Universidade Federal de Goiás
Instituto de Matemática e Estatística
Programa de Mestrado Profissional em Matemática em Rede Nacional

Números Reais: Um Corpo Ordenado e Completo

Jadson da Silva Souza

Goiânia
2013

TERMO DE CIÊNCIA E DE AUTORIZAÇÃO PARA DISPONIBILIZAR ELETRONICAMENTE OS TRABALHOS DE CONCLUSÃO DE CURSO NA BIBLIOTECA DIGITAL DA UFG

Na qualidade de titular dos direitos de autor, autorizo a Universidade Federal de Goiás (UFG) a disponibilizar, gratuitamente, por meio da Biblioteca Digital de Teses e Dissertações (BDTD/UFG), sem ressarcimento dos direitos autorais, de acordo com a Lei nº 9610/98, o documento conforme permissões assinaladas abaixo, para fins de leitura, impressão e/ou *download*, a título de divulgação da produção científica brasileira, a partir desta data.

1. Identificação do material bibliográfico: **Trabalho de Conclusão de Curso de Mestrado Profissional**

2. Identificação do Trabalho

Autor (a):	Jadson da Silva Souza						
E-mail:	jadson3636@hotmail.com						
Seu e-mail pode ser disponibilizado na página? [x]Sim [ ] Não							
Vínculo empregatício do autor	Secretaria de Educação do Estado de Goiás						
Agência de fomento:	Fundação Coordenação de Aperfeiçoamento de Pessoal de Nível Superior				Sigla:	CAPES	
País:	Brasil	UF:	GO	CNPJ:	00.889.834/0001-08		
Título:	Números Reais: Um Corpo Ordenado e Completo.						
Palavras-chave:	Números Reais, Corpo Ordenado Completo, Decimais, Reta.						
Título em outra língua:	Real Numbers: A Complete Ordered Field.						
Palavras-chave em outra língua:	Real Numbers, Complete Ordered Field, Decimals, Line.						
Área de concentração:	Matemática do Ensino Básico.						
Data defesa: (dd/mm/aaaa)	22/03/2013						
Programa de Pós-Graduação:	Mestrado Profissional em Matemática em Rede Nacional.						
Orientador (a):	Prof. Dr. Maurilio Márcio Melo						
E-mail:	melo@mat.ufg.br						
Co-orientador(a):*							
E-mail:							

*Necessita do CPF quando não constar no SisPG

3. Informações de acesso ao documento:

Concorda com a liberação total do documento [x] SIM [ ] NÃO[1]

Havendo concordância com a disponibilização eletrônica, torna-se imprescindível o envio do(s) arquivo(s) em formato digital PDF ou DOC do trabalho de conclusão de curso.

O sistema da Biblioteca Digital de Teses e Dissertações garante aos autores, que os arquivos contendo eletronicamente as teses, dissertações ou trabalhos de conclusão de curso, antes de sua disponibilização, receberão procedimentos de segurança, criptografia (para não permitir cópia e extração de conteúdo, permitindo apenas impressão fraca) usando o padrão do Acrobat.

Jadson da Silva Souza

Assinatura do (a) autor (a)

Data: 22 / 03 / 2013.

[1] Neste caso o documento será embargado por até um ano a partir da data de defesa. A extensão deste prazo suscita justificativa junto à coordenação do curso. Os dados do documento não serão disponibilizados durante o período de embargo.

Jadson da Silva Souza

Números Reais: Um Corpo Ordenado e Completo

Trabalho de Conclusão de Curso apresentado ao Programa de Pós–Graduação do Instituto de Matemática e Estatística da Universidade Federal de Goiás, como requisito parcial para obtenção do título de Mestre em matemática

Área de concentração: Matemática do Ensino Básico.

Orientador: Prof. Dr. Maurílio Márcio Melo

Goiânia
2013

Dados Internacionais de Catalogação na Publicação (CIP)
GPT/BC/UFG

Souza, Jadson da Silva.
S729n Números reais [manuscrito] : um corpo ordenado e completo / Jadson da Silva Souza. - 2013.
61 f. : figs.

Orientador: Prof. Dr. Maurílio Márcio Melo.
Dissertação (Mestrado) – Universidade Federal de Goiás, Instituto de Matemática e Estatística, 2013.
Bibliografia.
Inclui lista de figuras.

1. Números reais. 2. Corpo ordenado completo. 3. Decimais. I. Título.

CDU: 517.13

Jadson da Silva Souza

Números Reais: Um Corpo Ordenado e Completo

Trabalho de Conclusão de Curso defendido no Programa de Mestrado Profissional em Matemática em Rede Nacional – PROFMAT/UFG, do Instituto de Matemática e Estatística da Universidade Federal de Goiás, como requisito parcial para obtenção do título de Mestre em Matemática, área de concentração Matemática do Ensino Básico, aprovado no dia 22 de março de 2013, pela Banca Examinadora constituída pelos professores:

Prof. Dr. Maurílio Márcio Melo
Instituto de Matemática e Estatística-UFG
Presidente da Banca

Prof. Dr. Flávio Raimundo de Souza
Membro/IFG/Goiânia

Profa. Dra. Marina Tuyako Mizukoshi
Instituto de Matemática e Estatística-UFG

Jadson da Silva Souza

Licenciado em Matemática e Especialista em Educação Matemática pela UEG. Professor da Secretaria de Educação do Estado de Goiás e da Secretaria Municipal de Educação de Anápolis, atuando no ensino básico desde 2005.

