer de A. O elemento $a_2 \in A_1 = A\backslash\{a_1\}$ como $\sharp A_1 = n-1$ temos $n-1$ posibilidades para a_2. Agora $a_3 \in A_2 = A\backslash\{a_1,a_2\}$ como $\sharp A_2 = n-2$ temos $n-2$ posibilidades para a_3. Continuando desta forma, temos

$$\sharp(A_1 \times \cdots \times A_r) = n\cdot(n-1)\cdots(n-r+1)$$

possibilidades diferentes de montar o arranjo. O que prova o resultado. ■

Definição 21.2 Seja A um conjunto com n elementos. Uma permutação é um arranjo de n elementos de A.

Com isto, podemos interpretar o fatorial da seguinte forma.

Corolário 21.1 Seja A um conjunto com n elementos. O número de permutações dos elementos de n é $n!$.

Demonstração. Imediato de

$$\frac{n!}{(n-n)!} = \frac{n!}{1} = n!.$$

■

■ **Exemplo 21.5**
- De quantas formas diferentes podemos escolher um presidente, um secretário e um funcionario de um grupo de 9 pessoas? Devemos escolher, sem repetição. Então temos

$$\frac{9!}{6!} = 9\cdot 8\cdot 7,$$

arranjos diferentes.
- De quantas formas diferentes por três bolinhas diferentes entre si em três caixas diferentes? Temos 3! permutações diferentes entre as caixas. Portanto o resultado é 6.

■

Seja $s = (b_1,\ldots,b_r) \in A^r$ um elemento em que cada elemento $a_i \in A$ aparece r_i vezes em s (sendo permitido o caso $r_i = 0$), isto é

$$r_1 + \ldots + r_n = r.$$

Queremos saber quantos elementos diferentes podemos construir desta forma ou, dito de outra forma, o número de permutações distinguíveis de dos elementos de s.

■ **Exemplo 21.6** Considere $s = (A,B,C,B,C,B)$ queremos ver as possíveis permutações distinguíveis deste objeto.

Como são 6 elementos temos $6! = 720$ permutações. No entanto se trocarmos, por exemplo o elemento da posição 2 com o da posição 4 temos o mesmo objeto, portanto a permutação não é distinguível.

Começamos com a letra A. Ela só aparece 1 vez e portanto temos que qualquer permutação que troque A de lugar será distinguíveis. Portanto há

$$\frac{720}{1!}$$

permutações em que as letras B,C podem aparecer em locais diferentes.

A letra B se repite 3 vezes. Então cada palavra conta 3! permutações que não producem nenhum efeito pois só alteram a posição da letra B. Dividimos então as 720 permutações em 3! permutações que não alteram o lugar onde aparece a letra B e temos

$$\frac{720}{3!} = 120$$

grupos de permutações na qual C pode aparecer em lugares diferentes .

A letra C aparece 2 vezes, portanto dividimos estes 120 grupos pelas 2! permutações não váo alterar a posição da letra C e obtemos o conjunto de todas permutações diferentes entre si. Obtemos assim que, das 720 permutações originais, somente

$$\frac{120}{2!} = 60,$$

vão ser distinguíveis entre si. ■

Generalizamos isto no próximo resultado.

Teorema 21.3 Seja $s = (b_1, \ldots, b_r) \in A^r$ um elemento em que cada elemento $a_i \in A$ aparece r_i vezes em s (sendo permitido o caso $r_i = 0$), isto é

$$r_1 + \cdots + r_n = r.$$

o número de permutações distinguíveis de s é

$$\frac{r!}{r_1! \cdots r_n!}$$

Demonstração. Observamos que se s possui r elementos então temos $r!$ permutações possíveis. O elemento a_1 vai se repetir r_1 vezes, portanto podemos organizar as permutações em

$$\frac{r!}{r_1!}$$

conjuntos diferentes, que são todas as permutações obtidas de permutar todas as outras entradas diferentes de a_1. Da mesma forma procedemos com a_2, ele vai aparecer m_2 vezes. Então organizamos $\frac{r!}{r_1!}$ permutações em

$$\frac{r!}{r_1! \cdot r_2!}$$

conjuntos diferentes, que são todas as permutações obtidas de permutar todas as outras entradas diferentes de a_1 e a_2. Continuando o processo desta forma temos o resultado depois de n passos. ■

