Um conceito fundamental em matemática discreta é o de conjunto. **Conjunto** é uma coleção (agrupamento) de objetos **distintos** (não repetidos) e **não ordenados**. Os objetos de um conjunto são chamados de **elementos**. Os elementos de um conjunto podem ser objetos do mesmo tipo (que apresentam uma mesma característica ou natureza), ou seja, serem conjuntos formados apenas por números, funções, figuras geométricas, etc., ou ainda, de tipos diferentes. Um conjunto é representado, geralmente, por uma letra maiúscula, com seus elementos (representados por letras minúsculas) colocados entre chaves, { }, separados por vírgula: $M = \{m_1, m_2,..., m_i,...\}$.

Se um elemento m pertence a um conjunto M, dizemos que $m \in M$, caso contrário, $m \notin M$. Os símbolos "$\in$" e "$\notin$" significam "pertence a..." e "não pertence a..." respectivamente. O símbolo "$\in$" origina-se da estilização da primeira letra da palavra grega $\epsilon\sigma\tau\iota$ (ser, estar)

Um conjunto que possui um número finito de elementos, ou seja, $M = \{m_1, m_2,..., m_i,..., m_n\}$, é chamado de **conjunto finito**; por outro lado, se apresenta um número infinitos elementos, é chamado de **conjunto infinito**. Um conjunto que não apresenta elementos é chamado de **conjunto vazio** sendo representado pelo símbolo $\varnothing$ ou chaves sem conteúdo { }: $M = \varnothing$ ou $M = \{\ \}$. Dois conjuntos são **iguais** se possuírem os mesmos elementos. O número de elementos n de um conjunto finito M é representado por $|M|$ e será chamado de **potência** do conjunto M.

Um conjunto pode ser definido completamente por três formas: **por extensão total** ou **simplesmente extensão** (conjuntos finitos), onde são listados todos os seus elementos: $M = \{m_1, m_2,..., m_i,..., m_n\}$; por **extensão parcial** (conjuntos finitos e infinitos), onde apenas parte de seus elementos são listados, quando está evidente que tipo de elementos o conjunto é formado; e **por compreensão** (conjuntos finitos e infinitos), onde são definidas suas propriedades. A representação por compreensão geralmente tem a seguinte forma: $M = \{m \ / \ P(m)\}$, onde o símbolo "/" significa "tal que" e $P(m)$ representa determinada propriedade de m. Quando desejamos deixar claro que além de m apresentar determinada propriedade, também pertence a um conjunto mais geral A (ou seja, de maneira informal, m é certo "tipo" de objeto matemático) utilizamos a notação por compreensão $M = \{m \in A \ / \ P(m)\}$.

Exemplo:
a) Os conjuntos $A = \{1, 2, 3, 4\}$ e $B = \{1, 3, 2, 4\}$ são iguais (a ordem dos elementos não é relevante) e ambos são conjuntos finitos com potência igual a 4 (4 elementos);
b) Os conjuntos $D = \{a, b, c\}$ e $E = \{a, a, b, c, c\}$ são iguais (pois a repetição não é relevante) e ambos são conjuntos finitos com três elementos (potência 3).

Exemplo: Seja $A = \{a, 2, \{1, 4\}, \varnothing\}$. Então, a, 2, $\varnothing$ e $\{1, 4\} \in A$, mas 1 e $4 \notin$ A.

Exemplo: O **conjunto dos números naturais** e o **conjunto dos números inteiros**, que são denotados de forma especial, respectivamente por $\boldsymbol{N}$ e $\boldsymbol{Z}$, são definidos por extensão parcial: $\boldsymbol{N} = \{0, 1, 2, 3, 4,...\}$ e $\mathbf{Z} = \{...,-3, -2, -1, 0, 1, 2, 3,...\}$. Ambos são conjuntos infinitos, não podendo ser definidos por extensão. O conjunto dos números naturais sem o zero, {1, 2, 3, 4,...}, é também denominado de conjunto de inteiros positivos ou simplesmente representado por $\boldsymbol{N^*}$. O zero pode ser considerado ou não um número natural. Esta consideração deve-se a uma conveniência associada a um determinado ramo da Matemática. Por exemplo, em álgebra costuma-se definir o conjunto $\boldsymbol{N}$ com a inclusão do zero, enquanto que em análise matemática, não. A não inclusão do zero nos números naturais muitas vezes também envolve aspectos históricos, já que ele não foi criado para contagem (como os números naturais positivos), aparecendo bem depois dos demais. Aqui adotaremos o zero como um número natural.

Exemplo: O conjunto $A = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$, definido por extensão, pode também ser definido por compreensão $A = \{x \in \boldsymbol{N} \ / \ 0 \leq x \leq 9\}$ ou ainda por extensão parcial $A = \{0, 1, 2,...,$

9}. Este é o conjunto dos símbolos (chamados algarismos) utilizados no sistema de numeração decimal, um sistema de base 10 (utiliza 10 algarismos diferentes) para representar todos os números. É um sistema posicional, ou seja, a posição do algarismo no número modifica o seu valor. A palavra "algarismo" tem sua origem no nome do famoso matemático, astrônomo, astrólogo, geógrafo e autor persa *Al-Khwarizmi* (780 – 850).

Exemplo: **O conjunto dos números pares** é definido por compreensão como $\{x \in \boldsymbol{Z} \,/\, x = 2a, a \in \boldsymbol{Z}\}$. Também pode ser definido por extensão parcial: {...,-6, -4, -2, 0, 2, 4, 6,...}. Da mesma forma, o **conjunto dos números ímpares** pode ser definido por compreensão como $\{x \in \boldsymbol{Z} \,/\, x = 2b + 1, b \in Z\}$. Também pode ser definido por extensão parcial: {...,-5, -3, -1, 1, 3, 5,...}. Em todos os conjuntos expressos aqui por extensão parcial, fica claro a sua formação.

Exemplo: Podemos definir, por compreensão, o conjunto numérico $\boldsymbol{Q}$ tal que $\boldsymbol{Q} = \{\frac{q}{r} \,/\, q \text{ e } r \neq 0 \in \boldsymbol{Z}\}$, onde $\frac{q}{r}$ é a operação de divisão (ou razão) entre q e r. Tal conjunto é chamado de **conjunto dos números racionais.** Os números racionais podem ser números inteiros, como resultado de uma divisão exata de dois inteiros, ou **números decimais** (ou **fracionários**), como resultado de uma divisão inexata de dois números inteiros, ou seja, números racionais não inteiros expressos por vírgula (vírgula decimal) e que possuem **casas decimais** (os algarismos que vem depois da vírgula decimal). Os números decimais podem ter uma representação decimal exata (sendo chamados de **números decimais exatos**), ou seja, um número finito de algarismos depois da vírgula decimal; ou podem apresentar repetição periódica e infinita de um ou mais algarismos, sendo chamados de **números decimais periódicos** ou **dízimas periódicas**. O algarismo ou algarismos decimais que se repetem infinitamente constituem o **período** dessa dízima. São exemplos de números racionais:

$$\frac{4}{2} = 2 \rightarrow \text{racional inteiro;}$$

$$\frac{-6}{2} = -3 \rightarrow \text{racional inteiro;}$$

$$\frac{1}{2} = 0{,}5 \rightarrow \text{número decimal exato;}$$

$$\frac{3}{2} = 1{,}5 \rightarrow \text{número decimal exato;}$$

$$\frac{1}{6} = 0{,}1\boxed{3}3 \ldots = 0{,}1(3) \rightarrow \text{dízima periódica de período 3;}$$

$$\frac{2}{9} = 0{,}\boxed{2}2 \ldots = 0{,}(2) \rightarrow \text{dízima periódica de período 2;}$$

$$\frac{7}{99} = 0{,}\boxed{07}07 \ldots = 0{,}(07) \rightarrow \text{dízima periódica de período 07;}$$

$$\frac{7}{990} = 0{,}0\boxed{07}07 \ldots = 0{,}0(07) \rightarrow \text{dízima periódica de período 07;}$$

$$\frac{1}{7} = 0{,}\boxed{142857}142857 \ldots = 0{,}(142857) \rightarrow \text{dízima periódica de período } 142857.$$

Exemplo: O conjunto dos números que não podem ser representados por meio da razão de dois inteiros é denominado de **conjunto dos números irracionais *I*** ou ainda **conjunto dos números incomensuráveis**. Os números irracionais são sempre **dízimas não periódicas**, ou seja, são números decimais que não apresentam algarismos ou grupos de algarismos que se repetem periodicamente. São exemplos de números irracionais:

$$\left.\begin{array}{c}\sqrt{2} = 1{,}41421\ldots \\ \sqrt{3} = 1{,}25992\ldots \\ \sqrt{5} = 2{,}23606\ldots \\ \pi(\text{número } pi) = 3{,}14159\ldots \\ e(\text{número de } Euler \text{ ou número de } Napier) = 2{,}71828\ldots \\ \phi(\text{número de ouro ou razão áurea}) = \dfrac{\sqrt{5}+1}{2} = 1{,}61803\ldots\end{array}\right\} \text{dízimas não periódicas}$$

Exemplo: Um conjunto muito importante na matemática (principalmente no ramo da Análise Matemática) é o **conjunto dos números reais *R*** definido por compreensão tal que $\boldsymbol{R} = \{r \,/\, r \in \boldsymbol{Q} \text{ ou } r \in \boldsymbol{I}\}$. O conjunto dos números reais forma um conjunto ordenado, ou seja, para cada par *x* e *y* de números reais, uma e somente uma das relações a seguir é satisfeita:

$$x < y,\ x = y,\ x > y$$

Os números reais podem ser representados geometricamente pelos pontos do **eixo numérico** ou **reta numérica** (Fig. 1.1.1). Chama-se eixo numérico a uma reta infinita sobre a qual se escolheu: 1) um ponto *O* chamado origem; 2) um sentido positivo que se indica por uma seta; e 3) uma unidade de medida. Na maior parte das vezes utilizamos um eixo horizontal e escolhemos a direção da esquerda para direita como sentido positivo. Um número x_1 positivo é representado por um ponto M_1 à direita da origem e distante de *O* por um valor de x_1; e um número x_2 negativo é representado por um ponto M_2 à esquerda da origem, distante de *O* por um valor de $(-x_2)$. O ponto *O* corresponde ao número zero. A cada número real corresponde um único ponto no eixo numérico e a cada ponto do eixo numérico corresponde um único número real.

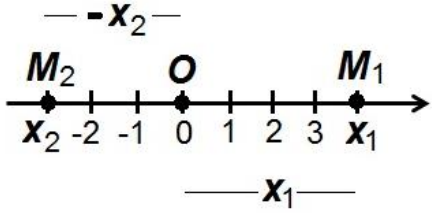

Fig. 1.1.1

A irracionalidade do número de $\sqrt{2}$ foi demonstrada pelo filósofo grego Aristóteles (384 a.C – 322 a.C.). A irracionalidade do número $\boldsymbol{\pi}$ foi demonstrada no século *XVIII* pelo matemático suíço *Johann Heinrich Lambert* (1728 – 1777). O número $\boldsymbol{\pi}$ (denotado pela letra grega *pi*, a partir da palavra grega para perímetro, "περίμετρος") representa a razão entre as medidas da circunferência *C* de um círculo (Fig. 1.1.2) e o seu diâmetro *D* (*D* = 2*r*, onde *r* é o raio do círculo), ou seja,

$$C = 2\pi r, \text{ e assim, } \pi = \frac{C}{2r} = \frac{C}{D}$$

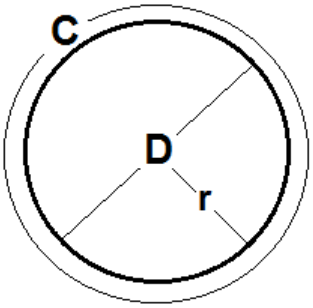

Fig. 1.1.2

A irracionalidade do número ***e*** foi demonstrada pela primeira vez pelo matemático suíço *Leonard Euler* (1707 – 1783) em 1737, sendo conhecido como **número de *Euler***. Esta notação foi escolhida por *Euler* provavelmente por que é a letra inicial da palavra exponencial. Também é denominado **número de *Napier*** (ou ***Neper***) ou ainda como **número neperiano** em homenagem aos trabalhos com logaritmos do matemático, físico e astrônomo escocês *John Napier* (1550 – 1617), conhecido pelo nome, em latim, de *Ioannes Neper*. Sejam b e $x \in \boldsymbol{R}$, com $b > 1$ e $x > 0$. Denominamos o número real y tal que $b^y = x$ de logaritmo de x na base b (representado por $y = \log_b x$). Se $b = e$, então $\log_e x$ é chamado de **logaritmo neperiano** ou **logaritmo natural** de x sendo representado geralmente por $Log\ x$ ou $\ln x$ (Fig. 1.1.3).