À minha esposa e filhas, pelo reconhecimento dos valiosos incentivos à conclusão de mais uma etapa de minha vida.

Agradecimentos

Aos professores, tutores e coordenadores do IME-UFG pelo empenho e dedicação mostrados ao longo do curso, em especial ao Prof. Dr. Maurílio Márcio Melo pela dedicação durante a orientação deste, aos colegas de turma pelo apoio e compreensão nos momentos difíceis e a CAPES pelo suporte financeiro.

“Não há ramo da Matemática, por mais abstrato que seja, que não possa um dia vir a ser aplicado aos fenômenos do mundo real.”

Nikolai Ivanovich Lobachevsky.

Resumo

Souza, Jadson da Silva . **Números Reais: Um Corpo Ordenado e Completo**. Goiânia, 2013. 61p. Trabalho de conclusão de curso. Instituto de Matemática e Estatística, Universidade Federal de Goiás.

Este trabalho tem como objetivo ampliar os conhecimentos sobre os números reais, proporcionando uma nova perspectiva sobre sua construção conceitual. Inicialmente, aborda-se alguns fatos históricos que foram de maior importância no processo da evolução conceitual dos números reais. Posteriormente, por meio do desenvolvimento das teorias de álgebra, de conjuntos e de análise matemática, utiliza-se de um método axiomático para expor uma construção do corpo ordenado e completo dos reais, enunciando e provando algumas de suas propriedades. Finalmente, abordam-se alguns aspectos relevantes da correspondência entre o corpo dos reais e a reta, e ainda da correspondência entre o corpo dos reais e os decimais.

Palavras–chave

Números Reais, Corpo Ordenado Completo, Decimais, Reta

Abstract

Souza, Jadson da Silva . **Real Numbers: A Complete Ordered Field**. Goiânia, 2013. 61p. Completion of course work. Instituto de Matemática e Estatística, Universidade Federal de Goiás.

This paper aims to expand knowledge about the real numbers, providing a new perspective on their conceptual construction. Initially, covers up some historical facts that were of utmost importance in the process of conceptual evolution of the real numbers. Secondly, through the development of theories of abstract algebra, sets and mathematical analysis, is used a axiomatic method to expose the complete ordered field of real, stating and proving some of its properties. Finally, we discuss some relevant aspects of the correspondence between the real field and line, and also the correspondence between the real field and decimals.

Keywords

Real Numbers, Complete Ordered Field, Decimals, Line

Sumário

Lista de Figuras

Introdução

Aspectos Históricos

Pode-se destacar como um dos marcos ao início do desenvolvimento histórico dos números reais a crise pitagórica na Grécia, ocasionada pela descoberta dos segmentos incomensuráveis, que provavelmente deve ter sido feita por um pitagórico, no período entre 500 e 350 a.C. Apesar de Proclus (450 d.C) parecer ter atribuído essa descoberta a Pitágoras. A prova mais antiga sobre medidas incomensuráveis que se conhece foi apresentada por Aristóteles, e se refere a diagonal e ao lado de um quadrado. A verificação trata-se de uma prova indireta, baseada no teorema de Pitágoras, e no fato de que, o quadrado de um número par é também um número par, mais detalhes dessa prova ([9] , p. 55).

A prova de que os lados de quadrados cujas áreas são os não-quadrados 3,5,7,...,17 não são comensuráveis com o lado de quadrado 1 foi atribuído a Teodoro de Cirene (c. 390 a.C.). Em linguagem moderna ele provou a irracionalidade de $\sqrt{3}$, $\sqrt{5}$, $\sqrt{7}$, ... , $\sqrt{17}$. Em consequência das grandezas incomensuráveis surge a necessidade de se construir uma teoria das proporções independente da comensurabilidade, tal construção foi feita por Eudoxo (c. 370 a.C.), a qual serviu como base do Livro V dos Elementos de Euclides([2], pp. 74 à 87), um dos livros escrito pelo matemático grego Euclides em Alexandria por volta de 300 a.C. Os Elementos de Euclides tiveram enorme importância para o desenvolvimento da geometria no que se refere à organização lógica e axiomática.

Esse processo de organização lógica e axiomática na álgebra foi tardio considerando que as primeiras tentativas nesse sentido ocorreram no início do século XIX e continuaram ao longo desse século por meio de trabalhos diversos como, por exemplo, os feitos pelo matemático norueguês Niels Henrik Abel (1802-1829) que no ano de 1824 provaram a impossibilidade de se obter uma fórmula geral por meio de radicais que expressasse as raízes de uma equação de grau ≥ 5. Mesmo assim, ainda restava uma questão. O que caracterizava no aspecto matemático os casos de equações de grau ≥ 5 que podem ter suas raízes expressas por meio de radicais através de uma fórmula geral? Esta questão surgiu do fato de que as equações de grau ≥ 5 não são, de modo geral, resolúveis por radicais, mas alguns tipos o são, como já se sabia bem antes de Abel. A resposta a

essa pergunta seria dada pelo matemático francês Evariste Galois (1811-1832) cuja obra delineava pela primeira vez o conceito de grupo.