Definição 21.3 Seja A um conjunto de n elementos e $m \in \mathbb{N}$ com $m \leq n$. Uma $m-$combinação de A é um subconjunto de m elementos de A

Teorema 21.4 Seja A um conjunto de n elementos e $m \in \mathbb{N}$ com $m \leq n$. O número de m combinações de A é dado por

$$\frac{n!}{m! \cdot (n-m)!}$$

Este valor recebe o nome de número combinatorio m de n e é denotado por

$$\binom{n}{m} = \frac{n!}{m! \cdot (n-m)!}.$$

Demonstração. Primeiramente observamos que temos

$$\frac{n!}{(n-m)!}$$

arranjos de m elementos possíveis. Cada arranjo dá origem a um conjunto ao fazer

$$(a_{i_1}, \ldots, a_{i_m}) \to \{a_{i_1}, \ldots, a_{i_m}\}.$$

Observamos que dois arranjos diferentes, e que sejam um permutação da posição dos elementos do outro, dão lugar ao mesmo subconjunto. Por exemplo, os arranjos

$$(a_{i_1}, a_{i_2}, \ldots, a_{i_m}) \quad \text{e} \quad (a_{i_2}, a_{i_1}, \ldots, a_{i_m})$$

são diferentes, porém dão lugar ao mesmo subconjunto

$$\{a_{i_1}, \ldots, a_{i_m}\}.$$

De fato temos como cada arranjo tem m elementos todos distintos entre si, temos

$$\frac{m!}{1! \cdot 1! \cdots 1!} = m!$$

arranjos dos mesmos elementos que dão origem ao mesmo conjunto.

Portanto, temos que dividir a quantidade de arranjos pelas $m!$ permutações dos seus elementos de onde segue que há

$$\frac{n!}{(n-m)! \cdot m!}$$

combinações possíveis. ■

■ **Exemplo 21.7** Vamos contar o número de contrasenhas possíveis de 8 entradas das quais uma deve ser uma letra maiúscula, uma deve ser um número e o restante são letras minúsculas.

Temos $26 \cdot 10$ (26 letras e 10 números) formas de escolher a letra maiúscula e o número.

Devemos escolher 6 lugares de 8 que devemos preencher com as 26 letras do alfabeto. Temos assim

$$(26 \cdot 10) \cdot \binom{8}{6} \cdot 26^6 = 4,497813699 \cdot 10^{12}.$$

possibilidades de contrasenhas. Se conseguirmos testar 100 contrasenhas por segundo, para testar todas as possibilidades vamos a demorar

$$\frac{4,497813699 \cdot 10^{12}}{(365 \cdot 24 \cdot 60 \cdot 60) \cdot 100} \simeq 1426 \text{ anos.}$$

■

Algumas propriedades da combinatoria são

Lema 21.1 Sejam $0 \leq m \leq n$ números naturais. Então

- $\binom{n}{m} = \binom{n}{n-m}$ e em particular $\binom{n}{1} = \binom{n}{n-1} = n$
- $\binom{n}{k} = \begin{cases} \binom{n}{k-1}\frac{n-k+1}{k} & \text{se } k > 1 \\ \binom{n-1}{k}\frac{n}{n-k} & \text{se } k < n \\ \binom{n-1}{k-1}\frac{n}{k} & \text{se } n,k > 1 \end{cases}$.

Demonstração.

