UNIVERSIDADE FEDERAL DO PARÁ
INSTITUTO DE CIÊNCIAS EXATAS E NATURAIS
MESTRADO PROFISSIONAL EM MATEMÁTICA EM REDE NACIONAL

MARCOS GARCIA DE SOUZA

CONJUNTOS E FUNÇÕES: conceitos, propriedades e demonstrações visando à formação continuada do professor de matemática da Educação Básica

Belém-Pará

2019

MARCOS GARCIA DE SOUZA

CONJUNTOS E FUNÇÕES: conceitos, propriedades e demonstrações visando à formação continuada do professor de matemática da Educação Básica

Dissertação apresentada ao Programa de Mestrado Profissional em Matemática em Rede Nacional – PROFMAT, da Universidade Federal do Pará – UFPA, como requisito parcial, para obtenção de título de Mestre em Matemática.
Orientador: Prof. Dr. Mauro de Lima Santos.

Belém-Pará
2019

Dados Internacionais de Catalogação na Publicidade (CIP) de acordo com ISBD
Biblioteca ICEN/UFPA-Belém-PA

S729c Souza, Marcos Garcia
Conjuntos e funções: conceitos, propriedades e demonstrações visando à formação continuada do professor de matemática da educação básica/ Marcos Garcia de Souza.-2019.
Orientador : Mauro de Lima Santos
Dissertação (Mestrado) – Universidade Federal do Pará, Instituto de Ciências Exatas e Naturais, Programa de Pós-Graduação em Matemática, 2019.

1. Matemática-Estudo e ensino (Ensino fundamental). 2. Teoria dos conjuntos. 3. Funções (Matemática). 4. Números racionais. 5. Números reais. I. Título.

CDD 22. ed. – 510.7

Elaborado por Leila Maria Lima Silva – CRB-458/81

MARCOS GARCIA DE SOUZA

CONJUNTOS E FUNÇÕES: conceitos, propriedades e demonstrações visando à formação continuada do professor de matemática da Educação Básica

Dissertação apresentada ao Programa de Mestrado Profissional em Matemática em Rede Nacional – PROFMAT, da Universidade Federal do Pará – UFPA, como requisito parcial, para obtenção de título de Mestre em Matemática.
Orientador: Prof. Dr. Mauro de Lima Santos.

APROVADO EM: 11 / 06 /2019.

BANCA EXAMINADORA:

Prof. Dr. Mauro de Lima Santos – PROFMAT/ICEN/UFPA
Orientador

Prof. Dr. Anderson David de Souza Campelo – PROFMAT/ICEN/UFPA
Titular

Prof. Dr. Sebastião Martins Siqueira Cordeiro
Faculdade de Matemática de Abaetetuba/UFPA

Dedico este trabalho à senhora Gerleide, por todo o incentivo, e também aos meus amores Edilena, Elionai, Gabriela e Guilherme, pelo apoio e compreensão de todo o tempo que dediquei a esta conquista.

AGRADECIMENTOS

Ao Senhor Deus, por tudo que proporcionou na minha vida.

Aos meus pais, Carlos Alberto e Martha Garcia, que me possibilitaram trilhar nos estudos e na vida profissional.

Ao Coordenador do PROFMAT/2017, Prof. Dr. Valcir, pela tranquilidade que nos proporcionou. Ademais, pela orientação aos procedimentos e tarefas para a realização do Curso de Mestrado Profissional em Matemática em Rede Nacional.

A CAPES, pelo investimento financeiro que contribuiu para a minha qualificação *stricto sensu*.

Ao meu Orientador, Prof. Dr. Mauro, pela confiança no meu trabalho e dedicação ao Curso de Mestrado. Além disso, pelas poucas palavras, mas de grandes ensinamentos, e também pelos conhecimentos complementares que proporcionou quando ministrou a disciplina de Teoria dos Números do PROFMAT/2017.

A todos os professores do Curso do Mestrado Profissional da UFPA/ICEN que dedicaram suas horas de trabalho em prol de nossa qualificação docente.

A todos os discentes da minha turma, PROFMAT/2017, que pude compartilhar minhas experiências, e também aprender com eles. Muito obrigado, companheiros!

Aos servidores da Secretaria Acadêmica do PROFMAT/ICEN/UFPA, que nos apoiaram com seus trabalhos administrativos.

A todos os outros servidores de apoio do ICEN que contribuíram para que os ambientes do Instituto estivessem disponíveis para o uso.

Por derradeiro, a todos que de alguma forma pensaram em nos dar condições para progredir até esta conquista.

"Aprender é trilhar sobre o conhecimento que se busca. A cada passada, descobrimos detalhes e aprendemos mais."

(William Douglas)

Resumo

Com o surgimento da matemática moderna no Brasil, a teoria de conjuntos e o estudo de funções ganharam relevância. Em qualquer conhecimento de Matemática, é necessário estabelecer um conjunto no qual se realizará o estudo – conjunto universo. No Ensino Fundamental, o conjunto dos números racionais é o que mais se utiliza para efetuar as quatro operações básicas da matemática (adição, subtração, multiplicação e divisão). Nesse sentido, este trabalho procura articular com demonstrações, propriedades, definições e conceitos referentes aos elementos de um conjunto, de uma relação dual e de funções, visando aprimorar os conhecimentos adquiridos pelo professor de matemática da Educação Básica assim como procura esclarecer a incompletude dos números racionais e criar possibilidades de o professor apresentar os detalhes de tal preferência, por meio da transposição didática. A preferência por trabalhar com o conjunto dos números racionais, em detrimento ao conjunto dos números reais, parece ser um tanto incomum, pois o conjunto dos números reais é um *corpo ordenado completo*, ao passo que o conjunto dos números racionais é um *corpo ordenado*, mas não é completo. Ao contrário do que se faz no Ensino Fundamental, no Ensino Médio o uso do conjunto dos números reais e o estudo de funções é predominante. Dessa forma, este trabalho apresenta a concepção de função, bem como suas propriedades, teoremas e demonstrações, de modo que o professor amplie seus saberes e mobilize esses conhecimentos para aprimorar o ensino da matemática na Educação Básica.

Palavras-chave: Conjunto; Corpo Ordenado; Demonstração; Função; Números Racionais; Números Reais.

Abstract

With the emergence of modern mathematics in Brazil, the theory of set and the study of functions have gained relevance. In any knowledge of Mathematics, it is necessary to establish a set, in which the study will be realized – universe set. In Elementary Education, the set of rational numbers is the four basic operations of mathematics (addition, subtraction, multiplication and division). In this sense, this work aims to articulate with demonstrations, properties, definitions and concepts referring to the elements of a set, dual reation and funtions, in order to improve the knowleng acquired by the mathematics teachers of Basic Education just as it aims to clarify the incompleteness of rational numbers and create possibilities of the teacher presente the details of such preference, through didactic transposition. The preference for working with the set of rational numbers, over the set of real numbers, seems to be somewhat unusual, because the set of real numbers is a complete ordered field, while the set of rational numbers is a ordered field, but not complete. Instead of what is done in Elementary School, in high school the use of the set of real numbers and the study of functions predominates. Therefone, this work presentes the conception of funtion, as well its properties, theorems and demonstrations, in order the theacher broadens and mobilizes his knowledge, to improve the teaching of mathematics in Basic Education.

Keywords: Set; Ordered Field; Demonstration; Function; Rational Numbers; Real Numbers.

Sumário

1 Introdução

A aprendizagem é uma dimensão fundamental que ocorre formalmente no ambiente escolar.

Nesse contexto, a atividade principal do professor é o ensino visando à aprendizagem do aluno. No processo de ensino e aprendizagem, o docente atua como mediador do aprendiz em desbravar o objeto de estudo, instigando o aluno a pensar, refletir, agir e produzir conhecimentos, priorizando mais o pensar do que, simplesmente, o calcular. Mas, para que isto ocorra, é necessário que o professor compreenda, com certa profundidade, e articule de diversos modos, os conceitos, as propriedades e as demonstrações do conteúdo matemático que vai ensinar.

Para isso, propomos Conjuntos e Funções: conceitos, propriedade e demonstrações visando à formação continuado do professor de matemática da Educação Básica, como uma forma de contribuir para a sua atuação profissional e possibilitar melhorias a sua prática pedagógica.

Os conceitos iniciais estudados em conjunto e funções são abstratos e possuem uma linguagem própria e formal. Além disso, os teoremas abordados exigem esforço, raciocínio criativo e ideias que propiciem articular conceitos e propriedades de modo consistente.

Em várias situações, a apresentação desses elementos requer uma dosagem de engenhosidade e “truques”, para construir um raciocínio lógico-indutivo ou lógico-dedutivo para a elaboração precisa e irrefutável dos argumentos utilizados nas demonstrações.

Por esse motivo, apresentamos tópicos que julgamos essenciais para o aprimoramento do professor de matemática, a saber: a noção de conjunto, a estrutura do conjunto dos números naturais, a conceito de função e os conjuntos dos números inteiros, racionais e reais construídos a partir do conjunto dos números naturais. Além disso, o conceito corpo ordenado, conjunto enumerável e não-enumerável, grandeza comensurável e não-comensurável, densidade e a noção de completude de um conjunto que são essenciais para a compreensão da extensão de

conjuntos numéricos, sobretudo, o conjunto dos números racionais e reais que predominam no ensino da matemática básica.

Com isso, espera-se contribuir para a formação continuada do professor de matemática, de modo que ele possa aperfeiçoar suas práticas pedagógicas e aprimorar o ensino da matemática na Educação Básica.

2 Noções sobre Conjunto

Segundo ÁVILA (1996, p. 32), o estudo sistemático de conjuntos começou por volta de 1872, pelo matemático alemão Georg Cantor (1845 – 1918).

Neste capítulo, apresentaremos os principais conceitos e resultados dessa teoria. Iniciaremos com a apresentação da noção de elemento e conjunto.

2.1 Elemento e Conjunto

A noção de conjunto constitui um dos fundamentos da matemática, do mesmo modo que o conceito de correspondência ou aplicação.

Para LIPSCHUTZ (1972, p. 1): "Intuitivamente, um conjunto é uma lista, coleção ou classe de objetos bem definidos."

Um conjunto fica *bem definido* (ou *determinado*) quando é dada uma propriedade (ou regra) que permita decidir se um objeto qualquer pertence ou não ao conjunto.

Os objetos que constituem o conjunto chamam-se *elementos* ou *membros* do conjunto.

A designação de um conjunto é feita por letras maiúsculas do nosso alfabeto A, B, C, $\cdots$, X, Y, Z; e os seus elementos, por letras minúsculas a, b, c, $\cdots$, x, y, z.

CARAÇA (1989, p. 12) apresenta duas condições para constituir um conjunto, a saber:

> "Em geral, dizemos que *é dado um conjunto de certos elementos* quando: *a*) eles são, de si, entidades determinadas; *b*) além disso, há a possibilidade de averiguar se um elemento qualquer, dado ao acaso, pertence ou não ao conjunto."

Quando um objeto qualquer x é um dos elementos de um conjunto X, dizemos que x pertence a X e, em símbolos, escreve-se:

$$x \in X.$$

(Lê-se: "*x pertence a X*" ou "*x está em X*")

Por outro lado, se x não é um dos elementos do conjunto X, dizemos que x não pertence a X e, simbolicamente, escreve-se:

$$x \notin X.$$

(Lê-se: "*x não pertence a X*" ou "*x não está em X*")

A relação "$\in$" (*pertence a*), que se estabelece entre elemento e conjunto, chama-se *relação de pertinência*.

2.2 Representação de um Conjunto

Sejam os elementos $x_1, x_2, x_3, \ldots$ de um conjunto X. Este conjunto pode ser representado por *listagem* de seus elementos. Neste caso, os elementos são separados uma a um por vírgula e todos eles ficam entre chaves "{ }", isto é:

$$X = \{x_1, x_2, x_3, \cdots\}.$$

Outra maneira de representar um conjunto X é por uma *propriedade característica* de seus elementos.

LIMA (2010, p. 3), propõe uma forma de construir este tipo de representação, vejamos: "parte-se de uma propriedade P. Ela define um conjunto X, assim: se um objeto X goza da propriedade P, então $x \in X$; se x não goza da propriedade P, então $x \notin X$ e escreve-se:

$$X = \{x \,;\, x \text{ goza da propriedade } P\}.$$"

(Lê-se: "*X é o conjunto dos elementos x, tais que x goza da propriedade P*").

Assim, uma propriedade P caracteriza um conjunto X, se todo elemento de X satisfaz a propriedade P e se, reciprocamente, todo elemento que satisfaz a propriedade P pertence ao conjunto.

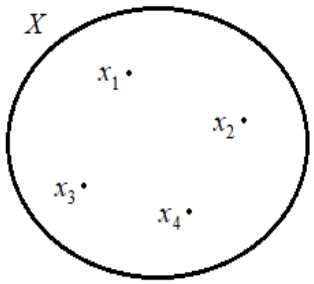
Em algumas situações, pode ocorrer que a propriedade P faça referência a elementos de um outro conjunto E específico, ou seja: $x \in E$, tal que x tem a propriedade P. Neste caso, escreve-se:

$$X = \{x \in E \,;\, x \text{ tem a propriedade } P\}.$$

Isto significa que o conjunto X é constituído por elementos x do conjunto E, que tem a propriedade P.

Um conjunto $X = \{x_1, x_2, x_3, x_4\}$ também pode ser representado pelo diagrama de John Venn[1], mais conhecido por "Diagrama de Venn", conforme a FIGURA 1.

FIGURA 1 – Diagrama de Venn.



FONTE: elaborada pelo autor.

Geralmente, este diagrama é utilizado para ilustrar algumas propriedades e operações com conjuntos. Além disso, amenizar o aspecto abstrato de certos raciocínios ou definições. Contudo, tais representações gráficas não devem interferir nas demonstrações.

LIMA (2010, p. 3) lembra que: "A maioria dos conjuntos mencionados em Matemática não são definidos [sic] especificando-se, um a um, os seus elementos. O método mais frequente de definir [sic] um conjunto é por meio de uma propriedade comum e exclusiva dos seus elementos."

2.3 Subconjunto

Nem sempre os elementos são exclusivos de um só conjunto, isto é, pode ocorrer que todo elemento de um conjunto é também elemento de outro conjunto. Isto sugere uma definição.

Definição[2] 1. Um conjunto X é *subconjunto* (ou *parte*) de um conjunto Y quando todo elemento de X é também elemento de Y.

[1] Este tipo de diagrama – concebido por John Venn (1834 – 1923), matemático inglês – foi utilizado para representar conjuntos e realizar operações com conjuntos.

[2] **Definição** é o nome que se dá, com precisão e clareza (sem ambiguidade) ao objeto de estudo da matemática, mediante uma propriedade que caracterize e o identifique plenamente. Os elementos estruturais de uma definição são: a) o objeto a ser definido; b) o verbo ser (é); c) o termo a ser especificado; d) as condições ou propriedades que este termo satisfaça. As definições têm a seguinte forma: Um [*objeto X*] é chamado [*o termo a ser definido*] desde que satisfaça a [*propriedade que o caracterize e o identifique plenamente*]. (CORDEIRO, 2014, p. 87)

Neste caso, os conjuntos X e Y podem ser comparados pela relação de inclusão, isto é, por:

$$X \subset Y.$$

(Lê-se: "*X está contido em Y*" ou, de outra forma, $Y \supset X$, lê-se: "*Y contém X*".)

A relação "$\subset$" ou "$\subseteq$", que relaciona conjunto com conjunto, chama-se *relação de inclusão*.

Se ocorrer $X \subseteq Y$ e existir pelo menos um elemento em Y que não está em X, dizemos que X *subconjunto próprio* (ou *parte própria*) de Y e denota-se $X \subsetneq Y$.

NACHBIN (1974, p. 5) menciona que a relação de inclusão tem propriedades básicas, a saber:

i) reflexiva: $X \subset X$, qualquer que seja o conjunto X.

Demonstração[3]: Seja x um elemento qualquer de X. Pela definição de subconjunto, temos: $X \subset X$, qualquer que seja o conjunto X.

□

ii) transitiva: se $X \subset Y$ e $Y \subset Z$, então $X \subset Z$.

Demonstração: De fato, para todo $x \in X$ implica $x \in Y$, pois $X \subset Y$. Por outro lado, $Y \subset Z$. Dessa forma, para todo $x \in Y$ acarreta $x \in Z$. Portanto, se $x \in X$ e $x \in Y$, consequentemente $X \subset Z$.

□

iii) antissimétrica: se $X \subset Y$ e $Y \subset X$, então $X = Y$.

Demonstração: Seja $x \in X$. Como $X \subset Y$, temos $x \in X$ implica $x \in Y$. Por outro lado, $Y \subset X$. Desse modo, $x \in Y$ implica $x \in X$. Portanto, $X = Y$.

□

A propriedade ***antissimétrica iii)*** apresenta *inclusão simultânea* de dois conjuntos. Isto estabelece o *critério de igualdade*, isto é, se todo elemento do conjunto X é elemento do

[3] *Demonstração* em Matemática é um processo de raciocínio lógico-indutivo ou dedutivo que mostra, de maneira irrefutável, a veracidade de uma proposição do tipo: *i)* Se (*hipótese*), então (*tese*).; *ii)* (*Hipótese*) se, e somente se, (*tese*). (IRRACIEL; JOSÉ, 2010, p. 9)

conjunto Y e, reciprocamente, se todo elemento do conjunto Y é elemento do conjunto X, dizemos que os conjuntos X e Y são *iguais*.

Definição 2. Um conjunto X é igual a um conjunto Y, escrevemos $X = Y$, se ambos possuem os mesmos elementos. Do contrário, dizemos que os conjuntos são diferentes e escreve-se $X \neq Y$.

Sejam dois conjuntos X e Y. Para provar que $X = Y$, devemos demonstrar, *necessariamente,* que $X \subset Y$ e, *reciprocamente*, $Y \subset X$.

Por outro lado, para mostrar que a inclusão $X \subset Y$ é falsa, temos que exibir um elemento $x \in X$, tal que $x \notin Y$.

A propriedade transitiva ***ii)*** mostra a possibilidade de conexão entre dois conjuntos, por meio de um conjunto, cujos elementos estejam nos dois conjuntos iniciais, e somente neles.

Por fim, a propriedade reflexiva ***i)*** é consequência imediata da definição de subconjunto.

Observações:
1) A ocorrência de $X \subset Y$ não exclui a possibilidade de $X = Y$. Por isso, escrevemos, precisamente, $X \subseteq Y$;
2) O símbolo "$\in$" (pertence a) relaciona *elemento* com *conjunto*;
3) A simbologia "$\subset$" (está contido) ou "$\subseteq$" (está contido e é igual a) ou "$\subsetneq$" (está contido, mas é diferente de) relaciona *conjunto* com *conjunto*.

As ideias apresentadas de subconjunto apoiam-se na noção intuitiva de conjunto, isto é, admitimos que todo conjunto tem pelo menos um elemento. Para excluir esta restrição, introduzimos o *conjunto vazio*, que indicaremos pelo símbolo $\varnothing$ ou $\{\ \}$ ou ainda $\varnothing = \{x\ ;\ x \neq x\}$. Este conjunto não possui elemento algum.

Proposição[4] 1. O conjunto vazio é subconjunto de qualquer conjunto.

Demonstração: Suponha, por absurdo[5], que a inclusão $\varnothing \subset X$ seja falsa. Então, existe um elemento $x \in \varnothing$, tal que $x \notin X$, o que é um absurdo! Pois, $\varnothing$ representa o conjunto vazio.

[4] **Proposição** é uma frase afirmativa de sentido completo que pode ser classificada em verdadeira ou falsa, sem que haja uma terceira possibilidade. (IRRACIEL; JOSÉ, 2010, p. 2)
[5] Ver nota de rodapé da página 28.

O absurdo ocorreu ao afirmar que $\varnothing \subset X$ é falso. Logo, $\varnothing \subset X$, qualquer que seja o conjunto X.

□

O conjunto vazio é um subconjunto próprio de qualquer conjunto, isto é, $\varnothing \subsetneq X$. Há conjuntos que possui apenas um único elemento $X = \{x\}$. Este conjunto chama-se *conjunto unitário*.

LIPSCHUTZ (1972, p. 7) chama atenção para o fato de que: "Em qualquer aplicação da teoria de conjuntos, todos os conjuntos sob verificação serão subconjuntos de um conjunto determinado. Chama-se a isso *conjunto universo* ou *conjunto de estudo*. Designa-se este conjunto por U."

2.4 Conjunto das Partes

Para NACHBIN (1974, p. 6): "Todo conjunto X determina um outro conjunto $\wp(X)$, a saber, o conjunto de todas as partes de X."

Isto significa que os elementos do conjunto $\wp(X)$ são as partes de X, isto é, se um conjunto $Y \in \wp(X)$ é porque $Y \subset X$.

As partes do conjunto X têm pelo menos os conjuntos $\varnothing$ e X, chamados *conjuntos triviais*, pois $\varnothing \subset X$ e $X \subset X$, qualquer que seja X. Assim, os conjuntos triviais $\varnothing$ e X são elementos do conjunto $\wp(X)$ que denominaremos "família de conjuntos".

Definição 3. A família de todos os subconjuntos de qualquer conjunto X é chamado *conjunto das partes de X* ou o *conjunto de potência de X* e indicaremos por $\wp(X)$.

Exemplo 1. Seja o conjunto $A = \{a, b\}$. Então, as partes de A são os conjuntos $\varnothing$, A, $\{a\}$ e $\{b\}$. Portanto, o conjunto das partes de A é:

$$\wp(A) = \wp(\{a, b\}) = \{\varnothing, \{a\}, \{b\}, \{a, b\}\}.$$

Exemplo 2. Considere o conjunto $B = \{a, b, c\}$. Assim, as partes de B são os conjuntos $\varnothing$, B, $\{a\}$, $\{b\}$, $\{c\}$ $\{a, b\}$ e $\{a, c\}$. Portanto, o conjunto das partes de B é:

$$\wp(B) = \wp(\{a, b, c\}) = \{\varnothing, \{a\}, \{b\}, \{c\}\ \{a, b\}, \{a, c\}, \{a, b, c\}\}.$$

Observação:

O conjunto das partes $\wp(X)$ nunca é vazio, pois sempre tem os conjuntos triviais $\varnothing$ e X.

2.5 Operações com Conjuntos

2.5.1 Interseção

Definição 4. A *interseção* de dois conjuntos X e Y é o conjunto $X \cap Y$ (lê-se: "*X interseção Y*") formado apenas pelos elementos comuns a X e Y.

Portanto, se $x \in X \cap Y$ significa dizer que x pertence, *simultaneamente*, aos dois conjuntos, isto é, $x \in X$ e $x \in Y$. Este fato, representa-se por:

$$X \cap Y = \{x \,;\, x \in X \text{ e } x \in Y\}.$$

Quando dois conjuntos X e Y não possuem elementos em comum, indica-se por $X \cap Y = \varnothing$. Neste caso, os conjuntos X e Y chamam-se *conjuntos disjuntos*.

2.5.2 União

Definição 5. A *união* (ou *reunião*) de dois conjuntos X e Y é o conjunto $X \cup Y$ (lê-se: "*X união Y*") formado pelos elementos que estão apenas em X, ou apenas em Y ou em ambos X e Y.

Assim, se $x \in X \cup Y$ significa dizer que $x \in X$ ou $x \in Y$, não há outra possibilidade. Em símbolos, escreve-se:

$$X \cup Y = X = \{x \,;\, x \in X \text{ ou } x \in Y\}.$$

Seja um conjunto X formado por subconjuntos A, B, C, ... , tais que:

i) a união de A, B, C, $\cdots$ é igual a X ; e

ii) a interseção de cada par desses subconjuntos distintos é o conjunto $\varnothing$.

Então, nessas condições, o conjunto $\{A, B, C, \cdots\}$ é uma *partição* de X.

2.5.3 Diferença

Definição 6. A *diferença* de dois conjuntos X e Y é o conjunto $X - Y$ (lê-se: "*X menos Y*") formado pelos elementos de X que não pertencem ao conjunto Y. Em símbolos, indica-se por:

$$X - Y = \{x \,;\, x \in X \text{ e } x \notin Y\}.$$

Nessa definição, não se exige que X esteja contido em Y. Quando se tem $Y \subset X$, a diferença $X - Y$ chama-se *complementar de Y em relação a X* e escreve-se:

$$X - Y = \mathrm{C}_Y X, \text{ com } Y \subset X.$$

Na teoria de conjuntos, quando lidamos com conjunto universo (ou conjunto de estudo) U, o *complementar* de *X em relação a U* indica-se por:

$$X^C = U - X.$$

Isto equivale dizer que: se $x \in X^C$, então $x \notin X$ e escrevemos:

$$X^C = U - X = \{x \in U \,;\, x \notin X\}.$$

A partir dessas definições, várias propriedades podem ser deduzidas. Para fins de ilustração, demonstraremos a propriedade no exemplo a seguir.

Exemplo 3. Sejam dois conjuntos quaisquer X e Y. Prove que $X^C - Y^C = Y - X$.

Resolução: Como se trata de uma igualdade de conjuntos, precisamos mostrar que: $(X^C - Y^C) \subset (Y - X)$ e $(Y - X) \subset (X^C - Y^C)$. Com efeito:
i) Para todo $x \in (X^C - Y^C)$, temos $x \in X^C$ e $x \notin Y^C$ acarreta $x \notin X$ e $x \in Y$, portanto, $x \in (Y - X)$. Assim, $(X^C - Y^C) \subset (Y - X)$.

ii) Por outro lado, qualquer que seja $x \in (Y - X)$, segue que $x \in Y$ e $x \notin X$. Logo, $x \notin Y^C$ e $x \in X^C$. Com isto, $x \in (X^C - Y^C)$. Portanto, $(Y - X) \subset (X^C - Y^C)$.

2.5.4 Produto Cartesiano

Além dessas operações com conjuntos, há outra operação importante que se baseia no conceito de par ordenado, a saber: o *produto cartesiano*[6] (ou *multiplicação de conjuntos*).

[6] *Cartesiano* provém do nome do filósofo e matemático francês René Descartes (1596 – 1650) que fundou a geometria cartesiana ou álgebra geométrica (hoje conhecida por geometria analítica), criando um sistema cartesiano de coordenadas para localizar pontos no plano e no espaço. (BOYER, 1996, p. 233)

Para LIPSCHUTZ (1972, p. 92, grifos nossos): “intuitivamente, um *par ordenado* consiste de dois elementos a e b, dos quais um, digamos a é o primeiro elemento e o outro como segundo elemento.” Representa-se um par ordenado por (a, b).

Em outras palavras, o par ordenado (a, b) fica constituído quando, dados dois objetos a e b, escolhe-se um desses objetos (por exemplo) a, para ser a *primeira coordenada* do par e, por conseguinte, o objeto b para ser a *segunda coordenada* do par. Entretanto, a definição de par ordenado é:

$$(a, b) = \{\{a\}, \{a, b\}\}^{7}.$$

De acordo com essa notação, o par ordenado (a, b) é um conjunto constituído, no máximo, de dois elementos: o conjunto $\{a\}$ e o conjunto $\{a, b\} = \{b, a\}$.

Quando $a = b$, segue que $(a, a) = \{\{a\}, \{a, a\}\}$. Mas, pela igualdade de conjuntos, temos $\{a, a\} = \{a\}$. Portanto, $(a, a) = \{\{a\}, \{a\}\}$. Daí, novamente pela igualdade de conjuntos, conclui-se $(a, a) = \{\{a\}\}$. Com isso, define-se:

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

Teorema[8] 1. (Propriedade Fundamental dos Pares Ordenados) Dois pares ordenados (x, y) e (a, b) são iguais se, e somente se, $x = a$ e $y = b$. Isto é:

$$(x, y) = (a, b) \iff x = a \text{ e } y = b.$$

Demonstração: De fato, se $x = a$ e $y = b$, tem-se $(x, y) = (a, b)$. Reciprocamente, se $(x, y) = (a, b)$, conclui-se, pela definição de par ordenado:

$$(x, y) = \{\{x\}, \{x, y\}\} \text{ e } (a, b) = \{\{a\}, \{a, b\}\}.$$

Dessa forma, há dois casos para considerar:

1º caso: quando $x = y$, temos:

$$(x, y) = (x, x) = \{\{x\}\}.$$

---

[7] Notação introduzida por Norbert Wiener (1894 – 1964) e C. Kuratowski (1896 – 1980). (DEAN, 1974, p. 7)

[8] **Teorema** é uma afirmação declarativa (ou proposição) do tipo hipótese *implica* tese ou hipótese *se, e somente se,* tese (ou ainda hipótese *implica* tese e, reciprocamente, tese *implica* hipótese), cuja veracidade exige demonstração. (ÁVILA, p. 4 e 5)

Assim, $\{\{x\}\} = \{\{a\}, \{a, b\}\}$, isto é, o conjunto $\{a, b\}$ é um elemento de $\{\{x\}\}$. Logo, $\{x\} = \{a, b\}$, o que implica $a = b = x$. Mas, por hipótese, $x = y$, então $x = a$ e $y = b$.

2º caso: quando $x \neq y$.

Considere a igualdade $(x, y) = (a, b)$, isto é, $\{\{x\}, \{x, y\}\} = \{\{a\}, \{a, b\}\}$. Suponha que $\{x, y\} = \{a\}$. Então, temos $x = y = a$. Mas isto contraria a hipótese de $x \neq y$. Logo, $\{x, y\} = \{a, b\}$ e, consequentemente, $a \neq b$.

Portanto, o elemento $\{x\}$ não pode ser $\{a, b\}$. Assim, $\{x\} = \{a\}$, o que acarreta $x = a$. Além disso, como $\{x, y\} = \{a, b\}$ e $x = a$, temos $\{a, y\} = \{a, b\}$. Portanto, $y = b$.

□

LIMA (2010, p. 12) observe que há distinção entre o par ordenado (a, b) e o conjunto $\{a, b\}$ e ressalta que: "Não se deve confundir o par ordenado (a, b) com o conjunto $\{a, b\}$. Com efeito, como dois conjuntos que possuem os mesmos elementos são iguais, temos $\{a, b\} = \{b, a\}$, sejam quais forem a e b. Por outro lado, pela definição de igualdade entre pares ordenados só temos $(a, b) = (b, a)$ quando $a = b$."

A ideia de par ordenado está presente na definição de produto cartesiano, a qual passamos a apresentar.

Definição 7. O *produto cartesiano* (ou *conjunto produto*) de dois conjuntos X e Y é o conjunto $X \times Y$ (lê-se: "X *cartesiano* Y") cujos elementos são pares ordenados (x, y), tais que a primeira coordenada pertence a X e a segunda coordenada pertence a Y. Mais precisamente:

$$X \times Y = \{(x, y) \; ; \; x \in X \text{ e } y \in Y\}.$$

O produto cartesiano $Y \times X$ é formado pelos mesmos elementos de $X \times Y$, porém, com os elementos *permutados*, isto é, $Y \times X = \{(y, x) \; ; \; x \in X \text{ e } y \in Y\}$.

Exemplo 4. Sejam $X = \{a, b\}$ e $Y = \{c\}$. Os elementos de $X \times Y$ são (a, c) e (b, c), isto é: $X \times Y = \{(a, c), (b, c)\}$. Daí, obtemos: $Y \times X = \{(c, a), (c, b)\}$.

Observação:

Em geral, $X \times Y \neq Y \times X$, a menos que um dos conjuntos seja $\varnothing$ ou $X = Y$.

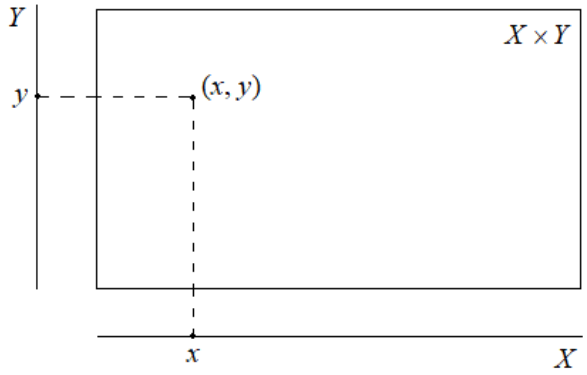
Se ocorrer $X = Y$, tem-se $X \times Y = X \times X = X^2$. Neste produto cartesiano, há um subconjunto $D \subset X \times X$, formado pelos pares ordenados cujas coordenadas são iguais, chamado *conjunto diagonal* (ou simplesmente, *diagonal*) de X^2 e escreve-se:

$$D = \{(x, x) ; x \in X\}.$$

Exemplo 5. Seja o conjunto $X = \{a, b\}$. Os elementos de $X \times X = X^2$ são (a, a), (a, b), (b, a), (b, b). Assim, $X \times X = \{(a, a), (a, b), (b, a), (b, b)\}$. O conjunto diagonal, neste caso, é $D = \{(a, a), (b, b)\}$.

No contexto geométrico, LIMA (2010, p. 12) menciona que: se X e Y são segmentos de reta, o conjunto $X \times Y = \{(x, y) ; x \in X \text{ e } y \in Y\}$ é um retângulo representado pela FIGURA 2, onde os pontos (x, y) descrevem todo o retângulo $X \times Y$.

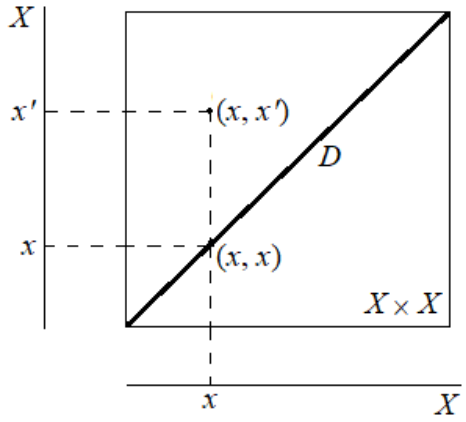
FIGURA 2 – Representação geométrica de $X \times Y$, onde X e Y são segmentos de reta.



FONTE: LIMA, Elon Lages, 2010, p. 12.

O conjunto $X \times X$ é um quadrado representado pela FIGURA 3, onde evidenciamos a diagonal $D = \{(x, x) ; x \in X\}$, descrita pelos pontos (x, x).

FIGURA 3 – Representação geométrica de $X \times X$, com o conjunto diagonal D, onde X representa um segmento de reta.



FONTE: LIMA, Elon Lages, 2010, p. 12.

Nesse contexto, os elementos de um par ordenado introduzem as coordenadas cartesianas no plano, de modo que cada ponto do plano é representado por um par ordenado (x, y), onde x chama-se *abscissa* e y, a *ordenada* deste ponto.

3 Conjunto dos Números Naturais

3.1 Os Axiomas[9] de Peano

No séc. XIX, o matemático italiano Giuseppe Peano (1858 – 1932) propôs a formalização do conjunto dos números naturais em seu livro *Arithmetices principia nova methodo exposita*, de modo que os números naturais podem ser estabelecidos por cinco axiomas (ou postulados), chamados *Axiomas de Peano*.

Segundo LIMA (1982, p. 26), pode-se apresentar os Axiomas de Peano do seguinte modo:

Sejam um conjunto de números naturais $\mathbb{N} = \{1, 2, 3, \cdots\}$ e uma correspondência $s : \mathbb{N} \to \mathbb{N}$ que a cada $n \in \mathbb{N}$ associe o número $s(n) \in \mathbb{N}$ chamado *sucessor de* n. Então:

Axioma I. 1 é número natural, ou seja, $1 \in \mathbb{N}$;

Axioma II. Para cada $n \in \mathbb{N}$, *existe* um *único* $s(n) \in \mathbb{N}$;

Axioma III. Para todo $n \in \mathbb{N}$, tem-se $1 \neq s(n)$, ou seja, 1 não é sucessor de nenhum número natural. Em outras palavras, a cada número natural $n \neq 1$, *existe* um *único* $n_0 \in \mathbb{N}$, tal que $n = s(n_0)$;

Axioma IV. Dados $n, m \in \mathbb{N}$, se $s(n) = s(m)$, então $n = m$. Neste caso, a correspondência $s : \mathbb{N} \to \mathbb{N}$ chama-se *injetiva* (ou *unívoca*);

Axioma V (Princípio de Indução Finita ou Princípio de Indução). Seja um conjunto $X \subset \mathbb{N}$ satisfazendo as propriedades:

i) $1 \in X$ (*verificar*); e

ii) para todo $n \in X$ implica $s(n) \in X$ (*demonstrar*).

Então, $X = \mathbb{N}$.

Dessa forma, podemos dizer que uma *correspondência* (ou *aplicação*) *injetiva* é caracterizada pelo ***Axioma IV***. Esta aplicação injetiva, pode ser enunciada de outra forma

[9] **Axioma (ou Postulado)** é uma palavra de origem grega que significa *axios* (digno ou válido). No contexto matemático, axioma é uma sentença afirmativa considerada evidente, verdadeira, inquestionável e indemonstrável, utilizada como sinônimo de *princípio* necessário à construção ou aceitação de uma teoria ou como base para uma argumentação. (Disponível em: Wikipédia – axioma). Acesso em: 31 jan 2019.

equivalente, a saber: dados n, $m \in \mathbb{N}$, se $n \neq m$, então $s(n) \neq s(m)$. A ideia subjacente a esta propriedade refere-se ao conjunto dos números naturais como um *conjunto discreto*. Isto será melhor esclarecido, quando estudarmos a propriedade de densidade de um conjunto de conjunto.

O ***Axioma III*** estabelece que *existe* um *único* primeiro número natural que não é sucessor de nenhum outro. Este número é indicado pelo símbolo 1 (um) e, de acordo com o ***Axioma I***, não carece de comentários.

O ***Axioma II*** põe em destaque a *existência* e a *unicidade* do sucessor de um número natural qualquer $n \neq 1$.

Por fim, segundo AYRES (1973, p. 47), o ***Axioma V*** **(Princípio de Indução Finita)** pode ser enunciado da forma:

Axioma V'. **Princípio de Indução Matemática.** Uma proposição $P(n)$ é verdadeira, para todo $n \in \mathbb{N}$, se:
i') $P(1)$ é verdadeira; e
ii') Para cada $k \in \mathbb{N}$, a hipótese de que $P(k)$ verdadeira *implica* $P(k + 1)$ verdadeira.

Para mostrar que uma proposição, referente a números naturais, é verdadeira, basta usar o **Princípio de Indução Matemática** descrito no ***Axioma V'***.

Neste postulado, a propriedade ***i')*** deve ser apenas *verificada*, fazendo $n = 1$. Na verdade, pode-se iniciar esta verificação por qualquer número natural, em particular.

A propriedade ***ii')*** exige *demonstração*! Isto é feito supondo-se que (*hipótese de indução*), para cada $n = k \in \mathbb{N}$, a proposição $P(k)$ é verdadeira e, com base nisto, prova-se que $P(k + 1)$ também é verdadeira.

Com a verificação de ***i')*** e a demonstração de ***ii')***, conclui-se, pelo Princípio de Indução Matemática, que a proposição $P(n)$ é verdadeira, para todo $n \in \mathbb{N}$.

Segundo AYRES (1973, p. 47), vajamos como aplicar os ***Axiomas de Peano*** de ***I*** a ***V*** na demonstração do exemplo a seguir, e depois usar o ***Axioma V'***.

Exemplo 6. Prove que a proposição $P(n) : s(n) \neq n$ é verdadeira, para todo $n \in \mathbb{N}$.

Resolução: Seja um conjunto X, definido por $X = \{k \; ; \; P(k)$ é verdadeira, para todo $k \in \mathbb{N}\}$. Então, pelo ***Axioma I***, temos $1 \in \mathbb{N}$.

Fazendo $k = 1$, o ***Axioma III*** permite escrever $s(1) \neq 1$. Portanto, $P(1)$ é verdadeira e $1 \in X$.

Agora, seja um elemento qualquer k de X. Vamos provar que $P(k) : s(k) \neq k$ é verdadeira, para todo $k \in \mathbb{N}$. **Demonstraremos por absurdo (ou contradição)**[10]. Suponha, por absurdo, que $s(s(k)) = s(k)$. Então, pelo ***Axioma IV***, segue $s(k) = k$, o que é uma contradição! Logo, $P(s(k)) : s(s(k)) \neq s(k)$ é verdadeira e, pelo ***Axioma II***, para todo $k \in \mathbb{N}$, existe um único $s(k) \in X$.

Como $1 \in X$ e, para cada $k \in \mathbb{N}$ implica $s(k) \in X$, então X tem as propriedades ***i)*** e ***ii)*** do ***Axioma V***. Logo, $X = \mathbb{N}$.

Portanto, pelo *Princípio de Indução Finita*, a proposição $P(n) : s(n) \neq n$ é verdadeira, para todo $n \in \mathbb{N}$.

□

Os axiomas de Peano permitem definir as operações de adição e multiplicação em $\mathbb{N}$, bem como demonstrar as suas propriedades.

3.2 Operações

3.2.1 Adição

LIMA (2010, p. 35) define a soma $m + n$, onde $m, n \in \mathbb{N}$, utilizando a correspondência sucessora $s : \mathbb{N} \to \mathbb{N}$.

Definição 8. (Adição) Seja uma correspondência $s : \mathbb{N} \to \mathbb{N}$, tal que a cada $n \in \mathbb{N}$ associe o número $s(n) \in \mathbb{N}$. A *operação de adição* é definida por:

(a) $s(n) = n + 1$, para todo $n \in \mathbb{N}$.

(b) $s(n) + m = s(n + m)$, sempre que $n + m \in \mathbb{N}$.

---

[10] A **demonstração por absurdo (ou contradição)** é utilizada quando queremos provar uma proposição do tipo *H (hipótese) implica T (tese)*. Para isso, negando-se apenas a tese *T* (hipótese do raciocínio por absurdo) e, durante todo o processo de demonstração, mantem-se a hipótese *H* como verdadeira até checarmos a um absurdo ou a uma contradição. Diante disto, somos forçados a desfazer a hipótese do raciocínio por absurdo e concluir que a tese *T* é verdadeira. (ÁVILA, p. 8)

A condição ***(a)*** da **Definição 8** estabelece que, dado $n \in \mathbb{N}$, existe $n + 1 \in \mathbb{N}$. Além disso, para representar o sucessor de n, pode-se usar $(n + 1)$ no lugar de $s(n)$. Isto possibilita definir um conjunto X por:

$$X = \{1, s(1), s(s(1)), \cdots\}.$$

O *isomorfismo*[11] entre os conjuntos X e $\mathbb{N}$ permite escrever:

$$X = \{1, s(1), s(s(1)), \cdots\} = \{1, s(1), s(2), \cdots\} = \{1, 2, 3, \cdots\} = \mathbb{N}.$$

Assim, o conjunto dos números naturais passa a ser representado por:

$$\mathbb{N} = \{1, 2, 3, \cdots, n, \cdots\}.$$

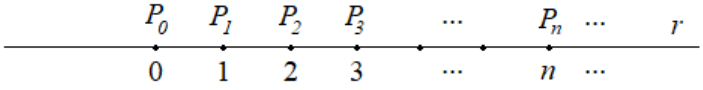
Segundo NERI e AURÉLIO (2011, p. 15): o conjunto dos números naturais $\mathbb{N} = \{1, 2, 3, \cdots\}$ foi o primeiro conjunto numérico construído pela civilização humana destinado à contagem.