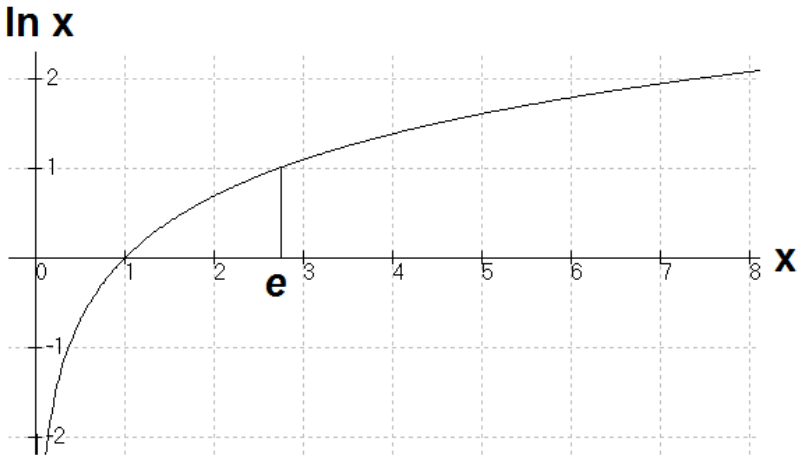

Fig. 1.1.3

O **número de ouro** ϕ (também chamado de **proporção áurea**, **razão áurea**, **seção áurea** ou ainda **proporção de ouro**), denotado pela letra grega ϕ (*Phi*), é definido como o resultado da razão de dois números positivos reais a e b com $a > b$, tal que:

$$\phi = \frac{a}{b} = \frac{a+b}{a}$$

Assim, de $\phi = \frac{a}{b}$ temos que $a = \phi b$ e consequentemente,

$\phi = \dfrac{a+b}{a} = \dfrac{\phi b + b}{\phi b} = \dfrac{b(\phi+1)}{\phi b} = \dfrac{\phi+1}{\phi}$. Daí, multiplicando ambos os lados por ϕ teremos,

$\phi\phi = \left(\dfrac{\phi+1}{\phi}\right)\phi$, obtendo-se $\phi^2 = \phi + 1$ e desta forma, $\phi^2 - \phi - 1 = 0$.

Resolvendo a equação de segundo grau, em busca de suas raízes pela fórmula de Bháskara:

$\phi = \dfrac{-b \pm \sqrt{b^2 - 4ac}}{2a}$, onde $a = 1, b = -1$ e $c = -1$, teremos:

$\phi = \dfrac{-(-1) \pm \sqrt{(-1)^2 - 4(1)(-1)}}{2(1)} = \dfrac{1 \pm \sqrt{1+4}}{2} = \dfrac{1 \pm \sqrt{5}}{2}$. Como a e $b > 0$ então $\phi > 0$.

Logo, $\phi = \frac{1+\sqrt{5}}{2} = 1{,}61803\ldots$ é a única solução positiva. Este é o valor do número de ouro ϕ. O número de ouro também pode se expresso como:

$$\phi = \frac{a}{b} = \frac{a+b}{a} = \frac{a}{a} + \frac{b}{a} = 1 + \frac{b}{a} = \frac{b}{b} + \frac{b}{a}$$

$$\frac{a}{b} = \frac{b}{b} + \frac{b}{a}$$

$$\frac{b}{a} = \frac{a}{b} - \frac{b}{b} = \frac{a-b}{b}$$

Assim,

$$\frac{b}{a} = \frac{a-b}{b}$$

Se $\frac{a}{b} = \phi$, então os números a e b estão em **razão áurea**. Chama-se retângulo áureo ou retângulo de ouro (Fig. 1.1.4), um retângulo ABCD onde os lados a e b estão em razão áurea, com a seguinte propriedade: se o dividirmos em um quadrado e em outro retângulo, o novo retângulo será semelhante ao original (apresentará também a razão áurea entre os lados b e a-b).

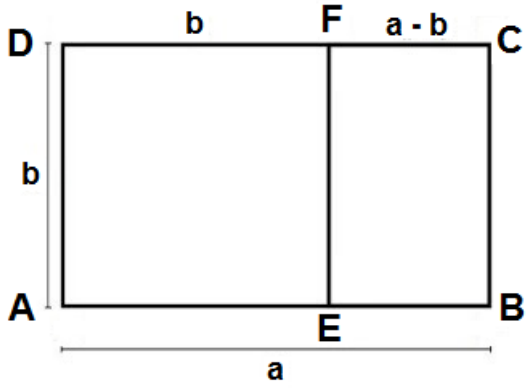

Fig. 1.1.4

O número de ouro é um número irracional conhecido desde a antiguidade. Ele aparece em muitas obras arquitetônicas e artísticas sendo encontrado de forma aproximada na conformação das conchas, dos girassóis, dos cristais, das galáxias, nas proporções do corpo humano (o tamanho das falanges, ossos dos dedos, por exemplo), nas pirâmides e até no famoso quadro a *Mona Lisa*, do cientista, matemático, engenheiro, inventor, anatomista, pintor, escultor, arquiteto, botânico, poeta e músico italiano *Leonardo da Vinci* (1452 – 1519). Está presente em inúmeros outros exemplos que envolvem crescimento na natureza. O escultor e arquiteto grego *Fídias* (que viveu entre 480 a.C. – 430 a.C.), utilizou o número de ouro na construção do *Partenon* (no retângulo da sua fachada), um templo dos deuses gregos, em *Atenas*.

Exemplo: Seja o conjunto $\boldsymbol{R_a}$ definido, por compreensão, de forma que:

$$\boldsymbol{R_a} = \{x \in \boldsymbol{R} / a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0 = 0, \text{com } a_0, a_1, \ldots, a_n \in \boldsymbol{Z}, n \in \boldsymbol{N}^*\}$$

Ou seja, $\boldsymbol{R_a}$ é o conjunto de todos os números reais que são soluções de uma equação polinomial com coeficientes inteiros. Este conjunto é denominado de **conjunto dos números reais algébricos**. Qualquer número racional é um número algébrico, já que para qualquer $\frac{q}{r}$ / q e $r \in \boldsymbol{Z}$, teremos que:

$$r \underbrace{\left(\frac{q}{r}\right)}_{x} - q = 0$$

Números irracionais também podem ser algébricos, já que para $n \in \boldsymbol{N}$:

$$\underbrace{\left(\sqrt{n}\right)^2}_{x^2} - n = 0$$

Se $n = 2$, teremos que:

$$\left(\sqrt{2}\right)^2 - 2 = 2 - 2 = 0$$

e assim, $\sqrt{2}$ (um número irracional) é algébrico. O número de ouro ϕ (irracional) também é algébrico, pois é solução da equação polinomial:

$$\underbrace{\phi^2}_{x^2} - \underbrace{\phi}_{x} - 1 = 0$$

Exemplo: Existem números irracionais que não são algébricos, ou seja, não são soluções de uma equação polinomial com coeficientes inteiros, como os números π, e, e^{π}, $\left(\sqrt{2}\right)^{\sqrt{2}}$, $\left(\sqrt{5}\right)^{\sqrt{7}}$. O conjunto dos números irracionais não algébricos é denominado de **conjunto dos números transcendentes** (ou **transcendentais**). A transcendentalidade de π foi demonstrada em 1882 pelo matemático alemão *Carl Louis Ferdinand von Lindemann* (1852 – 1939) e a do ***e***, pelo matemático francês *Charles Hermite* (1822 – 1901) em 1873.

Exemplo: Outro conjunto que desempenha um papel importante na matemática (principalmente no ramo da Teoria dos Números) é o conjunto dos **números naturais primos** (ou simplesmente **números primos**). Um número natural *p*, maior do que 1, é chamado de número primo somente se for divisível por 1 e por ele mesmo, ou seja, se os únicos números que dividem *p* em partes iguais e inteiras forem 1 e o próprio *p* (que são chamados de divisores de *p*). Então, o conjunto ***P*** dos números primos pode ser definido por compreensão como:

$$\boldsymbol{P} = \{p \in \boldsymbol{N} / p > 1 \text{ e os únicos dividores de } p \text{ são 1 e o próprio } p\}$$

Os números 2, 3, 5, 7, 59 e 359 são exemplos de primos. O número 2 é o único número primo par. O conjunto ***P*** dos números primos é infinito. Um número inteiro positivo maior que um que não seja primo é chamado de **número composto**. Desta forma, um número composto *n* é divisível por outro ou outros números diferentes de 1 e do próprio *n*. Denominamos **números primos entre si** (ou **coprimos**) ao conjunto de números onde o único divisor comum a todos eles é o número 1. Por exemplo, os números naturais 9, 5, 7 e 8 são primos entre si. Uma **fração é irredutível** se o numerador e denominador são números primos entre si. Qualquer número inteiro positivo maior que 1 pode ser expresso de forma única como o produto de números primos (chamados fatores), ou seja, pode ser **fatorado** em números primos. Os números naturais abaixo estão representados fatorados por números primos:

$4 = 2 \times 2$;
$6 = 2 \times 3$;
$100 = 2 \times 2 \times 5 \times 5 = 2^2 \times 5^5$;
$666 = 2 \times 3 \times 3 \times 37 = 2 \times 3^2 \times 37$;
$1368 = 2 \times 3 \times 3 \times 7 = 2 \times 3^2 \times 7$
$2.002 = 2 \times 7 \times 11 \times 13$;
$255.255 = 3 \times 5 \times 7 \times 11 \times 13 \times 17$;
$472.342.734.872.390.487 = 3 \times 7 \times 827 \times 978.491 \times 27.795.571$.

Até o momento, não se descobriu nenhuma expressão matemática que forneça um *n*-ésimo número primo qualquer, a partir de um valor *n* dado. Assim, o processo de procura por números primos é feito por testes manuais (para números pequenos) ou por testes automáticos via computador (para números grandes), usando a definição. O maior número primo que se sabe até o momento (2018) tem 23.249.425 dígitos (denominado "M77232917") e foi descoberto pelo engenheiro norte-americano da empresa FedEx, *Jonathan Pace*, em 2018. *Pace* participa de um programa chamado "Great Internet Mersenne Prime Search (*GIMPS*)", que se dedica a procura de números primos. Quanto maior o número natural mais difícil torna-se fatorá-lo em números primos. Não se tem até o momento, um conjunto de procedimentos eficientes para decompor um número grande em seus fatores primos, que não seja por tentativa e erro. A fatoração de números muito grandes pode levar muitos anos mesmo com grande capacidade computacional. Além disto, dados dois números primos grandes, pode-se obter outro número natural maior por intermédio de seu produto cuja fatoração (quando não se sabe quais os fatores que o formaram) seja quase impossível de se descobrir por meio de tentativa e erro. Daí sua possibilidade de uso

em sistemas de criptografia. **Criptografia** ou **criptologia,** do grego *kryptós* = "escondido" e *gráphein* = "escrita", é o estudo e prática de princípios e técnicas para comunicação segura na presença de terceiros. Um dos primeiros sistemas de criptografia denominado ***RSA*** (***Rivest-Shamir-Adleman***) é baseado na dificuldade prática da fatoração do produto de dois números primos grandes. Ele é amplamente utilizado para transmissão segura de dados e dua denominação vem das letras iniciais dos sobrenomes do matemático e criptologista norte-americano *Ron Rivest* (1947 -), do criptógrafo israelita *Adi Shamir* (1952 -) e do cientista da computação e biólogo molecular *Leonard Adleman* (1945 -), fundadores da empresa *RSA* Data Security, Inc.