- Da definição temos

$$\begin{aligned} \binom{n}{m} &= \frac{n!}{(n-m)! \cdot m!} \\ &= \frac{n!}{(n-m)! \cdot (n-(n-m))!} \\ &= \binom{n}{n-m} \end{aligned}$$

Em particular

$$\binom{n}{1} = \binom{n}{n-1} = \frac{n!}{(n-1)! \cdot 1!} = n.$$

- Mostramos cada caso por separado. Se $k > 1$ temos

$$\begin{aligned}\binom{n}{k-1}\frac{n-k+1}{k} &= \frac{n!}{(k-1)!\cdot(n-k+1))!}\cdot\frac{n-k+1}{k}\\ &= \frac{n!}{k!\cdot(n-k))!} = \binom{n}{k}.\end{aligned}$$

Se $k < n$

$$\begin{aligned}\binom{n-1}{k}\frac{n}{n-k} &= \frac{(n-1)!}{k!\cdot(n-k-1)!}\cdot\frac{n}{n-k}\\ &= \frac{n!}{k!\cdot(n-k))!} = \binom{n}{k}.\end{aligned}$$

E por último, se $n,\ k > 1$ temos

$$\begin{aligned}\binom{n-1}{k-1}\frac{n}{k} &= \frac{(n-1)!}{k-1!\cdot(n-k)!}\cdot\frac{n}{k}\\ &= \frac{n!}{k!\cdot(n-k))!} = \binom{n}{k}.\end{aligned}$$

■

■ **Exemplo 21.8** • De quantas formas diferentes podemos seleccionar 4 pessoas de um conjunto de 8? Como os conjuntos não são ordenados, o problema é o mesmo que procurar a quantidade de subconjuntos de 4 elementos de um conjunto de 8 elementos. Temos assim

$$\binom{8}{4} = \frac{8!}{4!\cdot 4!} = \frac{8\cdot 7\cdot 6\cdot 5}{4\cdot 3\cdot 2\cdot 1} = 70$$

formas diferentes.

- De um grupo de 11 pessoas, das quais são 6 mulheres e 5 homens. De quantas formas podemos formar uma comissão 6 pessoas de forma tal que 4 sejam mulheres e 2 homens. Observamos que as mulheres podem ser seleccionadas de

$$\binom{6}{4} = \frac{6!}{2!\cdot 4!} = 15$$

formas diferentes. Já os homens de

$$\binom{5}{2} = \frac{5!}{2!\cdot 3!} = 10$$

Então temos $15\cdot 10 = 150$ formas diferentes de formar a comissão.

- De quantas formas diferentes podemos escolher os números da Mega-Sena?
Devemos escolher um subconjunto de 6 números de um conjunto de 60 números distintos, portanto temos

$$\binom{60}{6} = \frac{60!}{6!\cdot 54!} = 50.063.860$$

escolhas diferentes.
Observe que se você pegar 962766 baralhos de poker. Cada baralho tem aproximadamente 2,5cm de altura, portanto isso dá uma torre de pouco mais de 24 km de altura. Agora, se juntamos todos eles e marcamos uma carta com seu nome. Observe que estaria marcando uma carta em

$$52\cdot 962766 = 50063832 \text{ cartas.}$$

Ou seja, você tem mais chance de escolher uma dessas cartas e pegar aquela que foi marcada do que acertar em um bilhete da Mega-Sena (o exemplo foi adaptado de um trecho pego do livro "Five-Minute Mathematics, Ehrhard Behrends).

■

■ **Exemplo 21.9** Considere um baralho de 52 cartas estândar para o jogo de poker. Em cada mão recebe 5 cartas.

- Na primeira mão recebemos um subconjunto de 5 cartas de um total de 52 distintas, portanto temos

$$T = \binom{52}{5} = 2.598.960$$

possibilidades diferentes para a mão.

- Se queremos que, por exemplo, dessas 5 cartas, nenhuma seja de ouro então temos que escolher essas 5 cartas de um conjunto $52 - 13 = 39$ cartas (que são o conjunto total menos as cartas que são ouro) no total, portanto há

$$= \binom{39}{5} = 575.757$$

possibilidades diferentes de receber 5 cartas e que nenhuma delas seja ouro.