Quando houver a necessidade de usar o número 0 (*zero*), indicaremos o conjunto dos números naturais por:

$$\mathbb{N}_0 = \{1, 2, 3, \cdots, n, \cdots\} \cup \{0\} \quad \text{ou} \quad \mathbb{N}_0 = \{0, 1, 2, 3, n, \cdots\}.$$

Do ponto de vista geométrico, os números naturais podem ser representados sobre uma reta, cujos pontos estejam espaçados igualmente numa escala (ou escala-padrão) pré-fixada. Para isto, é necessário e suficiente que se estabeleça uma *correspondência biunívoca* entre o número natural e o ponto da reta. Com efeito, sejam o conjunto dos números naturais $\mathbb{N}_0 = \{0, 1, 2, 3, n, \cdots\}$ e o conjunto dos pontos $P = \{P_0, P_1, P_2, P_3, \cdots, P_n, \cdots\}$ da reta r, igualmente espaçados, conforme representado na FIGURA 4.

FIGURA 4 – Correspondência biunívoca $\alpha : \mathbb{N}_0 \rightarrow P$.



FONTE: elaborada pelo autor.

[11] *Isomorfismo* entre dois conjuntos X e Y é uma função biunívoca $\alpha : X \rightarrow Y$, com as seguintes propriedades: ***i)*** $\alpha(a + b) = \alpha(a) + \alpha(b)$; e ***ii)*** $\alpha(a \cdot b) = \alpha(a) \cdot \alpha(b)$, para todo $a, b \in X$. (GUEDES, 1996, p. 5)

Seja uma correspondência $\alpha : \mathbb{N}_0 \rightarrow P$, definida por $\alpha(n) = P_n$, onde $n \in \mathbb{N}_0$. Assim, para todo $a, b \in \mathbb{N}_0$, $a \neq b$ implica $\alpha(a) = P_a \neq P_b = \alpha(b)$. Logo, α é *injetiva*.

Por outro lado, dado qualquer $P_k \in P$ existe pelo menos um $k \in \mathbb{N}_0$, tal que $\alpha(k) = P_k$, ou seja, α é *sobrejetiva*.

Como a correspondência $\alpha : \mathbb{N}_0 \rightarrow P$ é injetiva e sobrejetiva, portanto, é bijetiva. Estes conceitos serão detalhados no estudo das funções.

3.2.1.1 Propriedades da Adição

Na operação de adição, valem as seguintes propriedades:

A*$_1$) *fechamento: para todo $m, n \in \mathbb{N}$ implica $m + n \in \mathbb{N}$.

Em outras palavras, quaisquer que sejam dois números naturais, a soma destes números é um número natural.

Usaremos o ***Axioma V'*** para demonstrar esta propriedade, com a inserção da correspondência $s : \mathbb{N} \rightarrow \mathbb{N}$, tal que a cada $n \in \mathbb{N}$ associe o número $s(n) \in \mathbb{N}$.

Demonstração: Seja um número n natural fixo qualquer e considere a proposição:

$$P(m): n + m \in \mathbb{N}, \text{ para cada } m \in \mathbb{N}.$$

i') Fazendo $m = 1$, temos: $n + m = n + 1$. Mas, pelo item ***(a)*** da definição de adição, segue que $n + 1 = s(n)$ e, pelo item ***ii)*** do ***Axioma V***, conclui-se que $s(n) \in \mathbb{N}$. Portanto, $P(m)$ é verdadeira, para $m = 1$.

ii') Suponha, por hipótese de indução, que $P(k) : n + k \in \mathbb{N}$ seja verdadeira, para algum $m = k \in \mathbb{N}$. Vamos demonstrar que $P(s(k)) : n + s(k) \in \mathbb{N}$ é verdadeira. De fato, pelo item ***(b)*** da definição de adição, temos: $n + s(k) = s(n + k)$, sempre que $n + k \in \mathbb{N}$ (hipótese de indução). Logo, $s(n + k) \in \mathbb{N}$. Assim, $P(k)$ é verdadeira, para cada $k \in \mathbb{N}$.

Portanto, pelo Princípio de Indução Matemática, a propriedade de fechamento da adição é verdadeira, para todo $m, n \in \mathbb{N}$.

□

A_2) Comutativa: para todo $m, n \in \mathbb{N}$, $m + n = n + m$.

Isto significa que "a ordem das parcelas na operação de adição, não altera resultado (soma ou total)".

Antes de demonstrar esta propriedade, vamos demonstrar a proposição do exemplo a seguir.

Exemplo 7. Mostre que a proposição $P(n)$: $n + 1 = 1 + n$ é verdadeira, para todo $n \in \mathbb{N}$.

Resolução: ***i')*** Fazendo $n = 1$, temos: $1 + 1 = 1 + 1$. Logo, $P(n)$ é verdadeira, para $n = 1$.

ii') Suponha, por hipótese de indução, que $P(k) : k + 1 = 1 + k$ é verdadeira, para algum $m = k \in \mathbb{N}$. Devemos mostrar que $P(s(k)) : s(k) + 1 = 1 + s(k)$ é verdadeira. Com efeito, pelo item ***(a)*** da definição de adição, temos $s(k) = k + 1$.

Assim, $s(k) + 1 = (k + 1) + 1$. Mas, pela hipótese de indução, $k + 1 = 1 + k$. Logo, $s(k) + 1 = (1 + k) + 1$.

Usando novamente a hipótese de indução, temos: $(1 + k) + 1 = 1 + (k + 1)$. Portanto, $s(k) + 1 = 1 + (k + 1)$, mas $s(k) = k + 1$. Logo, $s(k) + 1 = 1 + s(k)$. Conclui-se que a proposição $P(s(k))$ é verdadeira, para cada $k \in \mathbb{N}$.

Portanto, pelo Princípio de Indução Matemática, a proposição é verdadeira, para todo $n \in \mathbb{N}$.

Usaremos esta proposição, que é verdadeira, para provar a propriedade comutativa.

Demonstração: Seja n um número natural fixo qualquer e considere a proposição:

$$P(m): n + m = m + n, \text{ para todo } m \in \mathbb{N}.$$

i') Fazendo $m = 1$, temos: $n + m = n + 1 = s(n)$, pelo item ***(a)*** da definição de adição.

Por outro lado, $m + n = 1 + n$. Mas, pela proposição do **Exemplo 7**, $1 + n = n + 1 = s(n)$. Logo, $P(m)$ é verdadeira, para $m = 1$.

ii') Suponhamos, por hipótese de indução, que $P(k) : n + k = k + n$ é verdadeira, para algum $m = k \in \mathbb{N}$. Vamos provar que $P(s(k)) : n + s(k) = k + s(n)$ é verdadeira. De fato, pelo item ***(b)*** da definição de adição, temos: $n + s(k) = s(n + k)$. Mas, por hipótese de indução, $n + k = k + n$.

Assim, $n + s(k) = s(n + k) = s(k + n) = k + s(n)$. Logo, $P(s(k)) : n + s(k) = k + s(n)$ é verdadeira, para cada $k \in \mathbb{N}$.

Portanto, pelo Princípio de Indução Finita, a propriedade comutativa da adição é verdadeira.

□

A_3) Cancelamento (ou Lei do Corte): para todo $m, n, p \in \mathbb{N}$, $m + p = n + p$ implica $m = n$.

Isto quer dizer que a igualdade não se altera quando adicionamos parcelas iguais a ambos os membros.

Demonstração: Sejam m e n números naturais fixos quaisquer e considere a proposição:

$$P(p): m + p = n + p \text{ implica } m = n, \text{ para algum } p \in \mathbb{N}.$$

i') Fazendo $p = 1$, temos: $m + 1 = n + 1$. Pelo item ***(a)*** da definição de adição, tem-se: $s(m) = s(n)$. Daí, pelo ***Axioma IV*** de Peano, segue que $m = n$.

Portanto, $P(p)$ é verdadeira, para $p = 1$.

ii') Suponha, por hipótese de indução, que a proposição $P(k)$: $m + k = n + k$ implica $m = n$ é verdadeira, para cada $k \in \mathbb{N}$. Precisamos mostrar que $P(s(k))$: $n + s(k) = m + s(k)$ implica $n = m$, para cada $k \in \mathbb{N}$. Com efeito, pelo irem ***(a)*** da definição de adição, temos: $m + s(k) = m + s(k)$ implica $m + k + 1 = n + k + 1$. Por conseguinte, $(m + k) + 1 = (n + k) + 1$. Pela proposição apresentada no **Exemplo 7**, segue $m + k = n + k$. E, pela hipótese de indução, tem-se $m = n$.

Portanto, pelo Princípio de Indução Matemática, a propriedade do cancelamento da adição é verdadeira.

□

A_4) Associativa: para todo $m, n, p \in \mathbb{N}$, $m + (n + p) = (m + n) + p$. Isto significa que a ordem em que adicionam as parcelas, não altera o resultado.

Demonstração: Sejam m e n números naturais fixos quaisquer e considere a proposição:

$$P(p): m + (n + p) = (m + n) + p, \text{ para todo } p \in \mathbb{N}.$$

i') Fazendo $p = 1$, temos: $m + (n + 1) = m + s(n) = s(m + n) = (m + n) + 1$. Portanto, $P(p)$ é verdadeira, para $p = 1$.

ii') Suponha, por hipótese de indução, que $P(k) : m + (n + k) = (m + n) + k$ é verdadeira, para algum $p = k \in \mathbb{N}$. Vamos provar que $P(s(k)) : m + (n + s(k)) = (m + n) + s(k)$ é verdadeira. De fato, pelo item ***(b)*** da definição de adição, temos: $n + s(k) = s(n + k)$. Assim:

$$m + (n + s(k)) = m + s(n + k)$$

$$= s[m + (n + k)].$$

Mas, por hipótese de indução, $m + (n + k) = (m + n) + k$. Logo:

$$m + (n + s(k)) = s[m + (n + k)]$$

$$= s[(m + n) + k]$$

$$= (m + n) + s(k).$$

Portanto, pelo Princípio de Indução Matemática, a propriedade associativa da adição é verdadeira.

□

3.2.2 Multiplicação

De modo semelhante, LIMA (2010, p. 37) define a multiplicação (ou produto) $m.n$, para $m, n \in \mathbb{N}$, a partir da operação de tomar o sucessor.

Definição 9. (Multiplicação) Seja uma correspondência $s : \mathbb{N} \rightarrow \mathbb{N}$, tal que a cada $n \in \mathbb{N}$ associe o número $s(n) \in \mathbb{N}$. A *operação de multiplicação* é definida por:
(a) $n \cdot 1 = n$, para todo $n \in \mathbb{N}$.
(b) $m \cdot s(n) = m \cdot (n + 1)$, para todo $m, n \in \mathbb{N}$.

A condição do item ***(b)*** sugere que o produto satisfaça a propriedade distributiva a seguir:

$$m \cdot (n + 1) = m \cdot n + m, \text{ para todo } m, n \in \mathbb{N}.$$

Demonstração: Considere o conjunto:

$$J_p = \{p \in \mathbb{N} \; ; \; m \cdot (n + p) = m \cdot n + m \cdot p, \text{ onde } m, n \in \mathbb{N}\}.$$

Vamos mostrar, por indução em p, que $J_p = \mathbb{N}$. De fato:

i) Para $p = 1$, temos: $J_1 = \{1 \in \mathbb{N} ; m\cdot(n + 1) = m\cdot n + m = m\cdot s(n)$, onde $m, n \in \mathbb{N}\} \ \therefore \ 1 \in J_1$.

ii) Para $p = k$, temos: $k \in J_k$ implica $s(k) \in J_{k+1}$. Com efeito:

$$\begin{aligned} m\cdot[n + (k + 1)] &= m\cdot[(n + k) + 1] \\ &= m\cdot(n + k) + m \\ &= (m\cdot n + m\cdot k) + m \\ &= m\cdot n + (m\cdot k + m) \\ &= m\cdot n + m\cdot(k + 1) \\ &= m\cdot n + m\cdot s(k). \end{aligned}$$

Assim, $s(k) \in J_{k+1}$. Então, pelo Princípio de Indução Finita, $J_p = \mathbb{N}$.

Em particular, para $p = 1$, $m\cdot(n + p) = m\cdot n + m\cdot p$ implica $m\cdot(n + 1) = m\cdot n + m$, para todo $m, n \in \mathbb{N}$.

□

Definição 10. (Número par e número ímpar) Os números naturais da forma $2\cdot n$ chamam-se *par*, e os da forma $2\cdot n + 1$, chamam-se *ímpar*, para todo $n \in \mathbb{N}$.

Segundo CARAÇA (1989, p. 51), a propriedade de um número natural ser, unicamente, par ou ímpar, chama-se *paridade* desse número.

3.2.2.1 Propriedades da Multiplicação

A operação de multiplicação possui as seguintes propriedades: dados $m, n, p \in \mathbb{N}$, temos:

M₁) fechamento: $m, n \in \mathbb{N}$ implica $m\cdot n \in \mathbb{N}$.

M₂) Comutatividade: $m\cdot n = n\cdot m$.

M₃) Lei do Corte: $m\cdot p = n\cdot p$ implica $m = n$.

M₄) Associatividade: $m\cdot(n\cdot p) = (m\cdot n)\cdot p$.

M₅) Distributividade em relação à adição: $m\cdot(n + p) = m\cdot n + m\cdot p$.

De modo semelhante às propriedades da adição, demonstra-se as propriedades da multiplicação.

A propriedade ***M₅)*** foi demonstrada logo acima e, para fixar as ideias, faremos apenas a demonstração da propriedade ***M₂)***, ou seja, para todo $m, n, p \in \mathbb{N}$ vale a ***propriedade comutativa*** $m \cdot n = n \cdot m$.

Demonstração: Fixando m, considere a proposição:

$$P(n) : m \cdot n = n \cdot m, \text{ para todo } n \in \mathbb{N}.$$

Para $n = 1$, temos:

$$m \cdot 1 = 1 \cdot m, \text{ para todo } m \in \mathbb{N}.$$

A veracidade desta última igualdade pode ser demonstrada usando-se indução sobre m.

Sabemos que é verdade que $m \cdot 1 = m$. Assim, devemos provar $1 \cdot m = m$. Com efeito, para $m = 1$, é verdade que $1 \cdot 1 = 1$.

Suponha que seja verdadeiro para algum $m \in \mathbb{N}$, isto é, $1 \cdot m = m$. Então:

$$1 \cdot (m + 1) = 1 \cdot m + 1 = m + 1.$$

Agora, suponha que $m \cdot n = n \cdot m$. Vamos mostrar que isto implica $m \cdot (n + 1) = (n + 1) \cdot m$. De fato:

$$m \cdot (n + 1) = m \cdot n + m = m \cdot n + m = (n + 1) \cdot m.$$

Logo, pelo Princípio de Indução Finita, a propriedade comutativa $m.n = n.m$ é verdadeira.

□

Exemplo 8. Sejam $p, q \in \mathbb{N}$.

a) Se p e q têm a mesma paridade de serem pares, então $p + q$ e $p \cdot q$ são pares.

b) Se p e q têm a mesma paridade de serem ímpares, então $p + q$ é par e $p \cdot q$ é ímpar.

Resolução: a) Como p e q são ambos pares, temos $p = 2 \cdot m$ e $q = 2 \cdot n$. Assim:

$$p + q = 2 \cdot m + 2 \cdot n = 2 \cdot (m + n) = 2 \cdot k, \text{ onde } k = m + n.$$

$$p \cdot q = 2 \cdot m \cdot 2 \cdot n = 2 \cdot (2 \cdot m \cdot n) = 2 \cdot k, \text{ onde } k = 2 \cdot m \cdot n.$$

b) Agora, p e q são ambos ímpares, logo, $p = 2 \cdot m + 1$ e $q = 2 \cdot n + 1$. Dessa forma:

$p + q = 2\cdot m + 1 + 2\cdot n + 1 = 2\cdot(m + n) + 2 = 2\cdot(m + n + 1) = 2\cdot k$, onde $k = m + n + 1$.

$p\cdot q = (2\cdot m + 1)\cdot(2\cdot n + 1) = 2\cdot m\cdot(2\cdot n + 1) + 2\cdot n + 1 = 2\cdot[m\cdot(2\cdot n + 1) + n] + 1 = 2\cdot k + 1$, onde $k = m\cdot(2n + 1) + n$.

3.3 Relação de Ordem

Antes de definirmos a relação de ordem entre números naturais, veremos uma proposição (**Exemplo 9**) que possibilitará conexão entre a relação de igualdade e a relação de ordem, por meio da operação de adição.

Exemplo 9. Seja uma correspondência $s : \mathbb{N} \to \mathbb{N}$, tal que a cada $n \in \mathbb{N}$ associe o número $s(n) \in \mathbb{N}$. Prove que cada número natural $n \neq 1$ é sucessor de algum outro número natural.

Resolução: De acordo com o ***Axioma III***, 1 não é sucessor de nenhum outro número natural, ou seja, para todo $n \in \mathbb{N}$, tem-se $1 \neq s(n)$.

Agora, considere o conjunto $S = \{1\} \cup \{n\ ;\ n \in \mathbb{N}$, com $n = s(m)$, para algum $m \in \mathbb{N}\}$. Então, pelo ***Axioma I***, $1 \in S$.

O ***Axioma II*** permite afirmar que, a cada $n \in \mathbb{N}$, *existe* um *único* $s(n) \in \mathbb{N}$. Como $s(n)$ é um sucessor, então, para cada $n \in \mathbb{N}$ implica $s(n) \in S$. Logo, pelo ***Axioma V***, $S = \mathbb{N}$.

Portanto, para todo $n \in \mathbb{N}$, temos $n = 1$ ou $n = s(m)$, para algum $m \in \mathbb{N}$.

□

De acordo com AYRES (1973, p. 48 - 49), a *relação de ordem* no conjunto dos números naturais pode ser assim definida:

Definição 11. Seja dois números naturais m e n quaisquer.
(a) m é *menor do que* n, e escrevemos $m < n$, se existe $p \in \mathbb{N}$, tal que $n = m + p$.
(b) m é *maior do que* n se, e somente se, $n < m$.

Quando m é menor ou igual a n, escreve-se $m \leq n$. Isto equivale a $m < n$ ou $m = n$. De modo semelhante, quando m é maior ou igual a n, escrevemos $m \geq n$, para significar que $m > n$ ou $m = n$.

Com a proposição do **Exemplo 9** (cada número natural $n \neq 1$ é sucessor de algum outro número natural) e a relação de ordem " $<$ " podemos escrever as proposições:

$$P(n) : 1 < n, \text{ para todo natural } n \neq 1.$$

e

$$P(n) : n < s(n) = n + 1, \text{ para todo } n \in \mathbb{N}.$$

Demonstração: No primeiro caso, temos: para todo $n \neq 1$, tem-se $n = s(m)$, para algum $m \in \mathbb{N}$. Mas, $n = s(m) = m + 1$, portanto, $m + 1 = n$ e, por conseguinte, $1 < n$. Assim, a proposição é verdadeira.

No outro caso, sabe-se $s(n) = n + 1$, para todo $n \in \mathbb{N}$. Então, fazendo $p = 1$, tem-se $n + 1 = n + p = s(n)$. Daí, $n < s(n)$, para todo $n \in \mathbb{N}$. Portanto, a proposição é verdadeira.

□

Em decorrência da validade da proposição $P(n) : 1 < n$, para todo natural $n \neq 1$, FERREIRA (2013, p. 31) menciona que: "não há naturais compreendidos entre n e $s(n)$, pois $s(n) = n + 1$".

Proposição 2. Não existe número natural entre dois números naturais consecutivos.

Demonstração: Suponha, por absurdo, que exista $m \in \mathbb{N}$, tal que $n < m < n + 1$, para todo $n \in \mathbb{N}$. Então, existem $r, s \in \mathbb{N}$, tais que $m = n + r$ e $n + 1 = m + s$.

Assim, $n + 1 = n + (r + s)$. Daí, pela Lei do Corte referente à operação de adição, segue que: $1 = r + s$, o que é um absurdo! Logo, não existe $m \in \mathbb{N}$, tal que $n < m < n + 1$, para todo $n \in \mathbb{N}$.

□

Em decorrência disso, pode-se definir o antecessor de um número natural.

Definição 12. Sejam $n, m \in \mathbb{N}_0$. Um número natural n chama-se o *antecessor* de m, se $n < m$ e não existe $p \in \mathbb{N}$, tal que $n < p < m$.

Exemplo 10. Para todo $m, n \in \mathbb{N}$, tem-se $m + n \neq m$.

Demonstração: De fato, fixando n, considere a proposição:

$$P(m) : m + n \neq m, \text{ para } m \in \mathbb{N}.$$

Para $m = 1$, temos: $P(1) : 1 + n \neq 1$ é verdadeira.

Suponha que, para algum $k \in \mathbb{N}$, a proposição $P(k) : k + n \neq k$ seja verdadeira. Assim, $s(k + n) \neq s(k)$, pois, pelo ***Axioma IV***, $s(k + n) = s(k)$ implica $k + n = k$, o que é um absurdo! Logo:

$$P(s(k)) : s(k) + n \neq s(k).$$

Portanto, pelo Princípio de Indução Finita, $m + n \neq m$, para todo $m, n \in \mathbb{N}$.

□

Proposição 3. A relação de ordem "<" é transitiva, mas não é reflexiva ou simétrica.

Demonstração: Com efeito, sejam $m, n, p \in \mathbb{N}$ e suponha que $m < n$ e $n < p$. Então, existem $r, s \in \mathbb{N}$, tais que $m + r = n$ e $n + s = p$. Logo:

$$n + s = p \text{ implica } (m + r) + s = m + (r + s) = m + t = p, \text{ para } t = r + s, \text{ logo, } m < p.$$

Portanto, a relação "<" é transitiva.

Agora, seja $n \in \mathbb{N}$. Temos: $n < n$ é falsa, pois, se fosse verdadeira, existiria algum $k \in \mathbb{N}$, tal que $n + k = n$, mas, pelo **Exemplo 10**, isto é um absurdo! Assim, a relação "<" não é reflexiva.

Finalmente, sejam $m, n \in \mathbb{N}$ e suponha que $m < n$ e $n < m$. Como "<" é transitiva, temos $m < n$ e $n < m$ implica $m < m$, o que é um absurdo! Pois, "<" não é reflexivo. Portanto, a relação "<" não é simétrica.

Dessa forma, a relação de ordem não é uma relação de equivalência, pois, não valem as propriedades reflexiva e simétrica; vale apenas a propriedade transitiva.

Conforme LIMA (2010, p. 37), as relações de igualdade e ordem de dois números naturais estabelecem a propriedade da tricotomia expressa a seguir.

Tricotomia. Sejam dois números naturais m e n quaisquer. Então, uma, e somente uma, das seguintes condições pode ocorrer:

T_1) ou $m > n$ (isto é, existe $p \in \mathbb{N}$, tal que $m = n + p$);

T_2) ou $m = n$;

T_3) ou $m < n$ (isto é, existe $p \in \mathbb{N}$, tal que $n = m + p$).

Demonstração: Para todo $m \in \mathbb{N}$, considere os subconjuntos de $\mathbb{N}$ a seguir:

$$N_1 = \{m\},$$

$$N_2 = \{x \in \mathbb{N} ; x < m\} \text{ e}$$

$$N_3 = \{x \in \mathbb{N} ; x > m\}.$$

Note que o conjunto $\{N_1, N_2, N_3\}$ é uma *partição* de $\mathbb{N}$ referente às relações ">" (maior do que), "=" (igual a) e "<" (menor do que). Com efeito, para $m = 1$, temos:

$$N_1 = \{1\},$$

$$N_2 = \varnothing \text{ e}$$

$$N_3 = \{x \in \mathbb{N} ; x > 1\}.$$

Neste caso, $N_1 \cup N_2 \cup N_3 = \mathbb{N}$.

Agora, devemos mostrar que $N_1 \cap N_2 = N_1 \cap N_3 = N_2 \cap N_3 = \varnothing$. De fato, suponha que $m \neq 1$. Assim, $1 \in N_2$, por conseguinte, $1 \in N_1 \cup N_2 \cup N_3$.

Escolhendo qualquer $p \in \mathbb{N}$, há três casos para considerar:

i) $n \in N_1$. Neste caso, temos $n = m$ e, portanto, $s(n) = n + 1 \in N_3$.

ii) $n \in N_2$. Dessa forma, $n < m$. Logo, existe $p \in \mathbb{N}$, tal que $m = n + p$. Daí, se $p = 1$, temos $s(n) = n + 1 = m \in N_1$. Mas, se $p \neq 1$, segue que $p = 1 + q$, para algum $q \in \mathbb{N}$. Então: $n + p = n + (1 + q) = (n + 1) + q = s(n) + q = m$, logo Daí, $s(n) <= m$ e, portanto, $s(n) \in N_2$.

iii) $n \in N_3$. Daí, $s(n) > n > m$, portanto, $s(n) \in N_3$.

Assim, para cada $n \in \mathbb{N}$, temos $n \in N_1 \cup N_2 \cup N_3$ implica $s(n) \in N_1 \cup N_2 \cup N_3$. Como $1 \in N_1 \cup N_2 \cup N_3$, segue que $N_1 \cup N_2 \cup N_3 = \mathbb{N}$.

Como $m \notin N_2$, temos $N_1 \cap N_2 = \varnothing$. De modo semelhante, $N_1 \cap N_3 = \varnothing$. Agora, suponha, por absurdo, que $N_2 \cap N_3 = \{p\}$, para algum $p \in \mathbb{N}$. Então, $p < m$ e $m < p$. Como "<" é uma relação transitiva, temos $p < p$, o que é uma contradição! Logo, devemos ter $N_1 \cap N_3 = \varnothing$.

□

Exemplo 11. (Coleção PORFMAT – Números e Funções) Dado o número natural a, seja um conjunto $J \subset \mathbb{N}$, com as seguintes propriedades:

(1) $a \in J$;

(2) $n \in J$ implica $n + 1 \in J$.

Prove que J contém todos os números naturais maiores do que ou iguais a a. (*Sugestão*: considere o conjunto $X = I_a \cup J$, onde I_a é o conjunto dos números naturais $\leq a$, e prove, por indução, que $X = \mathbb{N}$.)

Resolução: Seja um conjunto $J \subset \mathbb{N}$, com $a \in J$ e $n \in J$ implica $n + 1 \in J$. Para $a = 1$, temos $1 \in X = I_a \cup J$.

Suponha que $n \in X$. Então, $n \in I_a \cup J$ implica $n \in J$, portanto, pela propriedade (2), segue $n + 1 \in J$. Logo, $n + 1 \in I_a \cup J = X$.

Dessa forma, temos $1 \in X$ e $n \in X$ implicam $n + 1 \in X$. Logo, $X = \mathbb{N}$.

Por fim, considere $\mathbb{N} = X = I_a \cup J$, onde I_a é o conjunto dos números naturais $\leq a$. Assim, $I_a = \{1, 2, 3, \cdots, a\}$ e $\mathbb{N} = \{1, 2, 3, \cdots, n, \cdots\}$. Daí:

$$\mathbb{N} = I_a \cup J \iff \{1, 2, 3, \ldots, n, \ldots\} = \{1, 2, 3, \ldots, a\} \cup J \iff J = \{n \in \mathbb{N} ; a \leq n\}.$$

Proposição 4. Sejam $a, b \in \mathbb{N}$. Então, $a < b$ se, e somente se, $a + 1 \leq b$.

Demonstração: ($\Longrightarrow$) Temos: $a < b$, então existe $p \in \mathbb{N}$, tal que $b = a + p$. Mas, pelo ***Axioma II*** de Peano (para cada $n \in \mathbb{N}$, *existe* um *único* $s(n) \in \mathbb{N}$), segue que: dado $q \in \mathbb{N}$, existe um único $s(q) = q + 1$ em $\mathbb{N}$.

Fazendo $p = s(q)$, temos:

$$b = a + s(q) = a + (q + 1) = a + (1 + q) = (a + 1) + q \ \therefore^{12} \ a + 1 \leq b.$$

($\Longleftarrow$) Reciprocamente, se $a + 1 \leq b$, existe $p \in \mathbb{N}$, tal que $b = a + 1 + p$. Assim, pelo ***Axioma II*** de Peano, dado $p \in \mathbb{N}$, existe um único $s(p) = p + 1 = 1 + p$ em $\mathbb{N}$. Logo:

$$b = a + s(p) \ \therefore \ a < b.$$

□

[12] Em matemática, o símbolo "$\therefore$" significa "*portanto*" ou "*então*". (CORDEIRO, 2014, p. 83)

FERREIRA (2013, p. 31) destaca uma propriedade importante do conjunto dos números naturais, a qual "todo subconjunto não vazio de $\mathbb{N}$ possui um menor elemento".

Isto significa que o conjunto dos números naturais é *bem ordenado*. Na verdade, todo conjunto com esta propriedade é um conjunto *bem ordenado*.

Antes de demonstrarmos este fato, definiremos mínimo e máximo de um subconjunto do conjunto dos números naturais.

Definição 13. Seja um subconjunto X não vazio do conjunto dos números naturais. Um número $m \in X$ chama-se *o menor elemento* (ou *mínimo*) de X quando $m \leq x$, para todo $x \in X$.

O elemento mínimo de um conjunto X indica-se por: $min(X)$.

Conforme LIMA (2010, p. 39), $min(\mathbb{N}) = 1$. Mais ainda, qualquer que seja $X \subset \mathbb{N}$, com $1 \in X$, tem-se $min(X) = 1$.

Princípio da Boa Ordenação – PBO. Todo subconjunto não vazio de números naturais admite um único elemento mínimo.

Demonstração: **(*Existência)*** Seja um subconjunto X de $\mathbb{N}$, tal que $X \neq \varnothing$. Se $1 \in X$, então $1 = min(X)$.

Suponha que $1 \notin X$. Então, para todo $p \in X$, temos $1 < p$. Considere o conjunto:

$$J = \{n \in \mathbb{N} \,;\, n \leq x, \text{ para todo } x \in X\}.$$

Temos: $1 \in J$. Como $X \neq \varnothing$, tome $p \in X$. Daí, $p + 1 \notin J$. Logo, $J \neq \mathbb{N}$.

Dessa forma, $1 \in J$ e $J \neq \mathbb{N}$. Com isto, deve existir $m \in J$, tal que $m + 1 \notin J$, pois, do contrário, pelo Princípio de Indução Finita, teríamos $J = \mathbb{N}$, o que não pode ocorrer.

Assim, $m = min(X)$. De fato, como $m \in J$, segue $m \leq x$, para todo $x \in X$.

Agora, pela **Definição 13**, só falta mostrar que $m \in X$. Com efeito, suponha, por absurdo, que $m \notin X$. Então, para todo $x \in X$, temos $m < x$. Daí, pela **Proposição 4**, segue

$m + 1 \leq x$, para todo $x \in X$. Isto implica $m + 1 \in X$, o que é um absurdo! Pois, contraria a escolha de $m \notin X$. Logo, $m \in X$.

(*Unicidade*) Suponha que $p, q \in \mathbb{N}$ sejam ambos os menores elementos de X. Então, $p \leq q$ e $q \leq p$. Assim, $p = q$.

□

Teorema 2. (PIF e PBO) O Princípio de Indução Finita (PIF) é equivalente ao Princípio da Boa Ordenação (PBO).

Demonstração: ($\Longrightarrow$) Suponha válido o PIF, isto é: seja um conjunto não vazio $X \subset \mathbb{N}$ satisfazendo as seguintes propriedades:
i) $1 \in X$; e
ii) $n \in X$ implica $n + 1 \in X$.

Queremos provar que X possui um elemento mínimo, ou seja, para todo $x \in X$, existe $n \in X$, tal que $n \leq x$. De fato, suponha, por absurdo, que X não possui elemento mínimo. Assim, em particular, $1 \notin X$, pois, se pertencesse, seria o elemento mínimo.

Seja o conjunto $J = \{n \in \mathbb{N} \ ; \ n < x$, para todo $x \in X\}$. Assim, $J \cap X = \varnothing$, pois, se $J \cap X \neq \varnothing$, então existe $n \in J \cap X$, com $n \in J$ e $n < x$, para todo $x \in X$. Em particular, $n = x \in X$, obtemos $n < n$, o que é um absurdo! Então, $J \cap X = \varnothing$.

Agora, mostraremos que $J = \mathbb{N}$. Com efeito, sabemos que $1 \notin X$, portanto, $1 < x$, qualquer que seja $x \in X$. Assim, $n + 1 \leq x$. Se $n + 1 \in X$, temos $n + 1$ é um elemento mínimo de X. Mas, por hipótese, X não possui elemento mínimo. Daí, $n + 1 \notin X$ e, portanto, $n + 1 < x$, para todo $x \in X$. Dessa forma, $n + 1 \in J$.

Portanto, pelo Princípio de Indução Finita, $J = \mathbb{N}$.

($\Longleftarrow$) Suponha válido o PBO, isto é, todo subconjunto não vazio $X \subset \mathbb{N}$ possui elemento mínimo. Em outras palavras, para todo $x \in X$, existe $n \in X$, tal que $n \leq x$.

Vamos provar que X tem as propriedades:
i) $1 \in X$; e
ii) $n \in X$ implica $n + 1 \in X$.

De fato, suponha, por absurdo, que X satisfazendo as propriedades *i)* e *ii)*, porém, com $X \neq \mathbb{N}$. Isto significa que existe algum elemento em $\mathbb{N}$, que não pertence a X.

Assim, o conjunto $\mathbb{N} - X \neq \varnothing$. Daí, pelo Princípio da Boa Ordenação, o conjunto $(\mathbb{N} - X) \subset \mathbb{N}$ possui elemento mínimo. Seja $m = min(\mathbb{N} - X)$.

Como, pela hipótese *i)* $1 \in X$, temos $1 < m$. Assim, o "*antecessor* de m" é *menor do que* m. Mas este "*antecessor* de m", *não pertence* a $\mathbb{N} - X$, logo, pertence a X e, por conseguinte, o "*antecessor* de m" + 1 *pertence* a X, o que é um absurdo! Isto ocorreu, porque supomos $X \neq \mathbb{N}$. Logo, $X = \mathbb{N}$.

□

Definição 14. Seja um subconjunto X não vazio do conjunto dos números naturais. Um número $m \in X$ chama-se *o maior elemento* (ou *máximo*) de X quando $m \geq x$, para todo $x \in X$.

O elemento máximo de um conjunto X indica-se por: $max(X)$.

LIMA (2010, p. 39) destaca: "nem todo conjunto de números naturais possui um elemento máximo". E, com exemplo disto, ele apresenta o conjunto dos números naturais $\mathbb{N} = \{1, 2, 3, \cdots, n, \cdots\}$. De fato, para todo $p \in \mathbb{N}$, sempre temos $p < p + 1$.

Ainda nesse contexto, se existir o máximo de um conjunto $X \subset \mathbb{N}$, ele é único. Com efeito, suponha que $p, q \in \mathbb{N}$ sejam ambos os máximos de X. Então, $q \leq p$ e $p \leq q$. Logo, $p = q$.

Segundo LIMA (2010, p. 40), uma consequência do Princípio da Boa Ordenação é a proposição conhecida como o Segundo Princípio da Indução, o qual é apresentado e justificado a seguir.

Segundo Princípio da Indução. Seja um conjunto $X \subset \mathbb{N}$ com a seguinte propriedade: dado $n \in \mathbb{N}$, caso ocorra de todos os números naturais $p < n$ implicarem $p \in X$, assim, $n \in X$. Dessa forma, conclui-se que $X = \mathbb{N}$.

Demonstração: Suponha, por absurdo, que $X \neq \mathbb{N}$. Em outras palavras, considere o conjunto $J = \mathbb{N} - X$, com $J \neq \varnothing$. Então, $J \subset \mathbb{N}$ e $J \neq \varnothing$. Daí, pelo Princípio da Boa Ordenação, existe $y = min(J) \in \mathbb{N}$, tal que $y \notin X$. Assim, todos os números naturais $n < y$ pertencem a X, portanto,

$n \in X$. Mas, o que é uma contradição! Isto se deu pelo fato de assumir que $J \neq \varnothing$. Logo, $J = \varnothing$ e, por conseguinte, $X = \mathbb{N}$.

Nesse contexto e, semelhante ao Princípio de Indução Finita:

> O *Segundo Princípio de Indução constitui um método* útil *para demonstração de proposições referentes a números naturais*. Ele também pode ser enunciado assim: Seja P uma propriedade relativa a números naturais. Se, dado $n \in \mathbb{N}$, de modo que todo número natural $m < n$ gozar da propriedade P puder se inferido que n goza da propriedade P, então todo número natural goza de P. (LIMA, 2010, p. 40, grifos nossos)

Em outras palavras, seja uma propriedade $P(n)$ associada a cada $n \in \mathbb{N}$. Se, para cada $m \in \mathbb{N}$, a hipótese de que $P(m)$ é verdadeira, para todo $m < n$, implicar a validade de $P(n)$, então $P(n)$ é verdadeira para todo $n \in \mathbb{N}$.

Usa-se o Segundo Princípio de Indução quando uma propriedade $P(n)$, que se refere a números naturais n, falha na verificação de todos os números naturais *menores ou iguais* a $n \in \mathbb{N}$.

3.4 Potenciação

Seja $a \in \mathbb{N}$. Chama-se *potência* de *base* "a" com *expoente* "k", o número a^k definido por:

i) $a^1 = a$; e

ii) $a^{k+1} = a^k \cdot a$, onde $k \in \mathbb{N}$.

Dessa forma, pode-se escrever o número a^k como o produto de k fatores iguais à base a, ou seja:

$$a^k = a \cdot a \cdot a \cdot \cdots \cdot a$$
(k fatores)

Proposição 5. (Unicidade) Para todo $n, m \in \mathbb{N}$, temos $a^n = a^m$ se, e somente se, $n = m$, onde $a \in \mathbb{N}$.

Demonstração: Para $n = m = 1$, segue:

$$a^n = a^1 = a \text{ e } a^m = a^1 = a \text{ e, portanto, } a^1 = a^1.$$

Suponha que, para $n = m = k$, valha $a^n = a^m$. Mostraremos que, para $n = k + 1$, vale a igualdade $a^{k+1} = a^{k+1}$. De fato, por hipótese de indução, temos:

$$a^n = a^m \text{ implica } a^k = a^k.$$

Multiplicando ambos os membros desta última igualdade por a, obtém-se:

$$a^k \cdot a = a^k \cdot a = a^m \text{ e, por definição, } a^{k+1} = a^{k+1}.$$

Assim, pelo Princípio de Indução Finita, conclui-se a demonstração.

□

3.4.1 Propriedades de Potência

Para todo $n, m \in \mathbb{N}$, valem as propriedades:

P₁) $a^n \cdot a^m = a^{n+m}$.

P₂) $(a^m)^n = a^{m.n}$.

P₃) $(a \cdot b)^n = a^n \cdot b^n$.

P₄) $1^n = 1$.

Demonstração: Vamos fixar $a, m \in \mathbb{N}$ e usar a indução sobre n. Em ***P₁)***, para $n = 1$, temos:

$$a^1 \cdot a^m = a \cdot a^m = a^m \cdot a = a^{m+1}.$$

Suponha, por hipótese de indução, que $a^n \cdot a^m = a^{n+m}$ seja verdadeiro. Mostraremos que a propriedade é verdadeira para $n + 1$. De fato:

$$a^{n+1} \cdot a^m = a^n \cdot a^1 \cdot a^m = (a^n \cdot a^m) \cdot a^1.$$

Usando a hipótese de indução $a^n \cdot a^m = a^{n+m}$ e a definição $a^{k+1} = a^k \cdot a$, segue:

$$a^{n+1} \cdot a^m = (a^n \cdot a^m) \cdot a^1 = a^{n+m} \cdot a^1 = a^{(n+m)+1}.$$

Logo, pelo Princípio de Indução Finita, a propriedade ***P₁)*** é verdadeira.

Em ***P₂)***, para $n = 1$: $(a^m)^n = (a^m)^1 = a^m = a^{m.1}$.

Suponha, por hipótese de indução, que $(a^m)^n = a^{m.n}$ seja verdadeiro. Temos:

$$(a^m)^{n+1} = (a^m)^n \cdot (a^m)^1.$$

Usando a hipótese de indução $(a^m)^n = a^{m.n}$ e a definição $a^1 = a$ e $a^{k+1} = a^k \cdot a$, segue:

$$(a^m)^{n+1} = (a^m)^n \cdot (a^m)^1 = a^{m.n} \cdot a^m = a^{m.n+m} = a^{m.(n+1)}.$$

Assim, pelo Princípio de Indução Finita, a propriedade ***P₂)*** é verdadeira.

Em ***P₃)***, para $n = 1$: $(a \cdot b)^1 = a^1 \cdot b^1$.

Suponha, por hipótese de indução, que $(a \cdot b)^n = a^n \cdot b^n$ seja verdadeiro. Mostraremos que a propriedade é verdadeira para $n + 1$. De fato:

$$(a \cdot b)^{n+1} = (a \cdot b)^n \cdot (a \cdot b)^1.$$

Usando a hipótese de indução $(a \cdot b)^n = a^n \cdot b^n$ e a propriedade ***P₁)***, segue:

$$(a \cdot b)^{n+1} = (a \cdot b)^n \cdot (a \cdot b)^1 = a^n \cdot b^n \cdot a^1 \cdot b^1 = a^n \cdot a^1 \cdot b^n \cdot b^1 = a^{n+1} \cdot b^{n+1}.$$

Em ***P₄)***, para $n = 1$, temos: $1^1 = 1$.

Suponha, por hipótese de indução, que $1^n = 1$. Mostraremos que a propriedade é verdadeira para $n + 1$. De fato:

$$1^{(n+1)} = 1^n \cdot 1 = 1 \cdot 1 = 1.$$

Portanto, pelo Princípio de Indução Finita, a propriedade ***P₃)*** é verdadeira.

□

Observações:

Na potência a^k, tem-se:

- para $k = 0$ e $a \neq 0$, segue, de acordo com a definição, $a^{0+1} = a^0 \cdot a = a^1$. Mas, $a^1 = a$, portanto, $a = a^0 \cdot a$. Esta igualdade *exige* que $a^0 = 1$. Assim, definimos: $a^0 = 1$, com $a \neq 0$;
- se $a = k = 0$, ocorre que 0^0. Neste caso, segundo CARAÇA (1989, p. 246), trata-se de uma *indeterminação*, cujo resultado da operação, *a priori*, não pode ser obtido. Há autores que definem $0^0 = 1$.

Exemplo 12. Prove que $2^n > n^2$, para todo número natural $n \geq 5$.

Resolução: Observe que para $n = 1, 2, 3$ e 4, a proposição $P(n) : 2^n > n^2$ é falsa. Então, de fato, temos que mostrar que a partir de $n = 5$, a proposição é verdadeira. Com efeito, para $n = 5$, temos:

$$P(5) : 2^5 = 2 \times 2 \times 2 \times 2 \times 2 = 32 > 5^2 = 25.$$

Suponha, por hipótese de indução e para $n \geq 5$, que $P(n) : 2^n > n^2$. Então, para $n + 1$, segue:

$$P(n + 1) : 2^n > n^2 \text{ implica } 2^n \cdot 2 > n^2 \cdot 2 \text{ e, portanto, } 2^{n+1} > 2 \cdot n^2.$$

Porém, note que $2 \cdot n^2 > (n + 1)^2$, para $n \geq 3$, e também $n \geq 5$. Daí:

$$2^{n+1} > 2 \cdot n^2 > (n + 1)^2, \text{ portanto, } 2^{n+1} > (n + 1)^2, \text{ para todo } n \geq 5.$$

Assim, pelo Princípio de Indução Finita, a proposição $P(n) : 2^n > n^2$ é verdadeira, para todo número natural $n \geq 5$.

4 Relações Binárias

4.1 Conceito

No sentido intuitivo, quando há uma razão para associarmos certos objetos de uma coleção a certos objetos de outra coleção, usamos a palavra "relação".