Exemplo: Um conjunto que é fundamental em um ramo da matemática chamado de Análise Complexa é denominado **conjunto dos números complexos *C***, definido como:

$$\boldsymbol{C} = \{x + y\boldsymbol{i} \; / x \; \in \boldsymbol{R}, y \in \boldsymbol{R} \text{ com } \boldsymbol{i}^2 = -1\},$$

onde *x* é chamado de parte real e *y* de parte imaginária. O número *i* é denominado de unidade imaginária. Todo o número real pode ser interpretado como um número complexo cuja parte imaginária é igual à zero. Se a parte real for igual à zero e a parte imaginária não, então o número complexo é chamado de número imaginário. O número 2 + 4***i*** é um número complexo cuja parte real é igual a 2 e a parte imaginária é igual a 4. Em 7,5 + 0***i***, temos um número complexo cuja parte imaginária é nula, ou seja, o número real 7,5. Já em 0 + 58***i***, temos um número imaginário, ou seja, 58***i***, já que a parte real é nula.

Um conjunto M' é denominado **subconjunto** de um conjunto M ou ainda, dizemos que o conjunto M' **está contido** no conjunto M se, e somente se, todo o elemento m' que pertence a M', também pertence a M, ou seja,

$$M' \subseteq M \Leftrightarrow (\forall m' \in M', m' \in M' \Rightarrow m' \in M)$$

onde o símbolo "$\subseteq$" significa inclusão ("...está contido em..." ou "...é subconjunto de..."); "$\forall$" é chamado **quantificador universal** e significa "para todo..."; "$\Leftrightarrow$" representa uma bimplicação ("...se e somente se..." ou "...equivalente a...") e "$\Rightarrow$" significa implicação ("se...então..." ou "...implica que..."). Assim,

$M' \subseteq M$ (M' está contido em M) é equivalente ($\Leftrightarrow$) a afirmar-se que "para todo m' pertencente a M' ($\forall m' \in M'$) se m' pertence a M' ($m' \in M'$) então/implica que ($\Rightarrow$) m' pertence a M ($m' \in M$").

Ou, alternativamente, esta equivalência pode ser representada por duas implicações:

$$M' \subseteq M \Rightarrow (\forall m' \in M', m' \in M' \Rightarrow m' \in M)$$

e

$$(\forall m' \in M', m' \in M' \Rightarrow m' \in M) \Rightarrow M' \subseteq M$$

(este é o motivo da seta dupla "$\Leftrightarrow$" e o nome de bimplicação).

Quando M' não é subconjunto de M, representamos por $M' \nsubseteq M$, onde o símbolo "$\nsubseteq$" significa não-inclusão ("...não está contido em..." ou "...não é subconjunto de..."). Se $M' \subseteq M$ e $M \subseteq M'$ então os dois conjuntos são iguais (ou equivalentes): $M' = M$. Entretanto, se $M' \subseteq M$ mas $M \nsubseteq M'$, ou seja, existe pelo menos um $m_i \in M$ ($\exists m_i \in M$) / $m_i \notin M'$ então M' está contido propriamente em M sendo M' chamado **subconjunto próprio** de M e indicaremos por $M' \subset M$. Se M' não está contido propriamente em M dizemos que M' *não é* **subconjunto próprio** de M e indicaremos por $M' \not\subset M$. Desta forma, sempre $M \not\subset M$. O símbolo "$\exists$" é chamado **quantificador existencial** e significa "existe pelo menos um...".

Em matemática, uma afirmação declarativa (afirmação que representa a constatação de um fato matemático) deve poder ser avaliada como falsa ou verdadeira.

Exemplo: A afirmação declarativa "5 + 2 = 7" pode ser avaliada como falsa ou verdadeira, sendo verdadeira neste caso. Já a afirmação declarativa "10 × 8 = 70" é falsa.

Exemplo: A afirmação declarativa "*x* é par" pode ser avaliada como falsa ou verdadeira dependendo do valor de *x*: é verdadeira se *x* for par e falsa, caso contrário.

Exemplo: A afirmação declarativa "*x* é ímpar" pode ser avaliada como falsa ou verdadeira dependendo do valor de x: é verdadeira se *x* for ímpar e falsa, caso contrário.

Exemplo: A afirmação declarativa "seja um triângulo retângulo" pode ser avaliada como falsa ou verdadeira dependendo do triângulo a qual estamos nos referindo: é verdadeira se o triângulo for retângulo e falsa, caso contrário.

A partir de uma ou mais afirmações declarativas pode-se também, formar outras. Sejam *A* e *B* duas afirmações. Uma afirmação do tipo "*A* e *B*", chamada **conjunção**, só é verdadeira se ambas as afirmações *A* e *B* também o forem.

Na chamada **disjunção** "*A* ou *B*" sua veracidade é garantida desde que *A* ou *B* ou ambos sejam verdadeiros. Entretanto, se as afirmações forem mutuamente excludentes (não podem ser ambas verdadeiras simultaneamente) então *A* ou *B* será verdadeira se uma ou outra forem verdadeiras (mas não ambas).

Exemplo: A afirmação "sejam *x* e *y* pares" é uma afirmação declarativa formada pelas afirmações "*x* par" e "*y* par", separadas por "e". A afirmação "sejam *x* e *y* pares" só é verdadeira se *x* for par e *y* for par.

Exemplo: Entretanto, em "$x \geq 4$", *x* deve ser igual ou maior do que 4, mas não ambos pois são afirmações mutuamente excludentes (*x* não pode ser maior e igual a 4).

Na **negação** de uma afirmação *A*, ou seja, "não *A*", se a afirmação *A* é verdadeira então sua negação será falsa; mas, se a afirmação *A* é falsa então sua negação será verdadeira.

Exemplo: Seja a afirmação "todos os triângulos são retângulos" (que é falsa). Sua negação, ou seja, "não é verdade que todos os triângulos são retângulos" ou ainda "nem todos os triângulos são retângulos" é verdadeira.

Exemplo: Seja "$x \geq 7$". Então sua negação será "$x < 7$", que será verdadeira sempre que "$x \geq 7$" for falso e vice-versa.

Na afirmação $A \Rightarrow B$ ("se *A* então *B*", "*A* implica *B*" ou ainda "*B* se *A*") chamada de **implicação**, temos que se *A* for verdadeiro então *B* também será (mas não o inverso), ou seja, *B* será verdadeiro sempre que *A* for verdadeiro. Dizemos também que *A* é uma **afirmação suficiente** para *B* (para *B* ser verdadeira é suficiente que *A* seja verdadeira); ou que *B* é uma **afirmação necessária** para *A* (para *A* ser verdadeira é necessário que *B* seja verdadeira).

Exemplo: A afirmação "se *x* e *y* são dois números pares, então *x* + *y* é par", ou seja, "*x* e *y* pares $\Rightarrow$ *x* + *y* é par" significa que se a afirmação "*x* e *y* são dois números pares" é verdadeira então "*x* + *y* é par" também o será. Ou seja, "*x* + *y* é par" se "*x* e *y* forem pares". Assim, "*x* e *y* pares" é suficiente para "*x* + *y* ser par" e "*x* + *y* ser par" é necessária para "*x* e *y* serem pares".

Por outro lado, na afirmação $A \Leftrightarrow B$ ("*A* se, e somente se *B"* ou "*A* é equivalente a *B"*) chamada de **bimplicação** ou **equivalência**, se *A* for verdadeiro então *B* também será e se *B* for verdadeiro então *A* também o será (estas duas condições devem ocorrer simultaneamente). Neste caso, as afirmações *A* e *B* são **condições necessárias e suficientes** uma da outra. Em $A \Leftrightarrow B$, as afirmações *A* e *B* são ditas **afirmações equivalentes**.

Exemplo: A afirmação "x é par se e somente se $x + 1$ é ímpar" ou "x é par é equivalente a $x + 1$ é ímpar" ("x é par $\Leftrightarrow$ $x + 1$ é ímpar") significa que se a afirmação "x é par" é verdadeira então "$x + 1$ é ímpar" também o será; e se a afirmação "$x + 1$ é ímpar" é verdadeira então "x é par" também o será. Ou seja, x é par é condição suficiente e necessária para $x + 1$ ser ímpar (ou, equivalentemente, $x + 1$ é ímpar é condição necessária e suficiente para x ser par).

Exemplo: Manipulações algébricas em equações e inequações matemáticas representam equivalências. Por exemplo:

a) $x + 8 = 6 \Leftrightarrow (x + 8) - 8 = 6 - 8 \Leftrightarrow x = -2$

b) $-5x > 10 \Leftrightarrow (-1)(-5x) < (-1)10 \Leftrightarrow 5x < -10 \Leftrightarrow \frac{1}{5}(5x) < \frac{1}{5}(-10) \Leftrightarrow x < -2$

Exemplo:

$$\frac{5x-1}{x+1} > 8 \Leftrightarrow 5x - 1 > 8(x+1), \text{ para } x > -1 \text{ pois } x + 1 > 0 \text{ e assim}$$

$$\frac{5x-1}{x+1} > 8 \Leftrightarrow \left(\frac{5x-1}{x+1}\right)(x+1) > 8(x+1) \Leftrightarrow 5x - 1 > 8(x+1)$$

Entretanto,

$$\frac{5x-1}{x+1} > 8 \nLeftrightarrow 5x - 1 > 8(x+1), \text{ para } x < -1 \text{ pois } x + 1 < 0 \text{ e assim}$$

$$\frac{5x-1}{x+1} > 8 \Leftrightarrow \frac{(5x-1)}{x+1}(x+1) < 8(x+1) \Leftrightarrow 5x - 1 < 8(x+1)$$

Na afirmação $A \Rightarrow B$, se B não for verdadeira, então A também não será ("não B" $\Rightarrow$ "não A"). Da mesma forma, em "não B" $\Rightarrow$ "não A", se "não A" for falso (A verdadeiro), então "não B" também será (B verdadeiro) e assim, $A \Rightarrow B$. Ou seja, as afirmações $A \Rightarrow B$ e "não B" $\Rightarrow$ "não A" são equivalentes ($A \Rightarrow B \Leftrightarrow$ "não B" $\Rightarrow$ "não A"), fornecendo a mesma informação. A afirmação "não B" $\Rightarrow$ "não A" é chamada de **contrapositiva** de $A \Rightarrow B$.

Exemplo: A afirmação "x e y pares $\Rightarrow$ $x + y$ é par" é equivalente à afirmação contrapositiva "$x + y$ não par $\Rightarrow$ x e y não pares", ou seja, "x e y pares $\Rightarrow$ $x + y$ é par $\Leftrightarrow$ $x + y$ não par $\Rightarrow$ x e y não pares".

Exemplo: A afirmação "x^2 par $\Rightarrow$ x é par" é equivalente à afirmação contrapositiva "x não é par $\Rightarrow$ x^2 não é par", ou seja, "x^2 par $\Rightarrow$ x é par $\Leftrightarrow$ x não é par $\Rightarrow$ x^2 não é par".

Seja A com conjunto. Uma afirmação declarativa pode estar definida (ser verdadeira) sobre certos valores $x \in A$. Para especificar para quais valores de x uma afirmação declarativa é verdadeira, em geral utilizamos os chamados **quantificadores**.

O **quantificador universal,** representado por $\forall$ ("para todo..."), declara que para todos os valores de $x \in A$, uma determinada afirmação declarativa sobre x é verdadeira: $\forall x \in A$, "afirmação declarativa sobre x é verdadeira".