Observamos que o número de possiblidades de receber 5 cartas é a soma das possibilidades em que nenhuma seja ouro, nenhuma seja espada, nenhuma seja copas e nenhuma bastos.

Portanto, a quantidade de possibilidades de que, pelo menos uma, das cartas da mão seja de ouro é subtrair ao número total as possibilidades de que nenhuma seja ouro, isto é

$$2.598.960 - 575.757 = 2.023.203,$$

possibilidades. ■

■ **Exemplo 21.10** Se temos uma turma de 20 alunos dos quais 11 são mulheres e 9 homens. Podemos:

- escolher 3 estudantes de $\binom{20}{2}$ formas diferentes.
- escolher 3 estudantes mulheres de $\binom{11}{3}$ formas diferentes.
- escolher 3 estudantes dos quais 1 é um homem, de $\binom{11}{2} \cdot \binom{9}{1}$ formas diferentes.
- escolher 3 estudantes dos quais ao menos 1 é um homem de

$$\overbrace{\binom{20}{3}}^{\text{total}} - \overbrace{\binom{11}{3}}^{\text{só mulheres}}$$

formas diferentes.

■

■ **Exemplo 21.11** Sejam A e B dois conjuntos finitos de cardinalidade $\sharp A = n$ e $\sharp B = m$. Então , podemos assumir que

$$A = \{a_1, \ldots, a_n\} \quad \text{e} \quad B = \{b_1, \ldots, b_m\}$$

- O número de funções bijetoras de A em A é $n!$. De fato cada função bijetora associa biunívocamente os elementos de A. Assim se $f : A \to A$ é bijetora, temos

$$\begin{aligned}
f(a_1) &= a_{i_1} \quad (n \text{ possibilidades}) \\
f(a_2) &= a_{i_2} \in A \backslash \{a_{i_1}\} \quad (n-1 \text{ possibilidades}) \\
f(a_3) &= a_{i_3} \in A \backslash \{a_{i_1}, a_{i_2}\} \quad (n-2 \text{ possibilidades}) \\
&\vdots \qquad\qquad \vdots \\
f(a_n) &= a_{i_n} \in A \backslash \{a_{i_1}, a_{i_2}, \ldots, a_{n-1}\} \quad (1 \text{ possibilidade})
\end{aligned}$$

De onde temos que são $n!$ possibilidades para escolha da função f.

- Assumindo que $n \leq m$ podemos ver que o número de funções injetoras $f : A \to B$ é

$$\frac{m!}{(m-n)!}$$

De fato

$$\begin{aligned} f(a_1) &= b_{i_1} \quad (m \text{ possibilidades}) \\ f(a_2) &= b_{i_2} \in A \backslash \{b_{i_1}\} \quad (n-1 \text{ possibilidades}) \\ f(a_3) &= b_{i_3} \in A \backslash \{b_{i_1}, b_{i_2}\} \quad (n-2 \text{ possibilidades}) \\ &\vdots \qquad\quad \vdots \\ f(a_n) &= b_{i_n} \in A \backslash \{b_{i_1}, b_{i_2}, \ldots, b_{n-1}\} \quad (m-(n-1)) \text{ possibilidades}) \end{aligned}$$

de onde temos

$$m \cdot (m-1) \cdots (m-n+1) = \frac{m!}{(m-n)!}$$

possibilidades de escolhas para a função f.