A noção importante que reside na relação é que estamos escolhendo, por algum motivo, certos pares ordenados cujos termos estão relacionados. A razão desta escolha é uma forma de definir a relação entre os elementos duas coleções. Em outras palavras, é a essência da definição de relação, em matemática.

Para LIPSCHUTZ (1972, p. 114): uma relação $\mathcal{R}$ consiste em dois conjuntos A, B e uma *sentença aberta*[13] representada por $p(x, y)$, na qual é verdadeira ou falsa, para qualquer par ordenado $(a, b) \in A \times B$.

Em símbolos, representa-se uma relação $\mathcal{R}$ de A em B por:

$$\mathcal{R} = (A, B, p(x, y)).$$

Ademais, se a *sentença fechada*[14] $p(a, b)$ é verdadeira, escreve-se: "a está relacionado com b, pela relação $\mathcal{R}$" e denota-se por $a\mathcal{R}b$. Em outras palavras:

$$a\mathcal{R}b \text{ se, e somente se, } (a, b) \in \mathcal{R}.$$

Por outro lado, se a sentença $p(a, b)$ é falsa, escreve-se: "a não está relacionado com b, por $\mathcal{R}$" e representa-se por $a\tilde{\mathcal{R}}b$. Neste caso:

$$a\tilde{\mathcal{R}}b \text{ se, e somente se, } (a, b) \notin \mathcal{R}.$$

---

[13] Uma *sentença aberta* sobre um conjunto A é uma expressão designada por $p(x)$ que apresenta a propriedade de $p(a)$ é verdadeira ou falsa, para cada $a \in A$. (LIPSCHUTZ, 1973, p. 298)

[14] Uma *sentença fechada* sobre um conjunto A é uma expressão $p(a)$, que provém de uma sentença aberta $p(x)$, tal que $x = a$, para cada $a \in A$.

Exemplo 13. Sejam os conjuntos $X = \{a, b\}$ e $Y = \{c, d\}$. Considere $\mathcal{R} = \{X, Y, p(x, y)\}$, tal que $p(x, y)$, lê-se: "x vem primeiro que y".

Assim, $\mathcal{R}$ é uma relação de X para Y, porque $p(a, c)$ e $p(a, d)$ são verdadeiras e, portanto, $a\mathcal{R}c$ e $a\mathcal{R}d$. Além disso, $p(b, c)$ e $p(b, d)$ são falsas. Daí, $b\tilde{\mathcal{R}}c$ e $b\tilde{\mathcal{R}}d$.

4.2 Conjunto Solução

Seja uma relação $\mathcal{R} = (A, B, p(x, y))$ sobre o conjunto $A \times B$. O conjunto constituído pelos elementos de $(a, b) \in A \times B$, para o qual $p(a, b)$ é verdadeiro, chama-se *conjunto solução* (ou *conjunto verdade*) e denotamos por:

$$S_{\mathcal{R}} = \{(a, b)\ ;\ a \in X, b \in Y, p(a, b) \text{ é verdadeiro}\}.$$

Observe que, na relação $\mathcal{R}$ de X para Y, o conjunto verdade $S_{\mathcal{R}}$ é constituído por elementos de $A \times B$. Portanto, $S_{\mathcal{R}}$ é um *subconjunto* de $A \times B$, isto é, $S_{\mathcal{R}} \subset A \times B$.

Para LIPSCHUTZ (1972, p. 116): a cada relação $\mathcal{R}$ corresponde um único conjunto solução $S_{\mathcal{R}}$ e, reciprocamente, a cada conjunto solução $S_{\mathcal{R}}$ corresponde uma relação $\mathcal{R}$, para a qual $S_{\mathcal{R}}$ é o conjunto solução.

Dessa forma, pode-se *redefinir* o conceito de relação, sem usar o conceito de sentença aberta.

Definição 15. (Relação entre conjuntos) Sejam dois conjuntos X e Y. Dizemos que $\mathcal{R}$ é uma relação de X *para* Y, se $\mathcal{R}$ é um subconjunto de $X \times Y$, ou seja, se $\mathcal{R} \subseteq X \times Y$.

Na relação $\mathcal{R}$ de X para Y, há dois subconjuntos especiais para discussão, a saber: o *domínio* e a *imagem* (ou *amplitude*) de $\mathcal{R}$.

Definição 16. (Domínio) Seja uma relação $\mathcal{R}$ de $X \times Y$. Chama-se conjunto *domínio* de $\mathcal{R}$, o subconjunto $D_{\mathcal{R}} \subseteq X$, tal que, para cada $a \in X$, existe algum $b \in Y$, de modo que $a\mathcal{R}b$.

Em símbolo, escreve-se:

$$D_{\mathcal{R}} = \{a\ ;\ \text{existe algum } b \in Y, \text{com } a\mathcal{R}b\}.$$

De modo semelhante:

Definição 17. (Imagem) Seja uma relação $\mathcal{R}$ de $X \times Y$. Chama-se conjunto *imagem* de $\mathcal{R}$ o subconjunto $Im_{\mathcal{R}} \subseteq Y$, de modo que, para cada $b \in Y$, existe algum $a \in X$, tal que $a\mathcal{R}b$.

Em símbolo, escrevemos:

$$Im_{\mathcal{R}} = \{b \text{ ; existe algum } a \in X, \text{ com } a\mathcal{R}b\}.$$

O conjunto Y na relação $\mathcal{R}$ chama-se *contradomínio* e, em símbolos, denota-se por: $CD_{\mathcal{R}} = Y$.

Observação:

Em se tratando da *relação* $\mathcal{R}$ de X em Y, a *existência* de $b \in Y$, na definição de domínio de $\mathcal{R}$, não é única. Reciprocamente, a *existência* de $a \in X$, na definição de imagem de $\mathcal{R}$, também, não é única. Em outras palavras, não há (necessariamente) unicidade para estes elementos na *relação* $\mathcal{R}$.

Para simplificar a linguagem, e também por uma questão de estilo, usaremos a notação $\mathcal{R} : X \to Y$ para indicar uma relação $\mathcal{R}$ de X para Y, onde X e Y são conjuntos não vazios.

Com a notação $\mathcal{R} : X \to Y$ e sabendo que $S_{\mathcal{R}} \subset X \times Y$, pode-se dizer que o conjunto solução de uma relação $\mathcal{R}$ é uma relação de X para Y. Dessa forma, escrevemos: $S_{\mathcal{R}} : X \to Y$.

Exemplo 14. Sejam $A = \{a, b\}$ e $B = \{c, d\}$. Assim, o conjunto $\mathcal{R} = \{(a, d), (b, c)\}$ é uma relação $\mathcal{R} : A \to B$.

Resolução: Temos: $A \times B = \{(a, c), (a, d), (b, c), (b, d)\}$ e $\mathcal{R} \subset A \times B$. Portanto, $\mathcal{R}$ é uma relação.

Definição 18. (Relação sobre um conjunto) Seja um conjunto X. Dizemos que $\mathcal{R}$ é uma relação *sobre* X, se $\mathcal{R}$ é um subconjunto de $X \times X$, isto é, se $\mathcal{R} \subseteq X \times X$.

Exemplo 15. Sejam $A = \{a, b\}$ e $B = \{b, c, d\}$. Considere os conjuntos $C = \{(a, a), (b, b)\}$, $D = \{(a, b), (a, c), (a, d)\}$ e $E = \{(b, a), (c, a), (d, a)\}$.

Embora esses conjuntos sejam relações, note que o conjunto C é uma relação binária, pois $C \subset A \times A$. O conjunto D é uma relação de A para B, porque $D \subset A \times B$. Por fim, o conjunto E é uma relação de B para A, porque $E \subset B \times A$.

A relação de inclusão $E \subset B \times A$ motiva definir um tipo especial de relação, a saber: relação inversa.

Para LIPSCHUTZ (1972, p. 117): a cada relação $\mathcal{R} : X \to Y$, existe uma relação inversa $\mathcal{R}^{-1} : Y \to X$.

Definição 19. (Relação Inversa) Seja uma relação $\mathcal{R} : X \to Y$. A *relação inversa* de $\mathcal{R}$, que se indica por $\mathcal{R}^{-1} : Y \to X$, é o conjunto $\mathcal{R}^{-1} = \{(y, x) ; (x, y) \in \mathcal{R}\}$.

Observe que os elementos de $\mathcal{R}^{-1}$ são os pares ordenados de $\mathcal{R}$, porém, com os termos *permutados*.

Dessa forma, $a\mathcal{R}b$ ("a está relacionado com b, pela relação $\mathcal{R}$") se, e somente se, $b\mathcal{R}a$ ("b está relacionado com a, por $\mathcal{R}^{-1}$"). Isto significa escrever:

$$(a, b) \in \mathcal{R} \Leftrightarrow (b, a) \in \mathcal{R}^{-1}.$$

Exemplo 16. Sejam $A = \{a, b\}$ e $B = \{c, d, e\}$. Então, a relação $\mathcal{R} : A \to B$, definida por $\mathcal{R} = \{(a, c), (a, e), (b, d)\}$ tem inversa $\mathcal{R}^{-1} : Y \to X$, definida por $\mathcal{R}^{-1} = \{(c, a), (e, a), (d, b)\}$.

Exemplo 17. Seja $C = \{a, b, c\}$. A relação $\mathcal{R} : C \to C$, definida por $\mathcal{R} = \{(a, a), (a, c), (c, b)\}$ tem inversa $\mathcal{R}^{-1} : C \to C$, definida por $\mathcal{R}^{-1} = \{(a, a), (c, a), (b, c)\}$.

4.3 Gráfico

Para LIPSCHUTZ (1972, p. 115): dados dois conjuntos X e Y, o conjunto $X \times Y$ pode ser representado por pontos num *diagrama coordenado*[15].

[15] *Diagrama coordenado* é constituído por dois eixos perpendiculares, em geral, onde se fixa, em um dos eixos, o conjunto que representará o primeiro termo de um par ordenado e, no outro eixo, fixa-se o segundo termo do par ordenado, a fim de representá-lo. (LIPSCHUTZ, 1972, p. 94)

Nota: Para fins ilustrativos, a representação por meio de diagrama coordenado só é viável quando o conjunto tem "poucos" elementos.

Dessa forma, toda relação $\mathcal{R} : X \to Y$, bem como a sua relação inversa $\mathcal{R}^{-1} : Y \to X$ e o conjunto solução $S_{\mathcal{R}}$ de $\mathcal{R}$ têm representação no diagrama coordenado.

Definição 20. (Gráfico) O *gráfico* de uma relação $\mathcal{R} : X \to Y$ é o conjunto dos pontos de $X \times Y$, que pertencem ao conjunto solução $S_{\mathcal{R}}$ dessa relação.

Exemplo 18. Sejam $A = \{a, b, c\}$ e $B = \{d, e, f\}$. Considere a relação $\mathcal{R} : A \to B$, definida por $\mathcal{R} = \{(a, e), (a, f), (b, e), (b, f), (c, e), (c, f)\}$.

Suponha que o conjunto solução de $\mathcal{R}$ seja $S_{\mathcal{R}} = \{(a, f), (b, f), (c, f)\}$. Daí:

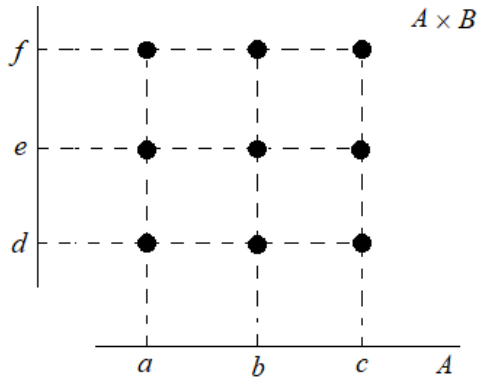
$$A \times B = \{(a, d), (a, e), (a, f), (b, d), (b, e), (b, f), (c, d), (c, e), (c, f)\}$$

e

$$\mathcal{R}^{-1} = \{(e, a), (f, a), (e, b), (f, b), (e, c), (f, c)\}.$$

Assim, o conjunto $A \times B$ está representado no diagrama coordenado da FIGURA 5 a seguir.

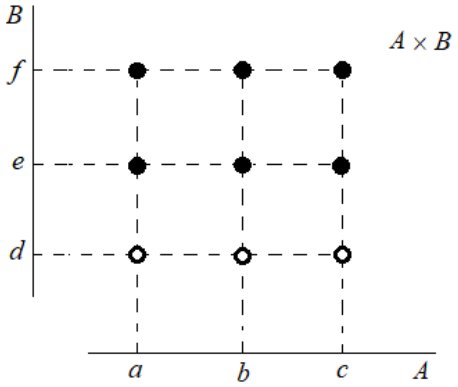
FIGURA 5 – Diagrama coordenado do conjunto $A \times B$.



FONTE: elaborada pelo autor.

O conjunto $\mathcal{R} = \{(a, e), (a, f), (b, e), (b, f), (c, e), (c, f)\}$ está representado no diagrama coordenado da FIGURA 6 a seguir.

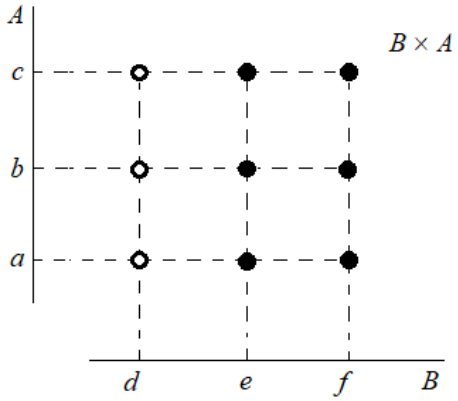
FIGURA 6 – Diagrama coordenado da relação $\mathcal{R} : A \to B$.



FONTE: elaborada pelo autor.

O conjunto $\mathcal{R}^{-1} = \{(e, a), (f, a), (e, b), (f, b), (e, c), (f, c)\}$ está representado no diagrama coordenado da FIGURA 7 a seguir

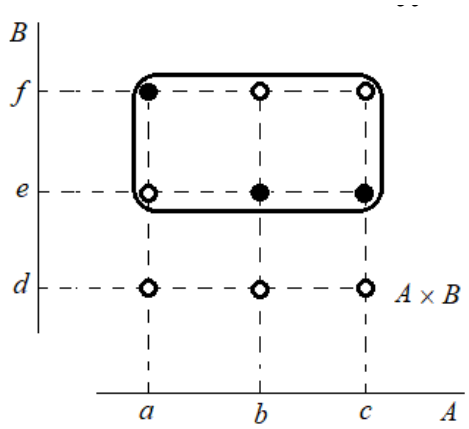
FIGURA 7 – Diagrama coordenado da relação inversa $\mathcal{R}^{-1}$.



FONTE: elaborada pelo autor.

O conjunto $S_{\mathcal{R}} = \{(a, f), (b, e), (c, e)\}$ está representado no diagrama coordenado da FIGURA 8 a seguir.

FIGURA 8 – Diagrama coordenado do conjunto solução $S_{\mathcal{R}}$.



FONTE: elaborada pelo autor.

4.4 Propriedades

Segundo SCHEINERMAN (2003, p. 77 e 80), as relações binárias determinam um conjunto de pares ordenados.

Nessa relação dual, podem ocorrer algumas propriedades, a saber: reflexiva, simétrica, antissimétrica e transitiva.

Definição 21. Seja uma relação $\mathcal{R}$ sobre um conjunto X. Para todo a, b, $c \in X$, a relação $\mathcal{R}$ chama-se:

i) *reflexiva* quando $a \in X$ implica $(a, a) \in \mathcal{R}$.

ii) *simétrica* quando $(a, b) \in \mathcal{R}$ implica $(b, a) \in \mathcal{R}$.

iii) *antissimétrica* quando $(a, b) \in \mathcal{R}$ e $(b, a) \in \mathcal{R}$ implicam $a = b$.

iv) *transitiva* quando $(a, b) \in \mathcal{R}$ e $(b, c) \in \mathcal{R}$ implicam $(a, c) \in \mathcal{R}$.

4.4.1 Relação Reflexiva

Segundo LIPSCHUTZ (1972, p. 118), para que uma relação $\mathcal{R}$ seja *reflexiva*, todos os pares ordenados da forma $(a, a) \in X \times X$ devem pertencer à relação $\mathcal{R}$.

Nesse sentido, uma relação $\mathcal{R}$ sobre um conjunto X *não* é reflexiva quando *existir* $a \in X$, tal que $(a, a) \notin \mathcal{R}$. Vejamos um *contraexemplo*[16].

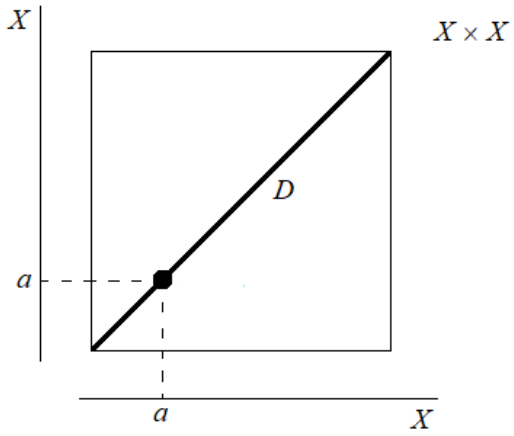
Exemplo 19. Seja a relação $\mathcal{R}$ sobre um conjunto $A = \{a, b, c\}$, definida por:

$$\mathcal{R} = \{(a, a), (b, b), (a, b), (b, c)\}.$$

Esta relação não é reflexiva, pois $(c, c) \notin \mathcal{R}$.

Do ponto de vista geométrico, se X representa um segmento de reta, então, toda relação *reflexiva* é o conjunto diagonal $D = \{(x, x)\,;\, x \in X\}$, conforme ilustrado pela FIGURA 9 a seguir.

FIGURA 9 – Diagrama coordenado de uma relação *reflexiva* sobre um conjunto X.



FONTE: elaborada pelo autor.

Exemplo 20. Sejam um conjunto A qualquer e o conjunto diagonal $D = \{(a, a)\,;\, a \in A\}$. Que relações há, se é que existe alguma, entre qualquer relação reflexiva $\mathcal{R}$ de A e D?

Resolução: Uma relação $\mathcal{R} : A \to D$ é tal que $a\mathcal{R}(a, a)$, para todo $a \in A$. Isto significa que D é um subconjunto de $\mathcal{R}$. Em outras palavras, cada relação reflexiva contém o conjunto diagonal.

[16] *Contraexemplo* é uma situação *particular*, porém, suficiente para verificar a falsidade de algumas sentenças ou proposições. (IRRACIEL; JOSÉ, 2010, p. 2)

4.4.2 Relação Simétrica

Conforme LIPSCHUTZ (1972, p. 118), a condição necessária e suficiente para que uma relação $\mathcal{R}$ seja *simétrica* é apresentada no teorema a seguir.

Teorema 3. Uma relação $\mathcal{R}$ sobre um conjunto X é *simétrica* se, e somente se, $\mathcal{R} = \mathcal{R}^{-1}$.

Demonstração: ($\Longrightarrow$) Suponha que $\mathcal{R}$ seja simétrica. Então, devemos mostrar que $\mathcal{R} = \mathcal{R}^{-1}$. De fato, para todo $(a, b) \in \mathcal{R}$ implica $(b, a) \in \mathcal{R}^{-1}$. Logo, $\mathcal{R} \subset \mathcal{R}^{-1}$.

Por outro lado, se $(b, a) \in \mathcal{R}^{-1}$, então, $(a, b) \in \mathcal{R}$. Isto significa que $\mathcal{R}^{-1} \subset \mathcal{R}$. Portanto, $\mathcal{R} = \mathcal{R}^{-1}$.

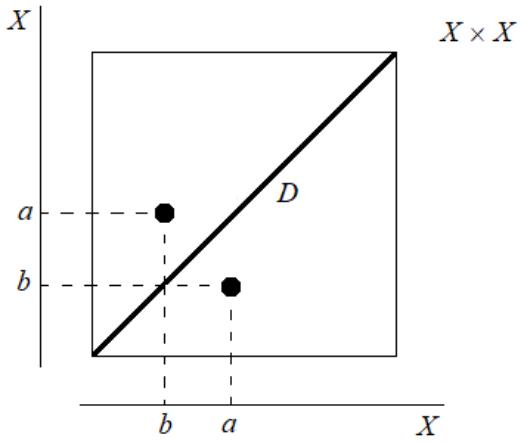
($\Longleftarrow$) Agora, suponha que $\mathcal{R} = \mathcal{R}^{-1}$. Então, vamos mostrar que $\mathcal{R}$ é simétrica. Com efeito, para todo $(a, b) \in \mathcal{R}$ implica $(a, b) \in \mathcal{R}^{-1}$, pois $\mathcal{R} = \mathcal{R}^{-1}$. Daí, segue $(b, a) \in \mathcal{R}$. Como (a, b) e (b, a) pertencem a $\mathcal{R}$, então, $\mathcal{R}$ é simétrica.

□

Dessa forma, uma relação $\mathcal{R} : X \to X$ *não* é simétrica quando existirem $a, b \in X$, tais que $(a, b) \in \mathcal{R}$ implica $(b, a) \notin \mathcal{R}$.

Geometricamente, se X é um segmento de reta, então, uma relação *simétrica* é formada por todos os pontos que são simétricos em relação ao conjunto diagonal $D = \{(x, x) ; x \in X\}$, pois $(b, a) \in \mathcal{R}^{-1}$ sempre que $(a, b) \in \mathcal{R}$, conforme indicado na FIGURA 10 abaixo.

FIGURA 10 – Diagrama coordenado de uma relação *simétrica* sobre um conjunto X.



FONTE: elaborada pelo autor.

Exemplo 21. Sejam duas relações simétricas $\mathcal{R}_1$ e $\mathcal{R}_2$ sobre um conjunto X. Prove que $\mathcal{R}_1 \cap \mathcal{R}_2$ é uma relação simétrica sobre X.

Demonstração: Observe que $\mathcal{R}_1$ e $\mathcal{R}_2$ são subconjuntos de $X \times X$. Logo, $\mathcal{R}_1 \cap \mathcal{R}_2$ é também um subconjunto de $X \times X$. Portanto, $\mathcal{R}_1 \cap \mathcal{R}_2$ é uma relação em X.

Agora, vamos mostrar que a relação $\mathcal{R}_1 \cap \mathcal{R}_2$ é simétrica sobre X. De fato, dado qualquer $(a, b) \in \mathcal{R}_1 \cap \mathcal{R}_2$, temos: $(a, b) \in \mathcal{R}_1$ e $(a, b) \in \mathcal{R}_2$. Mas, por hipótese, $\mathcal{R}_1$ e $\mathcal{R}_2$ são relações simétricas sobre X. Então, $(b, a) \in \mathcal{R}_1$ e $(b, a) \in \mathcal{R}_2$. Portanto, $(b, a) \in \mathcal{R}_1 \cap \mathcal{R}_2$.

Assim, para todo $(a, b) \in \mathcal{R}_1 \cap \mathcal{R}_2$ implica $(b, a) \in \mathcal{R}_1 \cap \mathcal{R}_2$. Logo, $\mathcal{R}_1 \cap \mathcal{R}_2$ é uma relação simétrica sobre X.

□

4.4.3 Relação Antissimétrica

Segundo LIPSCHUTZ (1972, p. 118 e 119), a condição necessária e suficiente para que uma relação $\mathcal{R}$ seja antissimétrica é apresentada pela propriedade a seguir.

Teorema 4. Uma relação $\mathcal{R}$ é antissimétrica sobre um conjunto X se, e somente se, $\mathcal{R} \cap \mathcal{R}^{-1} \subseteq D$, onde $D = \{(x, x) ; x \in X\}$ é o conjunto diagonal.

Demonstração: Para todo $(a, b) \in \mathcal{R} \cap \mathcal{R}^{-1}$ implica $(a, b) \in \mathcal{R}$ e $(a, b) \in \mathcal{R}^{-1}$. Esta última relação permite escreve $(b, a) \in \mathcal{R}$. Como $(a, b) \in \mathcal{R}$ e $(b, a) \in \mathcal{R}$, então $a = b$. Daí, $(a, b) = (a, a) \in D$. Portanto, $\mathcal{R} \cap \mathcal{R}^{-1} \subseteq D$.

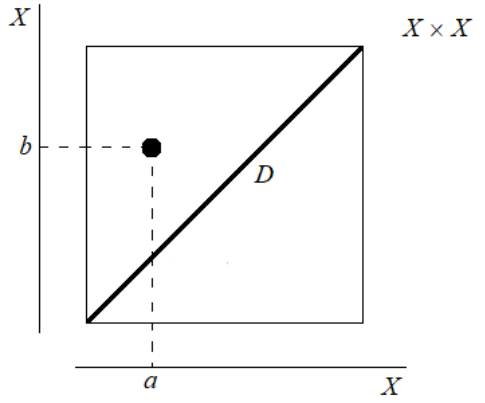
□

Em outras palavras, uma relação $\mathcal{R}$ sobre um conjunto X é *antissimétrica* quando, para todo $a, b \in X$, se $a \neq b$, então ou $(a, b) \in \mathcal{R}$ ou $(b, a) \in \mathcal{R}$, mas não simultaneamente.

Assim, uma relação $\mathcal{R}$ sobre um conjunto X *não* é antissimétrica quando existirem $a, b \in X$, tais que $(a, b) \in \mathcal{R}$ e $(b, a) \in \mathcal{R}$, com $a \neq b$.

No contexto geométrico, isto significa que, se X é um segmento de reta, então a relação antissimétrica não tem pontos sobre a diagonal $D = \{(x, x) ; x \in X\}$, conforme mostram as FIGURAS 11 e 12 a seguir.

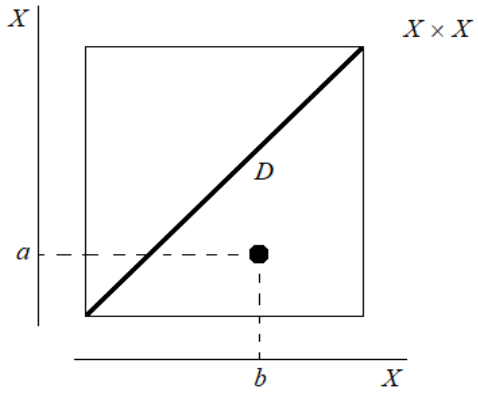
FIGURA 11 – Diagrama coordenado de uma relação *antissimétrica* sobre um conjunto X.



FONTE: elaborada pelo autor.

ou

FIGURA 12 – Diagrama coordenado de uma relação *antissimétrica* sobre um conjunto X.



FONTE: elaborada pelo autor.

Exemplo 22. Decidir se uma relação $\mathcal{R}$ sobre um conjunto X pode ser, simultaneamente, simétrica e antissimétrica.

Resolução: Seja uma relação simétrica $\mathcal{R}$ sobre um conjunto X. Então, para todo $(a, b) \in \mathcal{R}$ implica $(b, a) \in \mathcal{R}$. Como $(b, a) \in \mathcal{R}^{-1}$, então $(b, a) \in \mathcal{R} \cap \mathcal{R}^{-1}$.

Caso $\mathcal{R}$ seja também uma relação antissimétrica sobre X, teremos $\mathcal{R} \cap \mathcal{R}^{-1} \subseteq D$. Isto só é possível se, e somente se, $(b, a) \in D$, isto é, $a = b$.

4.4.4 Relação Transitiva

Segundo LIPSCHUTZ (1972, p. 119), uma relação $\mathcal{R}$ sobre um conjunto X é *transitiva* quando, para todo $a, b \in X$, temos $a\mathcal{R}b$ e $b\mathcal{R}c$ implicam $a\mathcal{R}c$.

Assim, uma relação $\mathcal{R}$ sobre um conjunto X *não* é transitiva quando, para todo $a, b \in X$, temos $a\mathcal{R}b$ e $b\mathcal{R}c$, mas $a\tilde{\mathcal{R}}c$.

Observe que na relação de transitividade é possível identificar dois pares ordenados de conexões entre os termos $a\mathcal{R}b$ e $a\mathcal{R}c$, a saber:

i) o par ordenado implícito (b, b), que pertence à diagonal $D = \{(x, x)\ ;\ x \in X\}$, mas não pertence à relação transitiva; e

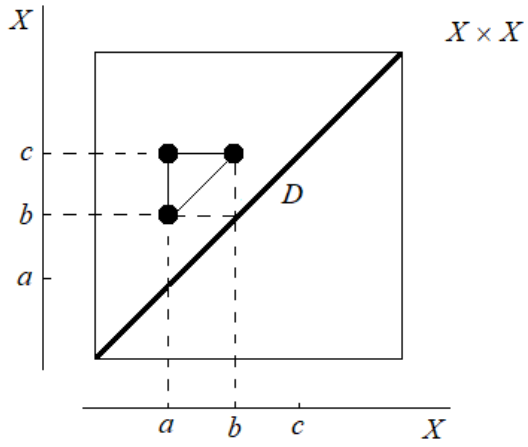
ii) o par ordenado explícito (b, c), que está entre os termos relacionais $a\mathcal{R}b$ e $a\mathcal{R}c$.

Isto sugere a definição.

Definição 22. Numa relação transitiva $a\mathcal{R}b$ e $b\mathcal{R}c$ implicam $a\mathcal{R}c$ sobre $X \times X$, o par ordenado (b, b) chama-se *conexão primária* e o par ordenado (b, c) chama-se *conexão de transição*.

Do ponto de vista geométrico, se X é um segmento de reta, então, os pares ordenados que constituem a relação *transitiva* formam um "triângulo retângulo isósceles", conforme ilustrado na FIGURA 13 a seguir.

FIGURA 13 – Diagrama coordenado de uma relação *transitiva* sobre um conjunto X.



FONTE: elaborada pelo autor.

Exemplo 23. Em que situação, uma relação $\mathcal{R}$ sobre um conjunto X não é transitiva?

Resolução: Uma relação $\mathcal{R}$ sobre um conjunto X é transitiva quando, para todo $a, b, c \in X$, temos $(a, b) \in \mathcal{R}$ e $(b, c) \in \mathcal{R}$ implicam $(a, c) \in \mathcal{R}$.

Assim, a relação $\mathcal{R}$ não é transitiva quando existirem $a, b \in X$, tais que $(a, b) \in \mathcal{R}$ e $(b, c) \in \mathcal{R}$, porém, $(a, c) \notin \mathcal{R}$.

Exemplo 24. Seja uma relação $\mathcal{R}$ transitiva sobre um conjunto X. Prove que $\mathcal{R}^{-1}$ é uma relação transitiva sobre X.

Resolução: Sejam (a, b) e $(b, c) \in \mathcal{R}^{-1}$. Precisamos mostrar que $(a, c) \in \mathcal{R}^{-1}$. De fato, temos (c, b) e $(b, a) \in \mathcal{R}$. Como, por hipótese, $\mathcal{R}$ é uma relação transitiva sobre um conjunto X, então $(c, a) \in \mathcal{R}$. Logo, $(a, c) \in \mathcal{R}^{-1}$. Portanto, $\mathcal{R}^{-1}$ é uma relação transitiva sobre X.

□

Exemplo 25. Sejam duas relações $\mathcal{R}_1$ e $\mathcal{R}_2$ sobre um conjunto X. Prove as seguintes asserções:
a) se $\mathcal{R}_1$ e $\mathcal{R}_2$ são duas relações simétricas sobre X, então $\mathcal{R}_1 \cup \mathcal{R}_2$ é uma relação simétrica sobre X.
b) se $\mathcal{R}_1$ é uma relação reflexiva e $\mathcal{R}_2$ é uma relação qualquer sobre X, então $\mathcal{R}_1 \cup \mathcal{R}_2$ é uma relação reflexiva sobre X.

Resolução: a) Mostraremos que, para todo $(a, b) \in \mathcal{R}_1 \cup \mathcal{R}_2$ implica $(b, a) \in \mathcal{R}_1 \cup \mathcal{R}_2$. De fato, seja $(a, b) \in \mathcal{R}_1 \cup \mathcal{R}_2$. Por hipótese, $\mathcal{R}_1$ e $\mathcal{R}_2$ são relações simétricas, então (b, a) pertence a $\mathcal{R}_1$ ou $\mathcal{R}_2$. Logo, $(b, a) \in \mathcal{R}_1 \cup \mathcal{R}_2$. Portanto, $\mathcal{R}_1 \cup \mathcal{R}_2$ é uma relação simétrica sobre X.

b) Temos: $\mathcal{R}_1$ é uma relação reflexiva se, e somente se, $D \subset \mathcal{R}_1$, onde D é o conjunto diagonal de $X \times X$. Além disso, podemos escrever $\mathcal{R}_1 \subset \mathcal{R}_1 \cup \mathcal{R}_2$. Assim, $D \subset \mathcal{R}_1$ e $\mathcal{R}_1 \subset \mathcal{R}_1 \cup \mathcal{R}_2$, por transitividade, implica $D \subset \mathcal{R}_1 \cup \mathcal{R}_2$. Logo, $\mathcal{R}_1 \cup \mathcal{R}_2$ é uma relação reflexiva sobre X.

□

4.5 Relação de Equivalência e Partição

Para DEAN (1974, p. 8):

> Uma classe especial de relação sobre um conjunto A que desempenha um papel fundamental em matemática consiste naquelas relações chamadas relações de equivalência. (...) A mais importante propriedade de uma relação de equivalência sobre um conjunto é que ela particiona o conjunto em subconjuntos mutuamente disjuntos chamados classes de equivalência.

A partir disso, nota-se a importância de definir relação de equivalência, partição de um conjunto e estabelecer propriedades da relação de equivalência sobre este conjunto.

Definição 23. (Relação de Equivalência) Uma relação $\mathcal{R}$ sobre um conjunto X chama-se *relação de equivalência* sobre X, se $\mathcal{R}$ tem as três propriedades seguintes:
i) *reflexiva* – para todo $a \in X$ implica $(a, a) \in \mathcal{R}$;
ii) *simétrica* – para todo $a, b \in X$, se $(a, b) \in \mathcal{R}$, então $(b, a) \in \mathcal{R}$; e
iii) *transitiva* – para todo $a, b, c \in X$, se $(a, b) \in \mathcal{R}$ e $(b, c) \in \mathcal{R}$), então $(a, c) \in \mathcal{R}$.

A mais importante e usual das relações de equivalência em matemática é "=" (*igualdade*).

Exemplo 26. Seja a relação $\mathcal{R}$ de igualdade sobre um conjunto X, definida por: para todo $a, b \in X$, $a\mathcal{R}b \iff a = b$. Mostre que $\mathcal{R}$ é uma relação de equivalência.

Resolução: De fato, para todo $a, b, c \in X$:
i) $\mathcal{R}$ é *reflexiva*, porque $a \in X$ implica $a = a$.
ii) $\mathcal{R}$ é *simétrica*, pois $a = b$ implica $b = a$.
iii) $\mathcal{R}$ é *transitiva*, pelo fato de $a = b$ e $b = c$ implicam $a = c$.

Outra importante relação de equivalência é "≡" (*congruência*) apresentada a seguir.

Exemplo 27. (Congruência módulo *m*) Seja $\mathcal{R}$ uma relação de congruência módulo m definida por:

$$\mathcal{R} = \{(x, y)\ ;\ m \text{ divide } x - y \iff x \equiv y\ (m), \text{ para } m \text{ fixo em } \mathbb{N} \text{ e } x, y \in \mathbb{N}_0\},$$

onde $x \equiv y\ (m)$, lê-se: "x é congruente a y, módulo m". A relação "*é congruente módulo m*", assim definida, é uma relação de equivalência.

Resolução: De fato:
i) Para todo $a \in \mathbb{N}_0$, temos: m divide $0 = a - a$. Assim, para todo $a \in \mathbb{N}_0$ implica $(a, a) \in \mathcal{R}$. Logo, $\mathcal{R}$ é reflexivo.

ii) Para todo $a, b \in \mathbb{N}_0$, seja $(a, b) \in \mathcal{R}$. Então, m divide $a - b$.

Note que $b - a = -(a - b)$, assim, m divide $b - a$. Logo, $(b, a) \in \mathcal{R}$. Como $(a, b) \in \mathcal{R}$ implica $(b, a) \in \mathcal{R}$, segue que $\mathcal{R}$ é simétrico.

iii) Finalmente, para todo $a, b, c \in \mathbb{N}_0$, sejam $(a, b), (b, c) \in \mathcal{R}$. Assim, m divide $a - b$ e m divide $b - c$.

Usando o fato de que $a - c = (a - b) + (b - c)$, segue que m divide $a - c$. Assim, $(a, b) \in \mathcal{R}$ e $(b, c) \in \mathcal{R}$ implicam $(a, c) \in \mathcal{R}$. Portanto, $\mathcal{R}$ é transitivo.

Como $\mathcal{R}$ é reflexivo, simétrico e transitivo, então, por definição, $\mathcal{R}$ é uma relação de equivalência.

Em uma relação de equivalência $\mathcal{R}$ sobre um conjunto X, existe um conjunto constituído pelos elementos de X que estão relacionados, por $\mathcal{R}$, com um dado elemento de X. Mais precisamente, escrevemos:

Definição 24. (Classe de Equivalência) Seja uma relação de equivalência $\mathcal{R}$ sobre um conjunto X. Dado $a \in X$, chama-se *classe de equivalência de a*, denotada por $[a]$, o conjunto formado apenas por elementos de X que estão relacionados com a, pela relação $\mathcal{R}$.

Em símbolo, escreve-se:

$$[a] = \{x \in X \,;\, x\mathcal{R}a, \text{ onde } a \in X\} = \{x \in X \,;\, (x, a) \in \mathcal{R}, \text{ com } a \in X\}.$$

Observe que $[a]$ é um subconjunto de X, com a característica de que todos os seus elementos estão relacionados com $a \in X$, por $\mathcal{R}$. Além disso, para todo $x, y \in X$, se $x, y \in [a]$, então $x\mathcal{R}y$. De fato, se $x, y \in [a]$, então, por definição de classe de equivalência, $x\mathcal{R}a$ e $y\mathcal{R}a$. Como $\mathcal{R}$ é uma relação de equivalência, segue que $\mathcal{R}$ é reflexiva e transitiva. Assim, $y\mathcal{R}a$ implica $a\mathcal{R}y$. E, por transitividade, $x\mathcal{R}a$ e $a\mathcal{R}y$ implica $x\mathcal{R}y$.

Exemplo 28. Seja a relação de equivalência $\mathcal{R} = \{(a, a), (b, b), (c, c), (a, c), (c, a)\}$ sobre $A = \{a, b, c\}$. Assim, temos as seguintes classes de equivalências:

$$[a] = \{x \in X \,;\, x\mathcal{R}a, \text{ onde } a \in A\} = \{a, c\} \;\; \therefore \;\; \mathbf{[a] = \{a, c\}}.$$

$$[b] = \{x \in X \,;\, x\mathcal{R}b, \text{ onde } b \in A\} = \{b\} \;\; \therefore \;\; \mathbf{[b] = \{b\}}.$$

$$[c] = \{x \in X \,;\, x\mathcal{R}c, \text{ onde } c \in A\} = \{c, a\} = \{a, c\} \;\; \therefore \;\; \mathbf{[c] = \{a, c\}}.$$

Dada uma relação de equivalência, a classe de equivalência dessa relação apresenta algumas características importantes que sintetizaremos no teorema a seguir.

Teorema 5. Seja uma relação de equivalência $\mathcal{R}$ sobre um conjunto X. As seguintes afirmações são verdadeiras:

i) para todo $a \in X$ implica $a \in [a]$.

ii) para todo $b \in X$, $b \in [a]$ se, e somente se, $[b] = [a]$.

iii) para todo $a, b \in X$, se $a \neq b$, então $[a] \cap [b] = \varnothing$.

Demonstração: Seja uma relação de equivalência $\mathcal{R}$ sobre um conjunto X. Assim, $\mathcal{R}$ tem as propriedades: reflexiva, simétrica e transitiva.

Em ***i)***, temos: $[a] = \{x \in X\,;\, x\mathcal{R}a$, onde $a \in X\}$. Então, para mostrar que $a \in [a]$, basta mostrar que $a\mathcal{R}a$. Mas isto é imediato pela propriedade reflexiva de $\mathcal{R}$, ou seja, para todo $a \in X$ implica $a\mathcal{R}a$.

Em ***ii)***: ($\Longrightarrow$) seja $\mathcal{R}$ uma relação de equivalência que define $[a]$. Precisamos mostrar que $b \in [a]$ implica $[b] = [a]$. De fato, para todo $b \in X$, se $b \in [a]$, temos, por definição de classe de equivalência, $b\mathcal{R}a$.

Agora, suponhamos $x \in [b]$. Então, por definição de classe de equivalência, tem-se $x\mathcal{R}b$.

Como $x\mathcal{R}b$ e $b\mathcal{R}a$, então, por transitividade, conclui-se que $x\mathcal{R}a$, isto é, $x \in [a]$. Portanto, $[b] \subseteq [a]$.

Analogamente, para todo $y \in [a]$ implica $y\mathcal{R}a$. Mas, $b \in [a]$ implica $b\mathcal{R}a$. Daí, por simetria, obtém-se $a\mathcal{R}b$. Como $y\mathcal{R}a$ e $a\mathcal{R}b$, conclui-se, por transitividade, $y\mathcal{R}b$. Desse modo, $y \in [b]$, assim, $[a] \subseteq [b]$. Então, $[b] = [a]$.

($\Longleftarrow$) Suponha que $[b] = [a]$. Assim, pela propriedade ***i)***, para todo $b \in X$ implica $b \in [b]$. Mas, $[b] = [a]$. Logo, $b \in [a]$.

Em ***iii)***, suponha, por absurdo, que $[a] \cap [b] \neq \varnothing$. Logo, existe $x \in X$, tal que $x \in [a] \cap [b]$. Daí, $x \in [a]$ e $x \in [b]$. Dessa forma, $x\mathcal{R}a$ e $x\mathcal{R}b$. Mas, por simetria, $a\mathcal{R}x$.

Como $a\mathcal{R}x$ e $x\mathcal{R}b$, temos, por transitividade, $a\mathcal{R}b$. Daí, pela definição de classe de equivalência, $a \in [b]$. Isto significa, pela propriedade ***ii)***, que $[a] = [b]$. Mas, pela propriedade da igualdade, conclui-se que $a = b$. Porém, isto é um absurdo! Pois, $a \neq b$. O absurdo ocorreu porque supomos que $[a] \cap [b] \neq \varnothing$. Assim, se $a \neq b$, então $[a] \cap [b] = \varnothing$.

□

Observe que no **Teorema 5**, a propriedade ***i)*** mostra que a cada elemento do conjunto X determina uma classe de equivalência.

É importante também notar que, na propriedade ***ii)***, todo elemento de X pertence a uma, e uma só, classe de equivalência. Assim, colecionando-se estas *classes de equivalência*, obtém-se um novo conjunto.

Definição 25. (Conjunto Quociente) O conjunto formado por classes de equivalência de uma relação de equivalência $\mathcal{R}$ sobre um conjunto X, chama-se *conjunto quociente de X por* $\mathcal{R}$ e denota-se por $X/_{\mathcal{R}}$.

No **Exemplo 28**, temos as classes de equivalência $[a] = \{a, c\}$ e $[b] = \{b\}$. Assim, os elementos do conjunto $A/_{\mathcal{R}}$ são $\{a, c\}$ e $\{b\}$, isto é:

$$A/_{\mathcal{R}} = \{[a], [b]\} = \{\{a, c\}, \{b\}\}.$$

Observe que o conjunto quociente $X/_{\mathcal{R}}$ apresenta duas características importantes: à primeira é que a reunião de seus elementos é o conjunto X; e à segunda, mostra que ou duas classes de equivalências não têm nenhum elemento comum ou se têm e, portanto, elas são idênticas.