Exemplo: "Para todo x pertencente aos números naturais, $x + 1$ é maior ou igual a 1", ou seja: $\forall x \in \boldsymbol{N}$, $x + 1 \geq 1$, onde a afirmação declarativa sobre x verdadeira é "$x + 1 \geq 1$". Por exemplo, os números naturais 0, 1, 2 e 3 satisfazem esta afirmação. Pode-se demonstrar que ela é verdadeira $\forall x \in \boldsymbol{N}$.

Exemplo: $\forall m' \in M'$, $m' \in M' \Rightarrow m' \in M$, onde a afirmação declarativa sobre x verdadeira é "$m' \in M' \Rightarrow m' \in M$". Se esta afirmação for verdadeira $\forall m' \in M'$ então $M' \subseteq M$

O **quantificador existencial**, representado por $\exists$ ("existe pelo menos um..."), declara que para ao menos um valor de $x \in A$ (podem existir mais de um), uma determinada afirmação

declarativa sobre x é verdadeira: $\exists x \in A$, "afirmação declarativa sobre x é verdadeira*"* ou ainda $\exists x \in A$ tal que "afirmação declarativa sobre x é verdadeira*"*.

Exemplo: "Existe x pertencente aos números naturais tal que x é menor que 5", ou seja: $\exists x \in \boldsymbol{N}$, $x < 5$ ou ainda, $\exists x \in \boldsymbol{N} \,/\, x < 5$. De fato, o natural 0 satisfaz afirmação, apesar de outros também satisfazerem. O importante é que existe pelo menos um.

Exemplo: "Existe x pertencente aos números inteiros tal que x cujo quadrado é 9", ou seja: $\exists x \in \boldsymbol{Z}$, $x^2 = 9$ ou ainda, $\exists x \in \boldsymbol{Z} \,/\, x^2 = 9$. De fato, os números inteiros -3 e 3 satisfazem tal afirmação, ou seja, existe pelo menos um.

Exemplo: "Existe x pertencente aos números naturais tal que x é primo e par", ou seja: $\exists x \in \boldsymbol{N}$, x é primo e par ou ainda $\exists x \in \boldsymbol{N} \,/\, x$ é primo e par. O número 2 satisfaz tal afirmação, ou seja, existe pelo menos um.

Existe ainda outro quantificador de uso menos comum, chamado **quantificador existencial de forma única**, representado por $\exists!$ ("existe um único..."), que declara para apenas um único valor de $x \in A$, uma determinada afirmação declarativa sobre x é verdadeira: $\exists! x \in A$, "afirmação declarativa sobre x é verdadeira*"* ou ainda $\exists! x \in A$ tal que "afirmação declarativa sobre x é verdadeira*"*.

Exemplo: "Existe um único x pertencente aos números naturais tal que $x - 1 = 0$", ou seja: $\exists! x \in \boldsymbol{N}$, $x - 1 = 0$ ou $\exists! x \in \boldsymbol{N} \,/\, x - 1 = 0$. De fato, só existe um número natural que satisfaz esta equação: 1.

Exemplo: "Existe um único x pertencente aos números naturais tal que x é primo e par", ou seja: $\exists! x \in \boldsymbol{N}$, x é primo e par ou ainda, $\exists! x \in \boldsymbol{N} \,/\, x$ é primo e par. O número 2 é o único número que satisfaz tal afirmação.

O conjunto vazio, $\varnothing$, é subconjunto de qualquer conjunto M ($\varnothing \subseteq M$). De fato, como não existem elementos pertencentes ao conjunto vazio que não estejam em M (pois não há elementos em $\varnothing$), então todo o elemento de $\varnothing$ deve pertencer a M e assim, o conjunto vazio é subconjunto de M e desta forma, a afirmação "O conjunto vazio, $\varnothing$, é subconjunto de qualquer conjunto M" foi demonstrada verdadeira (*cqd*).

A sigla ***cqd***, que significa "***c***omo ***q***ueríamos ***d***emonstrar", é normalmente colocada após a demonstração da veracidade de uma afirmação, indicando sua finalização. Também se costuma utilizar os símbolos "■" ou "□". Em inglês utiliza-se "**Q.E.D.**" (ou "***QED***") originado do latim "quod erat demonstrandum" significando "como se queria demonstrar".

Exemplo: Seja o conjunto $A = \{a, b, c, d, e\}$, $B = \{a, b, c\}$, $C = \varnothing$ e $D = \{a, b, f\}$. O conjunto B está contido em A (B é subconjunto de A ou $B \subseteq A$), pois todos os elementos que pertencem a B pertencem a A. Também B está contido propriamente em A ou B é subconjunto próprio de A ($B \subset A$), pois $\exists\, a_i \in A \,/\, a_i \notin B$ (os elemento d e e). Também $C \subseteq A$ e $C \subset A$. Entretanto, $D \not\subseteq A$ (e consequentemente $D \not\subset A$), pois o $f \in D$, mas $f \notin A$.

Exemplo: Os conjuntos dos números naturais, inteiros, racionais e reais seguem a seguinte ordem de continência: $\boldsymbol{N} \subset \boldsymbol{Z} \subset \boldsymbol{Q} \subset \boldsymbol{R}$.

Exemplo: Seja o conjunto $A = \{1, 2, 3\}$. Então os conjuntos $\varnothing$, $\{1\}$, $\{2\}$, $\{3\}$, $\{1, 2\}$, $\{1, 3\}$, $\{2, 3\}$ e $\{1, 2, 3\}$ são subconjuntos de A. Com exceção do subconjunto $\{1, 2, 3\}$, todos os outros estão contidos propriamente em A. Estes conjuntos são os únicos subconjuntos que podem ser formados a parti de A. Então, observa-se que podem ser formados, a partir de A, somente um subconjunto de tamanho 0, três subconjuntos de tamanho 1, três de tamanho 2 e por fim, um subconjunto de tamanho 1 (que é o próprio A).

Exemplo: As seguintes relações de pertinência e continência são válidas:
a) $3 \in \{3, 4, 5, 6\}$;
b) $3 \notin \{3, 4, 5, 6\}$;
c) $\{3\} \subseteq \{3, 4, 5, 6\}$;
d) $3 \notin \{\{3\}, \{4\}, \{5\}, \{6\}\}$;
e) $3 \notin \{\{3\}, \{4\}, \{5\}, \{6\}\}$;
f) $3 \in \{3, \{3\}, \{4\}, \{5\}, \{6\}\}$;
g) $3 \subseteq \{3, \{3\}, \{4\}, \{5\}, \{6\}\}$;
h) $\{3\} \in \{\{3\}, \{4\}, \{5\}, \{6\}\}$;
i) $\{3\} \notin \{\{3\}, \{4\}, \{5\}, \{6\}\}$;
j) $\varnothing \in \{\varnothing, 3, 4, 5, 6\}$;
k) $\varnothing \subseteq \{\varnothing, 3, 4, 5, 6\}$;
l) $\varnothing \notin \{3, 4, 5, 6\}$;
m) $\varnothing \subseteq \{3, 4, 5, 6\}$;
n) $\varnothing \subseteq \varnothing$

Axioma ou **postulado** é uma afirmação declarativa que não é provada ou demonstrada sendo considerada como verdadeira ou como um consenso inicial necessário para a construção ou aceitação de uma teoria. Um axioma é uma afirmação declarativa assumida verdadeira.

Exemplo: Os **Axiomas de Peano**, formulados pelo matemático italiano do século *XIX Giuseppe Peano* (1858 – 1932), são princípios básicos aceitos sem comprovação que caracterizam o conjunto dos números naturais $\boldsymbol{N}$. São eles:
1) Zero é um número;
2) Se n é um número, o sucessor de n é um número;
3) Zero não é o sucessor de um outro número.
4) Dois números cujos sucessores são iguais são eles próprios iguais.
5) Se um conjunto $\boldsymbol{S}$ de números contém o zero e também o sucessor de todo número de $\boldsymbol{S}$, então todo número está em $\boldsymbol{S}$ (também conhecido como **Axioma da indução**).

Exemplo: O **Princípio da boa ordenação** afirma que todo o conjunto S não vazio de números naturais tem um menor elemento m, ou seja, se $S \subseteq \boldsymbol{N}$, com $S \neq \varnothing$ então $\exists m \in S \,/\, \forall s \in S,\ m \leq s$. Esta afirmação declarativa é um axioma, pois é uma afirmação considerada verdadeira sem a necessidade de comprovação.

Exemplo: Outro exemplo de axioma vem da geometria plana. O **postulado da existência** afirma que em uma reta, bem como fora dela, existem infinitos pontos; e ainda, que em um plano ha infinitos pontos. Estas afirmações são aceitas como verdadeiras sem a necessidade de qualquer demonstração.

Prova formal (ou **demonstração formal**), também conhecida simplesmente por **prova** ou **demonstração**, é uma maneira irrefutável de se mostrar que uma afirmação é verdadeira. Ou ainda, é um conjunto de procedimentos que leva a veracidade irrefutável de uma afirmação. Uma afirmação que se mostra, por meio de um número finito de testes ou exemplos, verdadeira, mas que não foi formalmente provada é denominada de **conjectura**. Se um número finito de testes ou exemplos corrobora uma dada afirmação, não significa que esta seja verdadeira. Sua veracidade só é garantida pela prova formal. Uma prova formal representa, de certa maneira, uma maneira de se realizar "infinitos" testes em uma dada afirmação.

Exemplo: A afirmação "todo inteiro par maior que 2 é igual a soma de dois primos" aparentemente é verdadeira pois temos evidências numéricas para isto: $4 = 2 + 2$, $6 = 3 + 3$, $8 = 3 + 5$, etc...Entretanto, não existe até o momento, prova matemática formal para a veracidade desta afirmação, sendo chamada de uma conjectura. Esta conjectura é conhecida como **Conjectura de *Goldbach***, em homenagem ao matemático prussiano *Christian Goldbach* (1690 – 1764).

Um **teorema** é uma afirmação verdadeira no qual existe uma prova. Em geral, os teoremas assumem as formas $A \Rightarrow B$ (implicação) ou $A \Leftrightarrow B$ (equivalência). As afirmações A e B são chamadas de **hipótese** e **conclusão**, respectivamente. É impossível, em um teorema, que uma hipótese verdadeira resulte em uma conclusão falsa. Uma afirmação, cuja hipótese assumida como verdadeira resultar em uma conclusão falsa, é falsa não sendo um teorema, ou seja, $A \not\Rightarrow B$ (A não implica em B) ou ainda $A \not\Leftrightarrow B$ (A não é equivalente a B).

Exemplo: A afirmação de que "em um triângulo retângulo, o quadrado da hipotenusa é igual a soma dos quadrados dos catetos" pode ser provada formalmente, sendo chamada assim de **Teorema de *Pitágoras*** (demostrado pelo matemático grego *Pitágoras* que viveu entre 570 a.C. e 495 a.C.).

Exemplo (**Teorema Fundamental da Aritmética**): "Todo o número inteiro $n > 1$ pode ser representado como um produto de fatores primos de maneira única a menos da ordem". Este teorema envolve duas afirmações: a primeira, é que todo o número inteiro n pode ser fatorado em números primos (fatoração) e, a segunda, que esta fatoração é única a menos da ordem (unicidade da fatoração).

Exemplo: A afirmação de que "o conjunto dos números primos é infinito" pode ser provada formalmente verdadeira, sendo chamado assim de **Teorema de *Euclides*** (demostrado pelo matemático grego *Euclides* que viveu no século III a.C.).