- Se $n \geq m$ podemos ver que o número de funções sobrejetoras $f : A \to B$ é

$$\sum_{k=0}^{m-1} (-1)^k \cdot \binom{m}{k} \cdot (m-k)^n.$$

Podemos chegar a este resultado utilizando o princípio de inclussão-exclussão. A ideia é fazer o número total de funções menos o número de funções que não são sobrejetoras, isto é

$$m^n - \sharp(\cup_{j=1}^{m} A_j)$$

em que

$$A_j = \{f : A \to B,\ b_j \notin f(A)\}.$$

Como

$$\sum_{1 \leq j_1 \leq \cdots \leq j_k \leq m} \sharp(A_{j_1} \cap \cdots \cap A_{j_k}) = \binom{m}{k} \cdot (m-k)^n,$$

pois estamos contanto as diferentes escolhas de k elementos de B que não vaõ ser atingidos pelo número de funções que vão dos n elementos de A nos $(m-k)$ elementos restantes.
Temos, utilizando o princípio de inclussão-exclussão, que existem

$$\sum_{k=0}^{m-1} (-1)^k \cdot \binom{m}{k} \cdot (m-k)^n.$$

funções sobrejetoras.
Cada função sobrejetora $f : A \to B$ vai produzir uma partição

$$A_1 = f^{-1}(b_1), \ldots, A_m = f^{-1}(b_m)$$

de A. Assim, contar o número de funções sobrejetoras está relacionado a contar número de partições de A com m conjuntos. Para cada partição deste tipo, haverá $m!$ funções sobrejetoras que a geram obtidas de permitar os valores b_i que estão na imagem do conjunto A_j. Assim, o número de partições é

$$S(n,m) = \frac{1}{m!} \sum_{k=0}^{m-1} (-1)^k \cdot \binom{m}{k} \cdot (m-k)^n.$$

chamado de *Número de Stirling de segundo tipo* e é denotado por $S(n,m)$.
O leitor pode consultar ou trabalho de Fahd and Gulf, *Classroom note: An inductive derivation of Stirling numbers of the second kind and their applications in statistics*, Journal of Applied Mathematics and Decision Sciences (1997) para mais detalhes sobre o assunto.

Teorema 21.5 • O número de maneiras de distribuirmos n objetos distintos em $m < n$ compartimentos distintos é m^n.

- O número de maneiras de distribuirmos n objetos distintos em $m \geq n$ compartimentos distintos de forma que tenhamos em cada um, no máximo, um objeto é

$$\frac{m!}{n!}.$$

- O número de maneiras de distribuirmos n objetos distintos em $m \geq n$ compartimentos iguais de forma que tenhamos em cada um, no máximo, um objeto é

$$\binom{m}{n} = \frac{m!}{n!(m-n)!}.$$

- O número de maneiras de distribuirmos n objetos iguais em $m < n$ compartimentos distintos é

$$\binom{n+m-1}{n}.$$

- O número de maneiras de distribuirmos n objetos distintos em $m < n$ compartimentos distintos sem que nenhum fique vazio é

$$\sum_{k=0}^{m-1} (-1)^k \cdot \binom{m}{k} \cdot (m-k)^n.$$

- O número de maneiras de distribuirmos n objetos iguais em $m < n$ compartimentos distintos sem que nenhum fique vazio é

$$\binom{n-1}{m-1}.$$

- O número de maneiras de distribuirmos n objetos distintos em $m < n$ compartimentos iguais sem que nenhum fique vazio é

$$S(n,m) = \frac{1}{m!} \sum_{k=0}^{m-1} (-1)^k \cdot \binom{m}{k} \cdot (m-k)^n.$$

- O número de maneiras de distribuirmos n objetos distintos em m compartimentos iguais de forma que tenhamos em cada um, no máximo, um objeto é

$$\begin{cases} 0 & \text{se} \quad n > m \\ 1 & \text{se} \quad n \leq m \end{cases}$$

- O número de maneiras de distribuirmos n objetos distintos em $m < n$ compartimentos iguais é

$$\sum_{k=1}^{m} S(n,k).$$

Demonstração. • O primeiro é o número de funções de um conjunto com n elementos em um conjunto com m elementos.

- O número de maneiras de distribuirmos n objetos distintos em $m \geq n$ compartimentos distintos de forma que tenhamos em cada um, no máximo, um objeto é igual a contar o número de funções injetoras de um conjunto com n elementos em outro de m elementos. Portanto temos

$$\frac{m!}{n!}$$

possibilidades.