É sob essas duas perspectivas, que se conclui:

> "A mais importante propriedade de uma relação de equivalência sobre um conjunto é que ela *particiona o conjunto em subconjuntos mutualmente disjuntos* chamadas classes de equivalência." (DEAN, 1974, p. 8, grifos nossos)

Ainda nesse contexto, NACHBIN (1974, p. 27) menciona que:

> "A noção de relação de equivalência nunca deve ser dissociada da noção de partição, pois, (...) existe uma conexão simples, porém importante, entre as duas."

SCHEINERMAN (2003, p. 98) reforça que: "Uma partição de um conjunto A é um conjunto de subconjuntos, não vazios, disjuntos dois a dois, cuja união é A."

Nesse sentido, para definir formalmente uma partição de um conjunto, fixa-se o conjunto $I_n = \{1, 2, 3, \cdots, n\}$, o qual denominamos *conjunto dos índices*, a fim de listar os elementos do conjunto quociente. A partir daí, considere o conjunto $\mathcal{F} = \{A_i\}_{i \in In}$, denominaremos *uma família de conjuntos com índices*, onde a cada $i \in I_n$ corresponde um conjunto A_i. Em símbolos, escrevemos:

$$\mathcal{F} = \{A_i\}_{i \in In} = \{A_1\} \cup \{A_2\} \cup \{A_3\} \cup \cdots \cup \{A_n\}.$$

Definição 26. (Partição de um Conjunto) Uma família $\mathcal{F} = \{A_i\}_{i\in In}$ de subconjuntos não vazios de um conjunto X é uma *partição de X* se:

i) $\cup_{i\in In} A_i = A_1 \cup A_2 \cup A_3 \cup \cdots \cup A_n = X$;

ii) $A_i \cap A_j = \varnothing$, para $i \neq j$. Isto equivalente a $A_i \cap A_j \neq \varnothing$ implica $A_i = A_j$.

Observação:

Em vista do item ***i)***, dessa definição, escreve-se: $\cap_{i\in In} A_i = A_1 \cap A_2 \cap A_3 \cap \cdots \cap A_n$.

Exemplo 29. Listar todas as partições do conjunto $A = \{a, b, c\}$.

Resolução: Um conjunto P_α, onde $\alpha = 1, 2, 3, \cdots$, é uma partição de A se cumpre as condições ***i)*** e ***ii)*** da **Definição 26**.

Assim, as partições de A são os conjuntos a seguir:

$$P_1 = \{\{a, b, c\}\} = \{A\}.$$

$$P_2 = \{\{a\}, \{b\}, \{c\}\}.$$

$$P_3 = \{\{a\}, \{b, c\}\},\ P_4 = \{\{b\}, \{a, c\}\},\ P_5 = \{\{c\}, \{a, b\}\}.$$

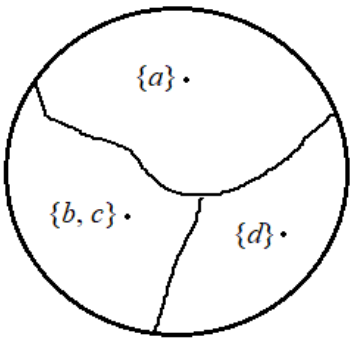
$$P_6 = \{\{a, b\}, \{c\}\},\ P_7 = \{\{a, c\}, \{b\}\} \text{ e } P_8 = \{\{b, c\}, \{a\}\}.$$

Portanto, há oito partições no conjunto $A = \{a, b, c\}$.

Quando uma partição tem "poucos" elementos, ela pode ser representada no diagrama de *Venn*.

Exemplo 30. O conjunto $F = \{\{a\}, \{b, c\}, \{d\}\}$ é uma partição do conjunto de $A = \{a, b, c, d\}$, pois cumpre as duas condições da **Definição 26**. Além disso, a FIGURA 14 é a representação desta partição no diagrama de *Venn*.

FIGURA 14 – Diagrama da partição F do conjunto A.



FONTE: elaborada pelo autor.

Teorema 6. (Teorema Fundamental sobre Relação de Equivalência e Partição) Uma relação $\mathcal{R}$ sobre um conjunto X é relação de equivalência se, e somente se, a família $\mathcal{F} = \{A_\alpha\}_{\alpha \in X}$ é uma partição de X, com $A_\alpha = \{x \in X\,;\, (x, \alpha) \in \mathcal{R}, \text{ com } \alpha \in X\}$.

Demonstração: ($\Longrightarrow$) Vamos mostrar que se $\mathcal{R}$ é uma relação de equivalência sobre um conjunto X, então a família $\mathcal{F} = \{A_\alpha\}_{\alpha \in X}$ é uma partição de X, com $A_\alpha = \{x \in X\,;\, (x, \alpha) \in \mathcal{R}, \text{ com } \alpha \in X\}$. De fato, seja $\mathcal{R}$ uma relação de equivalência sobre um conjunto X. Considere o conjunto $A_\alpha = \{x \in X\,;\, (x, \alpha) \in \mathcal{R}, \text{ com } \alpha \in X\}$. Como $\mathcal{R}$ é reflexivo, então, a cada $a \in X$ implica $a \in A_a$. Portanto, $\cup_{\alpha \in X} A_\alpha = X$.

Agora, vamos mostrar que $A_r \cap A_s \neq \varnothing$ implica $A_r = A_s$. Com efeito, suponha que $y \in A_r \cap A_s$, onde $A_r = \{x \in X\,;\, (x, r) \in \mathcal{R}, \text{ com } r \in X\}$ e $A_s = \{x \in X\,;\, (x, s) \in \mathcal{R}, \text{ com } s \in X\}$.

Como $A_r \cap A_s \neq \varnothing$, então, existe $y \in A_r \cap A_s$. Daí, $y \in A_r$ e $y \in A_s$. Portanto, $(y, r) \in \mathcal{R}$ e $(y, s) \in \mathcal{R}$.

Seja $w \in A_r$. Então, $(w, r) \in \mathcal{R}$ e $(y, r) \in \mathcal{R}$. Assim, por simetria, $(y, r) \in \mathcal{R}$ implica $(r, y) \in \mathcal{R}$.

Como $(w, r) \in \mathcal{R}$ e $(r, y) \in \mathcal{R}$, temos, por transitividade, $(w, y) \in \mathcal{R}$. Além disso, e também por transitividade, $(w, y) \in \mathcal{R}$ e $(y, s) \in \mathcal{R}$ implicam $(w, s) \in \mathcal{R}$. Portanto, $w \in A_s$. Dessa forma, mostramos que $A_r \subseteq A_s$.

De modo semelhante, mostra-se que $A_s \subseteq A_r$. Como $A_r \subseteq A_s$ e $A_s \subseteq A_r$, tem-se $A_r = A_s$.

Como *i)* $\cup_{\alpha\in X} A_\alpha = X$ e *ii)* $A_r = A_s$, então, a família $\mathcal{F} = \{A_\alpha\}_{\alpha\in X}$ é uma partição de X, onde $A_\alpha = \{x \in X\,;\, (x, \alpha) \in \mathcal{R}, \text{ com } \alpha \in X\}$.

($\Longleftarrow$) Reciprocamente, se a família $\mathcal{F} = \{A_\alpha\}_{\alpha\in X}$ é uma partição de X, com $A_\alpha = \{x \in X\,;\, (x, \alpha) \in \mathcal{R}, \text{ com } \alpha \in X\}$, então $\mathcal{R}$ é uma relação de equivalência sobre o conjunto X. De fato, seja $\mathcal{F} = \{A_\alpha\}_{\alpha\in X}$ é uma partição qualquer de X, onde $A_\alpha = \{x \in X\,;\, (x, \alpha) \in \mathcal{R}, \text{ com } \alpha \in X\}$. Além disso, considere uma relação $\mathcal{R}$ sobre um conjunto X, definida por $a\mathcal{R}b$ se, e somente se, existe um A_i na partição $\mathcal{F} = \{A_\alpha\}_{\alpha\in X}$, tal que $a, b \in A_i$. Assim:

i) $\mathcal{R}$ é *reflexivo*, pois, a cada $a \in X$, existe um A_a na partição $\mathcal{F} = \{A_\alpha\}_{\alpha\in X}$, tal que $a\mathcal{R}a$.

ii) $\mathcal{R}$ é *simétrico*, pois, pela definição da relação $\mathcal{R}$, dados $a, b \in X$, se $a\mathcal{R}b$, então, existe um A_i na partição $\mathcal{F} = \{A_\alpha\}_{\alpha\in X}$, tal que $a, b \in A_i$. Mas, $a, b \in A_i$ se, e somente se, $b, a \in A_i$. Daí, novamente pela definição de $\mathcal{R}$, temos $b\mathcal{R}a$.

iii) $\mathcal{R}$ é *transitivo*, pois, dados $a, b, c \in X$, suponha que $a\mathcal{R}b$ e $b\mathcal{R}c$. Assim, pela definição de $\mathcal{R}$, existem subconjuntos A_i e A_j (não necessariamente distintos), tais que $a, b \in A_i$ e $b, c \in A_j$. Logo, $A_i \cap A_j \neq \varnothing$ e, portanto, $A_i = A_j$. Daí, $a, c \in A_j$. Então, pela definição de $\mathcal{R}$, temos $a\mathcal{R}c$.

Assim, $a\mathcal{R}b$ e $b\mathcal{R}c$ implica $a\mathcal{R}c$. Portanto, $\mathcal{R}$ é uma relação de equivalência sobre o conjunto X.

□

A partir desse teorema fundamental, depreende-se que uma *relação de equivalência* $\mathcal{R}$ sobre um conjunto X realiza *partições* $A_\alpha = \{x \in X\,;\, (x, \alpha) \in \mathcal{R}, \text{ com } \alpha \in X\}$ em X, de modo que:

i) $\cup_{i\in I} A_i = X$; e

ii) $A_i \cap A_j = \varnothing$, para $i \neq j$.

Cada subconjunto A_α de X chama-se *classe de equivalência* determinada por α. O conjunto das classes de equivalência de X sob a relação $\mathcal{R}$ denomina-se *conjunto quociente* e denota-se por $X/_{\mathcal{R}} = \{A_\alpha\}_{\alpha\in X}$.

Reciprocamente, o conjunto quociente $X/_{\mathcal{R}} = \{A_\alpha\}_{\alpha\in X}$ é uma *partição* do conjunto X, onde A_α é uma *classe de equivalência* determinada por α que, por conseguinte, determina uma *relação de equivalência* $\mathcal{R}$ sobre o conjunto X, com a *família de conjuntos com índices* $\mathcal{F} = X/_{\mathcal{R}} = \{A_\alpha\}_{\alpha\in X}$.

5 Concepção de Função

Uma das noções fundamentais pertinente à Matemática é o conceito de função. Ele diz respeito à forma de como os elementos de dois conjuntos quaisquer podem ser associados por uma regra pré-definida.

5.1 Conceito

Para LIMA (2010, p. 13): Uma *função* consiste de dois conjuntos X e Y (não necessariamente disjuntos) e uma regra $f(x) = y$ que permite associar, de modo bem determinado, a cada elemento $x \in X$, um único elemento $f(x) \in Y$.

Usa-se a notação $f : X \to Y$ (lê-se: "*f de X em Y*") para representar uma função (aplicação ou correspondência), definida pela regra de associação $f(x) = y$, onde y é a *imagem* de x por f. O conjunto X chama-se *domínio de f* e denota-se por D_f. O conjunto Y chama-se *contradomínio de f* e indica-se por CD_f. De maneira simbólica, escreve-se:

$$D_f = X = \{x \in X \,;\, existe\ y \in Y, \text{com } y = f(x)\} \quad \text{e} \quad CD_f = Y.$$

Segundo o autor, o *domínio* da função é o conjunto em que a função está definida. Sobre os símbolos f e $f(x)$, menciona que: "Não se deve confundir f com $f(x)$: f é uma função, enquanto que $f(x)$ é o valor que a função assume num ponto x do seu domínio."

O elemento $f(x) \in Y$ obtido pela regra $y = f(x)$, que define a função $f : X \to Y$, chama-se *imagem* de $x \in X$. Todos os elementos de Y, com esta propriedade, dá origem ao *conjunto imagem de f* que denotaremos por $I_m(f)$. Em símbolos:

$$I_m(f) = \{y \in Y \,;\, y = f(x), \textit{para algum } x \in X\}.$$

Nesse contexto, dada uma função $f : X \to Y$, para saber se um certo elemento $b \in Y$ pertence ou não à imagem de $f(X)$, escrevemos a "equação" $f(x) = b$ e procuramos determinar algum $x \in X$ que a torne uma sentença verdadeira.

Observação:

Para $b = f(x)$, foi usada a palavra "equação" no sentido próprio de tentar achar o valor de x que a satisfaça. Mas, sabe-se que, formalmente, o uso das terminologias *incógnita* e *variável* é diferente. As funções possuem variáveis, enquanto que as equações possuem incógnitas.

5.1.1 Existência e Unicidade

O conceito de função também pode ser apresentado no contexto de relação e pares ordenados, de modo que uma relação f chama-se *função* se:

$$(a, b) \text{ e } (a, c) \in f \implies b = c.$$

LIMA (2010, p. 13) menciona duas condições sobre a *natureza da regra* que faz parte do conceito uma função $f : X \to Y$, a saber:

C₁) existência: a regra *deve fornecer* $f(x) \in Y$, para *todo* $x \in X$; e

C₂) unicidade: a cada $x \in X$, a regra deve fazer corresponder um *único* $f(x) \in Y$.

Assim, quando é dada uma função $f : X \to Y$, ficam estabelecidas duas condições: a *existência* e a *unicidade* de $f(x) \in Y$, para todo $x \in X$.

Com o propósito de sabermos se uma regra que associa os elementos de um conjunto X aos elementos de um conjunto Y define ou não uma função $f : X \to Y$, utiliza-se o seguinte critério:

> "Para termos certeza que esta lei (*regra*) define uma função $f : X \to Y$, devemos verificar que efetivamente a cada elemento de X é associado um único elemento de Y. Deve-se então *mostrar* que se $a = b$, então $f(a) = f(b)$." (HEFEZ, 2002, p. 13, grifos nossos)

Exemplo 31. (Função Constante) Sejam dois conjuntos X e Y. Seja um elemento k fixado em Y, tal que para todo $x \in X$ implica $f(x) = k$. Sob estas condições, $f : X \to Y$ é uma função.

Resolução: Dados $a, b \in X$, se $a = b$, então $f(a) = k$ e $f(b) = k$. Logo, $f(a) = f(b)$ e, portanto, $f : X \to Y$ é uma função.

Uma função com esta característica chama-se *função* (ou *aplicação*) *constante*.

Exemplo 32. (Função Identidade) Seja um conjunto X. A função $Id : X \to X$ que associa, a cada $x \in X$ nele próprio chama-se *função identidade* (ou *inclusão*) de X e representa-se por $Id(x) = x$ ou, em termos de conjunto, $Id_X = \{(x, x) ; x \in X\}$.

Resolução: De fato, $Id : X \to X$ definida por $Id(x) = x$ é uma função, pois, dados $a, b \in X$, temos $f(a) = a$ e $f(b) = b$. Assim, se $a = b$, então $f(a) = f(b)$. Logo, $Id : X \to X$ é uma função.

Exemplo 33. Sejam $A = \{a, b, c\}$ e $B = \{p, q, r\}$. Seja uma relação g de A em B, definida por: "$g(a) = q$, $g(b) = r$, $g(c) = p$ e $g(b) = q$". Verifique se $g : A \to B$ é ou não uma função.

Resolução: Observe que: *i)* a regra g fornece $g(x) \in B$, para cada $x \in A$. De fato:

$$a \in A \implies g(a) = q \in B.$$

$$b \in A \implies g(b) = r,\ q \in B.$$

$$c \in A \implies g(c) = p \in B.$$

Logo, a *existência* de $g(x) \in B$ está garantida, para cada $x \in A$.

Por outro lado, *ii)* a *unicidade* não. De fato, pela regra g, temos $b \in A$ implica $g(b) \neq g(b)$. Isto *compromete a unicidade* como um dos critérios para que g seja uma função de A em B. Portanto, $g : A \to B$ *não* é uma função.

Agora, dada uma função $f : X \to Y$ e um subconjunto A de X. Chama-se *imagem direta* de A, pela função f, o conjunto $f(A)$ formado pelos elementos $f(x) \in Y$, tais que $x \in X$. Em símbolos, representa-se:

$$f(A) = \{f(x) ; x \in A\}.$$

Em particular, $f(X)$ é a imagem de f e, por conseguinte, $f(X) \subseteq Y$.

Sejam uma função $f : X \to Y$ e um subconjunto B de Y. Chama-se *imagem inversa* de B e denota-se por $f^{-1}(B)$, o conjunto:

$$f^{-1}(B) = \{x \in X ; f(x) \in B\}.$$

Observe que $f^{-1}(B)$ é sempre um subconjunto de X. Seguem, também, por definição: $f(\varnothing) = \varnothing$, $f^{-1}(\varnothing) = \varnothing$ e $f^{-1}(Y) = X$.

Definição 27. (Gráfico de uma Função) Seja uma função $f: X \to Y$. O *gráfico* de f, denotado por G_f, é o subconjunto do produto cartesiano $X \times Y$ formado pelos pares ordenados $(x, f(x))$, para qualquer $x \in X$.

Em símbolos, escreve-se:

$$G_f = \{(x, y) \in X \times Y \,;\, y = f(x)\}.$$

Isto significa que os pares ordenados que constituem o gráfico de uma função $f: X \to Y$ têm, nos primeiros termos, os elementos do domínio e, nos segundos termos, os elementos da imagem da função f. Em símbolos, isto representa:

$$(x, f(x)) \in G_f \text{ se, e somente se, } x \in D_f \text{ e } f(x) \in Im_f.$$

Costuma-se escrever $(x, f(x)) \in f$ em lugar de $(x, f(x)) \in G_f$.

Nesse contexto, uma função $f: X \to Y$ é estabelecida por uma coleção (ou conjunto) de pares ordenados $(x, f(x)) \in f \subset X \times Y$, obtidos por uma regra bem definida, que associa a cada elemento $x \in X$, um único elemento $f(x) \in Y$.

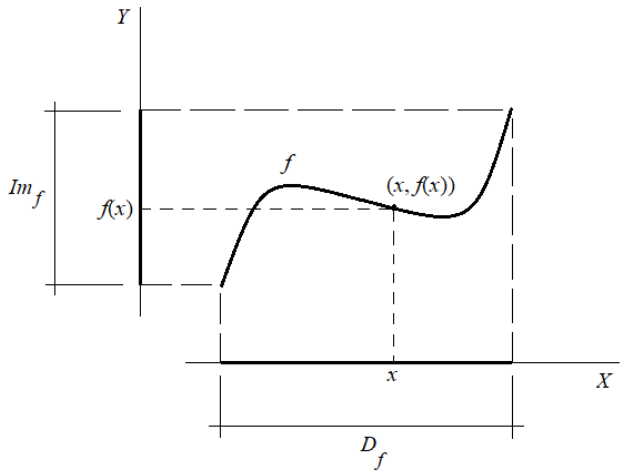
Em vista das propriedades de existência e unicidade de uma função, o gráfico da função $f: X \to Y$ também possui duas propriedades, a saber:

G₁) para cada $x \in X$ *existe* uma par ordenado $(x, f(x)) \in f$; e

G₂) se $(x, f(x)) \in f$ e $(x, y) \in f$, então $f(x) = y$.

Segundo LIMA (2010, p. 14), a condição necessária e suficiente para que um subconjunto $G_f \subset X \times Y$ seja o gráfico de uma função $f: X \to Y$ é que, para cada $x \in X$, exista um único par ordenado $(x, y) \in G_f$, cujo primeiro termo seja $x \in X$. A FIGURA 15 a seguir ilustra o gráfico de uma função $f: X \to Y$.

FIGURA 15 – Gráfico da função $f : X \to Y$.



FONTE: BARTLE, Robert G., 1983, p. 25.

Intuitivamente, quando duas funções que têm o mesmo gráfico, elas são iguais. Formalmente, temos:

Definição 28. (Funções Iguais) Sejam duas funções $f : A \to B$ e $g : C \to D$. Dizemos que f e g são *iguais*, se:
(a) $A = C$ (domínios iguais) e $B = D$ (contradomínios iguais); e
(b) para todo $x \in A = C$ implica $f(x) = g(x)$.

5.2 Função Injetiva, Sobrejetiva e Bijetiva

As funções podem apresentar outras características além da existência e unicidade inerentes ao seu conceito. Dentre elas, os tipos: injetiva, sobrejetiva e bijetiva.

Definição 29. (Função Injetiva) Uma função $f : X \to Y$ é *injetiva* (ou *um-a-um*) quando, para todo $x, y \in X$, $x \neq y$ implica $f(x) \neq f(y)$.

Para demonstrar que uma função é injetiva, é de praxe argumentar pela *contrapositiva*[17] (ou *contrarecíproca*) desta implicação, ou seja:

$f : X \to Y$ é *injetiva* se, para todo $x, y \in X$, $f(x) = f(y)$ implica $x = y$.

[17] A *contrapositiva* (ou *contrarecíproca*) de uma implicação é a negação da forma recíproca, ou seja, a partir da *forma positiva* [*hipótese*] implica [*tese*], obtém-se a *forma recíproca* [*tese*] implica [*hipótese*]. Em seguida, nega-se a forma recíproca para obter a contrapositiva. (IRRACIEL; JOSÉ, 2010, p. 4)

O esquema de demonstração a seguir apresenta duas possibilidades de justificar se uma função é injetiva.

Esquemas de Demonstração

***D_1)* Forma direta[18].**

Neste caso, parte-se da *hipótese* $f(x) = f(y)$ e, por meio de operações matemáticas e raciocínio lógico-dedutivo, conclui-se à *tese* $x = y$.

***D_2)* Redução ao absurdo[19].**

Inicia-se negando apenas à tese. Mantém-se à hipótese verdadeira por toda a construção dos argumentos verdadeiros até que se chegue a um absurdo (ou uma contradição). Daí, conclui-se que o absurdo (ou a contradição) surgiu em consequência da negação da tese. Portanto, a tese inicial era verdadeira.

Por outro lado, para demonstrar que uma função *não* é injetiva, é suficiente apresentar um *contraexemplo*, isto é, mostrar que *existem* $x, y \in X$, tais que $x \neq y$ implica $f(x) = f(y)$.

Exemplo 34. A função *inclusão* (ou *identidade*) $Id : X \to X$, definida pela regra $Id(x) = x$ é injetiva.

Resolução: Pela regra de associação, temos: $Id(x) = x$ e $Id(y) = y$, para todo $x, y \in X$. Assim, $Id(x) = Id(y)$ implica $x = y$. Portanto, a função $Id : X \to X$ *Id* é injetiva.

Exemplo 35. Considere $X = \mathbb{N}$. Seja a função $f_a : \mathbb{N} \to \mathbb{N}$, definida por $f_a(n) = n + a$, para todo $a \in \mathbb{N}$. A Lei do Corte da operação de adição é equivalente a afirmar que f_a é injetiva.

Resolução: Temos: $f_a(n) = n + a$ e $f_a(m) = m + a$, para todo $a \in \mathbb{N}$, com $n, m \in \mathbb{N}$. Assim, $f_a(n) = f_a(m)$ implica $n + a = m + a$ e, portanto, $n = m$. Logo, f_a é injetiva.

---

[18] **Forma direta** "é aquela em que assumimos a hipótese como verdadeira e através de uma série de argumentos verdadeiros e deduções lógicas concluímos a veracidade da tese." (IRRACIEL; JOSÉ, 2010, p. 11)

[19] **Redução ao absurdo:** nome que provém do latim *reductio ad absurdum* que consiste em "negar a tese e manter a hipótese verdadeira de uma proposição, por todo o processo de argumentação de demonstração até que se chegue a um absurdo ou uma contradição. Este método é um dos mais importantes e utilizados em demonstrações da Matemática. Ele está alicerçado na *lei do terceiro excluído* que diz: uma afirmação, que não pode ser falsa, deverá ser necessariamente verdadeira, não havendo uma terceira possibilidade. (IRRACIEL; JOSÉ, 2010, p. 13 e 14)

Definição 30. (Função Sobrejetiva) Uma função $f: X \to Y$ é *sobrejetiva* (ou *sobre* Y) quando, para todo $y \in Y$, *existe* pelo menos um $x \in X$, tal que $f(x) = y$.

LIMA (2013, p. 47) estabelece que: para mostrar que uma f de X *em* Y é *sobrejetiva*, deve-se demonstrar que a "equação" $f(x) = y$ tem pelo menos uma solução $x \in X$, para qualquer $y \in Y$.

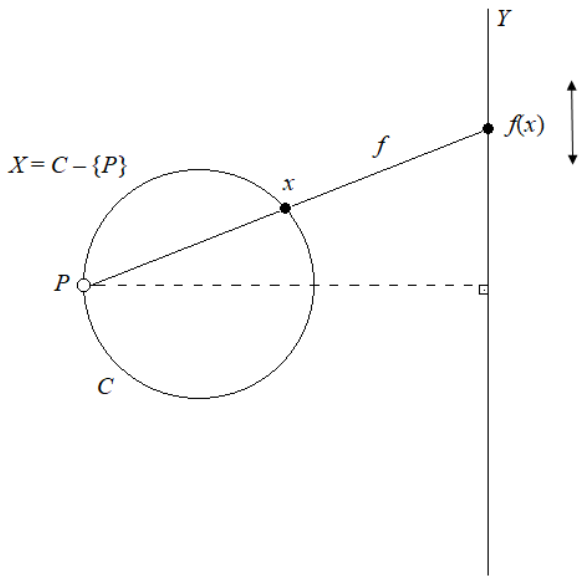
Ainda, segundo o autor: "uma condição necessária e suficiente para uma função $f: X \to Y$ seja sobrejetiva é $f(X) = Y$".

Para DEAN (1974, p. 11): "A distinção entre as palavras *em* e *sobre* é crucial! É claro que cada função *sobre* Y, é também uma função de X *em* Y."

Definição 31. (Função Bijetiva) Uma função $f: X \to Y$ é *bijetiva* (ou *biunívoca*) quando é, simultaneamente, injetiva e sobrejetiva.

Exemplo 36. (Geométrico) Na FIGURA 16, considere o conjunto X de pontos da circunferência C, exceto o ponto P, e o conjunto de pontos Y da reta perpendicular ao diâmetro dessa circunferência que passa pelo ponto P. A função $f: X \to Y$, definida por $f(x)$ = interseção da semirreta Px com a reta Y, para cada $x \in X$, é bijetiva.

FIGURA 16 – Função $f: X \to Y$ sobrejetiva.

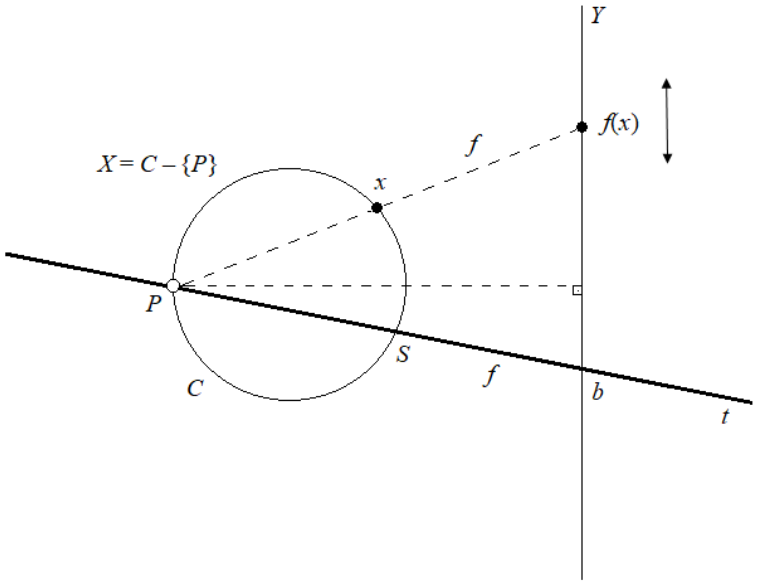


FONTE: LIMA, Elon Lages, 2013, p. 44.

Resolução: De fato, sabe-se da geometria plana que por dois pontos distintos determina-se uma única reta que passa por eles. Além disso, se um ponto está entre dois pontos de uma reta, então, aquele ponto com cada um destes determina duas semirretas opostas. Assim, para todo $b \in Y$, podemos traçar uma reta t, que passe por P e b.

Como a regra da função $f: X \to Y$ é $f(x)$ = interseção da semirreta Px com a reta Y, para cada $x \in X$, segue que existe um ponto $S \in t \cap C$, conforme ilustrado pela FIGURA 17.

FIGURA 17 – Construção do ponto S pela regra da função f.



FONTE: elaborada pelo autor.

Assim, a "equação" $b = f(x)$ = interseção da semirreta Px com a reta Y, onde $b \in Y$, tem solução $x = S$. Mais ainda, esta solução é *única*, pelo fato de $P \notin C$. Dessa forma, temos $I_m(f) = Y$. Portanto, a função $f: X \to Y$ é sobrejetiva.

Por outro lado, $P \notin C$, assim, a "equação" $b = f(x)$ tem uma única solução. Daí, para todo $x, y \in X$, $x \neq y$ implica $f(x) = f(y)$. Logo, a função $f: X \to Y$ é injetiva.

Como a função $f: X \to Y$ é injetiva e sobrejetiva, simultaneamente, conclui-se que ela é bijetiva.

Exemplo 37. Sejam uma função $f: X \to Y$ e os subconjuntos A e B de X. Mostre que $f(A \cup B) = f(A) \cup f(B)$.

Resolução: Como f é uma função, temos, para todo $y \in f(A \cup B)$, existe $x \in A \cup B$, tal que $f(x) = y$. Daí, se $x \in A$, segue que $y \in f(A)$, e se $x \in B$, temos $y \in f(B)$. Em qualquer caso, temos $y \in f(A) \cup f(B)$. Portanto, $f(A \cup B) \subset f(A) \cup f(B)$.

Reciprocamente, para qualquer $z \in f(A) \cup f(B)$, temos $z \in f(A)$ ou $z \in f(B)$. Daí, se $z \in f(A)$, existe $x \in A$, tal que $f(x) = z$.

De maneira análoga, se $z \in f(B)$, existe $y \in B$, tal que $z = f(y)$. Em qualquer dessas hipóteses, existe $w \in A \cup B$, tal que $f(w) = z$. Logo, $f(A) \cup f(B) \subset f(A \cup B)$.

Como $f(A \cup B) \subset f(A) \cup f(B)$ e $f(A) \cup f(B) \subset f(A \cup B)$, tem-se $f(A \cup B) = f(A) \cup f(B)$.

Exemplo 38. Sejam uma função $f : X \to Y$ e os subconjuntos A e B de Y. Mostre que $f^{-1}(A \cup B) = f^{-1}(A) \cup f^{-1}(B)$.

Resolução: Temos: $x \in f^{-1}(A \cup B) \Leftrightarrow f(x) \in A \cup B \Leftrightarrow f(x) \in A$ ou $f(x) \in B \Leftrightarrow x \in f^{-1}(A)$ ou $x \in f^{-1}(B) \Leftrightarrow x \in f^{-1}(A) \cup f^{-1}(B)$.

5.3 Restrição, Extensão e Composição de Funções

Dada uma função, pode ocorrer a necessidade de *restringirmos* seu domínio como parte de outro conjunto específico, mantendo a regra de associação. Neste caso, obtemos uma *nova* função.

Segundo LIMA (2010, p. 21), "a *restrição* de uma função $f : X \to Y$ a um subconjunto $A \subset X$ é uma função $f|_A : A \to Y$, definida por $f|_A(x) = f(x)$, para todo $x \in A$."

Observe que função restrição $f|_A : A \to Y$ tem a *mesma regra* da função $f : X \to Y$, com *domínio* A, que está contido no domínio X de f. Então, elas se relacionam da seguinte forma: $f|_A$ é um subconjunto de f, pois $x \in A$ implica $x \in X$, portanto, $(x, f(x)) \in f|_A$ implica $(x, f(x)) \in f$, para todo $x \in A$.

Na forma de conjunto, a função restrição é presentada por:

$$f_A = \{(x, y) \in f ; y = f(x), \text{ para } x \in A \subset X\}.$$

Por outro lado, a noção de *extensão* de uma função ocorre quando mantemos a regra de associação e *incluímos* seu domínio num outro conjunto, obtendo, assim, uma nova função com domínio neste conjunto mais extenso.

Nesse sentido, a *extensão* da função $f : X \to Y$ a um subconjunto $X \subset A$ é obter uma função $f|^A : A \to Y$, tal que $f|^A(x) = f(x)$, para todo $x \in X$.

Na representação de conjunto, a função extensão escreve-se:

$$f^A = \{(x, y) \in f ; y = f(x), \text{ para } x \in X \subset A\}.$$

Outra função importante é definida pela composição de funções, isto é, dadas as funções $f : X \to Y$ e $g : Y \to Z$, onde o domínio de g é igual ao contradomínio de f, chama-se *função composta*, a função $g \circ f : X \to Z$, com a regra de aplicar primeiro f, e depois, g. Em símbolos, isto equivale a:

$$(g \circ f)(x) = g(f(x)), \text{ para todo } x \in X.$$

LIMA (2010, p. 20) menciona que para fazer sentido a definição $(g \circ f)(x) = g(f(x))$, para todo $x \in X$, e tenhamos a função composta $g \circ f : X \to Z$, basta que a imagem $f(X)$ esteja contida no domínio de g, isto é, $f(X) \subset Y$.

Quando as funções f e g são iguais, temos: $g \circ f = g \circ g = g^2$ ou $g \circ f = f \circ f = f^2$. Este processo de composição de funções pode ser generalizado.

Dadas as funções $f_1 : X_1 \to Y_1$, $f_2 : X_2 \to Y_2, \cdots, f_n : X_n \to Y_n$, a função composta $f_n \circ \ldots \circ f_2 \circ f_1 : X_1 \to Y_n$ é obtida aplicando primeiro f_1, depois f_2 e assim, sucessivamente, de modo que:

$$(f_n \circ \cdots \circ f_2 \circ f_1)(x) = f_n(\cdots f_2(f_1(x))), \text{ para todo } x \in X_1, \text{ com } f_1(X_1) \subset X_2, \cdots, f_{n-1}(X_{n-1}) \subset X_n.$$

Observação:

Em geral, a propriedade *comutativa* não vale para as funções compostas, ou seja, dadas as funções $f : X \to Y$ e $g : Y \to Z$, temos $(g \circ f)(x) \neq (f \circ g)(x)$, para todo $x \in X$. Mas a propriedade *associativa* é satisfeita. De fato, além das funções dadas, considere a função $h : Z \to W$. Temos:

$$[(h \circ g) \circ f](x) = (h \circ g)(f(x)) = h[g(f(x))] = h[(g \circ f)(x)] = [h \circ (g \circ f)](x).$$

Exemplo 39. Sejam a função $f : X \to Y$ e a função identidade $Id : X \to X$ definida por $Id(x) = x$. Note que:

$$(f \circ Id)(x) = f(Id(x)) = f(x) = y$$

e

$$(Id \circ f)(x) = Id(f(x)) = f(x) = y.$$

Assim, qualquer que seja a função $f : X \to Y$, tem-se: $(f \circ Id)(x) = (Id \circ f)(x)$.

Com isso, dada uma função, podemos definir função inversa à esquerda e à direita de uma função.

5.4 Função Inversa

Segundo LIMA (2010, p. 21 e 22): Dadas as funções $f : X \to Y$ e $g : Y \to X$, dizemos que:

i) g é uma função *inversa à esquerda* de f quando $g \circ f = Id_X : X \to X$, isto é, $g(f(x)) = x$, para todo $x \in X$.

ii) g é uma função *inversa à direita* de f quando $f \circ g = Id_Y : Y \to Y$, ou seja, $f(g(y)) = y$, para todo $y \in Y$.

Definição 32. (Função Inversa) Uma função $g : Y \to X$ chama-se *inversa* da função $f : X \to Y$ quando $g \circ f = Id_X$ e $f \circ g = Id_Y$.

A existência de funções inversas à esquerda e à direita está relacionada às funções injetivas e sobrejetivas, respetivamente, conforme as **Proposições 6 e 7** a seguir.

Proposição 6. A função $f : X \to Y$ possui inversa à esquerda se, e somente se, é injetiva.

Demonstração: ($\Longrightarrow$) Suponha que exista a função $g : Y \to X$ inversa à esquerda de $f : X \to Y$. Então, $g \circ f = Id_X$. Assim, dados $a, b \in X$, temos $f(a) = f(b)$ implica $(g \circ f)(a) = (g \circ f)(b)$ e, portanto, $a = b$. Logo, f é injetiva.

($\Longleftarrow$) Reciprocamente, se a função $f : X \to Y$ é injetiva, então, para cada $y \in f(X)$, existe um único $x \in X$, tal que $y = f(x)$. Pondo $x = g(y)$, definimos a função $g : f(X) \to X$, tal que $g(y) = g(f(x)) = x$, para todo $x \in X$.

Fixando um elementos x_0 em X, considere a função $g : Y \to X$, tal que $g(y) = x_0$, para $y \in Y \setminus f(X)$, temos: $g \circ f = Id_X$. Dessa forma, a função $f : X \to Y$ possui inversa à esquerda.

□

Proposição 7. A função $f : X \to Y$ possui inversa à direita se, e somente se, é sobrejetiva.

Demonstração: ($\Longrightarrow$) Suponha que exista a função $g : Y \to X$ inversa à direita de $f : X \to Y$. Então, $f \circ g = Id_Y$. Assim, para cada $y \in Y$, pondo $g(y) = x$, temos $f(x) = f(g(y)) = y$. Portanto, a função $f : X \to Y$ é sobrejetiva.

($\Longleftarrow$) Reciprocamente, se a função $f : X \to Y$ é sobrejetiva, então, para cada $y \in Y$, existe pelo menos um $x \in X$, tal que $y = f(x)$. Isto significa que o conjunto $f^{-1}(Y) \neq \varnothing$. Assim, escolhemos, para cada $y \in Y$, um $x \in X$, tal que $f(x) = y$.

Pondo $g(y) = x$, definimos a função $g : Y \to X$, tal que $f(g(y)) = y$. Logo, g é a inversa à direita da função $f : X \to Y$.

□

Além da possibilidade de existência de uma função inversa, a unicidade também é uma das características dessa função, isto é, quando existe uma função inversa, ela é única. De fato, suponha que existam duas funções inversas $g : Y \to X$ e $h : Y \to X$ da função $f : X \to Y$. Assim: $f \circ g = Id_Y$ e $h \circ f = Id_X$. Daí:

$$h = h \circ Id_Y = h \circ (f \circ g) = (h \circ f) \circ g = Id_X \circ g = g \ \ \therefore \ \ h = g.$$

Observação:

Na justificativa apresentada sobre a unicidade da função inversa, mostramos que se f possui uma inversa à esquerda, h, e uma inversa à direita, g, então $h = g$.

Indicaremos por $f^{-1} : Y \to X$ a inversa, quando existir, da função $f : X \to Y$.

Nesse contexto, caso a função $f : X \to Y$ seja bijetiva, então, para cada $y \in Y$, existe um único elemento $x \in X$, tal que $f(x) = y$ implica $f^{-1}(y) = x$.

Com as **Proposições 6 e 7**, podemos escrever o teorema a seguir.

Teorema 7. Uma função $f : X \to Y$ possui uma única inversa se, e somente se, é bijetiva.

Demonstração: ($\Longrightarrow$) Suponha que a função $f : X \to Y$ tenha uma única inversa $f^{-1} : Y \to X$. Agora, suponha, por absurdo, que $a, b \in X$, com $a \neq b$. Então:

$$f(a) = f(b) \implies (f \circ f^{-1})(a) = (f \circ f^{-1})(b) \implies Id(a) = Id(b) \therefore a = b.$$

O que é um absurdo! Pois, $a \neq b$, logo, $f : X \to Y$ é uma bijeção.

($\Longleftarrow$) Reciprocamente, suponha que a função $f : X \to Y$ seja bijetiva. Então, para todo $a \in X$, temos $f(a) = b \in Y$. Além disso, existe um único $b \in Y$, tal que a função $g : Y \to X$ define $g(b) = a$, para algum $a \in X$. Daí:

$$(f \circ g)(b) = f(g(b)) = f(a) = b \therefore f \circ g = Id_Y$$

e

$$(g \circ f)(a) = g(f(a)) = g(b) = a \therefore g \circ f = Id_X.$$

Como $(f \circ g)(b) = (f \circ g)(b)$, segue que f tem inversa à esquerda e à direita que são iguais. Portanto, $g = f^{-1}$ é única.

□

Proposição 8. Se as funções $f : X \to Y$ e $g : Y \to X$ são bijetivas, então $(g \circ f)^{-1} = f^{-1} \circ g^{-1}$.

Demonstração: Sendo $f : X \to Y$ e $g : Y \to X$ funções bijetivas, existem as inversas $f^{-1} : Y \to X$ e $g^{-1} : X \to Y$, tais que:

$$f^{-1} \circ f = Id_X \text{ e } g^{-1} \circ g = Id_Y.$$

Daí, pela propriedade associativa da composição de funções, temos:

$$\begin{aligned}(f^{-1} \circ g^{-1}) \circ (g \circ f) &= f^{-1} \circ [g^{-1} \circ (g \circ f)] \\ &= f^{-1} \circ [(g^{-1} \circ g) \circ f] \\ &= f^{-1} \circ (Id_Y \circ f) \\ &= f^{-1} \circ f \\ &= Id_X.\end{aligned}$$

Portanto, $f^{-1} \circ g^{-1}$ é uma inversa (à direita) de $g \circ f$. Pelo **Teorema 7**, concluímos que tal inversa é única, assim, $f^{-1} \circ g^{-1} = (g \circ f)^{-1}$.

□

6 Conjunto Finito, Infinito e Conjuntos Equivalentes

6.1 Conjunto Finito

Segundo LIMA (2010, p. 42), a definição de conjunto finito e infinito está vinculada à existência ou não de uma correspondência bijetiva. Assim, dado $n \in \mathbb{N} = \{1, 2, 3, \cdots\}$, considere o conjunto I_n de números naturais de 1 até n, isto é:

$$I_1 = \{1\}$$

$$I_2 = \{1, 2\}$$

$$\cdots$$

$$I_n = \{1, 2, 3, \cdots, n\}.$$

Definição 33. Um conjunto X chama-se *finito* quando é vazio ($X = \varnothing$) ou quando existe uma bijeção $\alpha : I_n \to X$.

Se existir a bijeção $\alpha : I_n \to X$, dizemos que X tem o mesmo *número de elementos* (ou *número cardinal*) que I_n, ou seja, X e I_n têm n elementos. Em decorrência disso, cada conjunto I_j é finito, para $j = 1, 2, \cdots, n$. Caso $X = \varnothing$, o número de elementos de X é zero.

Ainda nesse contexto, LIMA (2010, p. 43) afirma que a bijeção $\alpha : I_n \to X$ representa "uma *contagem* dos elementos do conjunto X", e fazendo $\alpha(1) = x_1$, $\alpha(2) = x_2$, $\alpha(3) = x_3$, $\cdots$, $\alpha(n) = x_n$, o conjunto *finito* X pode ser representado da forma:

$$X = \{x_1, x_2, \cdots, x_n\}.$$

No caso da bijeção $\alpha : I_n \to X$, definida no conjunto *finito* I_n, seguem alguns resultados importantes, a saber:

Teorema 8. Seja $X \subset I_n$. Se existir uma bijeção $\alpha : I_n \to X$, então $I_n = X$.