Exemplo: O **Último Teorema de *Fermat*** é um famoso teorema matemático enunciado pelo matemático francês *Pierre de Fermat* (1601 – 1665), em 1637. *Fermat* afirmou ter uma demonstração deste teorema, mas nunca a publicou ou a fez conhecida. Testes mostravam que a afirmação de *Fermat* aparentemente funcionava (o que fazia dela uma conjectura). O teorema (ou mais corretamente, conjectura) afirma que não há solução para a equação $x^n + y^n = z^n$, se n for um inteiro maior do que 2 e x, y e z inteiros positivos. Somente em 1993, a afirmação de *Fermat* transforma-se em teorema, sendo demostrado pelo matemático britânico *Andrew John Wiles* (1953 –). Assim, o Último Teorema de *Fermat* também passou a ser conhecido como **Teorema de *Fermat-Wiles***.

Teoremas considerados de menor importância são, muitas vezes, denominados também de **proposições**. **Lema** é um teorema que deve ser utilizado para se demostrar a veracidade de uma afirmação declarativa de maior importância, ou seja, um teorema de maior interesse. É um teorema necessário para demonstração de outro teorema. Um **corolário** é um teorema mais específico originado de um teorema mais genérico.

Existem diversos tipos de provas. Provar um teorema por meio de **prova direta** ou **prova por dedução** é realizar um conjunto de procedimentos que, a partir da hipótese suposta verdadeira, obtém-se também uma conclusão verdadeira. A prova "liga" a hipótese à conclusão. No caso de teoremas na forma $A \Rightarrow B$, basta provarmos, por prova direta, que se A for verdadeiro, B também será.

Exemplo (**Teorema de *Pitágoras***): Um triângulo retângulo (Fig. 1.1.5) é uma figura geométrica formada por três lados. Ele possui um ângulo reto, cuja medida é de 90º, e dois ângulos agudos, menores que 90º. A hipotenusa é o lado oposto ao ângulo reto e o maior lado do triângulo. Já os catetos são os lados adjacentes e que formam o ângulo de 90°.

Queremos demonstrar o teorema de *Pitágoras*: "em um triângulo retângulo, o quadrado da hipotenusa é igual à soma dos quadrados dos catetos". Neste caso, a hipótese é "um triângulo retângulo" e a conclusão é que "o quadrado da hipotenusa é igual à soma dos quadrados dos catetos". A verdade desta afirmação pode ser demonstrada por prova direta. Seja um triângulo retângulo (hipótese verdadeira), com hipotenusa igual a h e catetos iguais a $c1$ e $c2$:

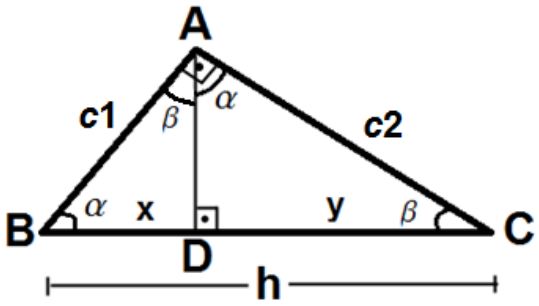

Fig. 1.1.5

onde $\alpha + \beta = 90°$ e a soma dos ângulos internos de um triângulo é igual a 180°.
Então:

$$\cos\beta = \frac{\text{Cateto adjacente}}{\text{hipotenusa}} = \frac{AC}{\underbrace{BC}_{=\frac{c2}{h}}} = \frac{DC}{\underbrace{AC}_{=\frac{y}{c2}}} \Leftrightarrow \frac{c2}{h} = \frac{y}{c2} \Leftrightarrow (c2)^2 = hy$$

$$\text{sen}\,\beta = \frac{\text{Cateto oposto}}{\text{hipotenusa}} = \frac{AB}{\underbrace{BC}_{\frac{c1}{h}}} = \frac{BD}{\underbrace{AB}_{\frac{x}{c1}}} \Leftrightarrow \frac{c1}{h} = \frac{x}{c1} \Leftrightarrow (c1)^2 = hx$$

Logo:

$$(c1)^2 + (c2)^2 = hx + hy = h\underbrace{(x+y)}_{h} = h^2$$

Ou seja,

$$h^2 = (c1)^2 + (c2)^2 \ (cqd)$$

Do Teorema de *Pitágoras*, o número irracional $\sqrt{2}$ representa a medida da diagonal de um quadrado de lado igual a 1 (pois $(\sqrt{2})^2 = 1^2 + 1^2$). Esta diagonal pode ser projetada sobre uma reta numérica, fornecendo a posição de $\sqrt{2}$ com relação aos números reais. (Fig. 1.1.6).

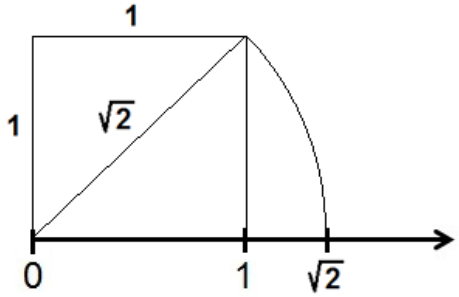

Fig. 1.1.6

Exemplo: Seja um número racional $\frac{q}{r}$. Se $r = 2^s5^l$, com $s, l \in \boldsymbol{N}$, então $\frac{q}{r}$ terá uma representação decimal exata (finita).
De fato, seja Se $r = 2^s5^l$, com $s, l \geq 0$ (hipótese). Então,

Se $s > l$, teremos:

$$\frac{q}{r} = \frac{q}{2^s5^l} = \frac{q}{2^s5^l}\left(\frac{5^{s-l}}{5^{s-l}}\right) = \frac{q5^{s-l}}{2^s5^l(5^{s-l})} = \frac{q5^{s-l}}{2^s5^s} = \frac{q5^{s-l}}{(2\times5)^s} = \frac{q5^{s-l}}{10^s} = q5^{s-l}10^{-s} = m10^{-s}$$

com $m \in \boldsymbol{Z}$

Se $s = l$, teremos:

$$\frac{q}{r} = \frac{q}{2^s 5^s} = \frac{q}{(2 \times 5)^s} = \frac{q}{10^s} = q10^{-s}$$

com $q \in \boldsymbol{Z}$

Se $s < l$, teremos:

$$\frac{q}{r} = \frac{q}{2^s 5^l} = \frac{q}{2^s 5^l}\left(\frac{2^{l-s}}{2^{l-s}}\right) = \frac{q2^{l-s}}{2^s 5^l (2^{l-s})} = \frac{q2^{l-s}}{5^l 2^l} = \frac{q2^{l-s}}{(5 \times 2)^l} = \frac{q2^{l-s}}{10^l} = n2^{l-s}10^{-l} = n10^{-s}$$

com $n \in \boldsymbol{Z}$

Logo, se $r = 2^s 5^l$, com $s, l \in \boldsymbol{N}$, então $\frac{q}{r}$ terá uma representação decimal exata (*cqd*).

Exemplo: Por definição, um **número *x* é par** se $\exists a \in Z \,/\, x = 2a$. Seja a afirmação "se *x* e *y* são dois números pares, então *x* + *y* é par", ou seja, "*x* e *y* pares ⇒ *x* + *y* é par". Temos como hipótese "*x* e *y* pares" e como conclusão, "*x* + *y* é par".
De fato, por prova direta, esta afirmação pode ser demonstrada verdadeira, partindo apenas da hipótese verdadeira (*x* e *y* pares). Se *x* e *y* são pares (hipótese verdadeira), então $\exists a$ e $b \in \boldsymbol{Z} \,/\, x = 2a$ e $y = 2b$. Logo, $x + y = 2a + 2b = 2(a + b) = 2c$ com $c = a + b$ e consequentemente, $c \in \boldsymbol{Z}$. Assim, $\exists c \in \boldsymbol{Z} \,/\, x + y = 2c$, caracterizando *x* + *y* como um número par (*cqd*). A afirmação é chamada então de teorema. Entretanto, se *x* + *y* é par não implica que *x* e *y* são também pares. Por exemplo, se *x* = 1 e *y* = 3, *x* + *y* = 4 é par, mas *x* e *y* não são pares (são ímpares).

Exemplo: Sejam *x* e $y \in \boldsymbol{Z}$, com $y \neq 0$. Dizemos que ***x* é divisível por *y*** ($y|x$) ou ainda que ***x* é múltiplo de *y***, se $\exists q \in \boldsymbol{Z} \,/\, x = qy$ onde *y* é denominado divisor de *x;* caso contrário, se $\nexists q \in \boldsymbol{Z} \,/\, x = qy$ dizemos que ***x* não é divisível por *y*** ($y \nmid x$) e assim, *y* não é divisor de *x* (ou ainda, que ***x* não é múltiplo de *y***). Por exemplo, $3|6$ pois $\exists q\ (q = 2) \in \boldsymbol{Z} \,/\, 6 = 2(3)$. Já $2 \nmid 5$ pois $\nexists q \in \boldsymbol{Z} \,/\, 5 = q(2)$. Se *x* é par, então $2|x$.
Agora, sejam *a, b* e $c \in \boldsymbol{Z}$. A afirmação "$a|b \Rightarrow a|(bc)$" é um teorema. De fato, por prova direta: se $a|b$ então $\exists x \in Z \,/\, b = xa$. Logo, $bc = (xa)c = (xc)a = za$, onde $z = xc$. Ou seja, $\exists z \in \boldsymbol{Z} \,/\, bc = za$ e assim, $a|(bc)$ (*cqd*).

Exemplo: Sejam *a, b* e $c \in \boldsymbol{Z}$. A afirmação "$b|a$ e $c|b \Rightarrow c|a$" é um teorema. De fato, por prova direta: se $b|a$ e $c|b$ então $\exists x$ e $y \in Z \,/\, a = xb$ e $b = yc$. Logo, $a = x(yc) = (xy)c = zc$, onde $z = xy$. Ou seja, $\exists z \in \boldsymbol{Z} \,/\, a = zc$ e assim, $c|a$ (*cqd*).

Equivalentemente a prova direta, podemos também provar que se *B* não for verdadeiro, então *A* também não será (não *B* ⇒ não *A*). Neste caso, apesar de ser uma prova direta, a demonstração é denominada **prova pela contrapositiva** (primeiro é feita a contrapositiva da afirmação e depois a prova direta sobre a contrapositiva). Em algumas situações, pode ser mais fácil provar a veracidade de uma afirmação por contrapositiva do que por prova direta.

Exemplo: A afirmação "se x^2 é par então *x* é par", ou seja, "x^2 par ⇒ *x* é par" é um teorema. De fato, podemos demonstrar a veracidade desta afirmação por meio da prova pela contrapositiva. Seja a contrapositiva de "x^2 par ⇒ *x* é par", "*x* não é par ⇒ x^2 não é par", ou seja, "*x* é ímpar ⇒ x^2 é ímpar". Por definição, um **número *y* é ímpar** se $\exists a \in Z \,/\, y = 2a + 1$. Ou seja, se *x* ímpar, então $2 \nmid x$.
Então, por prova direta, $\exists a \in \boldsymbol{Z} \,/\, x = 2a + 1$. Logo, $x^2 = (2a + 1)^2 = 4a^2 + 4a + 1 = 2(2a^2 + 2a) + 1 = 2c + 1$, com $c \in \boldsymbol{Z}$. Ou seja, $\exists c \in \boldsymbol{Z} \,/\, x^2 = 2c + 1$ e assim, x^2 é ímpar. Consequentemente, "*x* é ímpar ⇒ x^2 é ímpar" e assim, "x^2 par ⇒ *x* é par" (*cqd*).

Já em teoremas na forma $A \Leftrightarrow B$, temos que provar, por prova direta ou por contrapositiva, primeiramente que $A \Rightarrow B$ (⇒) e depois que $B \Rightarrow A$ (⇐), ou vice-versa.

Exemplo: Seja a afirmação "*x* é par se e somente se *x* + 1 é ímpar" ou "*x* é par é equivalente a *x* + 1 é ímpar" ou ainda, "*x* é par ⇔ *x* + 1 é ímpar". Para mostrarmos que esta proposição é

verdadeira, devemos mostrar que "x é par $\Rightarrow$ $x + 1$ é ímpar" e ainda que "$x + 1$ é ímpar $\Rightarrow$ x é par". Por prova direta:

($\Rightarrow$) Se x é par, então $\exists a \in \boldsymbol{Z}$ / $x = 2a$ (definição de número par). Então, $x + 1 = 2a + 1$ e consequentemente, $x + 1$ é ímpar (por definição de número ímpar).