- O número de maneiras de distribuirmos n objetos distintos em $m \geq n$ compartimentos iguais de forma que tenhamos em cada um, no máximo, um objeto é o mesmo que contar o número de subconjuntos de m elementos de um conjunto com n elementos. Isto é contar o número de arranjos de m objetos e fazer o quociente pelas permutações dos seus elementos, ou seja, o número de combinações. De onde segue que temos

$$\binom{m}{n}$$

- Para achar o número de maneiras de distribuirmos n objetos iguais em $m < n$ compartimentos distintos com, no máximo o objeto por compartimento observamos que existem distribuições indistingíveis por causa dos objetos serem iguais. Assim temos que se x_i é o número de objetos no compartimento i temos

$$x_1 + \cdots + x_m = n.$$

Então procuramos o número de soluções não negativas desta equação. Isto é equivalente a escolher n objetos entre $m+n-1$ símbolos formados por n estrelas e $m-1$ barras. Aqui as estrelas são os objetos e as barras o que delimitam os compartimentos. Por exemplo para $n = 8$ e $m = 4$ um caso seria.

$$\star\star\star|\star\star|\star|\star\star.$$

Assim o número destes arranjos é igual a $\binom{m+n-1}{n}$.

- O número de maneiras de distribuirmos n objetos distintos em $m < n$ compartimentos distintos sem que nenhum fique vazio é igual ao número obtido de contar o número de funções sobrejetoras de um conjunto de n elementos em um conjunto de n elementos.
- Para obter o número de maneiras de distribuirmos n objetos iguais em $m < n$ compartimentos distintos observamos que primeiramente devemos colocar um objeto em cada compartimento logo, os $n-m$ restante devem ser distribuídos novamente nos m compartimentos distintos que é

$$\binom{m+(n-m)-1}{n-m} = \binom{n-1}{n-m} = \binom{n-1}{m-1}.$$

- O número de maneiras de distribuirmos n objetos distintos em $m < n$ compartimentos iguais sem que nenhum fique vazio é igual ao número obtido ao contar o número obtido para compartimentos distintos e dividir pelas $m!$ possibilidades de escolhas de ordem das caixas (visto que são todas iguais).
- O número de maneiras de distribuirmos n objetos distintos em m compartimentos iguais de forma que tenhamos em cada um, no máximo, um objeto é 0 se $n > m$ pois, necessárimante uma vez preenchidos os m sobram objetos que devem ser colocados em algum dos compartimentos já preenchidos.
  No caso em que $n \leq m$ colocamos um objeto em cada compartimento, podendo sobrar compartimentos. Como os compartimentos são iguais, qualquer outra distribuição é equivalente a primeira (pios é uma permutação da mesma), então existe uma única forma neste caso.
- Aqui, novamente utilizamos o princípio de inclussão-exclussão para

$$A_k = \{\text{maneiras de distribuirmos } n \text{ objetos distintos em } k \leq m \text{ compartimentos iguais sem que nenhum fique vazio}\}$$

e observando que, neste caso as interseções $A_i \cap A_j = \emptyset$ para $i \neq j$ pois se, por exemplo, $i < j$ temos que uma maneira de distribuir n objetos em j compartimentos sem que nenhum fique vazio nunca pode ser uma maneira de distribuir n objetos em i compartimentos sem que nenhum fique vazio, pois necessáriamente teremos um número menor que n bolas nos i compartimentos.
O número de maneiras de distribuirmos n objetos distintos em $m < n$ compartimentos iguais é então igual à soma é a soma

$$\sum_{k=1}^{m} \sharp A_k$$

isto é, ao número obtido de somar número de maneiras de distribuirmos n objetos distintos em $k \leq m < n$ compartimentos iguais sem que nenhum fique vazio de $k = 1$ até m. Obtendo assim o resultado.

■

Só resta, na análise do resultado acima, o caso de distribuir objetos iguais em compartimentos iguais.