Demonstração: Por indução sobre n, temos:

Para $n = 1$, segue $\alpha : I_1 \to X$. Assim, $I_1 = \{1\}$. Como $X \subset I_1$, temos $X = \{1\}$. Portanto, $X = I_1$.

Suponha, por hipótese de indução, que seja verdadeiro para algum n e considere uma bijeção $\alpha : I_{n+1} \to X$.

Fazendo $\alpha(n + 1) = a \in X$, a restrição de α a I_n fornece à bijeção $\alpha^* : I_n \to X - \{a\}$. Daí:

i) se $X - \{a\} \subset I_n$, pela hipótese de indução, temos $I_n = X - \{a\}$, onde $X = I_{n+1}$.

ii) se $X - \{a\} \not\subset I_n$, temos $n + 1 \in X - \{a\}$. Logo, existe $p \in I_{n+1}$, tal que $\alpha(p) = n + 1$.

Assim, por *ii)*, definimos uma nova bijeção $\beta : I_{n+1} \to X$, tal que $\beta(x) = \alpha(x)$, se $x \neq p$ e $x \neq n + 1$, de modo que, enquanto $\beta(p) = a$, temos $\beta(n + 1) = n + 1$.

A *restrição* de β a I_n nos dá uma bijeção $\beta^* : I_n \to X - \{n + 1\}$, tal que $X - \{n + 1\} \subset I_n$. Logo, pela hipótese de indução, $X - \{n + 1\} = I_n$, com $X = I_{n+1}$.

Portanto, pelo Princípio de Indução Finita, $I_n = X$.

□

A partir desse teorema, os dois *corolários*[20] a seguir possibilitam saber quando dois conjuntos finitos têm o mesmo número de elementos e quando pode ocorrer uma bijeção entre um conjunto e a sua parte própria.

Corolário 1. Se existir uma bijeção $\alpha : I_m \to I_n$, então $m = n$. Consequentemente, se existem duas bijeções $\beta : I_n \to X$ e $\gamma : I_m \to X$, então $m = n$.

Demonstração: Sem perda de generalidade, suponha que $m \leq n$. Então, $I_m \subset I_n$. Fazendo $A = I_m$ e considerando que $\alpha : I_m \to I_n$ é uma bijeção, segue, pelo **Teorema 8**, que $I_m = I_n$ e, portanto, $m = n$.

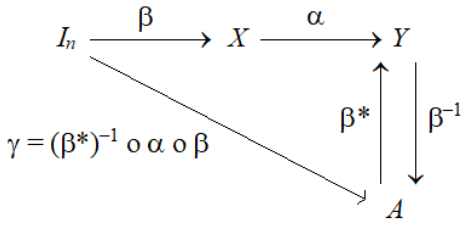
□

Corolário 2. Seja um conjunto X finito. Então, não pode existir uma bijeção $\alpha : X \to Y$, tal que Y seja uma parte própria de X.

Demonstração: Com efeito, suponha o contrário. Seja X um conjunto finito. Então, existe uma bijeção $\beta : I_n \to X$, para algum $n \in \mathbb{N}$. Além disso, β tem uma única inversa. Seja $A = \beta^{-1}(Y)$.

[20] *Corolário* é uma proposição que se obtém, por *consequência imediata*, de um teorema. (ÁVILA, 2006, p. 5)

Então, A é uma parte própria de I_n e a restrição de β a A fornece uma bijeção $\beta^* : A \to Y$. Veja o esquema de composição de funções a seguir.



Dessa forma, a função composta $\gamma = (\beta^*)^{-1} \circ \alpha \circ \beta : I_n \to A$ seria uma bijeção. Mas, pelo **Teorema 8**, isto é um absurdo! Logo, não existe a bijeção $\alpha : X \to Y$.

□

Teorema 9. Se um conjunto X é finito, então, um conjunto $Y \subset X$ é também finito. Neste caso, a cardinalidade de Y não excede a cardinalidade de X, e só é igual, quando $X = Y$.

Demonstração: É suficiente mostrar que $X = I_n$. Por indução sobre n, temos:

Para $n = 1$, as únicas partes de I_1 são $\varnothing$ e I_1.

Suponha, por hipótese de indução, que seja válido para algum $n \in \mathbb{N}$. Considere um subconjunto $Y \subset I_{n+1}$. Assim:

i) se $Y \subset I_n$, pela hipótese de indução, Y é um conjunto finito, com número de elementos menor ou igual a n e, portanto, menor ou igual a $n + 1$.

ii) se $n + 1 \in Y$, segue $Y - \{n + 1\} \subset I_n$. Assim, existe uma bijeção $\alpha : I_m \to Y - \{n + 1\}$, com $m \leq n$. Agora, considere a bijeção $\beta : I_{m+1} \to Y$, definida por $\beta(x) = \alpha(x)$, para $x \in I_m$ e $\beta(m + 1) = n + 1$. Assim, Y é finito, com número de elementos menor ou igual a $m + 1$. Como $m \leq n$, temos: $m + 1 \leq n + 1$.

Para mostrar o caso em que ocorre a igualdade, usa-se o **Corolário 2** do **Teorema 8**, ou seja, não pode existir a bijeção de I_n sobre uma parte própria de Y. Assim, a igualdade só ocorre quando $Y = I_n$.

□

Corolário 3. Seja uma função injetiva $\alpha : X \to Y$. Se Y for finito, então X também será, e o número de elementos de X não excede o de Y.

Demonstração: Note que a função $\alpha : X \to Y$ define uma bijeção de X sobre $\alpha(X)$. Como $\alpha(X) \subset Y$ e, por hipótese, Y é finito, segue, pelo **Teorema 9**:

i) $\alpha(X)$ finito implica X finito; e

ii) a cardinalidade de $\alpha(X)$, que é igual a de X, não excede a cardinalidade de Y.

□

Corolário 4. Seja uma função sobrejetiva $\alpha : X \to Y$. Se X é finito, então Y é finito e o número de elementos de Y não excede o de X.

Demonstração: A função $\alpha : X \to Y$ é sobrejetiva. Logo, possui uma inversa à direita, isto é, existe uma função $\alpha^{-1} : Y \to X$, tal que $\alpha \circ \alpha^{-1} = Id_Y$. Logo, a função α é inversa à esquerda de α^{-1}. Assim, α^{-1} é uma função injetiva de Y sobre X que é finito, por hipótese. Daí, pelo **Corolário 3** do **Teorema 9**, segue que Y é finito e seu número de elementos não excede o de X.

□

A forma apresentada na definição de um conjunto finito está vinculada ao conjunto dos números naturais $\mathbb{N}$, onde se fixou o subconjunto $I_n = \{1, 2, 3, \cdots, n\}$, com $n \in \mathbb{N}$. Contudo, esta definição pode ser desvinculada do conjunto $\mathbb{N}$. Isto se deve ao matemático Dedekind[21] (1831–1916). Para ele: "Um conjunto é finito se, e somente se, não admite uma bijeção com sua parte própria." LIMA (2010, p. 49)

6.2 Conjunto Infinito

A ideia sobre o infinito é antiga e surgiu à época de *Zeno*[22], através dos seus paradoxos sobre o movimento.

Um dos paradoxos mais conhecidos diz:

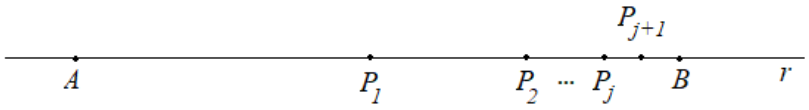
> antes que um objeto possa percorrer uma distância dada, deve percorre a primeira metade dessa distância; mas antes disto, deve percorrer o primeiro quarto; e antes disso, o primeiro oitavo e assim por diante, através de uma infinidade de subdivisões. O corredor que quer pôr-se em movimento precisa

[21] Um dos eminentes matemáticos do séc. XIX que elaborou o conceito de número real. (BOYER, 1996, p. 390)
[22] *Zeno* de Eléia, foi um dos grandes filósofos pré-socráticos da antiga Grécia que viveu por volta 450 a.C. Na matemática, ele é conhecido por seus paradoxos sobre o movimento e a partir disso a ideia de infinidade surgiu pata a reflexão. (BOYER, 1996, p. 51)

> fazer *infinitos* contatos num tempo finito; mas é impossível exaurir uma coleção infinita, logo é impossível iniciar o movimento. (BOYER, 1996, p. 53 e 54, grifo nosso)

De acordo com CARAÇA (1989, p. 13), ilustraremos este paradoxo, considerando dois pontos distintos A e B sobre uma reta r, obtendo o segmento AB, de modo que os pontos P_1, $P_2, \cdots$, são tais que: P_1 está na metade de AB; P_2 está na metade P_1B; etc., conforme a FIGURA 17.

FIGURA 17 – Infinitos pontos sobre uma reta.



FONTE: elaborada pelo autor.

Ainda, de acordo com CARAÇA: intuitivamente, só é possível uma de duas coisas: ou o ponto P_{j+1} está numa posição de P_jB, tal que o segmento $P_{j+1}B$ é tão pequeno que a operação de tomar ao meio termina quando se obter um segmento de comprimento igual $P_{j+1}B$ ou o comprimento do segmento $P_{j+1}B$ é zero. Neste caso, por menor que seja o segmento P_jB, obtido pelo processo de tomar ao meio, sempre será possível pensar num novo segmento P_kB, de modo que o comprimento do segmento P_kB seja menor do que o comprimento do segmento P_jB.

Dessa forma, a operação de "tomar ao meio" repete-se *ilimitadamente* e, por conseguinte, o segmento AB terá uma *infinidade* de pontos $P_1, P_2, \cdots , P_n, \cdots$. Assim, obtemos um *conjunto infinito*:

$$X = \{P_1, P_2, \cdots , P_n, \cdots\}.$$

De modo análogo, pode-se fazer para o segmento AP_1.

Após muitos séculos, o estudo sobre o infinito foi retomado e, a partir do séc. XIX, o matemático alemão Georg Cantor (1845 – 1918) dedicou-se profundamente ao estudo do infinito e da continuidade. Todo este esforço produziu um resultado que surpreendeu os matemáticos do mundo quando ele afirmou e demonstrou que "*existem conjuntos infinitos com*

diferentes cardinalidades[23]". Isto significa que há diversos tipos de infinitos. Esta foi a maior contribuição de Cantor para a matemática. Além disso, ele fez a distinção entre quatro tipos de conjuntos, a saber: conjunto finito, conjunto infinito, conjunto enumerável (ou contável) e conjuntos não-enumerável (ou não-contável, contínuo). (BOYER, 1996, p. 388 – 392, grifos nossos)

Observe que na FIGURA 17, não é possível estabelecer uma bijeção $\alpha : I_n \to X$. Usaremos este fato para definir um conjunto infinito.

Definição 34. Um conjunto X chama-se *infinito* quando *não é vazio* ($X \neq \varnothing$) e, para todo $n \in \mathbb{N}$, *não existe* uma bijeção $\alpha : I_n \to X$.

Tomando $\alpha(n) = x_n$, para todo $n \in \mathbb{N}$, temos: $\alpha(1) = x_1$, $\alpha(2) = x_2$, $\cdots$, $\alpha(n) = x_n$, $\cdots$ e a representação do conjunto X infinito, por listagem de seus elementos, é:

$$X = \{x_1, x_2, \cdots, x_n, \cdots\}.$$

Exemplo 40. O conjunto dos números naturais $\mathbb{N}$ é infinito.

Resolução: Dada qualquer função $\alpha : I_n \to \mathbb{N}$, considere o número:

$$p = \alpha(1) + \alpha(2) + \alpha(3) + \cdots + \alpha(n).$$

Note que $p \notin \alpha(I_n)$. Além disso, para todo $x \in I_n$, tem-se: $\alpha(x) < p$. Dessa forma, $\alpha : I_n \to \mathbb{N}$ não é sobrejetiva. Portanto, $\alpha : I_n \to \mathbb{N}$ não é bijetiva. Logo, $\mathbb{N}$ é infinito.

Outro raciocínio análogo seria considerar a função $\alpha : I_n \to \mathbb{N}$ e tomar o número $k = m + 1$, de modo que $m = max\{\alpha(x) ; x = 1, 2, \cdots, n\}$.

Assim, $\alpha(x) < k$, para todo $x \in I_n$. Portanto, $\alpha : I_n \to \mathbb{N}$ não é sobrejetiva e, portanto, $\alpha : I_n \to \mathbb{N}$ não é bijetiva.

Os *subconjuntos* (finitos ou infinitos) do conjunto dos números naturais $\mathbb{N}$ aprentam características de limitação, e também da existência ou não de um maior elemento.

[23] A *cardinalidade* de um conjunto é a generalização do conceito de número (ou quantidade) de elementos que possui o conjunto. (NERI; AURÉLIO, 2011, p. 18)

Definição 35. Um conjunto $X \subset \mathbb{N}$ é *limitado* se existe um $n \in \mathbb{N}$, tal que $x \leq n$, para todo $x \in X$. Caso $n \in X$, diz-se que n é o *maior elemento* de X.

Quando um conjunto $X \subset \mathbb{N}$ não é limitado, chama-se *ilimitado*. Isto significa que, dado qualquer $n \in \mathbb{N}$, existe algum $x \in X$, tal que $n < x$.

Segundo LIMA (2010, p. 46), todos os subconjuntos do conjunto dos números naturais são caracterizados pelo teorema a seguir.

Teorema 10. Seja um subconjunto X, não vazio, do conjunto dos números naturais $\mathbb{N}$. As seguintes afirmações são equivalentes:
i) X é finito;
ii) X é limitado;
iii) X possui um maior elemento.

Demonstração: De fato: ***i) ⟹ ii)*** Seja o conjunto finito $X = \{x_1, x_2, \cdots, x_n\}$. Considere o número $k = x_1 + x_2 + \cdots + x_n$. Assim, para todo $x \in X$, temos: $x \leq k$. Logo, X é limitado.

ii) ⟹ iii) Suponha que $X \subset \mathbb{N}$ é limitado, isto é, existe um $n \in \mathbb{N}$, tal que $x \leq n$, para todo $x \in X$. Considere o conjunto $C = \{c \in \mathbb{N};\ c \geq x, \text{ para todo } x \in X\}$. Assim, pelo Princípio da Boa Ordenação, o conjunto C possui um menor elemento. Seja $c_0 = min(C)$. Então, $c_0 \in X$. De fato, suponha (por absurdo) que $c_0 \notin X$. Logo, $c_0 > x$, para todo $x \in X$.

Como X é não vazio, segue $c_0 > 1$. Dessa forma, existe $p \in \mathbb{N}$, tal que $c_0 = 1 + p$. Daí, se existisse algum $x \in X$, com $p < x$, isto acarretaria $p + 1 \leq x$ e, portanto, $c_0 \leq x$, o que é um absurdo! Pois, supomos $c_0 \notin X$. Logo, $x \leq p$, para todo $x \in X$. Isto significa que $p \in C$. Assim, $p < c_0 = 1 + p$, o que também é um absurdo! Pois, $c_0 = min(C)$. Portanto, $c_0 \in X$. Mas, $x \leq c_0$, para todo $x \in X$, logo, c_0 é o maior elemento de X.

iii) ⟹ i) Suponha que $m \in X$ seja maior do que todos os elementos de X. Então, $X \subset I_m$ e, pelo **Teorema 9**, X é finito.

□

6.3 Conjuntos Equivalentes

Segundo CARAÇA (1989, p. 14), a operação de *contagem* possibilita comparar vários tipos de infinito.

Dessa forma, segundo LIPSCHUTZ (1972, p. 187): "é natural indagar se dois conjuntos têm ou não o mesmo número de elementos."

No caso de conjuntos são finitos, basta contar o número de elementos de cada conjunto. Mas, para conjuntos infinitos, a resposta dependerá de como se define que dois conjuntos têm o mesmo número de elementos. Sobre isto, pensava-se que todos os conjuntos infinitos possuíam o mesmo número de elementos, ou seja, a mesma cardinalidade. Porém, em 1874, Georg Cantor publicou no *Journal de Crelle* uma das mais importantes descobertas da matemática: "Os conjuntos infinitos não são todos iguais." (BOYER, 1996, p. 392)

Nesse contexto, surge a noção de *conjuntos equivalentes*, cuja definição é atribuída à Georg Cantor.

Definição 36. Um conjunto X é *equivalente* a um conjunto Y e, representa-se por $X \sim Y$, se *existe* uma bijeção $\alpha : X \to Y$.

Quando um conjunto X *não* é equivalente a um conjunto Y, significa que *não existe* a bijeção $\alpha : X \to Y$ e, escreve-se $X \nsim Y$ (lê-se: "*X não é equivalente a Y*")

Exemplo 41. O conjunto dos números naturais $\mathbb{N} = \{1, 2, 3, \cdots\}$ é equivalente ao conjunto dos números pares $\mathbb{P} = \{2, 4, 6, \cdots\}$, ou seja, o conjunto dos números naturais tem o mesmo número de elementos de seu subconjunto próprio.

Resolução: De fato, considere a função $\alpha : \mathbb{N} \to \mathbb{P}$, definida por $\alpha(n) = 2 \cdot n$. Assim, α é injetiva, pois, para todo $a, b \in \mathbb{N}$, temos:

$$\alpha(a) = \alpha(b) \implies 2 \cdot a = 2 \cdot b \implies a = b.$$

Além disso, α é sobrejetiva, porque, para todo $b \in \mathbb{P}$, existe pelo menos um $n \in \mathbb{N}$ que é solução da "equação" $\alpha(n) = b$. Basta tomar a "*metade* de b" e atribuir a n.

Portanto, $\alpha : \mathbb{N} \to \mathbb{P}$ é bijetiva, logo, $\mathbb{N}$ é equivalente a $\mathbb{P}$.

Observe que o conjunto dos números pares $\mathbb{P}$ infinito é um *subconjunto* de $\mathbb{N}$, que também é infinito. Além disso, $\mathbb{P}$ é *equivalente* ao conjunto $\mathbb{N}$. Isto significa que um conjunto infinito pode ser equivalente a um subconjunto próprio de si mesmo, isto é, o todo pode ser equivalente à parte. "Esta propriedade é característica dos conjuntos infinitos." LIPSCHUTZ (1972, p. 188). Entretanto, Georg Cantor, em 1874, descobriu que os conjuntos infinitos não são todos iguais.

Teorema 11. Sejam os conjuntos X e Y. A relação $X \sim Y$ é uma relação de equivalência.

Demonstração: A função identidade $Id : X \to X$ é bijetiva. Logo, $X \sim X$, para todo conjunto X. Dessa forma, a relação "~" é *simétrica*.

Agora, se $X \sim Y$, existe uma função bijetiva $\alpha : X \to Y$. Dessa modo, α tem uma única inversa $\alpha^{-1} : Y \to X$ que é também bijetiva. Assim, $Y \sim X$. Logo, a relação "~" é *reflexiva*.

Finalmente, se $X \sim Y$ e $Y \sim Z$, existem as funções bijetivas $\alpha : X \to Y$ e $\beta : Y \to Z$ e, por conseguinte, a função composta β o $\alpha : X \to Z$ é bijetiva. Então, $X \sim Z$, ou seja, $X \sim Y$ e $Y \sim Z$ implicam $X \sim Z$. Portanto, a relação "~" é *transitiva*.

Como a relação "~" é reflexiva, simétrica e transitiva, conclui-se que "~" é uma relação de equivalência.

□

6.3.1 Conjuntos Enumeráveis e Não-enumeráveis

Com a formalização do conjunto dos números naturais através dos Axiomas de Peano, o conjunto $\mathbb{N} = \{1, 2, 3, \cdots\}$ tornou-se o conjunto-base (ou referência) para o estudo de outros conjuntos.

A noção de enumerabilidade ou não-enumerabilidade de um conjunto X surge na possibilidade de existir uma correspondência bijetiva entre $\mathbb{N}$ e X, de modo que X seja equivalente a $\mathbb{N}$.

Seja o conjunto dos números naturais $\mathbb{N} = \{1, 2, 3, \cdots\}$.

Definição 37. Um conjunto $\mathbb{E}$ (finito ou infinito) chama-se *enumerável* (ou *comensurável*) quando é *equivalente* ao conjunto $\mathbb{N}$.

Em outras palavras, a equivalência entre um conjunto qualquer $\mathbb{E}$ e o conjunto dos números naturais $\mathbb{N}$ garante a existência da função bijetiva $\alpha : \mathbb{N} \to \mathbb{E}$, definida por $\alpha(n) = e_n$, onde $e_n \in \mathbb{E}$, de modo que α *enumera* os elementos do conjunto $\mathbb{E}$.

Nesse contexto, segundo LIMA (2010, p. 48), esta enumeração ocorre fazendo $\alpha(1) = e_1$, $\alpha(2) = e_2, \cdots$, $\alpha(n) = e_n, \cdots$, para todo $n \in \mathbb{N}$.

Dessa forma, a representação do conjunto $\mathbb{E}$, por listagem de seus elementos, é:

$$\mathbb{E} = \{e_1, e_2, \cdots, e_n, \cdots\}.$$

Além disso, diz-se que o conjunto $\mathbb{E}$ tem a *mesma cardinalidade* (ou *quantidade de elementos*) de $\mathbb{N}$.

Segundo LIPSCHUTZ (1972, p. 192): Para designar a cardinalidade dos conjuntos enumeráveis, Georg Cantor utilizava o símbolo $\aleph_o$ (lê-se: "*alef-zero*"). Hoje, porém, usa-se o símbolo $\#(\mathbb{N}) = \mathfrak{a}$, para representar o *número de elementos* (ou *tamanho*) do conjunto dos números naturais.

Quando um conjunto é enumerável, diz-se que é *contável*.

Definição 38. Um conjunto *infinito* $\widetilde{\mathbb{E}}$ chama-se *não-enumerável* (ou *incomensurável*) quando não é equivalente ao conjunto $\mathbb{N}$.

Exemplo 42. O conjunto dos números naturais $\mathbb{N} = \{1, 2, 3, \cdots\}$ é equivalente ao conjunto dos números pares $\mathbb{P} = \{2, 4, 6, \cdots\}$ (ver o **Exemplo 41**). Logo, $\mathbb{P}$ é enumerável.

Exemplo 43. O conjunto dos números ímpares $\mathbb{I} = \{1, 3, 5, \cdots\}$ é enumerável.

Resolução: Basta tomar a bijeção $\alpha : \mathbb{N}_0 \to \mathbb{I}$, definida por $\alpha(n) = 2 \cdot n + 1$. Assim, $\mathbb{N}$ é equivalente a $\mathbb{I}$ e, portanto, $\mathbb{I}$ é enumerável.

Exemplo 44. (Sequência) Uma *sequência* infinita de elementos de um conjunto X, representada por $x = (x_1, x_2, x_3, \cdots) = (x_n)$, onde $n \in \mathbb{N}$, é uma função $x : \mathbb{N} \to X$, definida por $x(n) = x_n$. Uma sequência qualquer de elementos distintos é enumerável.

Resolução: A função $f : \mathbb{N} \to X$, definida por $f(n) = x_n$ é bijetiva, com domínio $\mathbb{N}$. Logo, X é equivalente a $\mathbb{N}$. Portanto, a sequência $(x_1, x_2, x_3, \cdots)$, com $x_n \in X$ e $n \in \mathbb{N}$ é enumerável.

Teorema 12. Todo conjunto infinito possui um subconjunto infinito enumerável.

Demonstração: Vamos definir uma função $\alpha : \mathbb{N} \to X$ injetiva, de modo que um subconjunto infinito $D \subset X$ seja enumerável. De fato, dado um conjunto infinito $X = \{x_1, x_2, x_3, \cdots\}$. Considere o conjunto $A_n = X - J_n$, onde $J_n = \cup_{1 \leq j \leq n}\{x_j\}$, isto é:

$$A_1 = X - J_1 \text{ e } J_1 = \{x_1\}.$$

$$A_2 = X - J_2 \text{ e } J_2 = \{x_1, x_2\}.$$

$$\cdots$$

$$A_n = X - J_n \text{ e } J_n = \{x_1, x_2, x_3, \cdots, x_n\}.$$

Dessa forma, definimos a função $\alpha : \mathbb{N} \to D \subset X$, de modo que:

$$a_1 = \alpha(A_1).$$

$$a_2 = \alpha(A_2).$$

$$\cdots$$

$$a_n = \alpha(A_n).$$

$$\cdots$$

onde $D = \{a_1, a_2, \cdots\}$.

Como X é infinito e J_n é finito, temos que $A_n = X - J_n$ não é vazio, para todo $n \in \mathbb{N}$. Mostraremos que α é injetiva. De fato, dados $m, n \in \mathbb{N}$, com $m < n$, temos $a_m \in D - \{a_n\}$.

Portanto, $m \neq n$ implica $a_m \neq a_n$, logo, α é injetiva. Dessa forma, $D = \{a_1, a_2, \cdots\}$ é um subconjunto infinito enumerável de X.

□

Teorema 13. Todo subconjunto de um conjunto enumerável é finito ou enumerável.

Demonstração: Sejam um conjunto enumerável $X = \{x_1, x_2, x_3, \cdots\}$ e um subconjunto A de X. Então, existe uma função $x : \mathbb{N} \to X$, definida por $x(n) = x_n$, cuja sequência é:

$$x = (x_1, x_2, x_3, \cdots) = (x_n), \text{ onde } n \in \mathbb{N}.$$

Como $A \subset X$, temos:

i) se $A = \varnothing$, então A é finito e, portanto, enumerável.

ii) se $A \neq \varnothing$, seja a função bijetiva $\alpha : \mathbb{N} \rightarrow \{\alpha(1), \alpha(2), \alpha(3), \cdots\}$, definida por $\alpha(n) = a_{\alpha(n)}$, onde:

$a_{\alpha(1)} \in A$ é o primeiro elemento da sequência (x_n)

$a_{\alpha(2)} \in A$ é o segundo elemento da sequência (x_n)

...

$a_{\alpha(k)} \in A$ é o k–ésimo elemento da sequência (x_n)

...

Temos, a composição bijetiva β o $\alpha : \{\alpha(1), \alpha(2), \alpha(3), \cdots\} \rightarrow \{a_{\alpha(1)}, a_{\alpha(2)}, \cdots, a_{\alpha(k)}, \cdots\}$, definida por $\beta(\alpha(n)) = a_{\alpha(n)}$.

Dessa forma, $A = \{a_{\alpha(1)}, a_{\alpha(2)}, \cdots, a_{\alpha(k)}, \cdots\}$. Daí, se o conjunto $\{\alpha(1), \alpha(2), \alpha(3), \cdots\}$ é limitado, segue que A é finito. Do contrário, $A \subset X$ é infinito e, pelo **Teorema 12**, A é enumerável.

□

Corolário 5. Seja um conjunto X contável (enumerável). Então, todo subconjunto A de X é contável (enumerável).

Demonstração: Sendo X um conjunto contável (ou enumerável), pelo **Teorema 13**, o subconjunto A de X é finito ou enumerável. Em qualquer um dos casos, A é contável.

□

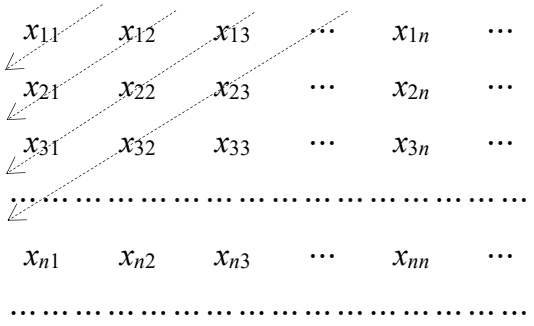
Teorema 14. Seja um conjunto X enumerável. Se a função $\alpha : X \rightarrow Y$ é sobrejetiva, então, o conjunto Y é enumerável.

Demonstração: Por hipótese, a função $\alpha : X \rightarrow Y$ é sobrejetiva. Então, existe uma função $\beta : Y \rightarrow X$, tal que α o $\beta = Id_Y$. Logo, α é uma *inversa à esquerda* de β e, portanto, β é injetiva. Além disso, o conjunto X é enumerável, assim, Y é enumerável.

□

Teorema 15. Sejam todos os conjuntos $X_1, X_2, X_3, X_4, \ldots$ enumeráveis. Então, $\cup X_j$, com $j \in \mathbb{N}$, é enumerável.

Demonstração: Considere esquema a seguir:



Por hipótese, cada um dos conjuntos $X_1, X_2, X_3, X_4, ...$ é enumerável. Então, para manter esta propriedade, considere o conjunto X_j formado pelos elementos da *diagonal secundária* deste esquema, de modo que:

$$X_1 = \{x_{11}\},$$
$$X_2 = \{x_{12}, x_{21}\},$$
$$X_3 = \{x_{13}, x_{22}, x_{31}\},$$
$$X_4 = \{x_{14}, x_{23}, x_{32}, x_{41}\}, \cdots$$

Dessa forma, Assim, cada X_j é finito e, portanto, enumerável. Além disso, a reunião $\cup X_j, = X_1 \cup X_2 \cup X_3 \cup X_4 \cup \cdots = \{x_{11}, x_{12}, x_{21}, x_{13}, x_{22}, x_{31}, x_{14}, x_{23}, x_{32}, x_{41}, \cdots\}$. Portanto, $\cup X_j$ é enumerável.

□

Sobre os conjuntos infinitos, o **Teorema 12** afirma que: "Todo conjunto infinito possui um subconjunto infinito enumerável." Mas será que todo conjunto infinito é enumerável?

Há muito tempo, pensava-se que todos os conjuntos infinitos possuíam a mesma cardinalidade do conjunto dos números naturais. Porém, em 1874, Georg Cantor surpreendeu os matemáticos de sua época ao afirmar e demonstrar que "os conjuntos infinitos não são todos iguais." Isto significa que *existe* conjunto com cardinalidade diferente da cardinalidade do conjunto dos números naturais e, portanto, infinito não-enumerável. (BOYER, 1996, p. 392)

Ainda nesse contexto, segundo ÁVILA (2006, p. 33), outro fato surpreendente é de haver equivalência entre um conjunto infinito e seu subconjunto próprio (ver os **Exemplos 41 e 42**).

Mais adiante, veremos em que situação ocorre a não-enumerabilidade de conjuntos infinitos.

7 Conjunto dos Números Inteiros

Um dos conjuntos numéricos importantes da Matemática é conjunto dos números naturais (ou conjunto-base) $\mathbb{N} = \{1, 2, 3, \cdots\}$, cuja formalização foi elaborada por Peano. Contudo, há situações em que a equação $m + x = n$, na incógnita x, não tem solução.

Nesse contexto, segundo AYRES (1973, p. 57): "O sistema dos números naturais tem um óbvio defeito no fato de que, dados $n, m \in \mathbb{N}$, a equação $m + x = n$ pode ter ou não uma solução."

Por exemplo, a equação $m + x = s(m)$, em x, onde $s(m)$ é o sucessor de $m \in \mathbb{N}$, tem solução $x = 1$. Mas, a equação $s(m) + x = m$ não tem solução em $\mathbb{N}$.

Não obstante, o autor afirma que: "o sistema dos números inteiros pode ser construído a partir do sistema dos números naturais." Isto significa que para solucionar este problema é necessário ampliar (ou estender) o conjunto dos números naturais.

A possibilidade de ampliação do conjunto dos números naturais deve-se ao *Princípio da Extensão* que, segundo CARAÇA (1989, 10):

> *o homem tem tendência a generalizar e estender todas as aquisições do seu pensamento, seja qual for o caminho pelo qual essas aquisições se obtêm, e a procurar o maior rendimento possível dessas generalizações pela exploração metódica de todas as suas consequências.*

7.1 Partição de um Conjunto em Classes de Equivalência

Considere o conjunto $\mathbb{N} \times \mathbb{N} = \{(n, m) \, ; \, n, m \in \mathbb{N}\}$. Se o par ordenado (n, m) fosse uma solução da equação $m + x = n$, então o par ordenado $(s(n), s(m))$ também seria uma solução da equação $s(m) + x = s(n)$, onde $s(k)$ é o sucessor de $k \in \mathbb{N}$. Isto motiva a partição de $\mathbb{N} \times \mathbb{N}$ em classes de equivalências, tais que (n, m) e $(s(n), s(m))$ sejam membros da mesma classe.

De acordo com FERREIRA (2013, p. 36, grifos nossos): "Um *número inteiro* será, então, definido como uma classe de equivalência dada por essa relação."

Ainda, segundo o autor, "o *conjunto dos números inteiros* será, portanto, conjunto dessas classes de equivalência." Este novo conjunto possui uma "*cópia algébrica*" do conjunto dos números naturais $\mathbb{N}$.

Definição 39. Seja a relação binária "$\sim$" (lê-se: "*equivalente a*"). Dados $(n, m), (p, q) \in \mathbb{N} \times \mathbb{N}$, diz-se que $(n, m) \sim (p, q)$ se, e somente se, $n + q = m + p$.

Já vimos que a relação "$\sim$" (ou "$\mathcal{R}$") é uma relação de equivalência e, portanto, realiza uma partição no conjunto $\mathbb{N} \times \mathbb{N}$, que resulta num conjunto de classes de equivalência. O conjunto quociente de $\mathbb{N} \times \mathbb{N}$ nesta relação desta relação é:

$$\mathbb{N} \times \mathbb{N} /\sim = \{[n, m], [p, q], \cdots\},$$

onde $[n, m] = \{(a, b)\ ;\ (a, b) \sim (n, m), \text{com } (a, b) \in \mathbb{N} \times \mathbb{N}\}$. Além disso, sabemos que:

$$[n, m] = [p, q] \iff (n, m) \sim (p, q).$$

Definição 40. **(Extensão de $\mathbb{N}$)** O conjunto quociente $\mathbb{N} \times \mathbb{N} /\sim$, que denotaremos por $\mathbb{Z}$, chama-se conjunto dos números inteiros.

Em símbolos, representa-se por $\mathbb{Z} = \mathbb{N} \times \mathbb{N} /\sim$ ou, de forma equivalente, $\mathbb{Z} = \{[n, m], [p, q], \cdots\}$.

Agora, definiremos as operações de adição e multiplicação em $\mathbb{Z}$, bem como a justificativa de algumas de suas propriedades.

7.2 Operações de Adição e Multiplicação

Para todo $[n, m], [p, q] \in \mathbb{Z}$, define-se:

i) a *adição*: $[n, m] + [p, q] = [(n + p), (m + q)]$, onde $[n, m]$ e $[p, q]$ são as *parcelas* e $[(n + p), (m + q)]$ a *soma*;

ii) a *multiplicação*: $[n, m] \cdot [p, q] = [(n \cdot p + m \cdot q), (n \cdot q + m \cdot p)]$, onde $[n, m]$ e $[p, q]$ são os *fatores* e $[(n \cdot p + m \cdot q), (n \cdot q + m \cdot p)]$ o *produto*.

Teorema 16. As operações de adição e multiplicação são *bem definidas* em $\mathbb{Z}$.

Demonstração: Precisamos mostrar que, para todo $[a, b], [c, d], [a', b'], [c', d'] \in \mathbb{Z}$, com $[a, b] = [a', b']$ e $[c, d] = [c', d']$ valem as igualdades:

i) Adição: $[a, b] + [c, d] = [a', b'] + [c', d']$; e

ii) Multiplicação: $[a, b] \cdot [c, d] = [a', b'] \cdot [c', d']$.

De fato, para a *i) Adição*, temos:

$$[a, b] = [a', b'] \iff (a, b) \sim (a', b') \iff a + b' = b + a' = a' + b \iff a + b' = a' + b \quad \ldots (*)$$

Analogamente:

$$[c, d] = [c', d'] \iff (c, d) \sim (c', d') \iff c + d' = d + c' = c' + d \iff c + d' = c' + d \quad \ldots (**)$$

Somando, membro a membro, as igualdades de (*) e (**), obtemos:

$$(a + c) + (b' + d') = (a' + c') + (b + d) \iff ((a + c), (b + d)) \sim ((a' + c'), (b' + d')) \iff$$

$$[(a + c), (b + d)] = [(a' + c'), (b' + d')] \iff [a, b] + [c, d] = [a', b'] + [c', d'].$$

No caso de *ii) Multiplicação*, considere a igualdade:

$$(a + b') \cdot (c + c') + (a' + b) \cdot (d + d') + (c + d') \cdot (a + a') + (d + c') \cdot (b + b')$$

$$= (a' + b) \cdot (c + c') + (a + b') \cdot (d + d') + (d + c') \cdot (a + a') + (c + d') \cdot (b + b').$$

Desenvolvendo cada produto, obtemos:

$$2(a \cdot c + b \cdot d + a' \cdot d' + b' \cdot c') + (a \cdot c' + b' \cdot c + a' \cdot d + b \cdot d') + (a' \cdot c + d' \cdot a + b \cdot c' + b' \cdot d)$$

$$= 2(a \cdot d + b \cdot c + a' \cdot c' + b' \cdot d') + (a \cdot c' + b' \cdot c + a' \cdot d + b \cdot d') + (a' \cdot c + d' \cdot a + b \cdot c' + b' \cdot d).$$

Aplicando a lei do cancelamento, resulta:

$$a \cdot c + b \cdot d + a' \cdot d' + b' \cdot c' = a \cdot d + b \cdot c + a' \cdot c' + b' \cdot d' \iff$$

$$(a \cdot c + b \cdot d) + (a' \cdot d' + b' \cdot c') \sim (a \cdot d + b \cdot c) + (a' \cdot c' + b' \cdot d') \iff$$

$$[(a \cdot c + b \cdot d), (a \cdot d + b \cdot c)] = [(a' \cdot c' + b' \cdot d'), (a' \cdot d' + b' \cdot c')] \iff$$

$$[a, b] \cdot [c, d] = [a', b'] \cdot [c', d'].$$

□

As operações de adição e multiplicação podem ser reescritas fixando $a \leftrightarrow [n, m]$ e $b \leftrightarrow [p, q]$, para todo $a, b \in \mathbb{Z}$. Dessa forma, escrevemos:

i') *adição*: $a + b \leftrightarrow [n, m] + [p, q] = [(n + p), (m + q)]$; e

ii') a *multiplicação*: $a \cdot b \leftrightarrow [n, m] \cdot [p, q] = [(n \cdot p + m \cdot q), (n \cdot q + m \cdot p)]$.

7.3 Números Inteiros Positivos

Para $m \in \mathbb{N}$, a equação $m + x = s(m)$ tem solução $x = 1$, pois, $s(m) = m + 1$ e, portanto, m é solução da equação $1 + x = s(m)$.

Dessa forma, AYRES (1973, p. 59) estabelece uma bijeção $\alpha : \mathbb{N} \to I^+$ que a cada elemento $n \in \mathbb{N}$ associa à classe de equivalência $[s(n), 1]$. Assim, pela definição de adição e multiplicação, para todo $p, q \in \mathbb{N}$, temos:

- $[s(p), 1] + [s(q), 1] = [(s(p) + s(q)), (1 + 1)] = [s(p + q), 1]$; e
- $[s(p), 1] \cdot [s(q), 1] = [(s(p) \cdot s(q) + 1 \cdot 1), (s(p) \cdot 1 + s(p) \cdot 1)] = [s(p \cdot q), 1]$.

Portanto, a função α define um isomorfismo de $\mathbb{N}$ em $\{[s(n), 1] ; n \in \mathbb{N}\} \subset \mathbb{Z}$.

Agora, suponha que $[p, q] = [s(n), 1]$, para todo $n, p, q \in \mathbb{N}$. Assim:

$$[p, q] = [s(n), 1] \Leftrightarrow (p, q) \sim (s(n), 1) \Leftrightarrow p + 1 = q + s(n) \Leftrightarrow p + 1 = q + n + 1 \therefore$$

$$p = n + q, \text{ com } p > n.$$

Assim, definimos o conjunto $\{[s(n), 1] ; n \in \mathbb{N}\}$ como o conjunto dos números *inteiros estritamente positivos*. Em símbolos, escrevemos:

$$I^+ = \{[s(n), 1] ; n \in \mathbb{N}\}.$$

Neste caso, I^+ é *isomorfo* com $\mathbb{N}$, ou seja, podemos escrever $I^+ = \{1, 2, 3, \cdots\}$.

7.4 Números Inteiros Negativos

Para AYRES (1973, p. 59), o número inteiro *zero* "0" corresponde à classe de equivalência $[n, n]$, onde $n \in \mathbb{N}$. Além disso, para todo $n, p, q \in \mathbb{N}$, temos $[n, n] = [p, q]$ se, e somente se, $p = q$.

Em outras palavras, definimos uma bijeção $\alpha : \mathbb{N} \to \{[n, n] ; n \in \mathbb{N}\}$ que, a cada número natural n associa ao número 0 (zero) representado pela classe de equivalência $[n, n]$. Em símbolos, escreve-se:

$$[n, n] \leftrightarrow 0.$$

Para as operações de adição e multiplicação de números inteiros, decorrem as propriedades: dados $n, m, p, q \in \mathbb{N}$:

i) $[p, q] + [n, n] = [p, q]$;

ii) $[p, q] + [q, p] = [n, n]$; e

iii) $[p, q] \cdot [n, n] = [n, n]$.

De fato, em ***i)***, temos $[p, q] + [n, n] = [(p + n), (q + n)]$.

Como $(p + n) + q = p + (q + n)$, segue que:

$$((p + n), (q + n)) \sim (p, q) \iff [(p + n), (q + n)] = [p, q] \iff [p, q] + [n, n] = [p, q].$$

Em ***ii)***, temos $[p, q] + [q, p] = [(p + q), (q + p)] = [(p + q), (p + q)] = [n, n]$, onde $n = p + q$.

Finalmente, em ***iii)***, temos $[p, q] \cdot [n, n] = [(p \cdot n + q \cdot n), (p \cdot n + q \cdot n)] = [n, n]$, pois, $(p \cdot n + q \cdot n) + n = (p \cdot n + q \cdot n) + n$.

□

Na propriedade ***i)***, onde temos operação de adição, a classe de equivalência $[n, n]$ representa o *zero* é *o elemento neutro da adição*. A classe de equivalência $[q, p]$ representa o *simétrico* (ou *oposto*) de $[p, q]$ na propriedade ***ii)***, e denota-se por $(-[p, q])$, que chamaremos o *negativo* (ou *inverso aditivo*) de $[p, q]$.

De acordo com AYRES (1973, p. 60), supondo $[p, q] \leftrightarrow n \in \mathbb{N}$. Como $[q, p] = -[p, q]$, introduzimos o símbolo $-n$, para denotar o *negativo* de $n \in \mathbb{N}$. Em símbolos, escreve-se:

$$[p, q] \leftrightarrow n \iff [q, p] \leftrightarrow -n.$$

A introdução do símbolo $-n$ (*simétrico* ou *oposto*, ou ainda, *inverso aditivo* de n) só foi possível devido a sua *unicidade*. Isto significa que, dado um número inteiro $[p, q] \leftrightarrow n$, *existe* um *único* inteiro $[q, p] \leftrightarrow -n$, tal que $[p, q] + [q, p] = [n, n] \leftrightarrow 0$. De fato, suponha que existam dois inversos aditivos de n, isto é, $[r, s] \leftrightarrow -a$ e $[t, u] \leftrightarrow -b$, com $[p, q] \leftrightarrow n$. Então:

$$[p, q] + [r, s] = [n, n] \text{ e } [p, q] + [t, u] = [n, n] \iff$$

$$[p, q] + [r, s] = [p, q] + [t, u] \iff$$

$$[p + r, q + s] = [p + t, q + u].$$

Mas, $[p + r, q + s] \leftrightarrow n + (-a)$ e $[p + t, q + u] \leftrightarrow n + (-b)$. Assim:

$$[p + r, q + s] = [p + t, q + u] \iff n\,(-a) = n + (-b) \iff -a = -b \iff [r, s] = [t, u].$$

Finalmente, a propriedade ***iii)*** significa que qualquer classe de equivalência $[p, q]$ multiplicada por uma classe de equivalência nula sempre resultará numa classe de equivalência nula.