($\Leftarrow$) Se x +1 é ímpar, então $\exists b \in \boldsymbol{Z}$ / x +1 = $2b + 1$ (definição de número ímpar). Então, $(x + 1) - 1 = (2b + 1) – 1 = 2b$. Ou seja, $x = 2b$ que é um número par (por definição de número par).
Assim, "x é par $\Leftrightarrow$ $x + 1$ é ímpar" (*cqd*).

Exemplo: Sejam x e $y \in \boldsymbol{Z}$. A afirmação $x < y \Leftrightarrow x \leq y – 1$. De fato, esta afirmação é verdadeira. Por prova direta:

($\Rightarrow$) Se $x < y$, então $y – x > 0$. Assim, como 1 é o maior inteiro positivo, então $y – x \geq 1 \Leftrightarrow (y – x) + x \geq 1 + x \Leftrightarrow y \geq 1 + x \Leftrightarrow y – 1 \geq (1 + x) – 1 \Leftrightarrow y – 1 \geq x$. Assim, $x \leq y – 1$.

($\Leftarrow$) Se $x \leq y – 1$ então $x – y \leq – 1$. Consequentemente, $x – y \leq – 1 \Leftrightarrow (-1)(x – y) \geq (-1)(-1) \Leftrightarrow y – x \geq 1$. Como 1 é o maior inteiro positivo, então $y – x \geq 1 \Leftrightarrow y – x > 0 \Leftrightarrow (y – x) + x > 0 + x \Leftrightarrow y > x \Leftrightarrow x < y$.
Assim, "$x < y \Leftrightarrow x \leq y – 1$" (*cqd*).

Por outro lado, basta um caso que contradiga (não confirme) uma afirmação para torná-la falsa. Esta forma de demonstrar a falsidade de uma afirmação (refutar) é chamada de **prova por contra-exemplo** ou **refutação**.

Exemplo: Sejam x e $y \in \boldsymbol{R}$. A afirmação "$x^2 = y^2 \Rightarrow x = y$" é falsa. De fato, por contra-exemplo, se $x = 2$ e $y = -2$, teremos que $(2)^2 = (-2)^2 = 4 \nRightarrow 2 = -2$, pois $2 \neq -2$.

Exemplo: Sejam $x, y \in \boldsymbol{Z}$. A afirmação "$x|y^2 \Rightarrow x|y$" é falsa. De fato, por contra-exemplo, se $x = 4$ e $y = 10$, teremos que $4|10^2$ pois $\exists a$ $(a = 25) \in \boldsymbol{Z}$ / $10^2 = 4(25)$. Entretanto, mas $4 \nmid 10$ pois . $\nexists a \in \boldsymbol{Z}$ / $10 = 4$b.

O método exaustivo de calcular cada caso possível com o objetivo de provar alguma afirmação matemática é chamado muitas vezes de **método da exaustão** (ou simplesmente **exaustão**), **prova por casos, força bruta e ignorância (FBI)** ou em inglês "***brute force and ignorance*** (***BFI***)". O método da exaustão é um método de prova válido se a afirmação a ser demonstrada apresenta um número finito de possibilidades. Não é considerada uma técnica de demonstração rigorosa (prova formal) em Matemática nas situações em que não se consegue analisar todos os casos possíveis (infinitas possibilidades). Entretanto, com o aumento da capacidade de processamento dos computadores (o que permite o estudo de um número muito grande de casos) tem sido utilizada no estudo de diversas conjecturas. Na situação em que o método da exaustão acuse um caso que contradiga a afirmação testada, então ele se configura uma prova rigorosa (ou seja, uma prova por contra-exemplo) mesmo em afirmações que envolvam infinitas possibilidades.

Exemplo: Seja $n \in \boldsymbol{N}$. A firmação "$n! > n + 1 \Rightarrow n > 2$" não pode ser provada por exaustão, pois existem infinitas possibilidades a serem avaliadas. Entretanto, a sua contrapositiva "$n \leq 2 \Rightarrow n! \leq n + 1$", pode ser demostrada por exaustão, pois temos apenas três casos possíveis (n = 0, 1 e 2):

$$0 \leq 2 \Rightarrow 0! (= 1) \leq 0 + 1 (= 1)$$
$$1 \leq 2 \Rightarrow 1! (= 1) \leq 1 + 1 (= 2)$$
$$2 \leq 2 \Rightarrow 2! (= 2) \leq 2 + 1 (= 3)$$

Exemplo: O **Teorema da Quatro Cores** que diz que "qualquer mapa pode ser colorido com apenas quatro cores, sem que regiões adjacentes tenham a mesma cor" foi conjecturado em 1846, mas foi demosntrado com o auxilio do computador IBM 360 (ou seja, pelo método da exaustão) em 1976 pelo matemático norte-americano *Kenneth Appel* (1932 – 2013) e pelo matemático alemão *Wolfgang Haken* (1928 –). O problema, inicialmente com infinitas

possibilidades (ou configurações), foi reduzido para 1936 (e posteriormente para 1476) sendo testado no computador, verificando assim a veracidade da afirmação. Ainda não existe uma demonstração sem o auxílio de um computador deste teorema.

Seja a afirmação $A \Rightarrow B$. A única forma de $A \Rightarrow B$ ser falsa é se a afirmação A for verdadeira e a afirmação B for falsa. Se A for falsa, $A \Rightarrow B$ é considerada matematicamente verdadeira já que a falsidade desta só é verificada a partir da falsidade de A (não teria como excluirmos $A \Rightarrow B$ da veracidade). Consequentemente, uma afirmação do tipo $A \Rightarrow B$ é verdadeira se conseguirmos provar que A é sempre falso (ou uma afirmação impossível). Esta forma de prova é denominada de **prova por vacuidade** e a afirmação $A \Rightarrow B$ é dita uma **afirmação verdadeira por vacuidade**.

Exemplo: Pode-se mostrar por vacuidade que $\varnothing \subseteq M$ é verdadeira para qualquer conjunto M, pois a afirmação "$m' \in \varnothing \Rightarrow m' \in M$" (definição de continência) é sempre verdadeira já que hipótese "$m' \in \varnothing$" é sempre falsa (impossível) pois $\varnothing$ não apresenta elementos por ser o conjunto vazio.

Exemplo: Seja $x \in \boldsymbol{Z}$. A afirmação "x par e ímpar $\Rightarrow$ x é primo" é verdadeira, pois por vacuidade, a hipótese "x par e ímpar" é sempre falsa, já que $\nexists x \in \boldsymbol{Z}$ que seja par e ímpar ao mesmo tempo.

Alguns termos utilizados na área da ciência da computação podem ser construídos por meio da teoria dos conjuntos (como é chamado o conjunto de definições e teoremas que envolvem objetos matemáticos chamados conjuntos).

Chamamos de **alfabeto**, todo o conjunto finito (representado geralmente pela letra grega maiúscula sigma $\boldsymbol{\Sigma}$). Cada elemento de um alfabeto $\boldsymbol{\Sigma}$ é chamado **símbolo** ou **caractere**. Uma **palavra** ou **cadeia de caracteres** sobre um alfabeto $\boldsymbol{\Sigma}$ é uma sequência finita de símbolos justapostos (concatenados) deste alfabeto. O **tamanho** ou **comprimento de uma palavra** é igual ao número de símbolos concatenados para a formação de uma palavra. Chamamos de **palavra vazia** ou **sequência vazia** (representada pela letra grega minúscula épsilon $\boldsymbol{\varepsilon}$), a sequência de comprimento zero. Em um alfabeto $\boldsymbol{\Sigma}$, $\boldsymbol{\Sigma^*}$ representa o conjunto de todas as palavras possíveis sobre este alfabeto. A palavra vazia sempre pertence a $\boldsymbol{\Sigma^*}$, ou seja, $\boldsymbol{\varepsilon} \in \boldsymbol{\Sigma^*}$. De fato, como não existem caracteres que formam $\boldsymbol{\varepsilon}$ que não pertencem a $\boldsymbol{\Sigma}$ (pois $\boldsymbol{\varepsilon}$ tem comprimento zero), então por vacuidade, $\boldsymbol{\varepsilon}$ deve pertencer a $\boldsymbol{\Sigma^*}$(*cqd*). Se $\boldsymbol{\Sigma}$ for não vazio ($\boldsymbol{\Sigma} \neq \varnothing$), então $\boldsymbol{\Sigma^*}$ será um conjunto infinito. Uma linguagem formal $\boldsymbol{L}$ (ou simplesmente **linguagem** $\boldsymbol{L}$), é um conjunto de palavras sobre um alfabeto. Assim, $\boldsymbol{L} \subseteq \boldsymbol{\Sigma^*}$.

Exemplo: Os conjuntos dos números naturais, inteiros, racionais, irracionais e reais não formam um alfabeto, pois são conjuntos infinitos.

Exemplo: O conjunto {0, 1} é um exemplo de um alfabeto (ou seja, $\boldsymbol{\Sigma}$ = {0, 1}). Então, $\boldsymbol{\Sigma^*}$ = {0, 1}* = {$\boldsymbol{\varepsilon}$, 0, 00..., 1, 11..., 01, 10, 11, 100, 010, 001,..., 1010101,...} ou seja, o conjunto infinito das palavras formadas por todas as possibilidades de concatenação de 0´s e 1´s (incluindo $\boldsymbol{\varepsilon}$). O conjunto $\boldsymbol{L}$ = {000, 100, 010, 001, 110, 101, 011, 111} forma uma linguagem sobre o alfabeto $\boldsymbol{\Sigma}$, pois $\boldsymbol{L} \subseteq \boldsymbol{\Sigma^*}$.

Exemplo: O conjunto $\varnothing$ é também um alfabeto (ou seja, $\boldsymbol{\Sigma} = \varnothing$), pois é finito. Então $\boldsymbol{\Sigma^*} = \varnothing^* = \{\boldsymbol{\varepsilon}\}$ e assim, $\boldsymbol{\Sigma^*}$ será um conjunto finito.

Exemplo: **Linguagens de programação *LP*** (Fortran, Pascal, Basic, C, etc...) são conjuntos de regras padronizadas que regem a transmissão de instruções a um computador. Estas regras envolvem aspectos de **sintaxe** (quanto à construção) e de **semântica** (quanto ao sentido, significado). Um **programa *p*** é um conjunto de instruções escrita em uma ***LP*** e que descreve uma tarefa a ser realizada por um computador. ***LP***´s são linguagens sobre um alfabeto formado

por dígitos, letras e símbolos especiais. Cada programa ***p*** representa uma palavra sobre o alfabeto da ***LP***, ou seja, $p \in LP$. O conjunto de todos os programas válidos em uma ***LP*** define esta linguagem. Assim, uma ***LP*** é um conjunto infinito.

O Matemático alemão *Georg Cantor* (1845 – 1928) é considerado o inventor da moderna teoria dos conjuntos. A versão inicial desta teoria é conhecida como **teoria ingênua dos conjuntos**, termo usado ocasionalmente na década de 40, estabelecido na década de 50 e popularizado pelo matemático americano (de origem húngara) *Paul Halmos* em seu livro *Nave Set Theory* (1960), na década de 60.

Os conceitos básicos normalmente utilizados na teoria de conjuntos (definição e especificação de um conjunto, pertinência, continência, etc...) fazem parte da chamada teoria ingênua dos conjuntos. A teoria ingênua dos conjuntos permite construir conjuntos cujos elementos são também conjuntos. Um dos princıpios básicos que está implícito informalmente nesta teoria é o **princıpio da compreensão** ou da **abstração**: dada uma propriedade qualquer, existe o conjunto dos objetos que tem tal propriedade. A suposição de que qualquer propriedade pode ser usada para formar um conjunto, sem qualquer restrição, dá origem a paradoxos na teoria ingênua dos conjuntos.