Começamos por estudar o caso de distribuir n objetos iguais em m compartimentos iguais sem que nehum fique vazio. Em geral esse número é denotado por

$$P(n,m),$$

e satisfaz uma relação de recorrência que passamos a descrever.

O número $P(n,m)$ é a soma das distribuições a seguir

- o caso em que existe um compartimento com um objeto só, e distribuimos os objetos restantes nos $m-1$ compartimentos restantes, que dá $P(n-1,m-1)$ possibilidades.
- o caso em que todas os compartimentos tem mais do que um objeto (pois como cada compartimento tem como mínimo um objeto, contamos o objeto a mais como sendo já distruibuído) . Neste caso, temos $n-m$ objetos a serem distribuídos em m compartimentos. Temos assim $P(n-m,m)$possibilidades.

Temos assim que

$$P(n,m) = P(n-1,m-1) + P(n-m,m),$$

que é a relação de recorrência procurada. Agora devemos achar os primeiros termos da recorrência. Logo o princípio da recursão nos garante a unicidade dos termos.

Observamos que, da definição, temos que para todo $n \geq 1$ temos

- $P(n,1) = 1$, pois a única possibilidade é colocar todos os objetos no único compartimento disponível.
- $P(n,n) = 1$, pois a única distribuição é uma bola em cada compartimento.
- $P(n,m) = 0$ para $m > n$, pois necesáriamente um compartimento ficará vazio.
- $P(n+1,n) = 1$, pois preenchemos primeiramente todos os compartimentos com um objeto e depois fica um objeto a distribuir a um dos n compartimentos. Temos n posibilidades de distibuição, mas como todos os compartimentos são iguais, estas n distribuições são indistinguíveis entre si e, portanto, são todas equivalentes. De onde segue que temos uma distribuição só.

Com isto, junto a relação de recorrência

$$P(n,m) = P(n-1,m-1) + P(n-m,m),$$

podemos achar todos os valores $P(n,m)$. Escrevemos alguns dos valores na tabela abaixo.

m	1	2	3	4	5	6	7	8	9	10
$n=1$	1	0	0	0	0	0	0	0	0	0
$n=2$	1	1	0	0	0	0	0	0	0	0
$n=3$	1	1	1	0	0	0	0	0	0	0
$n=4$	1	2	1	1	0	0	0	0	0	0
$n=5$	1	2	2	1	1	0	0	0	0	0
$n=6$	1	3	3	2	1	1	0	0	0	0
$n=7$	1	3	4	3	2	1	1	0	0	0
$n=8$	1	4	5	5	3	2	1	1	0	0
$n=9$	1	4	7	6	5	3	2	1	1	0
$n=10$	1	5	8	9	7	5	3	2	1	1

Por último, para obter a forma de distribuir n objetos iguais em m compartimentos iguais utilizamos o princípio de inclussão-exclussão para

$$\begin{aligned} A_k \quad = \quad & \{\text{maneiras de distribuirmos } n \text{ objetos iguais em} \\ & \qquad k \leq m \text{ compartimentos iguais sem que nenhum fique vazio}\} \end{aligned}$$

e observandos que, neste caso as interseções $A_i \cap A_j = \emptyset$ para $i \neq j$ pois se, por exemplo, $i < j$ temos que uma maneira de distribuir n objetos em j compartimentos sem que nenhum fique vazio nunca pode ser uma maneira de distribuir n objetos em i compartimentos sem que nenhum fique vazio, pois necessáriamente teremos um número menor que n bolas nos i compartimentos.

Portanto, forma de distribuir n objetos iguais em m compartimentos iguais é a soma

$$\sum_{k=1}^{m} \sharp A_k$$

isto é, a soma da possibilidade de distribuir em todos sem que nenhum fique vazio, com a de distribuir $m-1$ compartimentos sem que nenhum fique vazio, e assim seguindo. Chegamos então a

$$\sum_{k=1}^{m} P(n,k) \quad \text{possibilidades.}$$

■