Com isto, definimos o conjunto dos números *inteiros estritamente negativos*:

$$I^- = \{[n, m]\ ;\ n < m, \text{ com } n, m \in \mathbb{N}\}.$$

Assim, por *isomorfismo*, o conjunto dos números inteiros representa-se por:

$$\mathbb{Z} = I^+ \cup I^- \cup \{0\} = \{0, \pm 1, \pm 2, \pm 3, \cdots, \pm n, \cdots\}.$$

Neste novo conjunto, valem todas as propriedades da adição e multiplicação em $\mathbb{N}$.

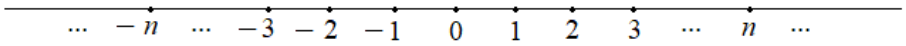
7.5 Relação de Ordem

De modo semelhante em $\mathbb{N}$, podemos comparar dois números inteiros através de uma relação de ordem, de modo que: dados $n, m \in \mathbb{Z}$, escreve-se "$n < m$" para significar que

"n está à esquerda de m" e, analogamente, escreve-se "$n > m$" para dizer que "n está à direita de m".

Do ponto de vista geométrico, os números inteiros podem ser representados sobre uma reta, de modo semelhante à representação dos números naturais. A FIGURA 18 ilustra esta representação.

FIGURA 18 – Representação dos números inteiros sobre uma reta.



FONTE: elaborada pelo autor.

De modo análogo, referente à **Proposição 2** para números naturais, observe que não existe um número inteiro entre dois inteiros consecutivos. Além disso, se $n \in \mathbb{Z}$, tal que $n > 0$, então $n \geq 1$.

Definição 41. Sejam $[n, m] \leftrightarrow a$ e $[p, q] \leftrightarrow b$, onde $a, b \in \mathbb{Z}$. A relação de ordem "$<$" (lê-se: "menor do que"), em $\mathbb{Z}$, é definida por:

$$a < b \text{ se, e somente se, } n + q < m + p.$$

Analogamente, define-se para "$>$", "$\geq$" e "$\leq$". Além disso, vale também a lei da tricotomia, isto é, para quaisquer dois números inteiros $a, b \in \mathbb{Z}$, uma, e somente uma, das afirmações pode ocorrer:

$$a > b \text{ ou } a = b \text{ ou } a < b.$$

Exemplo 45. Prove que, dados $a, b \in \mathbb{Z}$, $a < b$ se, e somente se, $a - b < 0$.

Resolução: Sejam $[n, m] \leftrightarrow a$ e $[p, q] \leftrightarrow b$. Então:

$$a - b = a + (-b) \leftrightarrow [n, m] + (-[p, q]) = [n, m] + [q, p] = [n + q, m + p].$$

Assim:

($\Longrightarrow$) se $a < b$, então $n + q < m + p$ e, portanto, $a - b < 0$.

($\Longleftarrow$) se $a - b < 0$, então $n + p < m + q$, logo, $a < b$.

Exemplo 46. Sejam $a, b \in \mathbb{Z}$, tais que $b < a$. Então, existe $c \in \mathbb{Z}$, de modo que $a = b + c$ ou $c = a - b$.

Resolução: De fato, para todo $a, b \in \mathbb{Z}$, sejam $[n, m] \leftrightarrow a$ e $[p, q] \leftrightarrow b$, com $n, m, p, q \in \mathbb{Z}$. Então:

$$a - b = a + (-b) \leftrightarrow [n, m] + (-[p, q]) = [n, m] + [q, p] = [n + q, m + p].$$

Pondo $c \leftrightarrow [n + q, m + p]$, temos:

$$a = b + c \leftrightarrow [p, q] + [n + q, m + p] = [n + p + q, m + p + q] = [n, m] + [p + q, p + q].$$

Mas, $[p + q, p + q] \leftrightarrow 0$, logo $a = b + c \leftrightarrow [n, m] + [p + q, p + q] = [n, m]$.

Portanto, se $b < a$, então, existe $c \in \mathbb{Z}$, tal que $a = b + c$ ou $c = a - b$.

Exemplo 47. (Regra de Sinais) Para todo $a, b \in \mathbb{Z}$, valem as "regras de sinais":
a) $(-a)\cdot(-b) = a\cdot b$.
b) $(+a)\cdot(-b) = -(a\cdot b)$.

Resolução: a) Sejam $[n, m] \leftrightarrow a$ e $[p, q] \leftrightarrow b$. Então, $[m, n] \leftrightarrow -a$ e $[q, p] \leftrightarrow -b$. Além disso:

$$a\cdot b \leftrightarrow [n, m]\cdot[p, q] = [n\cdot p + m\cdot q, n\cdot q + m\cdot p].$$

Por outro lado:

$$(-a)\cdot(-b) \leftrightarrow [m, n]\cdot[q, p] = [m\cdot q + n\cdot p, m\cdot p + n\cdot q] = [n\cdot p + m\cdot q, n\cdot q + m\cdot p].$$

Assim, $(-a)\cdot(-b) = a\cdot b$.

b) Temos: $(+a)\cdot(-b) \leftrightarrow [n, m]\cdot[q, p] = [n\cdot q + m\cdot p, n\cdot p + m\cdot q]$.

Por outro lado:

$$a\cdot b \leftrightarrow [n, m]\cdot[p, q] = [n\cdot p + m\cdot q, n\cdot q + m\cdot p] \ \therefore \ -(a\cdot b) \leftrightarrow [n\cdot q + m\cdot p, n\cdot p + m\cdot q].$$

Logo, $(+a)\cdot(-b) = -(a\cdot b)$.

Exemplo 48. (Lei do Produto Nulo) Prove que, para $a, b \in \mathbb{Z}$, se $a \cdot b = 0$, então, $a = 0$ ou $b = 0$.

Resolução: Sejam $[n, m] \leftrightarrow a$ e $[p, q] \leftrightarrow b$ e suponha que $a \neq 0$. Então, $n \neq m$ e, portanto, $n - m \neq 0$. Assim:

$$a \cdot b \leftrightarrow [n, m] \cdot [p, q] = [n \cdot p + m \cdot q, n \cdot q + m \cdot p] \leftrightarrow 0 \Leftrightarrow$$

$$n \cdot p + m \cdot q = n \cdot q + m \cdot p \Leftrightarrow$$

$$p \cdot (n - m) = q \cdot (n - m) \Leftrightarrow$$

$$p \cdot (n - m) - q \cdot (n - m) = 0 \Leftrightarrow$$

$$(n - m) \cdot (p - q) = 0.$$

Como, por hipótese, $n - m \neq 0$, temos, $p - q = 0$ e, portanto, $p = q$. Logo, $[p, q] = [p, p] \leftrightarrow 0 = b$.

De modo semelhante, mostra-se que se $b \neq 0$, então, $a = 0$.

□

Exemplo 49. Para todo $n, m, p, q \in \mathbb{Z}$, mostre que:

a) $[s(n), n] \leftrightarrow 1$.

b) $[n, s(n)] \leftrightarrow -1$.

c) $[(n + m), m] = [s(n), 1]$.

d) $[n, m] \cdot [s(p), p] = [n, m]$.

Resolução: a) De fato, suponha $[s(n), n] \leftrightarrow a \in \mathbb{Z}$. Como $s(n) = n + 1$, temos:

$$[s(n), n] = [n + 1, n] = [n, n] + [1, 0].$$

Mas $[n, n] \leftrightarrow 0$, logo: $[s(n), n] = [n, n] + [1, 0] = [1, 0] = [a, 0] \Leftrightarrow a = 1$. Portanto, $[s(n), n] \leftrightarrow 1$.

b) Temos: $[n, s(n)] = -[s(n), n] \leftrightarrow 1$. Mas $s(n), n] \leftrightarrow 1$, portanto, $[n, s(n)] \leftrightarrow -1$.

c) $[(n + m), m] = [s(n), 1] \Leftrightarrow ((n + m), m) \sim (s(n), 1) \Leftrightarrow n + m + 1 = m + s(n) \Leftrightarrow n + 1 = s(n)$.

d) Do item a), temos: $[s(n), n] \leftrightarrow 1$. Logo, $[n, m] \cdot [s(p), p] = [n, m]$.

7.6 Valor Absoluto

Conforme AYRES (1972, p. 63): O *valor absoluto* (ou *módulo*) de um número inteiro x, denota-se por $|x|$, é definido por:

$$|x| = x, \text{ se } x \geq 0 \quad \text{e} \quad |x| = -x, \text{ se } x < 0.$$

Dessa forma, o valor absoluto de um número inteiro é sempre positivo ou nulo, isto é, $|x| \in I^+ \cup \{0\}$.

Nesse contexto, conforme LIMA (2010, p. 71), podemos entender o valor absoluto de um número inteiro da seguinte forma: dado $x \in \mathbb{Z}$, ou x e $-x$ são ambos iguais a zero, ou um é positivo e o outro é negativo. O número inteiro entre x e $-x$ que não for negativo, chama-se *valor absoluto* (ou *módulo*) de x e denota-se por $|x|$. Isto significa que $|x|$ é o maior dos números x e $-x$. Em símbolos, escreve-se:

$$|x| = max\{x, -x\}.$$

A partir disso, podemos escrever que $|x| \geq x$ e $|x| \geq -x$. Além disso, $|x| \geq -x$ é equivale a $-|x| \leq x$. Em suma, para todo $x \in \mathbb{Z}$, temos:

$$-x \leq |x| \leq x.$$

Mais ainda, para todo $x \in \mathbb{Z}$, vale a propriedade $|x| = |-x|$. De fato:

$$|x| = max\{x, -x\} \implies |-x| = max\{-x, -(-x)\} = max\{-x, x\} = max\{x, -x\} = |x|.$$

Ainda, segundo LIMA, o teorema a seguir mostra a equivalência da relação de desigualdade modular.

Teorema 17. Seja $a \in \mathbb{Z}$. Então, para todo número inteiro x, as seguintes afirmações são equivalentes:

i) $-a \leq x \leq a$.

ii) $-a \leq x$ e $x \leq a$.

iii) $|x| \leq a$.

Demonstração: De fato, ***i)*** $-a \leq x \leq a \iff$ ***ii)*** $-a \leq x$ e $x \leq a$. Como $|x| = max\{x, -x\}$, temos $-a \leq x$ e $x \leq a \iff$ ***iii)*** $|x| \leq a$.

□

Corolário 6. Sejam $a, b \in \mathbb{Z}$. Então, para todo número inteiro x, $|x - a| \leq b$ se, e somente se, $a - b \leq x \leq a + b$.

Demonstração: Pelo **Teorema 17**, temos:

$$|x - a| \leq b \iff -b \leq x - a \leq b \iff a - b \leq x + a - a \leq a + b \iff a - b \leq x \leq a + b.$$

□

O valor absoluto de um número inteiro tem outras propriedades, a saber:

7.6.1 Propriedades do Valor Absoluto

Para todo $a, b \in \mathbb{Z}$, as afirmações a seguir são verdadeiras:

VA₁) $-|a| \leq a \leq |a|$.

VA₂) $-(|a| + |b|) \leq a + b \leq |a| + |b| \iff |a + b| \leq |a| + |b|$. (*Desigualdade triangular*)

VA₃) $|a - b| \leq |a| + |b|$.

VA₄) $|a| - |b| \leq |a - b|$.

VA₅) $|a| - |b| \leq |a + b|$.

VA₆) $|a \cdot b| = |a| \cdot |b|$.

Demonstração: Em ***VA₁)***, para todo $a \in \mathbb{Z}$, temos:

$$|a| = max\{a, -a\} \iff |a| \geq a \text{ e } |a| \geq -a.$$

Mas, $|a| \geq -a$ é equivalente a $-|a| \leq a$. Então:

$$|a| \geq a \text{ e } -|a| \leq a \iff -|a| \leq a \leq |a|.$$

Em ***VA₂)***, temos, em vista de ***VA₁)***: $-|a| \leq a \leq |a|$ e $-|b| \leq b \leq |b|$.

Somando estas duas desigualdades, obtém-se:

$$-(|a| + |b|) \leq a + b \leq |a| + |b|.$$

Pelo **Teorema 17**, ***i)*** é equivalente a ***iii)***, então:

$$-(|a|+|b|) \leq a+b \leq |a|+|b| \iff |a+b| \leq |a|+|b|.$$

Outra maneira de demonstrar esta propriedade é: por definição, temos $|a| \geq a$ e $|b| \geq b$, logo, $-|a| \leq a$ e $-|b| \leq b$. Assim:

$$a+b \leq |a|+|b| \text{ e } -(a+b) = -a-(+b) = -a+(-b) \leq |a|+|b|.$$

Como, por definição, $|a+b| = a+b$ ou $-(a+b)$, temos:

$$|a+b| \leq |a|+|b|.$$

Em ***VA₃)***, temos, pela *Desigualdade triangular*:

$$|a-b| = |a+(-b)| \leq |a|+|(-b)| = |a|+|b| \iff |a-b| \leq |a|+|b|.$$

Em ***VA₄)***, segue, pela *Desigualdade triangular*, que:

$$|a| = |(a-b)+b| \leq |a-b|+|b| \iff |a|-|b| \leq |a-b|.$$

Em ***VA₅)***, temos, por ***VA₄)***:

$$|a|-|b| \leq |a-b| \leq |a+b| \iff |a|-|b| \leq |a+b|.$$

Em ***VA₆)***: Para todo $x \in \mathbb{Z}$, temos $|x| = x$, se $x \geq 0$ e $|x| = -x$, se $x < 0$. Assim:

- se $a, b > 0$, tem-se $|a| = a$, $|b| = b$ e $a \cdot b > 0$. Portanto, $|a \cdot b| = a \cdot b = |a| \cdot |b|$.
- se $a, b < 0$, segue que $|-a| = -(-a)$ e, portanto, $|a| = a$. Analogamente para b, isto é, $|b| = b$. Além disso, $a \cdot b > 0$, logo $|a \cdot b| = a \cdot b = |a| \cdot |b|$.
- se $a > 0$ e $b < 0$ (o caso $a < 0$ e $b > 0$ é semelhante), então $|a| = a$ e $|b| = -(-b) = b$. Além disso, $a \cdot b < 0$ e, por conseguinte, $|a \cdot b| = -(-a \cdot b) = a \cdot b = |a| \cdot |b|$.

Outra maneira de demonstrar esta propriedade é: Como $|x| = max\{x, -x\}$, temos $|x|$ é um dos elementos x ou $-x$. Assim, $|a|^2 = a^2$ e $|(-a)|^2 = (-a)^2$ são equivalentes. De modo análogo, $|b|^2 = b^2$.

Portanto, $|a\cdot b|^2 = (a\cdot b)^2 = a^2\cdot b^2 = |a|^2 \cdot |b|^2$. Daí:

$$|a\cdot b|^2 = |a|^2 \cdot |b|^2 \iff |a\cdot b|^2 - |a|^2 \cdot |b|^2 = 0 \iff (|a\cdot b| + |a|\cdot|b|)\cdot(|a\cdot b| - |a|\cdot|b|) = 0.$$

Pela **Lei do Produto Nulo**, obtém-se:

$$|a\cdot b| + |a|\cdot|b| = 0 \text{ ou } |a\cdot b| - |a|\cdot|b| = 0 \iff |a\cdot b| = -|a|\cdot|b| = 0 \text{ ou } |a\cdot b| = +|a|\cdot|b| \iff |a\cdot b| = \pm|a|\cdot|b|.$$

Como $|a\cdot b|$ e $|a|\cdot|b|$ são não-negativos, conclui-se:

$$|a\cdot b| = |a|\cdot|b|.$$

□

7.7 Operações de Subtração e Divisão

CARAÇA (1989, p. 20) menciona que, em relação as operações de adição e multiplicação, pode-se estabelecer os *problemas inversos* a seguir:

No caso da adição, dada uma soma e uma das parcelas, determinar a outra parcela, ou seja:

"Dados $a, b \in \mathbb{Z}$, determinar $c \in \mathbb{Z}$, tal que $a = c + b$.

Para a multiplicação, dado o produto e um dos fatores, determinar o outro fato, isto é:

"Dados $a, b \in \mathbb{Z}$, determinar $c \in \mathbb{Z}$, tal que $a\cdot c = b$.

Já sabemos que a operação de adição é bem-definida e vale a propriedade comutativa. Assim, dado qualquer $b \in \mathbb{Z}$, existe um único *inverso aditivo* "$(-b)$", tal que $b + (-b) = 0$. Dessa forma, $a = c + b$ equivale a $a + (-b) = c + b + (-b)$ e, portanto, $c = a + (-b)$. Isto sugere a definição de subtração.

7.7.1 Operação de Subtração

Segundo AYRES (1973, p. 62): dados $a, b \in \mathbb{Z}$, a *subtração* é definida por $a - b = a + (-b)$.

Em outras palavras, a *subtração* $a - b$ é um número $c \in \mathbb{Z}$, tal que:

$$a - b = c \iff a = c + b.$$

Dessa forma, pode-se dizer que a subtração é a *operação inversa* da adição e vice-versa.

Exemplo 50. Mostre que, para todo $a, b \in \mathbb{Z}$:
a) $a + (-a) = 0$.
b) se $a + x = b$ é uma equação em x, então $x = b + (-a)$ é solução desta equação. Além disso, prove que a solução é única.

Resolução: a) Seja $[n, m] \leftrightarrow a$. Então, $[m, n] \leftrightarrow -a$. Assim:

$a + (-a) \leftrightarrow [n, m] + [m, n] = [n + m, m + n] = [n + m, n + m] \leftrightarrow 0$. Portanto, $a + (-a) = 0$.

Isto dignifica que para cada $a \in \mathbb{Z}$, existe um *inverso aditivo* $(-a) \in \mathbb{Z}$, tal que $a + (-a) = 0$.

b) Sejam $[n, m] \leftrightarrow a$ e $[p, q] \leftrightarrow b$. Temos:

$$x = b + (-a) \leftrightarrow [p, q] + (-[n, m]) = [p, q] + [m, n] = [p + m, q + n] \therefore x \leftrightarrow [p + m, q + n].$$

Assim:

$$a + x \leftrightarrow [n, m] + [p + m, q + n] = [n + p + m, m + q + n] = [p, q] + [n + m, n + m] \leftrightarrow b \therefore$$

$$a + x = b.$$

Logo, $x = b + (-a)$ é uma solução da equação $a + x = b$.

Agora, suponha que exista outra solução y da equação $a + x = b$. Então:

$$a + x = b = a + y \iff a + x = a + y.$$

Pela lei do cancelamento da adição, obtém-se $x = y$ e, portanto, a solução é única.

Na operação de subtração, não valem as propriedades comutativa e associativa. Porém, vale a propriedade distributiva em relação à subtração. De fato:

i) *Comutativa:* Sejam $[n, m] \leftrightarrow a$ e $[p, q] \leftrightarrow b$. Temos:

$$a - b = a + (-b) \leftrightarrow [n, m] + (-[p, q]) = [n, m] + [q, p] = [n + q, m + p]$$

e

$$b - a = b + (-a) \leftrightarrow [p, q] + (-[n, m]) = [p, q] + [m, n] = [p + m, q + n].$$

Como $[n + q, m + p] \neq [p + m, q + n]$, conclui-se que $a - b \neq b - a$.

ii) *Associativa:* Sejam $[n, m] \leftrightarrow a$, $[p, q] \leftrightarrow b$ e $[r, s] \leftrightarrow c$. Então:

$$b - c = b + (-c) \leftrightarrow [p, q] + (-[r, s]) = [p, q] + [s, r] = [p + s, q + r] \ \therefore$$

$$-(b - c) \leftrightarrow [q + r, p + s]$$

e

$$a - b = a + (-b) \leftrightarrow [n, m] + (-[p, q]) = [n, m] + [q, p] = [n + q, m + p].$$

Assim:

$$a - (b - c) = a + (-(b - c)) \leftrightarrow [n, m] + [q + r, p + s] = [n + q + r, m + p + s]$$

e

$$(a - b) - c = (a - b) + (-c) \leftrightarrow [n + q, m + p] + [s, r] = [n + q + s, m + p + r].$$

Como $[n + q + r, m + p + s] \neq [m + p + s, n + q + r]$, segue:

$$a - (b - c) \neq (a - b) - c, \text{ com } c \neq 0.$$

iii) *Distributiva em relação à subtração:* Sejam $[n, m] \leftrightarrow a$, $[p, q] \leftrightarrow b$ e $[r, s] \leftrightarrow c$. Então:

$b - c = b + (-c) \leftrightarrow [p, q] + (-[r, s]) = [p, q] + [s, r] = [p + s, q + r] \ \therefore \ b - c \leftrightarrow [p + s, q + r]$.

Assim:

$$a \cdot (b - c) \leftrightarrow [n, m] \cdot [p + s, q + r] = [n \cdot (p + s) + m \cdot (q + r), n \cdot (q + r) + m \cdot (p + s)]$$

$$= [n \cdot p + n \cdot s + m \cdot q + m \cdot r, n \cdot q + n \cdot r + m \cdot p + m \cdot s].$$

Por outro lado:

$$a\cdot b - a\cdot c \leftrightarrow [n, m]\cdot[p, q] + (-[n, m]\cdot[r, s]) = [n\cdot p + m\cdot q, n\cdot q + m\cdot p] + (-[n\cdot r + m\cdot s, n\cdot s + m\cdot r])$$

$$= [n\cdot p + m\cdot q, n\cdot q + m\cdot p] + [n\cdot s + m\cdot r, n\cdot r + m\cdot s]$$

$$= [n\cdot p + m\cdot q + n\cdot s + m\cdot r, n\cdot q + m\cdot p + n\cdot r + m\cdot s]$$

$$= [n\cdot p + n\cdot s + m\cdot q + m\cdot r, n\cdot q + n\cdot r + m\cdot p + m\cdot s].$$

Portanto, $a\cdot(b - c) = a\cdot b - a\cdot c$.

Exemplo 51. (Lei do Cancelamento - multiplicação) Mostre que, para a, b, $c \in \mathbb{Z}$, $a\cdot c = b\cdot c$ se, e somente se, $a = b$, sempre que $c \neq 0$.

Resolução: De acordo com a propriedade distributiva da multiplicação em relação à subtração, temos:

$$a\cdot c = b\cdot c \Leftrightarrow a\cdot c - b\cdot c = c\cdot(a - b) = 0 \Leftrightarrow a - b = 0, \text{ com } c \neq 0.$$

De fato, sejam $[n, m] \leftrightarrow a$, $[p, q] \leftrightarrow b$ e $[r, s] \leftrightarrow c$. Então:

$$a - b = a + (-b) \leftrightarrow [n, m] + (-[r, s]) = [n, m] + [s, r] = [n + s, m + r] \therefore$$

$$a - b = 0 \leftrightarrow [n + s, m + r].$$

Assim, $c\cdot(a - b) \leftrightarrow [r, s]\cdot[n + s, m + r]$, com $[r, s] \leftrightarrow c \neq 0$. Logo, $c\cdot(a - b) = 0$ se, e somente se, $a - b = 0$, com $c \neq 0$.

A outra questão, refere-se ao caso em que dados a, $b \in \mathbb{Z}$, determinar $c \in \mathbb{Z}$, tal que $a\cdot c = b$.

Nas palavras de AYRES (1973, p. 88), isto equivale a afirmar que: "O sistema dos números inteiros possui um defeito óbvio, que dados os inteiros $a \neq 0$ e b, a equação $a\cdot x = b$ pode ter ou não solução."

Neste sentido, indaga-se: "Que restrição implicaria na existência ou não do *c inteiro*, de modo que $a\cdot c = b$?".

Para responder esta pergunta, observe que o membro da esquerda de $a\cdot c = b$ sugere a definição de *múltiplo* de um número inteiro.

7.7.2 Múltiplo e Operação de Divisão em $\mathbb{Z}$

Dados $a, b \in \mathbb{Z}$, o número b é *múltiplo* do número a, se *existe* um número inteiro c, tal que $b = a \cdot c$.

Se isto ocorrer, dizemos que a é *divisor* (ou *fator*) de b e, escreve-se $a \mid b$ (lê-se: "*a divide b*"). Neste caso, *existe* $c \in \mathbb{Z}$. Em outras palavras, para todo $a, b \in \mathbb{Z}$, $a \mid b$ se, e somente se, existe $c \in \mathbb{Z}$, tal que $b = a \cdot c$.

Quando temos os múltiplos $a = m \cdot x$ ("*a* é *múltiplo* de *m*") e $b = n \cdot y$ ("*b* é *múltiplo* de *n*"), para todo $a, b, n, m \in \mathbb{Z}$, o número inteiro $m \cdot x + n \cdot y$ chama-se *combinação linear* dos números m e n.

Teorema 18. Sejam $a, b, c \in \mathbb{Z}$. Se $a \mid b$ e $a \mid c$, então $a \mid (b \cdot x \pm c \cdot y)$, para todo $x, y \in \mathbb{Z}$.

Demonstração: Temos, por hipóteses, que $a \mid b$ e $a \mid c$. Então, existem $r, s \in \mathbb{Z}$, tais que $b = a \cdot r$ e $c = a \cdot s$. Logo:

$$b \cdot x \pm c \cdot y = a \cdot x \cdot r \pm a \cdot y \cdot s = a \cdot (x \cdot r \pm y \cdot s).$$

Fazendo $t = x \cdot r \pm y \cdot s$, para algum $t \in \mathbb{Z}$, obtém-se: $b \cdot x \pm c \cdot y = a \cdot t \ \therefore \ a \mid b \cdot x \pm c \cdot y$.

□

Observação:

A escrita $a \mid b$, com $a, b \in \mathbb{Z}$, não representa operação em $\mathbb{Z}$, trata-se apenas de uma notação.

Quando a não é *divisor* (ou *fator*) de b, escreve-se $a \nmid b$ (lê-se: "*a não divide b*"). É justamente neste caso, que reside o "defeito" dos números inteiros, no qual a equação $a \cdot x = b$, com $a \neq 0$, não possui solução em $\mathbb{Z}$.

A restrição $a \neq 0$ é *necessária*, porque se $a = 0$, temos $b = a \cdot c$ implica $b = 0 \cdot c$, para algum $c \in \mathbb{Z}$. Daí, se $b \neq 0$, segue que, $c \in \mathbb{Z}$, o que é impossível! Logo, é necessário garantir que $a \neq 0$.

Agora, se $b = 0$, conclui-se que $0 = 0 \cdot c$ é verdadeiro, para todo $c \in \mathbb{Z}$.

As propriedades a seguir serão muito importantes para compreender o fato da existência de um número inteiro entre dois múltiplos inteiros consecutivos.

Proposição 9. (Propriedade Arquimediana em $\mathbb{Z}$) Sejam $a, b \in \mathbb{Z}$, com $b \neq 0$. Então, existe $n \in \mathbb{N}$, tal que $b \cdot n > a$.

Demonstração: Por hipótese, $b \neq 0$. Então, $|b| > 0$. Assim, $|b| \geq 1$ e, portanto, $|b| \cdot n \geq n$. Daí:

- se $b > 0$, temos $|b| \cdot n = b \cdot n$. Pondo $n = |a| + 1$, segue:

$$|b| \cdot n = b \cdot n = b \cdot (|a| + 1) \geq |a| + 1 > |a| \geq a \quad \therefore \quad b \cdot n > a.$$

- se $b < 0$, temos $|b| \cdot n = -(-b) \cdot n = b \cdot n$. Daí, pondo $n = |a| + 1$, segue:

$$|b| \cdot n = -(-b) \cdot n = b \cdot n = b \cdot (|a| + 1) \geq |a| + 1 > |a| \geq a \quad \therefore \quad b \cdot n > a.$$

Em qualquer caso, segue o resultado que queríamos.

□

Proposição 10. (Propriedade da Limitação) Sejam $a, b \in I^+ = \{1, 2, 3, \cdots\}$. Se $a \mid b$, então, $a \leq b$.

Demonstração: Por hipóteses, $a \mid b$. Então, existe $q \in I^+$, tal que $b = a \cdot q$, com $q \geq 1$. Daí, multiplicando esta desigualdade por a, obtém-se:

$$a \cdot q \geq a \text{ implica } b = a \cdot q \geq a \text{ e, portanto, } b \geq a.$$

□

Note que a recíproca desta propriedade não é verdadeira, pois, o contraexemplo a seguir justifica isto.

Contraexemplo: $a = 3$ e $b = 5$. Temos: $5 \geq 3$, mas, $3 \nmid 5$. Consequentemente, a relação "*divide*" não é uma relação de equivalência, pois, não vale a propriedade simétrica.

Teorema 19. (Eudoxo[24]) Dados $a, b \in I^+ = \{1, 2, 3, \cdots\}$, com $0 < b \leq a$, então existe um número $q \in I^+$, tal que $b \cdot q \leq a < (q + 1) \cdot b$.

[24] **Eudoxo** (408 – 355? a.C.), discípulo de Platão, foi o mais eminente matemático da sua época. Uma de suas criações foi a Teoria das Proporções que compõe o Livro V de *Os elementos* de Euclides. (BOYER, 1996, p. 62)

Demonstração: Mostraremos que *i)* $a < (q + 1)\cdot b$ e *ii)* $b\cdot q \leq a$. De fato, em *i)*, por hipótese, temos:

$$a \geq b.$$

Multiplicando esta desigualdade por $q \in I^+$, obtém-se:

$$a\cdot q \geq b\cdot q.$$

Somando b em ambos os lados nesta última desigualdade, segue que:

$$a\cdot q + b \geq b\cdot q + b \iff a\cdot q + b \geq b\cdot(q + 1) > a \therefore b\cdot(q + 1) > a.$$

Em *ii)*, considere o número inteiro $r \in I^+ \cup \{0\}$, tal que $r = a - b\cdot q$. Mostraremos que $r < b$. De fato, suponha, por absurdo, que $r \geq b$. Então:

$$r = a - b\cdot q \geq b \iff (a - b\cdot q) + b\cdot q \geq b + b\cdot q \therefore a \geq b\cdot(q + 1).$$

Pelo item anterior, isto é um absurdo! Logo, $r < b$.

Como $r \in I^+ \cup \{0\}$, segue $0 \leq r$ implica $r = a - b\cdot q \geq 0$ e, portanto, $a \geq b\cdot q$.

□

Dessa forma, mostramos que: dado um número inteiro $b > 0$, qualquer outro número inteiro positivo a ou é igual a um múltiplo de b ou está entre dois múltiplos consecutivos de b. Em outras palavras, existe um único inteiro positivo q que satisfaz a desigualdade:

$$b\cdot q \leq a < (q + 1)\cdot b \iff$$

$$b\cdot q \leq a < b\cdot q + b \iff$$

$$b\cdot q - b\cdot q \leq a - b\cdot q < b\cdot q - b\cdot q + b \iff$$

$$0 \leq a - b\cdot q < b.$$

Esta última desigualdade sugere a existência de outro número inteiros positivo, digamos r, tal que $r = a - b\cdot q$ se, e somente se, $0 \leq r < b$.

O teorema a seguir garante a existência e a unicidade dos números inteiros q e r.

Teorema 20 (Divisão Euclidiana). Dados a, $b \in \mathbb{Z}$, com $b > 0$, existem os inteiros q e r, univocamente determinados, tais que $r = a - b \cdot q$ ou $a = b \cdot q + r$ se, e somente se, $0 \leq r < b$.

Demonstração: Pelo **Teorema 19 (Eudoxo)**, já demonstramos a *existência* dos números inteiros q e r, onde definimos $r = a - b \cdot q$ ou $a = b \cdot q + r$ se, e somente se, $0 \leq r < b$.

Outra maneira de mostrar a *existência* de q e r é a seguinte: considere o conjunto $M = \{a - b \cdot x \, ; \, x \in \mathbb{Z}\}$. Então, temos dois casos a analisar em relação ao inteiro $b \neq 0$ (condição necessária), a saber:

- se $b < 0$, temos $b \leq -1$. Assim, $b \cdot |a| \leq -|a| \leq a$ e, portanto, $a - b \cdot |a| \geq 0$.
- se $b > 0$, segue que $b \geq 1$ implica $b \cdot (-|a|) \leq -|a| \leq a$ e, portanto, $a - b \cdot (-|a|) \geq 0$.

Isto mostra que $M \subset \mathbb{N}$ e $M \neq \varnothing$. Logo, pelo **Princípio da Boa Ordenação**, existe no conjunto M um menor elemento. Seja $r \geq 0$, o menor elemento de M. Então, pondo $r = a - b \cdot q$, temos: $r < |b|$. De fato, suponha, por absurdo, que $r \geq |b|$. Assim, $r - |b| \geq 0$. Daí:

$$r - |b| = a - b \cdot q - |b| = a - b \cdot (q + 1) < r \text{ implica } a - b \cdot (q - 1) = s < r.$$

Mas isto é um absurdo! Pois, contraria a condição de r ser o mínimo do conjunto de M. Logo, $r < |b|$.

Agora, vamos demonstrar a *unicidade* de q e r. Com efeito, suponha que exista um outro par de inteiros s e t, além de q e r, tal que: $a = b \cdot s + t$, com $0 \leq t < b$.

Como $a = b \cdot q + r$, com $0 \leq r < b$ e $a = b \cdot s + t$, com $0 \leq t < b$, então:

$$b \cdot q + r = b \cdot s + t, \text{ com } 0 \leq r, t < b \iff b \cdot q + (r - t) = b \cdot s, \text{ com } 0 \leq r, t < b.$$

Observe que $b \cdot q + (r - t)$ é um múltiplo de b e $b \mid b \cdot q$. Então, $b \mid r - t$. Mas, $r, t < b$, logo, $|r - t| < |b|$.

Assim, $b \mid r - t$ se, e somente se, $r - t = 0$, ou seja, $r = t$.

Como $r - t = 0$, temos $b \cdot q + (r - t) = b \cdot s$, com $0 \leq r, t < b$ é equivalente a $b \cdot q = b \cdot s$. Mas, por hipótese, $b > 0$ e b é fator comum, então $q = s$.

□

Observe que, se $r = 0$, a expressão $a = b \cdot q + r$, com $0 \leq r < b$, reduz-se a $a = b \cdot q$. Isto significa que a é um *múltiplo* de b ou, de modo equivalente, b é um divisor de a. Em outras palavras, "b 'cabe', no máximo, q vezes em a". Neste caso, a *divisão* de a por b chama-se *exata*. Mais ainda, *existe* um *único* $q \in I^{+}$, tal que $a = b \cdot q$. Os números inteiros a e b chamam-se, respectivamente, *dividendo* e *divisor*. O inteiro q chama-se *o quociente* e r, *o resto* da divisão de a por b, sempre com $0 \leq r < b$ ou $0 \leq r \leq b - 1$. O número $(b - 1)$ chama-se *maior resto possível*. Em símbolos, escreve-se $r_{max} = b - 1$.

Quando a divisão de a por b não é exata, isto é, quando $r \neq 0$ na expressão $a = b \cdot q + r$, com $0 < r < b$, então:

$$0 < r < b \iff 0 < a - b \cdot q < b \iff b \cdot q < a < b \cdot q + b \iff b \cdot q < a < b \cdot (q + 1) \iff$$

$$q < \frac{a}{b} < q + 1.$$

Ponto $n = \frac{a}{b}$, com $b > 0$, temos $q < n < q + 1$. Porém, não existe um número inteiro entre dois números inteiros consecutivos, isto é, o conjunto $\{n \in \mathbb{Z} \, ; \, a < n < a + 1$, para todo $a \in \mathbb{Z}\}$ é vazio.

Segundo AYRES (1973, p. 88), para corrigir este "defeito" dos números inteiros, é preciso fazer a junção, aos números inteiros, os números da forma $n = \frac{a}{b}$ (símbolo de fração ordinária), para formar um novo sistema de números.

8 Conjunto dos Números Racionais

8.1 Extensão dos Inteiros

Para ampliar o campo numérico do conjunto $\mathbb{Z}$, de modo a formar um novo campo numérico, considere o conjunto:

$$\mathbb{Z} \times (\mathbb{Z} \setminus \{0\}) = \{(n, m) \,;\, n \in \mathbb{Z} \text{ e } m \in \mathbb{Z} \setminus \{0\}\}.$$

Agora, definimos neste conjunto a relação "~", de modo que, para todo $(a, b), (c, d) \in \mathbb{Z} \times (\mathbb{Z} \setminus \{0\})$:

$$(a, b) \sim (c, d) \text{ se, e somente se } a \cdot d = b \cdot c.$$

Dessa forma, a relação "~" é uma relação de equivalência, pois valem as propriedades reflexiva, simétrica e transitiva. Com efeito, para todo $(a, b), (c, d), (e, f) \in \mathbb{Z} \times (\mathbb{Z} \setminus \{0\})$, temos:

i) reflexiva: $(a, b) \sim (a, b)$, pois, $a \cdot b = b \cdot a = a \cdot b$.

ii) simétrica: $(a, b) \sim (c, d) \iff a \cdot d = b \cdot c \iff c \cdot b = d \cdot a \iff (c, d) \sim (a, b) \;\; \therefore$

$$(a, b) \sim (c, d) \implies (c, d) \sim (a, b).$$

iii) transitiva: $(a, b) \sim (c, d)$ e $(c, d) \sim (e, f) \iff a \cdot d = b \cdot c$ e $c \cdot f = d \cdot e$. Multiplicando a primeira igualdade por f e a segunda por b, obtém-se:

$$a \cdot d \cdot f = b \cdot c \cdot f \text{ e } c \cdot f \cdot b = d \cdot e \cdot b \iff a \cdot d \cdot f = d \cdot e \cdot b.$$

Como $(c, d) \in \mathbb{Z} \times (\mathbb{Z} \setminus \{0\})$, segue que $d \neq 0$. Então, podemos cancelar o fator d desta última igualdade (por isso que consideramos o conjunto $\mathbb{Z}$ sem o zero). Assim:

$$a \cdot d \cdot f = d \cdot e \cdot b \iff a \cdot f = e \cdot b \iff (a, b) \sim (f, e).$$

Mas, por ***i)***, temos: $(f, e) \sim (e, f)$. Logo:

$$(a, b) \sim (c, d) \text{ e } (c, d) \sim (e, f) \implies (a, b) \sim (e, f).$$

Além disso, a relação de equivalência "~" faz uma partição do conjunto $\mathbb{Z} \times (\mathbb{Z} \setminus \{0\})$ em classes de equivalência, de modo que:

$$\mathbb{Z} \times (\mathbb{Z} \setminus \{0\})/_{\sim} = \{[n, m], [p, q], \cdots\},$$

onde a classe de equivalência $[n, m]$ denotaremos por $\frac{a}{b}$ (lê-se: "a sobre b"), com $b \neq 0$. Assim:

$$\frac{a}{b} = \{(x, y) \in \mathbb{Z} \times (\mathbb{Z} \setminus \{0\}); (x, y) \sim (a, b) \iff x \cdot b = y \cdot a\}.$$

Isto significa que $(x, y) \in \frac{a}{b}$ se, e somente se, $(x, y) \sim (a, b)$ que, por conseguinte, é equivalente a $x \cdot b = y \cdot a$.

Exemplo 52. Seja $\frac{2}{3} = \{(x, y) \in \mathbb{Z} \times (\mathbb{Z} \setminus \{0\}); (x, y) \sim (2, 3) \iff 3 \cdot x = 2 \cdot y\}$. Assim:

a) $(4, 6) \in \frac{2}{3}$, pois, $(4, 6) \sim (2, 3) \iff 3 \cdot 4 = 2 \cdot 6 = 12$.

b) $(1, 2) \notin \frac{2}{3}$, porque $(1, 2) \nsim (2, 3)$. De fato, $3 \cdot 1 \neq 2 \cdot 2 \iff 3 \neq 4$.

Definição 42. O conjunto quociente $\mathbb{Z} \times (\mathbb{Z} \setminus \{0\})/_{\sim}$, que denotaremos por $\mathbb{Q}$, será chamado de conjunto dos números racionais.

Em símbolos, escreve-se: $\mathbb{Q} = \mathbb{Z} \times (\mathbb{Z} \setminus \{0\})/_{\sim}$ ou, usualmente, por:

$$\mathbb{Q} = \{\frac{a}{b}\ ; a, b \in \mathbb{Z}, \text{com } b \neq 0\}.$$

Para DOMINGUES (1991, p. 195), "cada representação $\frac{a}{b}$, com $a, b \in \mathbb{Z}$ e $b \neq 0$, chama-se número racional dado de uma *fração ordinária* de numerador 'a' e denominador 'b'."

Teorema 21. (Propriedade Fundamental da Igualdade) Sejam $\frac{a}{b}, \frac{c}{d} \in \mathbb{Z} \times (\mathbb{Z} \setminus \{0\})$ dois números racionais. Então, $\frac{a}{b} = \frac{c}{d}$ se, e somente se, $a \cdot d = b \cdot c$.

Demonstração: Sejam $[n, m] \leftrightarrow \frac{a}{b}$ e $[p, q] \leftrightarrow \frac{c}{d}$, onde $[n, m], [p, q] \in \mathbb{Z} \times (\mathbb{Z} \setminus \{0\})/_{\sim}$.

Então:

$$\frac{a}{b} = \frac{c}{d} \leftrightarrow [n, m] = [p, q] \iff (n, m) \sim (p, q) \iff n \cdot q = m \cdot p \iff a \cdot d = b \cdot c \ \therefore$$

$$\frac{a}{b} = \frac{c}{d} \iff a \cdot d = b \cdot c.$$

□

Agora, segundo AYRES (1973, p. 89), define-se no conjunto dos números racionais $\mathbb{Q}$: *o zero*, *o um*, *o inverso aditivo* e *o inverso multiplicativo*, e também *o elemento de imersão* de $\mathbb{Z}$ em $\mathbb{Q}$.

Para todo $n, m \in \mathbb{Z}$, definimos:

$$\textit{o zero}:\ [0, n] \leftrightarrow 0 \iff \frac{0}{n} = 0.$$

$$\textit{o um}:\ [n, n] \leftrightarrow 1 \iff \frac{n}{n} = 1.$$

$$\textit{o inverso aditivo}:\ -[n, m] = [-n, m].$$

$$\textit{o inverso multiplicativo}:\ [n, m]^{-1} = [m, n], \text{ se } n \neq 0 \text{ ou } [n, m] \leftrightarrow \frac{n}{m} \iff [n, m]^{-1} \leftrightarrow \frac{m}{n}.$$

$$\textit{o elemento de ``imersão'' de } \mathbb{Z} \text{ em } \mathbb{Q}\text{: } [n, 1] \leftrightarrow n \iff \frac{n}{1} = n, \text{ com } n \in \mathbb{Z}.$$

Esta última definição (a imersão de $\mathbb{Z}$ em $\mathbb{Q}$), veremos adiante com mais detalhes que permitirá escrever:

$$\mathbb{Z} = \{ \frac{n}{m} \in \mathbb{Q} \ ; m = 1\}.$$

8.1.1 Operações de Adição e Multiplicação

Para todo $[n, m], [p, q] \in \mathbb{Q}$, define-se:

i) a *adição*: $[n, m] + [p, q] = [n \cdot q + m \cdot p, m \cdot q]$; e

ii) a *multiplicação*: $[n, m] \cdot [p, q] = [n \cdot p, m \cdot q]$.