Um **paradoxo** (do grego "***paradoxos"*** que significa algo contrário ao senso comum) é uma afirmação aparentemente verdadeira construída a partir de definições válidas, mas que se mostra contraditória. Um paradoxo reúne ideias contraditórias em um mesmo contexto. A identificação de um paradoxo baseado em conceitos aparentemente simples e racionais tem, por vezes, auxiliando significativamente o progresso da ciência, filosofia e matemática.

Exemplo: Paradoxo do mentiroso. Este paradoxo compõe-se de afirmações do tipo: se um homem diz "Eu sempre minto", ele está mentindo ou falando a verdade? Se, por hipótese, ele estiver mentindo, então "Eu sempre minto" é mentira e ele fala a verdade, o que é uma contradição, pois por hipótese ele está mentindo. Se, por hipótese, ele estiver falando a verdade, então "Eu sempre minto" é verdade e ele está mentindo, o que é uma contradição, pois por hipótese, ele está falando a verdade. Uma versão do paradoxo mentiroso é atribuída ao filósofo grego *Eubulides de Mileto*, que viveu no século *IV* a.C.

O paradoxo mais conhecido originado pela teoria ingênua dos conjuntos é o chamado **paradoxo de *Russell***. O paradoxo de *Russel* foi descoberto em 1901, pelo matemático, filósofo e lógico inglês *Bertrand Russell* (1872 – 1970) e publicado pela primeira vez em seu livro *The Principles of Mathematics* (1903). Este paradoxo mostra que não podemos ter um conjunto de todos os conjuntos.

O paradoxo de *Russell* envolve a definição de conjunto ordinário. Um **conjunto ordinário** é todo conjunto que não pertence a si mesmo. Ou seja, se *O* é ordinário, então $O \notin O$.

Exemplo: Os conjuntos $\{0,1\}$, $\{a, b, c, d\}$, $\boldsymbol{N}$, $\boldsymbol{Z}$, $\boldsymbol{Q}$, I, $\boldsymbol{R}$, o conjunto de todos os cavalos e o conjunto de todas as funções são exemplos de conjuntos ordinários, pois não são conjuntos de si mesmos. Podemos construir um número infinito de conjuntos ordinários.

Exemplo: A definição de um conjunto por compreensão, na teoria ingênua dos conjuntos, permite-nos definir conjuntos que são elementos de si mesmo. Por exemplo, o conjunto de todos os conjuntos com mais de 5 elementos é um conjunto que pertence a si mesmo, pois ele mesmo certamente tem mais de 5 elementos. O conjunto de todas as definições, que por ser também uma definição, deve pertencer a si mesmo. Outro exemplo, importante no paradoxo de Russel, é o conjunto de todos os conjuros, que por ser um conjunto, deve pertencer a si mesmo.

Agora, seja $\boldsymbol{\Omega}$ o conjunto de todos os conjuntos ordinários O. Assim, definindo $\boldsymbol{\Omega}$ por compreensão, teremos que $\boldsymbol{\Omega} = \{O \,/\, O \notin O\}$, onde $\boldsymbol{\Omega}$ é um conjunto perfeitamente definido por compreensão e infinito. Então, a seguinte afirmação prova-se verdadeira:

Teorema de *Russel* (ou como é mais conhecido, paradoxo de *Russel*): Se $\boldsymbol{\Omega}$ é um conjunto de todos os conjuntos ordinários ($\boldsymbol{\Omega} = \{O \,/\, O \notin O\}$, por compreensão), então $\boldsymbol{\Omega} \in \boldsymbol{\Omega}$ se e somente se $\boldsymbol{\Omega} \notin \boldsymbol{\Omega}$**,** ou seja:

$$\boldsymbol{\Omega} = \{O \,/\, O \notin O\} \Rightarrow \boldsymbol{\Omega} \in \boldsymbol{\Omega} \Leftrightarrow \boldsymbol{\Omega} \notin \boldsymbol{\Omega}.$$

ou, equivalentemente,

$$\boldsymbol{\Omega} = \{O \,/\, O \notin O\} \Rightarrow \nexists \boldsymbol{\Omega}$$

Prova:
O paradoxo nos diz que se $\boldsymbol{\Omega} = \{O \,/\, O \notin O\}$ então chegaremos a uma equivalência entre $\boldsymbol{\Omega} \in \boldsymbol{\Omega}$ e $\boldsymbol{\Omega} \notin \boldsymbol{\Omega}$, o que é um absurdo, pois $\boldsymbol{\Omega}$ não pode pertencer e não pertencer a si mesmo. Consequentemente, $\boldsymbol{\Omega}$ não deve existir. Para provar isto, devemos demonstrar que se $\boldsymbol{\Omega} = \{O \,/\, O \notin O\}$ então $\boldsymbol{\Omega} \in \boldsymbol{\Omega} \Rightarrow \boldsymbol{\Omega} \notin \boldsymbol{\Omega}$ e $\boldsymbol{\Omega} \notin \boldsymbol{\Omega} \Rightarrow \boldsymbol{\Omega} \in \boldsymbol{\Omega}$. De fato, suponhamos por hipótese que exista um conjunto $\boldsymbol{\Omega} = \{O \,/\, O \notin O\}$. Então**:**

($\Rightarrow$) Se $\boldsymbol{\Omega} \in \boldsymbol{\Omega}$, então $\boldsymbol{\Omega}$ não será ordinário e assim, $\boldsymbol{\Omega} \notin \boldsymbol{\Omega}$ pois $\boldsymbol{\Omega} = \{O \,/\, O \notin O\}$. Logo, $\boldsymbol{\Omega} \in \boldsymbol{\Omega} \Rightarrow \boldsymbol{\Omega} \notin \boldsymbol{\Omega}$**,** o que contradiz a hipótese inicial ($\boldsymbol{\Omega} \in \boldsymbol{\Omega}$);

($\Leftarrow$) Se $\boldsymbol{\Omega} \notin \boldsymbol{\Omega}$, então $\boldsymbol{\Omega}$ será ordinário e assim, $\boldsymbol{\Omega} \in \boldsymbol{\Omega}$ pois $\boldsymbol{\Omega} = \{O \,/\, O \notin O\}$. Logo, $\boldsymbol{\Omega} \notin \boldsymbol{\Omega} \Rightarrow \boldsymbol{\Omega} \in \boldsymbol{\Omega}$**,** o que contradiz a hipótese inicial ($\boldsymbol{\Omega} \notin \boldsymbol{\Omega}$).

Consequentemente, $\boldsymbol{\Omega} = \{O \,/\, O \notin O\} \Rightarrow \boldsymbol{\Omega} \in \boldsymbol{\Omega} \Leftrightarrow \boldsymbol{\Omega} \notin \boldsymbol{\Omega}$ (*cqd*) e assim, não pode existir um conjunto $\boldsymbol{\Omega} = \{O \,/\, O \notin O\}$.

Outra forma de se demonstrar que uma afirmação matemática é verdadeira (que é um teorema) é por meio da chamada **prova por contradição** ou **redução ao absurdo** (do latim *reductio ad absurdum*). Este tipo de prova consiste em se demostrar a veracidade de uma afirmação "Se $A \Rightarrow B$", supondo que a afirmação A é verdadeira e que a afirmação B é falsa. Posteriormente, argumenta-se até chegar a uma contradição (absurdo) o que resulta na veracidade da afirmação "Se $A \Rightarrow B$".

Exemplo: Se $x \in \boldsymbol{Z}$, então x não pode ser par e ímpar ao mesmo tempo.
De fato, da definição de número par, se x for par então $\exists a \in \boldsymbol{Z} \,/\, x = 2a$ e da definição de número ímpar, se x for ímpar então $\exists b \in \boldsymbol{Z} \,/\, x = 2b + 1$. Vamos supor, por absurdo, que x possa ser par e ímpar ao mesmo tempo. Então, $\exists a$ e $b \in \boldsymbol{Z} \,/\, x = 2a$ e $x = 2b + 1$. Logo, $2a = 2b + 1 \Leftrightarrow 2a - 2b = 1 \Leftrightarrow 2(a - b) = 1 \Leftrightarrow a - b = ½$, o que contradiz a hipótese inicial de que a e $b \in \boldsymbol{Z}$, pois a diferença entre dois inteiros é um número inteiro e não um racional. Logo, se $x \in \boldsymbol{Z}$ então x não pode ser par e ímpar ao mesmo tempo (*cqd*).

Exemplo: O número $\sqrt{2}$ é irracional ($\sqrt{2} \in \boldsymbol{I}$), ou seja, não pode ser expresso como uma fração irredutível (fração que não pode ser simplificada) de dois inteiros.
De fato, vamos supor (por absurdo) que existam p e $q \in \boldsymbol{Z}$ tal $\sqrt{2} = \frac{p}{q}$ seja uma fração irredutível. Então,
$\left(\frac{p}{q}\right)^2 = 2 \Leftrightarrow p^2 = 2q^2 \Leftrightarrow p^2 = 2a$, com $a \in \boldsymbol{Z}$. Consequentemente, p^2 é par e p^2 é par $\Rightarrow p$ é par. Se p é par então $\exists b \in \boldsymbol{Z} \,/\, p = 2b$. Logo, $p^2 = (2b)^2 = 2q^2$. Desta forma, $2(2b^2) = 2q^2$ e assim, $q^2 = 2b^2 \Leftrightarrow q^2 = 2c$, com $c \in \boldsymbol{Z}$. Consequentemente, q^2 é par e q^2 é par $\Rightarrow q$ é par. Se q é par então $\exists d \in \boldsymbol{Z} \,/\, q = 2d$. Como p e q são pares, sua razão não é uma fração irredutível, pois

$\left(\frac{p}{q}\right) = \left(\frac{2b}{2d}\right) = \left(\frac{b}{d}\right)$. Isto é uma contradição (absurdo), pois contraria a hipótese inicial da fração ser irredutível. Logo, $\nexists p$ e $q \in \boldsymbol{Z}$ tal $\sqrt{2} = \frac{p}{q}$ e assim, $\sqrt{2}$ é irracional (*cqd*).

Exemplo: Seja *n* um número natural maior que 1. Se $m > 1$ é o menor divisor inteiro de *n*, então *m* é primo (claro que se *n* é primo então $m = n$).
De fato, seja $m > 1$ o menor divisor inteiro de *n* e por absurdo, que *m* é composto. Então $\exists k \in \boldsymbol{N}$ com $1 < k < m$ tal que $k|m$. Como $k|m$ e $m|n$ então $k|n$. Como $k < m$ e *k* é um divisor de *n* então temos uma contradição já que por hipótese, *m* é o menor divisor inteiro de *n*,. Assim, todo o número natural maior que um tem um divisor primo (*cqd*).

Exemplo: Se *n* é um número natural maior que 1 então ou *n* é primo ou pode ser representado como um produto finito de números primos.
De fato, vamos supor por absurdo que existam números compostos que não possam ser representados como o produto de números primos. Seja *m* o menor destes números. Se $1 < n < m$ então o teorema é verdadeiro para *n*. Como todo o número natural maior que um tem um divisor primo então seja *p* um divisor primo de *m*. Logo,

$$1 < \frac{m}{p} < m$$

E desta forma,

$$\frac{m}{p} = p_1 p_2 \dots p_k \text{ onde } p_1 p_2 \dots p_k \text{ são números primos.}$$

Consequentemente,

$m = p_1 p_2 \dots p_k p$ o que é uma contradição já que, por hipótese, *m* é o menor dos números compostos que não podem ser representados como o produto de números primos. Assim, se *n* é um número inteiro maior que 1 então ou *n* é primo ou pode ser representado como um produto finito de números primos (*cqd*).