Teorema 22. As operações de adição e multiplicação são *bem definidas* em $\mathbb{Q}$.

Demonstração: Precisamos mostrar que, para todo $[a, b], [c, d], [p, q], [r, s] \in \mathbb{Q}$, com $[a, b] = [c, d]$ e $[p, q] = [r, s]$, valem as igualdades:

i) Adição: $[a, b] + [p, q] = [c, d] + [r, s]$; e

ii) Multiplicação: $[a, b] \cdot [p, q] = [c, d] \cdot [r, s]$.

De fato, no caso de *i)*, *adição*, temos: $[a, b] = [c, d] \iff (a, b) \sim (c, d) \iff a \cdot d = b \cdot c$. Analogamente, $[p, q] = [r, s] \iff (p, q) \sim (r, s) \iff p \cdot s = q \cdot r$. Portanto:

$$[a, b] + [p, q] = [a\cdot q + b\cdot p, b\cdot q]$$

$$= [(a\cdot q + b\cdot p)\cdot d\cdot s, b\cdot q\cdot d\cdot s]$$

$$= [(\boldsymbol{a\cdot d}\cdot q\cdot s + b\cdot d\cdot \boldsymbol{p\cdot s}), b\cdot q\cdot d\cdot s].$$

Mas, $\boldsymbol{a\cdot d} = b\cdot c$ e $\boldsymbol{p\cdot s} = q\cdot r$. Assim:

$$[a, b] + [p, q] = [\boldsymbol{a\cdot d}\cdot q\cdot s + b\cdot d\cdot \boldsymbol{p\cdot s}, b\cdot q\cdot d\cdot s]$$

$$= [b\cdot c\cdot q\cdot s + b\cdot d\cdot q\cdot r, b\cdot q\cdot d\cdot s]$$

$$= [\boldsymbol{b\cdot q}\cdot(c\cdot s + d\cdot r), \boldsymbol{b\cdot q}\cdot d\cdot s]$$

$$= [c\cdot s + d\cdot r, d\cdot s]$$

$$= [c, d] + [r, s].$$

No caso de *ii)*, *multiplicação*, segue que:

$$[a, b]\cdot[p, q] = [a\cdot p, b\cdot q]$$

$$= [a\cdot p\cdot \boldsymbol{d\cdot s}, b\cdot q\cdot \boldsymbol{d\cdot s}]$$

$$= [\boldsymbol{a\cdot d\cdot p\cdot s}, b\cdot q\cdot d\cdot s].$$

Mas, $\boldsymbol{a\cdot d} = b\cdot c$ e $\boldsymbol{p\cdot s} = q\cdot r$. Logo:

$$[a, b]\cdot[p, q] = [\boldsymbol{a\cdot d\cdot p\cdot s}, b\cdot q\cdot d\cdot s]$$

$$= [b\cdot c\cdot q\cdot r, b\cdot q\cdot d\cdot s]$$

$$= [\boldsymbol{b\cdot q}\cdot c\cdot r, \boldsymbol{b\cdot q}\cdot d\cdot s]$$

$$= [c\cdot r, d\cdot s]$$

$$= [c, d]\cdot[r, s].$$

□

Com isto, para todo $[n, m], [p, q] \in \mathbb{Q}$, com $[n, m] \leftrightarrow \frac{a}{b}$ e $[p, q] \leftrightarrow \frac{c}{d}$, a adição e a multiplicação podem ser reescritas da forma:

i') *Adição:* $[n, m] + [p, q] = [n\cdot q + m\cdot p, m\cdot q] \leftrightarrow \frac{a}{b} + \frac{c}{d} = \frac{a\cdot d + c\cdot b}{b\cdot d}$; e

ii') *Multiplicação:* $[n, m]\cdot[p, q] = [n\cdot p, m\cdot q] \leftrightarrow \frac{a}{b}\cdot\frac{c}{d} = \frac{a\cdot c}{b\cdot d}$.

Observações:
1) Os elementos de $\mathbb{Q}$, conjuntos dos números racionais, são classes de equivalência de pares de inteiros e, portanto, com natureza diferente dos números inteiros, do conjunto $\mathbb{Z}$;
2) A propriedade transitiva da relação de equivalência definida em $\mathbb{Z} \times (\mathbb{Z} \setminus \{0\})$ justifica o motivo de considerar o conjunto $\mathbb{Z} \setminus \{0\}$, o qual se exclui o zero de $\mathbb{Z}$.

Nesse contexto, segundo FERREIRA (2013, p. 55 e 59), não é apropriado escrevermos $\mathbb{Z} \subset \mathbb{Q}$. Apesar disso, "existe uma aplicação *injetiva* (grifo nosso) de $\mathbb{Z}$ em $\mathbb{Q}$ que 'preserva' as operações aritméticas e, dessa forma, permite que a imagem de $\mathbb{Z}$ em $\mathbb{Q}$, por esta aplicação, seja uma *cópia algébrica* de $\mathbb{Z}$ em $\mathbb{Q}$".

O que motiva a existência desta função injetiva é o elemento de imersão que definimos no conjunto $\mathbb{Q}$, isto é, a classe de equivalência:

$$[n, 1] \leftrightarrow n \Leftrightarrow \frac{n}{1} = n, \text{ com } n \in \mathbb{Z}.$$

Assim, para fazer a inserção de $\mathbb{Z}$ em $\mathbb{Q}$, considere a função $\alpha : \mathbb{Z} \to \mathbb{Q}$, definida por $\alpha(n) = \frac{n}{1}$. Então:

i) α é injetiva, para todo $n \in \mathbb{Z}$; e

ii) α preserva as operações de isomorfismo $\alpha(n + m) = \alpha(n) + \alpha(m)$ e $\alpha(n\cdot m) = \alpha(n)\cdot\alpha(m)$; e a relação de ordem $n \leq m$ implica $\alpha(n) \leq \alpha(m)$, para todo $n, m \in \mathbb{Z}$.

De fato, em *i)*, temos: $\alpha(n) = \alpha(m) \implies \frac{n}{1} = \frac{m}{1} \implies n = m$. Logo, α é injetiva, para todo $n, m \in \mathbb{Z}$.

Em *ii)*, segue: $\alpha(n) + \alpha(m) = \frac{n}{1} + \frac{n}{1} = n + m = \alpha(n + m)$ e $\alpha(n\cdot m) = \frac{n}{1}\cdot\frac{m}{1} = \alpha(n)\cdot\alpha(m)$; e $n \leq m \implies \frac{n}{1} \leq \frac{m}{1} \implies \alpha(n) \leq \alpha(m)$, para todo $n, m \in \mathbb{Z}$.

Portanto, a imagem de $\mathbb{Z}$ em $\mathbb{Q}$, isto é, o conjunto $\alpha(\mathbb{Z}) = \left\{\frac{n}{1};\ n \in \mathbb{Z}\right\}$ é uma *cópia algébrica* de $\mathbb{Z}$ em $\mathbb{Q}$.

Ainda, conforme o autor: “essa *imersão* de $\mathbb{Z}$ em $\mathbb{Q}$ também mostra que $\mathbb{Q}$ é *infinito*, já que $\mathbb{Z}$ contém uma cópia de $\mathbb{N}$.” (grifos nossos)

Por consequência disso, todas as propriedades referentes aos números inteiros valem também no conjunto dos números racionais.

Proposição 11. Todo número racional, não nulo, possui um único *inverso multiplicativo*, cujo produto deles é 1.

Demonstração: De fato, seja $[n, m] \leftrightarrow a \neq 0$ um número racional, com $n \neq 0$. Então, por definição, temos $[n, m]^{-1} = [m, n]$.

Pondo $[m, n] \leftrightarrow a^{-1} \in \mathbb{Q}$, para todo $[n, m]^{-1} \in \mathbb{Q}$, com $n \neq 0$, segue:

$$a \cdot a^{-1} \leftrightarrow [n, m] \cdot [m, n] = [n \cdot m, m \cdot n] = [n \cdot m, n \cdot m] \leftrightarrow 1.$$

Assim, $a \cdot a^{-1} = 1$.

Agora, suponha que exista outro inverso multiplicativo $[r, s] \leftrightarrow b^{-1} \in \mathbb{Q}$ de $[n, m] \leftrightarrow a \neq 0$, com $s \neq 0$. Então:

$$a \cdot a^{-1} = 1 = a \cdot b^{-1}.$$

Pela **Lei do Corte**, $a \cdot a^{-1} = 1 = a \cdot b^{-1}$ é equivalente a $a^{-1} = b^{-1}$. Assim, existe um único inverso multiplicativo para cada número racional, não nulo, cujo produto é 1.

□

Dessa forma, podemos substituir $[n, m]^{-1} = [m, n]$ por $\frac{m}{n}$, com $n \neq 0$, de modo que $a \cdot b^{-1} = \frac{a}{b}$, com $b \neq 0$.

Em particular, para $m = 1$, temos $[n, 1]^{-1} = [1, n] \leftrightarrow \frac{1}{n}$, com $n \neq 0$. Assim, $a \cdot b^{-1} = a \cdot \frac{1}{b}$.

8.1.2 Operações de Subtração e Divisão

A operação de subtração é análoga a que foi definida para os números inteiros, porém, com *inverso aditivo* definido em $\mathbb{Q}$, isto é, a classe de equivalência $-[n, m] = [-n, m]$, para todo $[n, m], [p, q] \in \mathbb{Q}$.

Para todo $r, s \in \mathbb{Z}$, chama-se *diferença* entre r e s, o número $t \in \mathbb{Z}$, tal que $t = r + (-s)$ ou, de forma equivale, $r = s + t$.

Assim, para todo $[n, m], [p, q] \in \mathbb{Q}$, com $[n, m] \leftrightarrow r = \frac{a}{b}$ e $[p, q] \leftrightarrow s = \frac{c}{d}$, temos:

$$r - s = r + (-s) = \frac{a}{b} - \frac{c}{d} \leftrightarrow [n, m] + (-[p, q]) = [n, m] + [-p, q] = [n \cdot q - m \cdot p, m \cdot q] \leftrightarrow \frac{a \cdot d - c \cdot b}{b \cdot d}.$$

Observe que, em relação à operação de adição, para obter a *diferença*, basta trocar o sinal de *mais* "+" pelo sinal de *menos* "–", ou seja:

$$\textit{Adição: } \frac{a}{b} + \frac{c}{d} = \frac{a \cdot d + c \cdot b}{b \cdot d} \quad \text{e} \quad \textit{Subtração: } \frac{a}{b} - \frac{c}{d} = \frac{a \cdot d - c \cdot b}{b \cdot d}.$$

Para definir a operação de divisão em $\mathbb{Q}$, seguiremos o raciocínio análogo à subtração em relação à adição, porém, fazendo uso do inverso multiplicativo em $\mathbb{Q}$.

Sabemos que a cada número racional $[n, m]$, não nulo, existe um *inverso multiplicativo* denotado por $[n, m]^{-1} = [m, n]$, com $n \neq 0$, de modo que:

$$[n, m] \cdot [m, n] \leftrightarrow 1.$$

Com isto, é possível definir a divisão de dois números racionais, sempre observando que o divisor não pode ser nulo. Em relação à classe de equivalência $[n, m]$, isto significa, $n \neq 0$.

Definição 43. Sejam $[n, m]$ e $[p, q] \in \mathbb{Q}$, não nulos, com $n, m, p, q \in \mathbb{Z}$. A *divisão* de $[n, m]$ por $[p, q]$ é a classe de equivalência $[n, m] : [p, q] = [n, m] \cdot [q, p]$, onde $[q, p]$ é o inverso multiplicativo de $[p, q]$.

Com isso, sejam $[n, m], [p, q] \in \mathbb{Q}$, não nulos. Pondo $[n, m] \leftrightarrow \frac{a}{b}$ e $[p, q] \leftrightarrow \frac{c}{d}$, temos:

$\frac{a}{b} : \frac{c}{d} \leftrightarrow [n, m] : [m, n] = [n, m]\cdot[q, p] = [n\cdot q, m\cdot p] \leftrightarrow \frac{a}{b} \cdot \frac{d}{c}$. Portanto, $\frac{a}{b} : \frac{c}{d} = \frac{a}{b} \cdot \frac{d}{c}$.

Na prática, isto significa que, dividir um número racional $\frac{a}{b}$ por outro racional, não nulo, $\frac{c}{d}$, basta "repetir racional $\frac{a}{b}$ e *multiplicá-lo* por $\frac{c}{d}$, porém, com os *termos invertidos*."

Em particular, dados $a, b, n \in \mathbb{Z}$, com $b, n \neq 0$, temos:

$$a : b = a : \frac{b}{1} = a \cdot \frac{1}{b} = \frac{a}{b}$$

e

$$\frac{a}{b} : n = \frac{a}{b} \cdot \frac{1}{n} = \frac{a}{b.n}.$$

Segundo FERREIRA (2013, p. 63): "É usual, nos textos elementares de matemática, adotar-se a notação $\frac{a/b}{c/d}$ para $\frac{a}{b} : \frac{c}{d}$."

Portanto, a existência de um inverso multiplicativo em $\mathbb{Q}$, que não existe em $\mathbb{Z} \setminus \{0, \pm 1\}$, é uma das características que os diferenciam.

Os números racionais têm as seguintes propriedades, para todo $r, s, t \in \mathbb{Q}$:

i*) *Comutativa: $r + s = s + r$ e $r\cdot s = s\cdot r$.

ii*) *Associativa: $(r + s) + t = r + (s + t)$ e $(r\cdot s)\cdot t = r\cdot(s\cdot t)$.

iii*) *Existência de um zero e de uma unidade: $0 \in \mathbb{Q}$ e $1 \in \mathbb{Q}$.

iv*) *Existência de inversos (aditivo e multiplicativo): dado $r \in \mathbb{Q}$, existem $-r$, $r^{-1} \in \mathbb{Q}$, tais que $r + (-r) = 0$ e $r\cdot r^{-1} = 1$.

v*) *Lei distributiva: $r\cdot(s + t) = r\cdot s + r\cdot t$.

Um sistema numérico, onde estão definidas as operações de adição e multiplicação com estas cinco propriedades (comutativa, associativa, existência de um zero e de uma unidade, existência de inversos – aditivo e multiplicativo – e a lei distributiva), chama-se *corpo*.

Assim, o conjunto dos números racionais $\mathbb{Q}$ é um corpo. Mas, o conjunto dos números inteiro $\mathbb{Z}$ não é um corpo, pois, para todo número inteiro, não vale a propriedade do inverso multiplicativo e, por consequência imediata, o conjunto dos números naturais também não é um corpo, porque não possui a propriedade de existência dos inversos (aditivo e multiplicativo).

Observações:

1) Todo número racional, não nulo, possui um único inverso multiplicativo.

2) No conjunto dos números inteiros, apenas 1 e –1 possuem inverso multiplicativo.

3) O zero não possui inverso multiplicativo.

8.2 Relação de Ordem e a Enumerabilidade em $\mathbb{Z}$ e $\mathbb{Q}$

8.2.1 Relação de Ordem

Segundo FERREIRA (2013, p. 58), a relação "$\leq$", em $\mathbb{Q}$, é definida por: dados os números racionais $\frac{a}{b}$ e $\frac{c}{d}$, com $b, d \neq 0$, dizemos que $\frac{a}{b}$ é "*menor do que ou igual a*" $\frac{c}{d}$ e escreve-se $\frac{a}{b} \leq \frac{c}{d}$, quando $a \cdot d \leq b \cdot c$.

Dessa forma, vale a seguinte propriedade:

Proposição 12. Sejam dois números racionais $\frac{a}{b}$ e $\frac{c}{d}$, com $b, d > 0$. Então, $\frac{a}{b} < \frac{c}{d}$ se, e somente se, $a \cdot d < b \cdot c$.

Demonstração: Observe que $\frac{a}{b} < \frac{c}{d}$ é equivalente a $a \cdot \frac{1}{b} < c \cdot \frac{1}{d}$. Isto significa que $\frac{1}{b}$ e $\frac{1}{d}$ são, respectivamente, os inversos multiplicativos de b e d, onde $b, d > 0$. Além disso, $b \cdot d > 0$. Portanto:

$$a \cdot \frac{1}{b} < c \cdot \frac{1}{d} \iff a \cdot \frac{1}{b} \cdot (b \cdot d) < c \cdot \frac{1}{d} \cdot (b \cdot d) \iff a \cdot d < b \cdot c.$$

□

Proposição 13. Sejam os números racionais positivos r e s. Se $r < s$, então $\frac{1}{s} > \frac{1}{r}$.

Demonstração: Sejam $[n, m] \leftrightarrow r$ e $[p, q] \leftrightarrow s$. Então, $[m, n] \leftrightarrow \frac{1}{r}$ e $[q, p] \leftrightarrow \frac{1}{s}$. Então:

$$r < s \leftrightarrow n/m < p/q \Leftrightarrow n \cdot q < m \cdot p \Leftrightarrow m \cdot p > n \cdot q \Leftrightarrow m/n > q/p \leftrightarrow \frac{1}{s} > \frac{1}{r}.$$

□

Isto significa que "quanto maior for um número racional positivo, menor será seu inverso." (LIMA, 2013, p. 72)

8.2.2.1 Propriedades da Relação de Ordem

Para todo $a, b, c, d \in \mathbb{Q}$, valem as seguintes propriedades:

i) se $a > b$, então $a + c > b + c$.

ii) se $a > b$ e $c > d$, então $a + c > b + d$.

iii) se $a > b$, então $a \cdot c > b \cdot c$, para $c > 0$ e $a \cdot c < b \cdot c$, para $c < 0$.

Demonstração: Em ***i)***, observe que $(a + c) - (b + c) = a - b$. Mas, $a > b$ implica $a - b > 0$. Então, $(a + c) - (b + c) = a - b > 0$. Logo, $a + c > b + c$.

Em ***ii)***, como $a > b$ e $c > d$, segue que $a - b > 0$ e $c - d > 0$. Assim:

$$(a + c) - (b + d) = (a - b) + (c - d) > 0 \text{ e, portanto, } a + c > b + d.$$

Em ***iii)*** Temos: $a > b$ e $c > 0$. Então, $a - b > 0$ e $c > 0$, isto é, $a \cdot c - b \cdot c = (a - b) \cdot c > 0$. Logo, $a \cdot c > b \cdot c$.

Por outro lado, se $c < 0$, temos: $a - b > 0$ e $c > 0$ e, portanto, $a \cdot c - b \cdot c = (a - b) \cdot c < 0$. Assim, $a \cdot c < b \cdot c$.

□

8.2.2 Enumerabilidade em $\mathbb{Z}$ e $\mathbb{Q}$

Conforme ÁVILA (2006, p. 34): "é surpreendente que o conjunto dos números naturais seja equivalente a vários de seus subconjuntos próprios (...)". Mais intrigante ainda, é o fato de

que o conjunto dos números racionais $\mathbb{Q}$ seja equivalente ao conjunto dos números naturais $\mathbb{N}$, isto é, $\mathbb{Q}$ seja enumerável.

Antes de abordarmos esta questão, mostraremos que o conjunto dos números inteiros $\mathbb{Z}$ é enumerável, isto é, existe uma bijeção de $\mathbb{N}$ em $\mathbb{Z}$.

Proposição 14. O conjunto dos números inteiros $\mathbb{Z}$ é enumerável.

Demonstração: De fato, considere o conjunto dos números inteiros a seguir:

$$\mathbb{Z} = \{0, \pm 1, \pm 2, \pm 3, \cdots, \pm n, \cdots\}.$$

Em vista das condições de partição de um conjunto, podemos reescrever o conjunto $\mathbb{Z}$ da forma:

$\mathbb{Z} = \{0, \pm 1, \pm 2, \pm 3, \cdots, \pm n, \cdots\} = \{0, \pm 2, \pm 4, \cdots, \pm 2\cdot n, \cdots\} \cup \{\pm 1, \pm 3, \cdots, \pm (2\cdot n - 1), \cdots\}$, para todo $n \in \mathbb{N}_0 = \{0, 1, 2, \cdots\}$. Isto cumpre as condições de partição de conjunto, pois, fazendo $P^{\pm} = \{0, \pm 2, \pm 4, \cdots, \pm 2\cdot n, \cdots\}$ e $I^{\pm} = \{\pm 1, \pm 3, \cdots, \pm (2\cdot n - 1), \cdots\}$, temos:

i) $P^{\pm} \cup I^{\pm} = \mathbb{Z}$; e

ii) $P^{\pm} \cap I^{\pm} = \varnothing$.

Agora, considere a função $\alpha : \mathbb{Z} \to \mathbb{N}_0$, definida por $\alpha(n) = -2\cdot n$, se $n \leq 0$ e $\alpha(n) = 2\cdot n - 1$, se $n > 0$. Então, α é uma bijeção e, portanto, possui inversa $\alpha^{-1} : \mathbb{N}_0 \to \mathbb{Z}$, definida por $\alpha^{-1}(n) = -\frac{n}{2}$, se n é *par* e $\alpha^{-1}(n) = \frac{n+1}{2}$, se n é *ímpar*. De fato:

$$\alpha(n) = -2\cdot n, \text{ s e } n \leq 0 \implies n = -2\cdot\alpha^{-1}(n) \implies \alpha^{-1}(n) = -\frac{n}{2}, \text{ se } n \text{ é } par$$

e

$$\alpha(n) = 2\cdot n - 1, \text{ se } n > 0 \implies 2\cdot\alpha^{-1}(n) - 1 = n \implies \alpha^{-1}(n) = \frac{n+1}{2}, \text{ se } n \text{ é } ímpar.$$

A função inversa α^{-1}, assim definida, enumera o conjunto $\mathbb{Z}$.

□

Proposição 15. O conjunto dos números racionais $\mathbb{Q}$ é enumerável.

Demonstração: Para justificar este fato, usaremos ideia apresentada no **Teorema 15**. Para tanto, é suficiente mostrar que o conjunto dos números racionais positivos $\mathbb{Q}^+$ é enumerável. De fato, considere todos os subconjuntos, cujos elementos são números racionais positivos, escritos na ordem crescente das somas constantes do numerador com o denominador, um após outro, conforme o esquema seguir:

$A_1 = \{ \frac{1}{1} \}$, com soma igual a $2 = 1 + 1$.

$A_2 = \{ \frac{1}{2}, \frac{2}{1} \}$, com soma igual a $3 = 1 + 2 = 2 + 1$.

$A_3 = \{ \frac{1}{3}, \frac{3}{1} \}$, com soma igual a $4 = 1 + 3 = 3 + 1$.

$A_4 = \{ \frac{1}{4}, \frac{2}{3}, \frac{3}{2}, \frac{4}{1} \}$, com soma igual a $5 = 1 + 4 = 2 + 3 = 3 + 2 = 4 + 1$.

$A_5 = \{ \frac{1}{5}, \frac{5}{1} \}$, com soma igual a $6 = 1 + 5 = 5 + 1$.

...

Note que cada $A_j \subset \mathbb{Q}^+$, onde $j \in \mathbb{N}$, é contável e a $\cup A_j = \mathbb{Q}^+$, logo, pelo **Teorema 15**, $\mathbb{Q}^+$ é enumerável.

□

Teorema 23. (Arquimediana) Sejam $a, b \in \mathbb{Q}$. Se $a > 0$, então, existe pelo menos um $n \in \mathbb{N}$, tal que $a \cdot n > b$.

Demonstração: De fato, por hipótese, $a > 0$. Logo, existe $n \in \mathbb{N}$, tal que $\frac{b}{a} < n$, para todo $b \in \mathbb{Q}$. Mas isto é equivalente a $b \cdot \frac{1}{a} < n$.

Note que $\frac{1}{a}$ é o inverso multiplicativo de a. Assim, $b \cdot \frac{1}{a} < n$ é equivalente a $\frac{b}{a} \cdot a < n \cdot a$. Pela **Lei do Corte**, obtemos: $b < a \cdot n$.

□

Corolário 7. Dado qualquer $a > 0$ em $\mathbb{Q}$, existe $n \in \mathbb{N}$, tal que $a \cdot n > 1$ ou $0 < \frac{1}{n} < a$.

Demonstração: Pelo **Teorema 23**, temos: $b < a \cdot n$. Assim, basta fazer $b = 1$, para obtermos o resultado.

□

9 Corpo Ordenado e Corpo Arquimediano

9.1 Corpo Ordenado

Dado um corpo K, chama-se *corpo ordenado* ao subconjunto K^+ do corpo K, o qual cumpre as seguintes condições:

i) K^+ é fechado para as operações de adição e multiplicação, isto é, para todo $a, b \in K^+$ implica $a + b \in K^+$ e $a \cdot b \in K^+$.

ii) Dado $a \in K^+$ uma, e somente uma, das três possibilidades podem ocorrer: ou $a = 0$ ou $a \in K^+$ ou $-a \in K^+$.

Denotando-se por K^- o conjunto dos elementos $-a$, onde $a \in K^+$, o corpo K pode ser escrito da forma:

$$K = K^- \cup \{0\} \cup K^+,$$

onde K^-, $\{0\}$ e K^+ são disjuntos dois a dois. Os elementos do conjunto K^- chamam-se *negativos*.

Proposição 16. Em todo corpo ordenado K, se $a \in K^+$, com $a \neq 0$ e $K^+ \subset K$, então $a^2 \in K^+$.

Demonstração: Como $a \in K^+$ e $a \neq 0$, então, pelo item ***ii)*** da definição de corpo ordenado, só restam duas possibilidades: ou $a \in K^+$ ou $-a \in K^+$.

- se $a \in K^+$, temos: $a^2 = a \cdot a$. Logo, pelo item ***i)*** da definição de corpos ordenado, segue que $a^2 \in K^+$.

- se $-a \in K^+$, temos $a^2 = (-a) \cdot (-a)$ e, por conseguinte, $a^2 \in K^+$.

Observação:

Num corpo ordenado K, não existe $a \in K^+$, com $K^+ \subset K$, tal que $a^2 = -1$. Em outras palavras, -1 não é quadrado de nenhum elemento.

Ainda, segundo o autor, num *corpo ordenado*, para dizer que a é *menor do que* b, escreve-se $a < b$ e isto significa que $b - a \in K^+$, isto é, $b - a = c > 0$. Em outras palavras, se $a < b$, então existe um único $c \in K^+$, tal que $b = a + c$. A unicidade se justifica devido a operação de adição ser bem definida.

De modo análogo, diz-se que a é *maior do que* b, e escreve-se $a > b$, para significar que existe $c \in K^+$, tal que $a = b + c$.

Num corpo ordenado K, além das propriedades que valem para a relação de ordem $a < b$ no conjunto dos números racionais $\mathbb{Q}$, valem também as propriedades de *transitividade* (dados $a, b \in K$, se $a < b$ e $b < c$, então $a < c$) e *tricotomia* (dados $a, b \in K$, então uma, e só uma, das opções ocorre: ou $a < b$ ou $a = b$ ou $a > b$).

Do exposto, $\mathbb{Q}$ é um subconjunto de corpo ordenado K. Mais ainda, podemos dizer que o conjunto dos números racionais $\mathbb{Q}$ é um *corpo ordenado*, pois é possível formar um subconjunto K^+ de $\mathbb{Q}$, cujos elementos são números racionais a/b, com $a \cdot b \in \mathbb{N} = \{1, 2, 3, \cdots\}$.

Depreende-se que o conjunto dos números racionais $\mathbb{Q}$ tem as propriedades de relação de ordem, é arquimediano e enumerável e, sobretudo, é um *corpo ordenado*.

9.2 Corpo Arquimediano

FERREIRA (2013, p. 31, 63 e 65) adverte que o Princípio da Boa Ordenação – *todo subconjunto, não vazio, de número naturais possui um menor elemento* – não se verifica no conjunto dos números racionais $\mathbb{Q}$, pois existem subconjuntos não vazios no conjunto dos números racionais que são limitados inferiormente, mas não possuem um menor elemento. De fato, por exemplo, considere o subconjunto $R^+ \subset \mathbb{Q}$ formado pelos números racionais positivos a seguir:

$$R^+ = \{1/n \, ; \, n \in n \in \mathbb{N}\}.$$

Então, fazendo n percorrer $\mathbb{N} = \{1, 2, 3, \cdots\}$, obtemos a sequência decrescente de números racionais positivos:

$$\frac{1}{1}, \frac{1}{2}, \frac{1}{3}, \frac{1}{4}, \cdots, \frac{1}{n}, \cdots$$

Esta sequência não possui um elemento mínimo e, portanto, o conjunto R^+ não tem um menor elemento. Assim, o conjunto $\mathbb{Q}$ *não é bem ordenado*, embora seja um *corpo ordenado*.

Ainda, segundo o autor, "os corpos ordenados para os quais sua cópia de números naturais é ilimitada superiormente chamam-se *corpos arquimedianos*."

Teorema 24. Em um corpo ordenado $K - \{0\}$, as seguintes afirmações são equivalentes:
i) K é arquimediano;
ii) para todo $a, b \in K$, se $a > 0$, existe pelo menos um $n \in \mathbb{N}$, tal que $a \cdot n > b$;
iii) qualquer que seja $a \in K$, se $a > 0$, existe pelo menos um $n \in \mathbb{N}$, tal que $0 < 1/n < a$.

Demonstração: ***i)*** $\Longrightarrow$ ***ii)*** Como K é arquimediano, então, K é ilimitado superiormente. Dessa forma, para todo $a, b \in K$, com $a > 0$, existe $n \in \mathbb{N}$, tal que $\frac{b}{a} < n$ e, portanto, $a \cdot n > b$.

ii) $\Longrightarrow$ ***iii)*** Para todo $a, b \in K$, com $a > 0$, existe $n \in \mathbb{N}$, tal que $a \cdot n > b$. Fazendo $b = 1$, temos: $a \cdot n > 1$ ou $1/n < a$. Como $n \in \mathbb{N} = \{1, 2, 3, \cdots\}$, segue que $n > 0$ e, portanto, $0 < 1/n$. Assim, $0 < 1/n < a$.

iii) $\Longrightarrow$ ***i)*** Qualquer que seja $a \in K$, com $a > 0$, existe, por ***iii)***, um $n \in \mathbb{N}$, tal que $0 < 1/n < 1/a$, logo, $a < n \in \mathbb{N} = \{1, 2, 3, \cdots\}$. Portanto, K é arquimediano.

□

Segundo LIMA (2010, p. 75), para que um corpo ordenado K seja *arquimediano* é suficiente que satisfaça qualquer uma das condições deste **Teorema 24**. Então, o corpo ordenado do conjunto dos números racionais $\mathbb{Q}$ é *arquimediano*, pois, ele possui a condição ***ii)*** deste teorema, basta ver o **Teorema 23**.

Exemplo 53. (PROFMAT/2014 - adaptado) Seja o conjunto dos números racionais *diádicos* $D = \{ \frac{m}{2^n} ; m, n \in I^+, \text{com } n \geq 1\}$. Mostre que dados $a, b \in K - \{0\}$, corpo ordenado, com $a < b$, existe $d \in D$, tal que $a < d < b$.

Resolução: Temos: $a < b$ implica $b - a > 0$. Assim, pelo item ***iii)*** do **Teorema 24**, existe pelo menos um $n \in I^+$, tal que $0 < \frac{1}{2^n} < b - a$, portanto, $1 < 2^n \cdot b - 2^n \cdot a$. Consequentemente, existe

pelo menos um $m \in I^+$, tal que $2^n \cdot a < m < 2^n \cdot b$ e, por conseguinte, $a < \frac{m}{2^n} < b$. Fazendo $d = \frac{m}{2^n}$, conclui-se que existe $d \in D$, tal que $a < d < b$.

Exemplo 54. (Desigualdade de *Bernoulli*[25]) Seja um corpo ordenado qualquer K. Se $a > -1$, então, para todo $n \in \mathbb{N}$ vale a desigualdade:

$$(1 + a)^n \geq 1 + a \cdot n.$$

Demonstração: Seja a proposição:

$$P(n) : (1 + a)^n \geq 1 + a \cdot n, \text{ com } a > -1 \text{ e } n \in \mathbb{N}.$$

Então, por indução sobre n, temos:

i) Para $n = 1$, a proposição $P(1) : (1 + a)^1 = 1 + a \geq 1 + a \cdot 1$ é verdadeira.

ii) Suponha, por hipótese de indução, que a proposição seja verdadeira para algum $n \in \mathbb{N}$. Vamos demonstrar que $P(n)$ implica $P(n + 1)$. De fato, temos:

$$(1 + a)^{n+1} = (1 + a)^n \cdot (1 + a).$$

Mas, por hipótese de indução, $(1 + a)^n \geq 1 + a \cdot n$, além disso, $a > -1$ ou $1 + a > 0$, logo:

$$\begin{aligned}(1 + a)^{n+1} = (1 + a)^n \cdot (1 + a) &\geq (1 + a \cdot n) \cdot (1 + a) \\ &= (1 + a) + a \cdot n \cdot (1 + a) \\ &= 1 + a + a \cdot n + a^2 \cdot n \\ &= 1 + a \cdot (1 + n) + a^2 \cdot n.\end{aligned}$$

Como a parcela $a^2 \cdot n$ é sempre um número positivo, segue que:

$$(1 + a)^{n+1} \geq 1 + a \cdot (1 + n) + a^2 \cdot n \geq 1 + a \cdot (1 + n).$$

Então, pelo Princípio de Indução Finita, a proposição é verdadeira, para todo $n \in \mathbb{N}$.

□

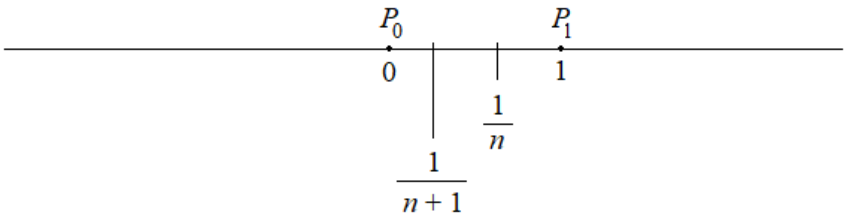
[25] *Jacques Bernoulli* (1654 – 1705), ilustre matemático suíço que dedicou seus estudos sobre as séries infinitas. Em 1689, publicou um artigo sobre este assunto, no qual apresentou a desigualdade binomial, hoje conhecida por "*desigualdade de Bernoulli*". (BOYER, 1996, p. 287, grifos nossos)

9.3 Densidade de um Conjunto

Do ponto de vista geométrico, segundo GUEDES (1996, p. 4), os números racionais podem ser associados aos pontos de uma reta, onde se fixam dois pontos: P_0, para corresponder ao *zero*; e P_1, para corresponder ao *um*, de modo que o segmento P_0P_1 representa a unidade.

Dessa forma, "os números racionais são obtidos por subdivisões adequadas do segmento unidade", conforme a FIGURA 19, onde $n \in \mathbb{N}$.

FIGURA 19 – Representação dos números racionais por subdivisão da unidade na reta.



FONTE: elaborada pelo autor.

Observe que o número racional $1/n$ é maior do que $1/(n+1)$, pois, pela **Proposição 12**, temos: $n < n+1$ implica $1/n > 1/(n+1)$, para todo $n \in \mathbb{N}$.

Ainda, segundo o autor: "dado um ponto qualquer da reta, podemos obter racionais tão perto dele quanto se queria; basta tomar *subdivisões* cada vez *mais finas* da unidade." (grifos nossos) Isto motiva definir *densidade* de um conjunto.

Definição 44 (Densidade). Um conjunto X chama-se *denso* quando, entre dois de seus elementos quaisquer, existe uma infinidade de elementos de X.

Dessa forma, é imediato que o conjunto dos números naturais $\mathbb{N}$ e dos inteiros $\mathbb{Z}$ não são densos. Para justificar isto, basta ver **Proposição 2**.

Proposição 17. O conjunto dos números racionais $\mathbb{Q}$ é denso.

Demonstração: De fato, sejam os números racionais r e s, com $r < s$. Então, decorre do item ***i)*** da propriedade de relação de ordem que: $r < s \implies r + a < s + a$.

Fazendo $a = r$, temos:

$$r + r < s + r \implies 2 \cdot r < r + s \implies r < (r + s)/2.$$

Analogamente, fazendo $a = s$, segue que:

$$r + s < s + s \implies r + s < 2 \cdot s \implies (r + s)/2 < s.$$

Portanto, $r < (r + s)/2 < s$. Definindo $x = (r + s)/2$, temos $r < x < s$. Assim, mostramos que existe racional entre dois racionais.

Note que este racional foi obtido pela média aritmética entre os racionais r e s. Para demonstrar que existe uma infinidade desses racionais, basta proceder do mesmo modo, isto é:

$$x_1 = \frac{r+s}{2}.$$

$$x_2 = \frac{r+x_1}{2} = \frac{r+\frac{r+s}{2}}{2} = \frac{3 \cdot r+s}{4}.$$

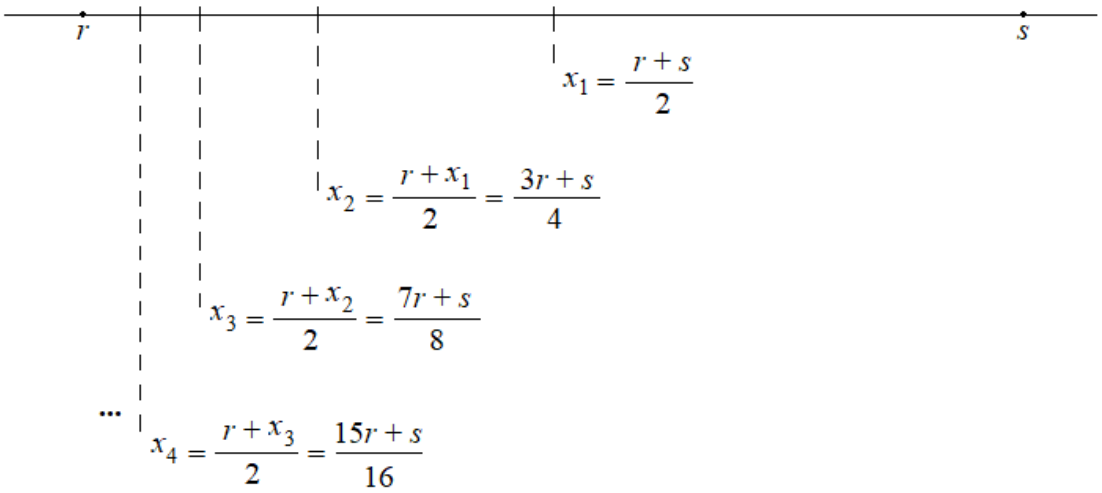
$$x_3 = \frac{r+x_2}{2} = \frac{r+\frac{3 \cdot r+s}{4}}{2} = \frac{7 \cdot r+s}{8}.$$

$$x_4 = \frac{r+x_3}{2} = \frac{r+\frac{7 \cdot r+s}{8}}{2} = \frac{15 \cdot r+s}{16}.$$

$$\vdots$$

Isto pode ser ilustrado pela A FIGURA 20 a seguir.

FIGURA 20 – Uma infinidade de números racionais entre r e s, com $r < s$.



FONTE: elaborada pelo autor.

Continuando este procedimento, obtemos uma sequência decrescente $(x_n) = (x_1, x_2, x_3, x_4, \cdots)$, com uma infinidade de elementos, cujo temo geral é:

$$x_n = \frac{(2^n - 1)\cdot r + s}{2^n}, \text{ onde } n \geq 1.$$

De fato, por indução em n, temos: para $n = 1$,

$$x_1 = \frac{(2^1 - 1)\cdot r + s}{2^1} = \frac{r+s}{2}.$$

Agora, suponha que, para algum $n \in \mathbb{N}$, seja verdade. Demonstraremos que vale também para $n + 1$. Com efeito:

$$x_{n+1} = \frac{r + x_n}{2} = \frac{r + \frac{(2^n - 1)\cdot r + s}{2^n}}{2} = \frac{2^n \cdot r + (2^n - 1)\cdot r + s}{2^n . 2} = \frac{(2^n + 2^n - 1)\cdot r + s}{2^{n+1}} = \frac{(2^{n+1} - 1)\cdot r + s}{2^{n+1}}.$$

Assim, pelo Princípio de Indução Finita, $x_n = \frac{(2^n - 1)\cdot r + s}{2^n}$, para todo $n \geq 1$ natural.

□

9.4 Um Óbice em $\mathbb{Q}$ na Reta

Diante da propriedade de densidade dos números racionais, pensava-se que eles cobriam (ou preenchiam completamente) a reta, pois, "as frações racionais são tão densas que entre duas quaisquer delas, por mais próximas que estejam, há sempre outra." (BOYER, 1996, p. 393) No entanto, Georg Cantor mostrou que isto não é verdade. Por exemplo, é possível estabelecer uma correspondência bijetiva entre o conjunto dos números naturais e o conjunto das frações apresentadas na **Proposição 14**.

A propriedade de densidade, segundo CARAÇA (1989, p. 57), "(...) depende apenas do caráter *infinito* do conjunto (...)".

Dessa forma, para cada número racional existe um ponto sobre uma reta. Em outras palavras, existe uma função de $\mathbb{Q}$ em P, onde P é o conjunto de pontos da reta, que é *injetiva*. Com efeito, sabemos que dados dois números racionais $r < s$, existe uma sequência decrescente $(x_n) = (x_1, x_2, x_3, x_4, \cdots)$, com uma infinidade de elementos, cujo temo geral é o número racional:

$$x_n = \frac{(2^n - 1)\cdot r + s}{2^n}, \text{ onde } n \geq 1.$$

Assim, considere a função $\alpha : \mathbb{Q} \to P$, onde P é o conjunto de pontos da reta, definida por $\alpha(x_n) = P_n$, tal que $P_n \in P$, onde $n \in \mathbb{N}$. Então, para todo $i, j \in \mathbb{N}$, temos:

$$x_i \neq x_j \implies \frac{(2^i-1)\cdot r+s}{2^i} \neq \frac{(2^j-1)\cdot r+s}{2^j} \implies$$

$$r\cdot 2^{i+j} - r\cdot 2^j + s\cdot 2^j \neq r\cdot 2^{i+j} - r\cdot 2^i + s\cdot 2^i \implies (s-r)\cdot 2^j \neq (s-r)\cdot 2^i.$$

Mas, por hipótese, $r < s$, isto é, $0 < s - r$, de modo que, pela Lei do Corte, segue:

$$(s-r)\cdot 2^j \neq (s-r)\cdot 2^i \implies 2^j \neq 2^i \implies j \neq i \implies P_i \neq P_j \implies \alpha(x_i) \neq \alpha(x_j).$$

Portanto, a função $\alpha : \mathbb{Q} \to P$ é injetiva.

Agora, resta saber se esta função é sobrejetiva. Em caso afirmativo, os números racionais preencherão toda a reta. Mas, do contrário, existirá pelo menos um ponto da reta que, pela função α, não corresponderá a nenhum número racional. Neste caso, surge a pergunta: a que número, então, tal ponto estará associado pela função α?

Para responder esta indagação, será necessário ampliar o conjunto $\mathbb{Q}$, de modo a incluir estes números "estranhos" ao conjunto dos racionais e, portanto, formar um "novo" conjunto mais amplo do que o conjunto $\mathbb{Q}$, com a propriedade de ser um corpo ordenado *completo*.

10 Conjunto dos Números Reais

10.1 Um Óbice Aritmético-Geométrico: a incomensurabilidade na reta

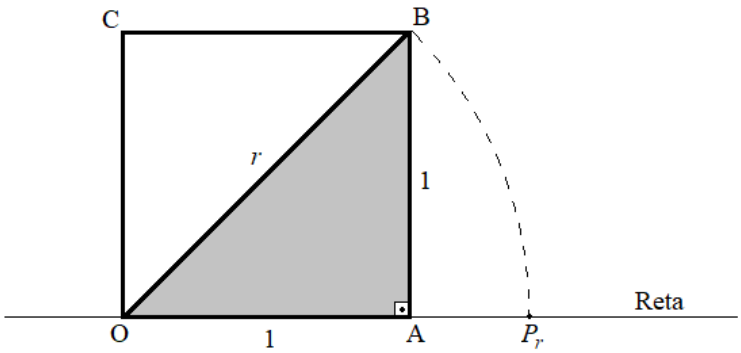
O problema que abalou os pitagóricos[26] foi a descoberta da incomensurabilidade – atribuída por alguns a Hipasus de Metaponto (ou Crotona) durante o fim de 500 a.C. – na qual a medida da diagonal um quadrado, com seu lado, não pode ser expresso por uma unidade de medida comum, por menor que seja esta unidade. Em outras palavras, a divisão entre a mediada da diagonal e do lado de um quadrado não é um número racional. (BOYER, 1996, p. 49 e 50)

Segundo CARAÇA (1989, p. 75):

> o caráter de seita da escola pitagórica, em que os aspectos místico e político (...) ombreavam com o aspecto científico, prestava-se a essa tentativa de segredo à volta de questão de tal maneira embaraçosa, onde só havia a ganhar com o debate público e extenso; os pitagóricos instituíram como norma, pelo contrário, o segredo, o silêncio.

A demonstração mais antiga deste óbice geométrico baseia-se em considerar, sem perda de generalidade, um quadrado OABC de lado OA = 1, sobre uma reta, e a diagonal OB = *r*, conforme a FIGURA 21 a seguir.

FIGURA 21 – Quadrado OABC de lado 1 e diagonal *r*.



FONTE: elaborada pelo autor.

[26] Os pitagóricos eram os discípulos de Pitágoras (580 – 600 a.C. aproximadamente) – profeta e místico que fundou em Crotona (hoje, costa sudeste da Itália) uma sociedade secreta: a Escola Pitagórica. Nesta instituição de ensino e conhecimentos, o lema era: "Tudo é número". (BOYER, 1996, p. 33)

Dessa forma, $r \notin \mathbb{Q}$. Com efeito, P_r é um ponto de interseção do arco de circunferência de raio OP_r com a reta. Assim, deve existir um número racional r = OB, tal que P_r esteja associado a r.

Aplicando o Teorema de Pitágoras no triangulo retângulo OAB, obtemos:

$$r^2 = 1^2 + 1^2 \iff r^2 = 2.$$

Isto significa que existem $m, n \in I^+$, *irredutíveis*, tais que $r = \frac{m}{n}$, ou seja:

$$\left(\frac{m}{n}\right)^2 = 2 \iff m^2 = 2 \cdot n^2.$$

Agora, observe que m^2 é um número par, logo, m é par. De fato, suponha, por absurdo, que m seja um número ímpar, isto é, $m = 2 \cdot p + 1$. Então:

$$m^2 = (2 \cdot p + 1)^2 = 4 \cdot p^2 + 2 \cdot p + 1 = 2 \cdot (2 \cdot p^2 + p) + 1 = 2 \cdot q + 1, \text{ onde } q = 2 \cdot p^2 + p.$$

Assim, m^2 é ímpar, mas isto é um absurdo! Pois, por hipótese, m^2 é um número par. Portanto, m é par e podemos escrever $m = 2 \cdot k$.

Como $m^2 = 2 \cdot n^2$, temos $2 \cdot n^2 = (2 \cdot k)^2 = 4 \cdot k^2$ implica $n^2 = 2 \cdot k^2$. Daí, pelo mesmo motivo, n^2 sendo par implica n par.

Portanto, m e n são números pares e, portanto, ambos divisíveis, o que é um absurdo! Pois, $m, n \in I^+$ são irredutíveis. Logo, não existe um número racional r cujo quadrado seja igual a 2.

Segundo CARAÇA (1989, p. 54), esta constatação mostra que os dois segmentos de reta – o lado e a diagonal do quadrado – não têm medida comum. Sempre que isto acontecer, diz-se que estes segmentos são *incomensuráveis*.

Ainda, segundo o autor, trata-se de uma "*insuficiência geral* do campo numérico racional para traduzir as relações geométricas (...)".

Do ponto de vista de função, isto significa existe número racional que corresponde a um ponto da reta, mas nem todo ponto da reta corresponde a um número racional. Em outras

palavras, a função $\alpha : \mathbb{Q} \rightarrow P$, onde P é o conjunto dos pontos de uma reta, é injetiva, mas não é sobrejetiva, ou seja, não é bijetiva.

Nesse sentido, a existência da *incomensurabilidade* revela a insuficiência dos números racionais.

10.2 A Natureza da Partição da Reta e a Incomensurabilidade

Desde a época de Hipasus e Pitágoras da Magna Grécia, o problema da incomensurabilidade perdurou há séculos e muitos matemáticos dedicaram esforços na tentativa de resolvê-lo, como por exemplo:

> Galileu e Leibniz tinham julgado que a 'continuidade' de dois pontos sobre uma reta era consequência de sua densidade – isto é, o fato que entre dois pontos quaisquer existe sempre um terceiro. Porém, os números racionais têm essa propriedade, no entanto não formam um *contínuum*. (BOYRE, 1996, p. 390)

Segundo FERREIRA (2013, p. 67), Georg Cantor, já citado em outras contribuições à matemática, e Dedekind[27] (1831 – 1916) construíram, a partir dos números racionais e por métodos distintos, o conceito de incomensurabilidade dando origem a um novo conjunto, isto é, uma extensão do conjunto dos números racionais.

Ainda, segundo o autor, Georg Cantor baseou-se nas Classes de Equivalências de Sequências de Cauchy e Dedekind inspirou-se na Teoria das Proporções de Eudoxo criando o conceito de corte. Neste estudo, optaremos pelo método de Dedekind.

Em 1859, Dedekind perguntou:

> "O que há na grandeza geométrica contínua que a distingue dos números racionais." (BOYRE, 1996, p. 390)

Para resolver o problema da incompletude dos números racionais em relação à reta, ele percebeu que o conjunto dos números racionais "podia ser estendido de modo a formar um *continuum* de números reais". Mais ainda, concluiu que:

[27] Julius Wilhelm Richard Dedekind, um dos eminentes matemáticos alemães do séc. XIX que formalizou o conceito de número real com sua Teoria de Corte. (BOYER, 1996, p. 390)

> a essência da continuidade de um segmento de reta não se deve a uma vaga propriedade de ligação mútua, mas a uma propriedade exatamente oposta – a natureza da divisão do segmento em duas partes por meio de um ponto sobre o segmento. Em qualquer divisão dos pontos de um segmento em duas classes, tais que cada ponto pertence a uma e somente uma, e tal que todo ponto numa classe está à esquerda de todo ponto da outra, existe um e um só ponto que realiza a divisão. (...) Por essa observação trivial o segredo da continuidade será revelado. (BOYER, 1996, p. 390).

10.3 Cota Inferior e Ínfimo, Cota Superior e Supremo

Segundo ÁVILA (2006, p. 62 – 64), um subconjunto C de um corpo ordenado K chama-se *limitado inferiormente* quando existe $k \in K$, tal que $k \leq c$, para todo $c \in C$. Se isto acontecer, cada $k \in K$ com esta propriedade chama-se *cota inferior* de C.

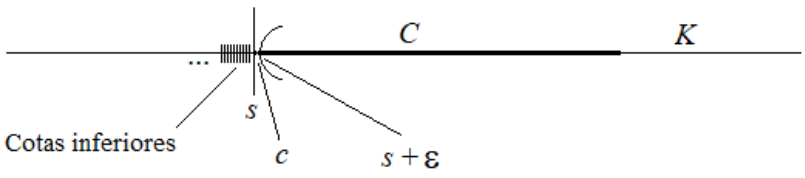
Definição 45. Chama-se *ínfimo* (*caso exista*) de C a maior das cotas inferiores. Para que um número s seja o ínfimo de um conjunto C é necessário e suficiente que satisfaça as duas condições a seguir:

i) $s \leq c$, para todo $c \in C$;

ii) dado qualquer $\varepsilon > 0$, existe $c \in C$, tal que $c - \varepsilon < s$ (ou $c < s + \varepsilon$).

Note que o *ínfimo* (*quando existe*) de um conjunto pode ou não pertencer a este conjunto. A limitação inferior de um conjunto C contido no corpo ordenado K assim como as cotas interiores e o ínfimo estão ilustrados pela FIGURA 22 a seguir.

FIGURA 22 – Cotas inferiores e ínfimo de um conjunto C contido num corpo ordenado K.



FONTE: elaborada pelo autor.

Nesta figura, observe que as cotas inferiores formam um conjunto de aproximações, por falta, do ínfimo s, de modo que satisfaça as propriedades ***i)*** e ***ii)*** do ínfimo de um conjunto.

De modo semelhante, um subconjunto C de um corpo ordenado K chama-se *limitado superiormente* quando existe $k \in K$, tal que $c \leq k$, para todo $c \in C$. Neste caso, cada $k \in K$ com esta propriedade chama-se *cota superior* de C.

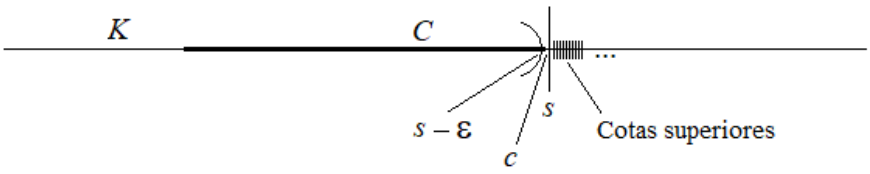
Definição 46. Chama-se *supremo* (*caso exista*) de C a menor das cotas superiores. Para que um número s seja o supremo de um conjunto C é necessário e suficiente que satisfaça as duas condições a seguir:

i) $c \leq s$, para todo $c \in C$;

ii) dado qualquer $\varepsilon > 0$, existe $c \in C$, tal que $s - \varepsilon < c$ (ou $s < c + \varepsilon$).

Observe que o *supremo* (*quando existe*) de um conjunto pode ou não pertencer a este conjunto. A limitação superior do conjunto C contido no corpo ordenado K assim como as cotas superiores e o supremo estão ilustrados pela FIGURA 23 a seguir.

FIGURA 23 – Cotas superiores e o supremo de um conjunto C contido num corpo ordenado K.



FONTE: elaborada pelo autor.

Nesta ilustração, note que as cotas superiores formam um conjunto de aproximações, por excesso, do supremo s, tal que satisfaça as propriedades ***i)*** e ***ii)*** do supremo de um conjunto.

Exemplo 55. Considere o corpo ordenado de números racionais $\mathbb{Q}$. Seja o conjunto $X \subset \mathbb{Q}$, tal que $X = \{x\ ;\ a < x \leq b\}$. Prove que o ínfimo de X é a e o supremo de X é b.

Resolução: O ínfimo de X é a. De fato: *i)* Como $a < x$, segue que a é cota inferior de X.

ii) Seja c uma cota inferior X. Para que a seja o ínfimo de X, não pode ocorrer $a < c$. Com efeito, caso isto aconteça, pela propriedade de densidade, existe $d \in X$, tal que $a < d < c$. Basta tomar $d = (a + c)/2$.

Assim, $d \leq c$. Logo, c não é cota inferior de X, o que é um absurdo! Então, $c \leq a$ e, portanto, a é o ínfimo de X. Note que o ínfimo de X *não pertence* a X.

O supremo de X é b. Com efeito: *i)* $x \leq b$ implica b é cota superior de X.

ii) Seja s uma cota superior de X. Para que b seja o supremo de X, não pode ocorrer $s < b$, pois, caso isto aconteça, segue, pela propriedade de densidade, que existe $d \in X$, tal que $s < d < b$. É suficiente tomar $d = (s + b)/2$.

Dessa forma, $d \leq b$. Logo, d não é cota superior de X, o que é uma contradição. Assim, $b \leq s$ e, portanto, b é o supremo de X. Observe que o supremo de X é também elemento de X.

Exemplo 56. Considere o corpo ordenado de números racionais $\mathbb{Q}$. Mostre que o subconjunto $C = \{\frac{n}{n+1}\,;\, n \in \mathbb{N}\}$ de $\mathbb{Q}$ tem supremo igual a 1.

Resolução: i) Temos: $n \in \mathbb{N}$ implica $n + 1 \in \mathbb{N}$. Como $n < n + 1$, segue que $\frac{n}{n+1} < 1$, para todo $n \in \mathbb{N}$. Logo, 1 é cota superior de C. Observe que $1 \notin C$.

ii) Agora, precisamos mostrar que 1 é a menor das cotas superiores do conjunto C. Inicialmente, note que, para $n = 1$, temos $\frac{n}{n+1} = \frac{1}{1+1} = 1/2$. Então, suponha que exista um número $\varepsilon \in \mathbb{Q}$, tal que $1/2 < \varepsilon < 1$. Assim, $1 - \varepsilon > 0$.

Como $\mathbb{Q}$ é arquimediano, existe $n \in \mathbb{N}$ tal que $n\cdot(1 - \varepsilon) > \varepsilon$ que é equivalente a $\varepsilon < n/(n + 1)$ e, portanto, $\varepsilon < n/(n + 1) < 1$, para todo $n \in \mathbb{N}$. Assim, nenhum número racional $\varepsilon < 1$ é cota superior de C. Portanto, 1 é o supremo de C.

Exemplo 57. Seja o conjunto $D = \{\frac{1}{2^n}\,;\, n \in \mathbb{N}\} \subset \mathbb{Q}$. Prove que o ínfimo de D é zero.

Resolução: i) Observe que, para todo $n \in \mathbb{N}$, $0 < \frac{1}{2^n}$. Logo, 0 é cota inferior de D. Além disso, note que $0 \notin D$.

ii) Agora, mostraremos que 0 é a maior das cotas inferiores de D. Em outras palavras, nenhum $c > 0$ é cota inferior de D. De fato, sabemos que o conjunto dos números racionais

$\mathbb{Q}$ é arquimediano. Como $D \subset \mathbb{Q}$, segue que o conjunto D é também arquimediano, logo, para todo $c > 0$, existe $n \in \mathbb{N}$, tal que:

$$\frac{1}{n} < c \iff \frac{1}{c} < n \iff \frac{1}{c} < 1 + n.$$

Pela desigualdade de Bernoulli, temos:

$$1 + n \leq (1 + 1)^n = 2^n.$$

Assim, $\frac{1}{c} < 1 + n \leq (1 + 1)^n = 2^n$, ou seja, $\frac{1}{c} < 2^n$ e, portanto, $\frac{1}{2^n} < c$. Dessa forma, nenhum $c > 0$ é cota inferior do conjunto D. Então, 0 é o ínfimo de D.

Utilizaremos esta mesma ideia para resolver o exemplo a seguir.

Exemplo 58. Mostre que o ínfimo do conjunto $X = \{ \frac{1}{n} ; n \in \mathbb{N}\}$ é zero.

Resolução: i) Temos: $0 < \frac{1}{n}$, para todo $n \in \mathbb{N}$. Assim, 0 é cota inferior de X. Além disso, note que $0 \notin X$.

ii) 0 é a maior das cotas inferiores de X, ou seja, nenhum $x > 0$ é cota inferior de X. De fato, o conjunto dos números racionais $\mathbb{Q}$ é arquimediano e, como $X \subset \mathbb{Q}$, segue que X é também arquimediano. Assim, pela propriedade arquimediana, para todo $x > 0$, existe $n \in \mathbb{N}$, tal que:

$$n \cdot x > 1 \iff 0 < \frac{1}{n} < x.$$

Dessa forma, nenhum $x > 0$ é cota inferior do conjunto X. Então, o ínfimo de X é zero.

Quando o ínfimo (resp. supremo) pertencer ao conjunto será chamado de mínimo (resp. máximo).

Observações:
1) Em geral, o ínfimo ou o supremo de um conjunto pode ou não pertencer ao conjunto.
2) O ínfimo de um conjunto, quando existe, é único. Da mesma forma para o supremo.
3) Se o conjunto é $\varnothing$, então, não possui ínfimo nem supremo, pois, não existe menor elemento nem maior.

10.4 Corte de Dedekind

Para LIMA (2010, p. 78), a incompletude dos racionais para formar o *contínuum* deve-se ao fato de que "alguns conjuntos limitados de números racionais não possuem supremo (ou ínfimo)." De fato, vimos que não existe um número racional r, tal que $r^2 = 2$. Então, considere os conjuntos E e D limitados por números racionais contidos num corpo ordenado K:

$$E = \{r \in \mathbb{Q} \,;\, r^2 < 2, \text{ com } r > 0\} \quad \text{e} \quad D = \{r \in \mathbb{Q} \,;\, r^2 > 2, \text{ com } r > 0\}.$$

Mostraremos que o conjunto E não tem máximo e o conjunto D não tem mínimo em $\mathbb{Q}$.

De fato, no primeiro caso (E não tem máximo em $\mathbb{Q}$), suponha que existe um número racional positivo s, tal que $s > r$. Vamos mostrar que, mesmo assim, teremos $s^2 < 2$.

Em outras palavras, o conjunto E não tem máximo se, para todo $r \in \mathbb{Q}$, é possível encontrar $q \in \mathbb{Q}$, de modo que $(r + q)^2 < 2$.

Como $s > r$, seja $s = r + q$. Sem perda de generalidade, pode-se considerar $q = 1/n$ uma quantidade bem pequena o quanto se queira, tomando n bem grande, onde $n \in \mathbb{N}$. Dessa forma, $s = r + 1/n$. Logo:

$$s^2 < 2 \iff (r + 1/n)^2 < 2 \iff r^2 + 2{\cdot}r/n + 1/n^2 < 2 \iff (2{\cdot}r + 1/n)1/n < 2 - r^2.$$

Majorando o termo $(2r + 1/n)1/n$, obtemos:

$$(2{\cdot}r + 1/n)1/n \leq (2{\cdot}r + 1)1/n.$$

Logo, $(2{\cdot}r + 1)1/n < 2 - r^2 \iff n > (2{\cdot}r + 1)/(2 - r^2)$. Portanto, tomando n nestas condições, obtemos $s^2 < 2$. Desta forma, o conjunto E não possui elemento máximo. Em outras palavras, o conjunto E não admite supremo em $\mathbb{Q} \subset K$.

Analogamente, no segundo caso (D não tem mínimo em $\mathbb{Q}$), suponha que existe um número racional positivo s, tal que $r > s$. Então, $r = s + 1/n$ ou $s = r - 1/n$. Assim:

$$s^2 = (r - 1/n)^2 = r^2 - 2{\cdot}r/n + 1/n^2.$$

Minorando o termo $r^2 - 2{\cdot}r/n + 1/n^2$, obtemos:

$$r^2 - 2{\cdot}r/n + 1/n^2 > r^2 - 2{\cdot}r/n.$$

Logo, $r^2 - 2 \cdot r/n > 2 \iff n > 2 \cdot r/(r^2 - 2)$. Assim, tomando n nessas condições, tem-se $s^2 > 2$. Portanto, o conjunto D não possui elemento mínimo. Isto significa que o conjunto D não possui ínfimo em $\mathbb{Q} \subset K$.

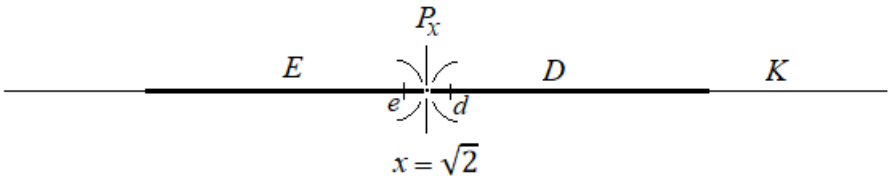
Agora, considere o *corpo ordenado* $\mathbb{Q} \subset K$. Seja um ponto P_x sobre uma reta associado a $x \in K$, tal que $x^2 = 2$. Suponha que P_x realize uma partição $\{E, D\}$ dessa reta, onde $E = \{r \in \mathbb{Q} \,;\, r^2 < 2, \text{ com } r > 0\}$ e $D = \{r \in \mathbb{Q} \,;\, r^2 > 2, \text{ com } r > 0\}$, sob as duas condições:

- nenhum ponto está fora desta partição $\{E, D\}$; e
- todo elemento $e \in E$ está à esquerda de todo elemento $d \in D$ e, reciprocamente, todo elemento $d \in D$ está à direita de todo elemento $e \in E$.

Definindo $x^2 = 2$ se, e somente se, $x = \sqrt{2}$, temos: $x = \sqrt{2} \notin E$ e D.

Nesse contexto, AYRES (1973, p. 97) menciona que: se x associado ao ponto P_x, que corta a reta, não é um número racional (já demonstramos isto), então, todo número racional está ou no conjunto E ou no conjunto D, porém, nunca em ambos. Analogamente, se x é um número racional, então, com exceção dele, todo número racional está ou no conjunto E ou no conjunto D, mas não em ambos, conforme ilustrado pela FIGURA 24 a seguir.

FIGURA 24 – Corte de uma reta pelo ponto P_x, com separador $x = \sqrt{2}$.



FONTE: elaborada pelo autor.

Aqui, chegamos à insuficiência do corpo ordenado $\mathbb{Q} \subset K$ e, portanto, no óbice do problema da continuidade da reta apresentado por Dedekind.

Segundo CARAÇA (1989, p. 59 – 60): Em 1872, Dedekind publicou uma obra que tratava sobre a *Continuidade e Números Irracionais*. Neste escrito, ele conseguiu responder à questão que propôs em 1859, acima citada. Em suas palavras:

> (...) *nós atribuímos à reta a qualidade de ser completa, sem lacunas, ou seja, contínua. Mas esta continuidade, em que consiste? A resposta a esta pergunta deve compreender*

> *em si tudo, e somente ela permitirá desenvolver em bases científicas o estudo de todos os campos contínuos (...). Pensei nisso sem resultado por muito tempo, mas, finalmente achei o que procurava. Consiste ela (...): todo ponto da reta determina uma decomposição da mesma em duas partes, de tal natureza que todo o ponto de uma delas está à esquerda de todo o ponto da outra.* Ora, eu vejo a essência da continuidade na inversão desta propriedade *e, portanto, no princípio seguinte: 'se uma repartição de todos os pontos da reta em duas classes está à esquerda de todo o ponto da outra, então existe um e só um ponto pelo qual é produzida esta repartição de todos os pontos em duas classes, ou esta decomposição da reta em duas partes'. (...) A propriedade da reta expressa por este princípio não é mais que um axioma, e é sob a forma deste axioma que nós pensamos a continuidade da reta, que reconhecemos à reta a sua continuidade.*

Ainda, conforme o autor, Dedekind resolve o problema da continuidade da reta a partir do *copo ordenado* dos números racionais e propõe um postulado ou Axioma da Continuidade da Reta.

Axioma de Dedekind. Todo *corte* da reta é produzido por um ponto dela, isto é, qualquer que seja o corte (E, D) *existe* sempre um ponto da reta que separa as duas classes E e D.

Nesse sentido, com a propriedade da relação de ordem, segundo ÁVILA (2006, p. 58), todo corte (E, D) na reta possui elemento de separação, que pode *pertencer* à classe E, como seu *máximo* (ou *supremo*, neste caso), ou *pertencer* à classe D, como seu *ínfimo* (ou *mínimo*, nesta situação). Assim, se r é um elemento de separação do corte (E, D), podemos representar por C_r este corte, isto é: $C_r = (E, D)$.

Com esta notação de corte e o axioma de Dedekind, podemos definir corte em $\mathbb{Q}$, de acordo com AYRES (1973, p. 98).

Definição 47. (Corte em $\mathbb{Q}$) Um conjunto de números racionais C_r é um corte, com elemento separador r, quando cumpre as três propriedades a seguir:

i) C_r é um subconjunto próprio (não vazio) de $\mathbb{Q}$;

ii) se $a \in \mathbb{Q}$, com $a < r$, então $a \in C_r$;

iii) para todo $c \in C_r$, existe $b \in C_r$, tal que $c < b$.

Ainda, segundo o autor: "A essência destas propriedades é que um corte não possui nem um elemento mínimo (primeiro) nem um elemento máximo (último)."

Observe que na propriedade ***i)***, temos que demonstrar duas coisas: C_r é um subconjunto próprio de $\mathbb{Q}$ e C_r não é vazio.

Na propriedade ***ii)***, devemos demonstrar que todo racional menor do que o elemento separador pertence ao corte.

Finalmente, a propriedade ***iii)*** menciona que, em todo corte racional, não existe elemento máximo. Em outras palavras, não existe supremo que pertença ao corte.

Proposição 18. Sejam C_r um corte, com elemento separador r, e $c \in \mathbb{Q}$. Então, c é cota superior de C_r se, e somente se, $c \in \mathbb{Q}\backslash C_r$.

Demonstração: ($\Longrightarrow$) Suponha que c seja cota superior do corte C_r. Então, $c \notin C_r$, pois, do contrário, c seria elemento máximo de C_r, contrariando a condição ***iii)*** de definição de corte. Logo, $c \in \mathbb{Q}\backslash C_r$.

($\Longleftarrow$) Reciprocamente, suponha que $c \in \mathbb{Q}\backslash C_r$. Então, c é cota superior do corte C_r, pois, caso contrário, teríamos: $c \in \mathbb{Q}$, com $c < r$. Isto implicaria $c \in C_r$, pela propriedade ***ii)*** da definição de corte. Mas, isto é uma contradição.

□

Proposição 19. Se $r \in \mathbb{Q}$ e $C_r = \{a\ ;\ a \in \mathbb{Q}$, com $a < r\}$, então C_r é um corte em $\mathbb{Q}$ e o elemento separador r é a menor cora superior de C_r.

Demonstração: Parte ***i)*** da definição de corte: o conjunto $\mathbb{Q}$ é ilimitado inferior e superiormente. Logo, não tem ínfimo nem supremo. Assim, existem $p, q \in \mathbb{Q}$, tais que:

- $p < r$ e, portanto, $C_r \neq \varnothing$; e
- $r < q$, segue que $C_r \neq \mathbb{Q}$.

Logo, C_r é um subconjunto próprio não vazio de $\mathbb{Q}$.

Parte ***ii)*** da definição de corte: seja $s \in C_r$. Então, $s < r$. Assim, para todo $a \in \mathbb{Q}$, tal que $a < s$ implica $a < s < r$. Logo, $a \in C_r$.

Parte ***iii)*** da definição de corte: para todo $s \in C_r$, temos: $s < r$. Daí, pela propriedade da densidade em $\mathbb{Q}$, existe $d \in \mathbb{Q}$, tal que $s < d < r$, basta tomar $d = (s + r)/2$.

Sendo $d < r$ implica $d \in C_r$. Isto significa que, para todo $s \in C_r$ existe $d \in C_r$, tal que $s < d$. Portanto, s não é elemento máximo de C_r.

O fato que, para todo $s \in C_r$, existe $d \in C_r$, tal que $s < d$ e, portanto, s não é elemento máximo de C_r, justifica que r é a menor cota superior de C_r.

□

Vimos que o conjunto dos números racionais $\mathbb{Q}$ não satisfaz o axioma da continuidade de Dedekind, pois, os conjuntos $E = \{r \in \mathbb{Q} ; r^2 < 2\}$ e $D = \{r \in \mathbb{Q} ; r^2 > 2\}$ de número racionais, por exemplo, carecem (respectivamente) de elementos máximo e mínimo. Logo, há "lacunas" no conjunto $\mathbb{Q}$ e, portanto, não forma um *contínuum*, isto é, *não completam* à reta, embora seja muito denso nela.

Com isso, Dedekind resolve o problema da continuidade (ou completude) da reta.

10.5 Número Real

A definição de corte de Dedekind, a partir do conjunto do número racionais, gera números que não são racionais.

Dessa forma, CARAÇA (1989, p. 62) menciona a necessidade de uma definição para esses números de separação que não pertencem ao conjunto $\mathbb{Q}$.

Definição 48. Chama-se *número real* ao elemento separador x do corte C_x de Dedekind na reta, tal que:
i) se x é um número racional, o corte chama-se *racional*; e
ii) se x não é racional, o corte chama-se número *irracional* e seu elemento separador será um número irracional.

O conjunto constituído por todos os números que não são racionais chama-se *conjunto dos números irracionais* e denota-se por $\mathbb{R}\backslash\mathbb{Q}$.

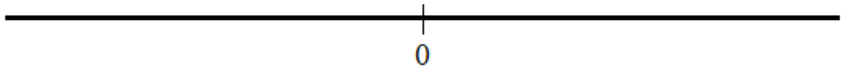
CARAÇA (1989, p. 63) destaca que para se definir um número racional a/b são necessários *dois números inteiros* a e b, com $b \neq 0$ e não é necessário "percorrer" o infinito. Mas, para definir um número real, de acordo com Dedekind, são necessárias *duas classes* (conjuntos infinitos), ou seja, há necessidade do conceito de infinito.

Ao conjunto de todos os números *racionais* e *irracionais*, chama-se *conjunto dos números reais* e indica-se por $\mathbb{R} = \mathbb{Q} \cup (\mathbb{R} \backslash \mathbb{Q})$.

Com isso, obtemos o conjunto dos números reais $\mathbb{R}$ que representa um "contínuo numérico", de modo que os números irracionais vêm preencher as "lacunas" de descontinuidade existentes no conjunto dos números racionais $\mathbb{Q}$.

Por não haver "lacunas" no conjunto $\mathbb{R}$, a reta passa a ser o *modelo geométrico* que exatamente o representa, conforme ilustrado pela FIGURA 25 a seguir.

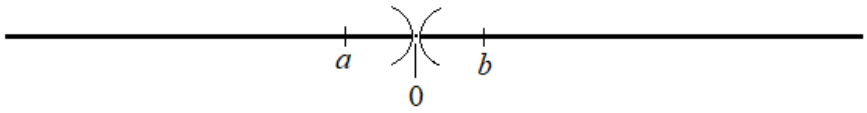
FIGURA 25 – Modelo geométrico do conjunto dos números reais $\mathbb{R}$.



FONTE: elaborada pelo autor.

O zero é um número real que separa as classes (ou conjuntos) $\mathbb{R}^- = \{a \; ; \; a < 0\}$ e $\mathbb{R}^+ = \{b \; ; \; 0 < b\}$ do corte $(\mathbb{R}^-, \mathbb{R}^+)$, conforme representado na FIGURA 26 a seguir.

FIGURA 26 – Representação das classes $\mathbb{R}^- = \{a \; ; \; a < 0\}$ e $\mathbb{R}^+ = \{b \; ; \; b > 0\}$ do corte $(\mathbb{R}^-, \mathbb{R}^+)$ na reta.



FONTE: elaborada pelo autor.

A classe (ou conjunto) $\mathbb{R}^- = \{a \; ; \; a < 0\}$ chama-se *semirreta negativa* e os número reais associados aos pontos que pertencem desta semirreta chamam-se número reais *negativos*. De modo semelhante, a classe (ou conjunto) $\mathbb{R}^+ = \{b \; ; \; b > 0\}$ chama-se semirreta *positiva* e os números reais que correspondem aos pontos desta semirreta chamam-se números reais *positivos*.

Em virtude da completeza da reta estruturada no axioma de Dedekind, o conjunto dos números reais $\mathbb{R}$ chama-se *corpo ordenado completo*.

No contexto de função, o que faltava para a aplicação $\alpha : \mathbb{Q} \to P$, onde P é o conjunto dos pontos de uma reta, ser sobrejetiva, agora, o conjunto $\mathbb{R}$ cumpre este papel e, desse modo, existe uma função $\alpha : \mathbb{R} \to P$ bijetiva.

Ademais, segundo GUEDES (1996, p. 9), o axioma de Dedekind pode ser escrito em termos de ínfimo e supremo, conforme descrito a seguir:

Postulado do Ínfimo (Dedekind). Todo subconjunto (não vazio) de $\mathbb{R}$, limitado inferiormente, possui um ínfimo em $\mathbb{R}$.

De modo semelhante:

Postulado do Supremo (Dedekind). Todo subconjunto (não vazio) de $\mathbb{R}$, limitado superiormente, admite um supremo em $\mathbb{R}$.

Segundo LIMA (2010, p. 80): "todo corpo ordenado completo é arquimediano." Como o conjunto dos números reais é um corpo ordenado completo, temos a proposição a seguir.

Teorema 25. (Arquimediano) $\mathbb{R}$ é aquimediano, ou seja, vale qualquer uma das propriedades a seguir:
i) dados $a, b \in \mathbb{R}$, com $0 < a < b$, existe pelo menos um $n \in \mathbb{N}$, tal que $n \cdot a > b$;
ii) para todo $a \in \mathbb{R}$, com $0 < a$, existe pelo menos um $n \in \mathbb{N}$, tal que $0 < 1/n < a$.

Demonstração: ***i)*** Suponha, por absurdo, que $n \cdot a \leq b$, para todo $n \in \mathbb{N}$. Considere o conjunto dos múltiplos de a:

$$M(a) = \{n \cdot a \; ; \; n \in \mathbb{N}\}.$$

Este conjunto não é vazio, pois, sendo $0 < a$, temos: $1 \cdot a \in \mathbb{N}$. Além disso, $M(a)$ é limitado superiormente por b, logo, pelo Postulado de Dedekind, o conjunto $M(a)$ admite supremo.

Seja s o supremo de $M(a)$. Como o conjunto $\mathbb{N}$ tem a propriedade $n \in \mathbb{N}$ implica $n + 1 \in \mathbb{N}$, segue, para todo $n \in \mathbb{N}$, que:

$$n \cdot a \leq s \implies (n + 1) \cdot a \leq s \implies n \cdot a + a \leq s \implies n \cdot a \leq s - a.$$

Mas, por hipótese, $0 < a$. Logo, $s - a$ é uma cota superior de $M(a)$ menor do que o supremo s, o que é um absurdo! Assim, existe pelo menos um $n \in \mathbb{N}$, tal que $n \cdot a > b$.

ii) Temos: $0 < a$. Então, por ***i)***, existe pelo menos um $n \in \mathbb{N}$, tal que $n \cdot a > b$, com $b > 0$. Fazendo $b = 1$, segue que: $n \cdot a > 1$. Como $0 < 1/n$, temos: $0 < 1/n < a$.

□

Teorema 26. (Densidade) Os conjuntos $\mathbb{Q}$ e $(\mathbb{R}\backslash\mathbb{Q})$ são ambos densos em $\mathbb{R}$.

Demonstração: ***i)*** Densidade de $\mathbb{Q}$ em $\mathbb{R}$.

Sejam $a, b \in \mathbb{R}$, tais que $a < b$. Então, $b - a > 0$. Como $\mathbb{R}$ é arquimediano, existe pelo menos um $n \in \mathbb{N}$, tal que $0 < 1/n < b - a$ e, portanto, $1 < n \cdot b - n \cdot a$.

Como a diferença $n \cdot b - n \cdot a$ é maior do que 1, existe pelo menos um $m \in \mathbb{Z}$, tal que:

$$n \cdot a < m < n \cdot b \ \ \therefore \ \ a < m/n < b, \text{ com } n \in \mathbb{N}.$$

Isto significa que existem infinitos números racionais entre os números reais a e b. Portanto, $\mathbb{Q}$ é denso em $\mathbb{R}$.

ii) Densidade de $(\mathbb{R}\backslash\mathbb{Q})$ em $\mathbb{R}$.

Para obter um número irracional, considere $1/n < (b - a)/\sqrt{2}$, isto é, $\sqrt{2}/n < (b - a)$. Assim, os números da forma $m \cdot \sqrt{2}/n$, com $m \in \mathbb{Z}\backslash\{0\}$ são irracionais e dividem a reta com espaçamento de tamanho $\sqrt{2}/n$, pois:

$$(m + 1) \cdot \sqrt{2}/n \ - \ m \cdot \sqrt{2}/n = \sqrt{2}/n.$$

Como $\sqrt{2}/n < (b - a)$, então, algum $m \cdot \sqrt{2}/n$ deve estar entre a e b, isto é, $a < m \cdot \sqrt{2}/n < b$, para algum $m \in \mathbb{Z}\backslash\{0\}$.

Agora, se $m_0 \in \mathbb{Z}\backslash\{0\}$ for o menor, tal que $b \leq m_0 \cdot \sqrt{2}/n$, então o número irracional $(m_0 - 1) \cdot \sqrt{2}/n$ está entre a e b, ou seja, $a < (m_0 - 1) \cdot \sqrt{2}/n < b$. Dessa forma, há infinitos números irracionais entre dois números reais. Portanto, o conjunto $(\mathbb{R}\backslash\mathbb{Q})$ é denso em $\mathbb{R}$.

Outra maneira de demonstrar a densidade de $(\mathbb{R}\backslash\mathbb{Q})$ em $\mathbb{R}$.

Pelo item ***i)***, sabe-se que $\mathbb{Q}$ é denso em $\mathbb{R}$. Então, para todo a, $b \in \mathbb{R}$, tais que $a < b$, existem $r, s \in \mathbb{Q}$, tais que: $a < r < s << b$.

O conjunto $\mathbb{Q}$ é denso e, portanto, existem $(r + s)/2 \in \mathbb{Q}$, tais que: $r < (r + s)/2 < s$ ou $r < r + (s – r)/2 < s$ ou ainda, $r < r + (s – r)\cdot\lambda < s$, com $r + (s – r)\cdot\lambda \in \mathbb{Q}$ e $0 < \lambda < 1$.

Portanto, $a < r + (s – r)\cdot\lambda < b$, com $0 < \lambda < 1$.

Agora, note que $\sqrt{2}/n > \sqrt{2}/(n + 1)$, para todo $n \in \mathbb{N}$. Então, pondo $\lambda = \sqrt{2}/(n + 1)$, com $n \in \mathbb{N}$, tem-se infinitos números irracionais λ, tais que: $a < r + (s – r)\cdot \sqrt{2}/(n +1) < b$.

Definindo $d = r + (s – r)\cdot \sqrt{2}/(n +1)$, obtém-se infinitos números irracionais d, de modo que $a < d < b$.

□

Exemplo 59. Sejam $r, s \in \mathbb{Q}$, com $r < s$. Prove que o número $r + (s – r)/\sqrt{2}$ é irracional e $r < r + (s – r)/\sqrt{2} < s$.

Resolução: i) Suponha, por absurdo, que o número $a = r + (s – r)/\sqrt{2}$ seja racional. Então, $a – r = (s – r)/\sqrt{2}$ é racional e, portanto, $\sqrt{2} = (s – r)/(a – r)$, com $a \neq r$ é racional, o que é um absurdo!

Portanto, o número $r + (s – r)/\sqrt{2}$ é irracional.

ii) Dado que o número $\sqrt{2}$ é irracional, então, pela propriedade arquimediana de $\mathbb{R} = \mathbb{Q} \cup (\mathbb{R}\backslash\mathbb{Q})$, tem-se $1 \in \mathbb{N}$, tal que $1\cdot \sqrt{2} > 1$ e, portanto, $1 > 1/\sqrt{2}$ ou $0 < 1/\sqrt{2} < 1$. Mas, $r < s$ implica $s – r > 0$.

Multiplicando a desigualdade $0 < 1/\sqrt{2} < 1$ por $s – r$, obtemos:

$$0 < (s – r)/\sqrt{2} < (s – r).$$

Somando r nesta última desigualdade, tem-se: $r < r + (s – r)/\sqrt{2} < s$.

Conclusão

Ao propor a temática Conjuntos e Funções articulando conceitos, propriedades e demonstrações visando à formação continuada do professor da Educação Básica, abrem-se possibilidades de abordar a relação professor, conteúdo e aluno.

Nesse contexto, o ensino e a aprendizagem da matemática ganham importâncias significativos. Assim, procuramos refletir sobre a noção de conjuntos e funções, fazendo uso de conceitos, definições, exemplos, observações, esquemas, teoremas e figuras para construir uma perspectiva que possibilite o aprimoramento da linguagem técnica, a elaboração de conceitos e estratégias, à prática de enunciar e demonstrar teoremas, visando à atuação do professor de matemática na sala de aula e a construção dos conhecimentos matemáticos, de modo com prioridade ao pensar em detrimento ao calcular, contribuindo significativamente à aprendizagem dos alunos.

Dessa forma, acreditamos ter contribuído para o aperfeiçoamento do professor, a fim de que ele conduza com mais segurança suas práticas pedagógicas e proporcione melhor qualidade no ensino da matemática na Educação Básica.

Referências

AURÉLIO, Marco Palumbo Cabral; NERI, Cassio Moreira. *Curso de Análise Real*. 2ª ed. Rio de Janeiro, 2011.

ÁVILA, Geraldo S. de Souza. *Análise Matemática para a Licenciatura*. 3ª ed. São Paulo, 2006.

AYRES, Frank. *Álgebra Moderna*. São Paulo, 1973.

AZEVEDO, Israel Belo de. *O Prazer da Produção Científica*. 4ª ed. Piracicaba-SP, 1996.

BARTLE, Robert G. *Elementos de Análise Real*. Rio de Janeiro: Campus, 1983.

BOYER, Carl B. *História da Matemática*. 2ª ed. São Paulo, 1996.

CARAÇA, Bento de Jesus. *Conceitos Fundamentais da Matemática*. 9ª ed. Lisboa, 1989.

CASTRO, Luciano Lima; ORIOSVALDO, Manoel de Moura; PERIDES, Roberto Moisés;

CORDEIRO, Daniel de Morais Filho. *Manual de Redação Matemática*. 1ª ed. Rio de Janeiro: SBM, 2014.

DEAN, Richard A. *Elementos de Álgebra Abstrata*. Rio de Janeiro, 1974.

DOMINGUES, Hygino H. *Fundamentos de Aritmética*. São Paulo, 1991.

DOMINGUES, Hygino H.; IEZZI, Gelson. *Álgebra Moderna*. 3ª ed. São Paulo, 1982.

FERREIRA, Jamil. *A Construção dos Números*. 3ª ed. Rio de Janeiro: SBM, 2013.

GUESDES, D. de Figueiredo. *Análise I*. 2ª ed. Campinas-SP, 1996.

HEFEZ, Abramo. *Curso de Álgebra, v.1*. 3ª ed. Associação Instituto Nacional de Matemática Pura e Aplicada, Rio de Janeiro, 2002.

IRRACIEL, Krerley Martins Oliveira; JOSÉ, Adán Corcho Fernández. *Iniciação à Matemática: um curso com problemas e soluções*. Rio de Janeiro: SBM, 2010.

LIMA, Elon Lages. *Curso de análise v.1*. 12ª ed. Associação Instituto Nacional de Matemática Pura e Aplicada, Rio de Janeiro, 2010.

LIMA, Elon Lages. *Números e Funções Reais*. Coleção PROFMAT. Rio de Janeiro: SBM, 2013.

LIPSHUTZ, Seumour. *Teoria dos Conjuntos*. São Paulo, 1972.

NACHBIN, Leopoldo. *Introdução à Álgebra*. Rio de Janeiro, 1974.

REGINA, Anna L. de Moura. *Educar com a Matemática Fundamentos*. 1ª ed. São Paulo, 2016.

SCHEINERMAN, Edward R. *Matemática Discreta: uma introdução*. São Paulo, 2003.

TAHN, Malba. *O Homem que Calculava*. 79ª ed. Rio de Janeiro, 2010.