Exemplo (**Teorema de *Euclides***): O conjunto dos números primos é infinito.
De fato, vamos supor por absurdo, que o conjunto dos números primos é finito. Então,

$$\boldsymbol{P} = \{p_1, p_2, \dots p_i \dots p_n / \ p_i, n \in \boldsymbol{N}^*, p_i \neq 1 \text{ e os únicos dividores de } p_i \text{ são 1 e } p_i\}$$

Seja $m \in \boldsymbol{N^*}$ / $m = (p_1 p_2 \dots p_n) + 1$. Sabemos que $\exists p$ primo tal que $p|m$. Se $p \in \boldsymbol{P}$ então $p|p_1 p_2 \dots p_i \dots p_n$ e assim, $\exists x, y \in \boldsymbol{Z}$ / $m = xp$ e $p_1 p_2 \dots p_n = yp$. Logo, $m = (p_1 p_2 \dots p_i \dots p_n) + 1 \Leftrightarrow m - (p_1 p_2 \dots p_i \dots p_n) = 1 \Leftrightarrow xp - yp = 1 \Leftrightarrow 1 = (x - y)p \Leftrightarrow p|1$ o que é impossível (1 não é divisível por qualquer número primo) e desta forma, $p \notin \boldsymbol{P}$. Consequentemente, um conjunto finito *P* de números primos não pode ser o conjunto de todos os números primos e portanto, *P* deve ser infinito (*cqd*).

Exemplo: Seja *p* um número primo. Então $\sqrt{p}$ é irracional ($\sqrt{p} \in \boldsymbol{I}$), ou seja, não pode ser expresso como uma fração irredutível de dois inteiros. De fato, vamos supor por absurdo que $\sqrt{p}$ pode ser expresso com uma fração irredutível (seja racional), ou seja, que existam dois primos entre si *m* e $n \in \boldsymbol{Z}$ tal $\sqrt{p} = \frac{m}{n}$. Então,

$\left(\frac{m}{n}\right)^2 = p \Leftrightarrow m^2 = pn^2 \Leftrightarrow m^2 = pa$, com $a \in \boldsymbol{Z}$. Consequentemente, $\exists a \in \boldsymbol{Z}$ / $m^2 = pa$ e assim, m^2 é divisível por *p*. Lembrando que qualquer inteiro *m* pode ser fatorado em números primos: $m = p_1 p_2 \dots p_i \dots p_j$, onde p_i é o *i*-ésimo primo da fatoração. Logo,

$$m^2 = (p_1 p_2 \dots p_i \dots p_j)^2 = {p_1}^2 {p_2}^2 \dots {p_i}^2 \dots {p_j}^2$$

Como $p|m^2$ então

$$m^2 = {p_1}^2 {p_2}^2 \dots {p_i}^2 \dots {p_j}^2 = pa$$

Como *p* é primo, então um dos p_i´s é igual a *p* (*p* é um dos fatores). Ou seja,

$$m^2 = {p_1}^2{p_2}^2 \dots p^2 \dots {p_j}^2 \Rightarrow m = p_1 p_2 \dots p \dots p_j \Rightarrow m = pb, \text{ com } b \in \boldsymbol{Z}$$

Ou seja, $p|m^2 \Rightarrow p|m$. Como $m = pb$ então $m^2 = (pb)^2 = pn^2$. Desta forma, $p(pb^2) = pn^2$ e assim, $n^2 = pb^2 \Leftrightarrow n^2 = pc$, com $c \in \boldsymbol{Z}$. Consequentemente, $p|n^2$ e ainda, $p|n^2 \Rightarrow p|n$ o que significa que $\exists d \in \boldsymbol{Z}$ / $n = pd$. Como m e n são divisíveis por p, sua razão não é uma fração irredutível, pois $\left(\frac{m}{n}\right) = \left(\frac{pb}{pd}\right) = \left(\frac{b}{d}\right)$. Isto é uma contradição (absurdo), pois contraria a hipótese inicial da fração ser irredutível. Logo, $\nexists m$ e $n \in \boldsymbol{Z}$ tal $\sqrt{p} = \frac{m}{n}$ e assim, $\sqrt{p}$ para p primo é irracional (*cqd*).

Exemplo: O número de ouro ϕ é irracional. De fato, vamos supor (por absurdo) que existam p e $q \in \boldsymbol{Z}$ tal $\phi = \frac{p}{q}$ seja uma fração irredutível (seja racional). Então,

$$\phi = \frac{1+\sqrt{5}}{2} = \frac{p}{q} \Leftrightarrow 1 + \sqrt{5} = \frac{2p}{q} \Leftrightarrow \sqrt{5} = \frac{2p}{q} - 1 = \frac{2p-q}{q} = \frac{r}{q}, \text{ com } r, q \in Z,$$

E assim $\sqrt{5}$ seria um número racional que é um absurdo, já que 5 é primo e toda a raiz quadrada de um número primo é irracional. Logo, ϕ é irracional (*cqd*).

Como consequência do paradoxo de *Russell*, a coleção (agrupamento de objetos quaisquer) formada por todos os conjuntos ordinários não é um conjunto, apesar de ser construída por compreensão, de maneira totalmente válida na teoria ingênua dos conjuntos. Logo, não existe um conjunto de todos os conjuntos ordinários e consequentemente, não existe também um conjunto de todos os conjuntos, já que o conjunto de todos os conjuntos ordinários seria um elemento deste conjunto. A teoria ingênua dos conjuntos permite construir tal afirmação paradoxal.

Exemplo: O **Paradoxo do barbeiro** é um paradoxo, originado a partir do Paradoxo de *Russell*, que demonstra como uma afirmação do cotidiano e aparentemente plausível é logicamente impossível. Digamos que em uma cidade, onde todos os homens andem sempre barbeados (ou eles se barbeiam ou são barbeados), vive um e somente um barbeiro. Este barbeiro faz a barba de todos aqueles homens cidade (e somente deles) que não barbeiam a si mesmos. Podemos tentar fazer a seguinte pergunta: o Barbeiro se barbeia? Ou ainda, quem barbeia o barbeiro? Entretanto, se o barbeiro barbear-se a si mesmo, então o barbeiro (ele mesmo) não deve barbear a si mesmo. Se o barbeiro não se barbeia a si mesmo, então ele (o barbeiro) deve barbear a si mesmo. Ou seja, nenhuma destas possibilidades é válida (são logicamente impossíveis). Este tipo de paradoxo é chamado de **paradoxo auto-referente** (pois envolve uma afirmação que se refere a si mesma).

A solução de *Bertrand Russell* para seu paradoxo foi desenvolver a **teoria dos tipos**, que basicamente introduziu uma hierarquia aos objetos. Elemento, conjunto de elementos, conjunto de conjuntos de elementos e assim sucessivamente, representam objetos hierarquicamente diferentes, chamados de tipos. O objeto "elemento" é hierarquicamente inferior (ou de ordem inferior) ao objeto "conjunto de elementos" que por sua vez é hierarquicamente inferior ao objeto "conjunto de conjuntos de elementos". Objetos de um determinado tipo são construídos exclusivamente a partir de objetos de tipos hierarquicamente inferiores. Consequentemente, o conjunto de todos os conjuntos é hierarquicamente superior a um conjunto. Logo, a teoria dos tipos não admite a indagação se o conjunto de todos os conjuntos é ou não membro de si mesmo, pois são conjuntos de tipos diferentes. Na teoria dos tipos, cada objeto tem um "tipo" e operações definidas e restritas neste tipo.

A teoria dos tipos tem encontrado aplicação prática na ciência da computação, em particular dentro das linguagens de programação, na forma dos chamados sistemas de tipos.

Um **sistema de tipos** é basicamente um método que divide os valores de um programa em conjuntos chamados tipos e torna certos comportamentos do programa não permitidos com base nos tipos que são atribuídos neste processo.

Em matemática, uma **variável** é um objeto (ou entidade) que pode representar um valor ou expressão. Em linguagem de programação, uma **variável** é uma posição de memória onde poderemos guardar determinado dado ou valor e modificá-lo ao longo da execução do programa.

O sistema de tipos permite construir, em uma linguagem de programação ***LP***, o conceito de tipo de dado de uma variável. Denominamos **tipo de dado de uma variável** as possibilidades de valores que uma variável pode assumir juntamente com as operações permitidas a esta. Um programa válido em uma ***LP*** que permite a definição do tipo de dado de uma variável (programa permitido no sistema de tipos da ***LP***) não apresentará erros decorrentes de atribuição ou de operações que sejam incompatíveis com os tipos definidos. Desta forma, o sistema de tipos reduz os erros em programas de computador. Muitas ***LP´***s apresentam um conjunto pré-definidos de tipos de dado (considerados tipos elementares) tais como: caractere ("char"), cadeia de caracteres ("string"), inteiro, real e booleano (falso ou verdadeiro). As ***LP´***s permitem a definição de novos tipos, a partir destes tipos elementares.

Exemplo: Uma ***LP*** com sistema de tipos (que permite a definição do tipo de dado de uma variável) pode classificar o valor 20 como um tipo inteiro e o valor "*cadeira*" como um tipo cadeia de caracteres (comumente chamado de "string"). Ao tentar adicionar estes dois valores em um programa, o sistema de tipos pode tornar proibitiva (ilegal) esta operação, com base nessa atribuição de tipos.

Exemplo: As ***LP´***s como Pascal, Java, C e C++ são linguagens com sistemas de tipos. As variáveis utilizadas nestas linguagens devem ser declaradas (denominação do processo no qual se define o nome e o tipo de uma determinada variável) no início do programa. Cada ***LP*** tem uma forma específica de declaração de variáveis. Por exemplo, se uma variável *x* é inteira, em C declararíamos como "int *x*;". Já em Pascal seria "*x*: integer;".

Na tentativa de evitar paradoxos, além da teoria dos tipos criada por *Bertrand Russell*, a teoria ingênua dos conjuntos foi reformulada, posteriormente, dando origem diversos **sistemas axiomático**s (teorias fundamentadas em axiomas), chamados de **teorias axiomáticas dos conjuntos**. Uma teoria axiomática dos conjuntos não parte de uma compreensão informal ou intuitiva de conjuntos (como na teoria ingênua), mas sim, de afirmações sobre conjuntos e seus membros demonstráveis a partir de uma lista definida de axiomas. Um dos sistemas axiomáticos mais conhecidos proposto no início do século *XX* é a **teoria dos conjuntos de *Zermelo-Fraenkel*** ou ***ZFC***, em homenagem a seus idealizadores, os matemáticos alemães *Ernst Zermelo* (1871 – 1953) e *Abraham Fraenkel* (1891 – 1965). Neste sistema, um de seus axiomas, o **axioma da regularidade** (também chamado de **axioma da fundação**), afirma que todo conjunto $A \neq \varnothing$ possui um elemento tal que nenhum outro elemento do conjunto *A* pertence a ele, ou seja,

$$\forall A \neq \varnothing \Rightarrow \exists b \in A \,/\, \forall a \in A,\, a \notin b$$

Este axioma impossibilita a existência de um conjunto que pertence a sim mesmo e consequentemente, evita o paradoxo de *Russell*. De fato, seja *x* um conjunto e seja $A = \{x\}$. Então como $A \neq \varnothing$, pelo axioma da regularidade, $\exists b \in A \,/\, \forall a \in A,\, a \notin b$. Como o conjunto *A* é unitário, então $b = x$ e $a = x$ e assim $x \notin x$, ou seja, um conjunto não pode pertencer a si mesmo (*cqd*).

Exemplo: Sejam *x* e *y* conjuntos quaisquer. Então, $x \notin y$ ou $y \notin x$. De fato, seja o conjunto $A = \{x, y\}$. Como $A \neq \varnothing$, pelo axioma da regularidade, $\exists b \in A \,/\, \forall a \in A,\, a \notin b$. Se $b = x$, então $x \notin x$ e $y \notin x$; ou, se $b = y$, então $y \notin y$ e $x \notin y$. Assim, $x \notin y$ ou $y \notin x$ (*cqd*).