Apesar do conceito de corpo já estar nessa época, implícito em trabalhos de Abel e Galois foi o matemático alemão Richard Dedekind (1831-1916) que conseguiu explicitá-lo. Tal feito ocorreu no ano de 1879 quando publicou o livro "Über die Theorie der Ganzen Zahlen algebraischen"que definiu a noção de corpo numérico como uma coleção de números que formam um grupo abeliano com relação às operações de adição e multiplicação (com a exceção do zero), e na qual a multiplicação é distributiva com relação à adição. Dedekind fez muitas contribuições importantes no campo da álgebra, especialmente, para teoria dos números algébricos, nos fundamentos dos números reais e teoria de anel, sua obra prima foi o "Corte de Dedekind"([2], p. 411).

Deve-se, também, destacar a teoria dos Conjuntos criada por Georg Cantor (1845-1918), a qual foi publicada em uma série de artigos a partir de 1874. Em seus trabalhos Cantor estendeu a ideia de cardinal para conjuntos finitos e seu grande mérito foi perceber a existência de uma hierarquia para os cardinais transitivos, ou seja, desenvolveu o conceito de enumerável. Cantor ainda conseguiu mostrar que os inteiros e os racionais são enumeráveis ([2], p. 414). Ainda mostrou que o conjunto dos números reais tem cardinal maior que os dos conjuntos enumeráveis e que esse cardinal é igual ao dos conjuntos irracionais, contrariando a velha ideia de que o todo tinha que ser maior do que a parte.

Em virtude dos conceitos desenvolvidos pelos matemáticos aqui citados, dentre outros de importância relevante, durante o século XIX, foi possível desenvolver ideias da Álgebra, do Cálculo e da Análise Matemática que contribuíram para a construção dos números reais.

Situação Atual

A análise de livros didáticos de matemática constitui um parâmetro indicador do estado atual em que se encontra o ensino da mesma. Especificamente no ensino básico pode-se constatar, pela leitura de [18], que o conteúdo dos números reais, na maioria das vezes é equivocadamente, apresentado simplesmente como a união dos racionais com os irracionais criando assim um problema de circularidade nesse conceito. Observa-se a necessidade do conhecimento prévio dos reais para se definir os números irracionais. No ensino superior, pela leitura de [3], percebe-se que muitos dos livros didáticos de matemática persistem no equívoco da circularidade do conceito dos reais, ou ainda, tratam dos reais como um objeto de conhecimento dos alunos, no caso futuros professores de matemática. Então como solucionar esse problema de circularidade do conceito dos números reais?

Ao se deparar com essa situação no ensino básico, uma abordagem mais axiomática é visivelmente inviável, pois para isso teria-se que introduzir conceitos matemáticos complexos a nível básico. No entanto, no ensino superior, o tratamento mais estruturado e axiomático dos conceito dos reais se faz necessária, no âmbito de preparar o futuro professor de matemática a lidar e construir ferramentas pedagógicas que permitam minimizar ou resolver o problema da circularidade do conceito dos reais, a nível de ensino básico.

Considerando os reais como apenas a união dos racionais com os irracionais, deixa-se de apresentar fatos relacionados ao mesmo que são importantes em contextos mais amplos, por exemplo, de que as propriedades dos reais são consequências diretas do fato dos reais serem um corpo ordenado e completo.

Diante do exposto faz-se necessária uma reformulação na exposição dos conteúdos matemáticos que privilegie a correção dos conceitos, bem como a apresentação sistemática fundamentada das proposições enunciadas.

Apresentação dos Capítulos

Esse trabalho está dividido em 4 capítulos:

O capítulo 1, que desenvolve-se no momento, contém alguns aspectos históricos que motivaram o desenvolvimento desse trabalho e uma abordagem sobre como atualmente se ensina os números reais.

O capítulo 2, inicia-se com a linguagem de conjuntos de forma a apresentar algumas de suas definições, exemplos, teoremas ou proposições e suas demonstrações focando conceitos relacionados a: operações entre conjuntos, comparação entre conjuntos, conjuntos finitos e infinitos, conjuntos enumeráveis, dentre outros. Ainda nesse capítulo, são dadas as definições e propriedades consequentes de algumas das estruturas fundamentais da álgebra: grupo, anel e corpo, focando principalmente a estrutura denominada corpo que é peça fundamental para o desenvolvimento deste trabalho.

O capítulo 3, contém o desenvolvimento da proposta deste trabalho que é definir os reais como um corpo, ordenado e completo. Inicialmente, defini-se esse fato de maneira formal, ou seja, usando as definições, axiomas, teoremas e postulados da linguagem de conjuntos, da álgebra e da análise desenvolvidos no capítulo anterior. Ainda nesse capítulo, aborda-se o corpo dos reais de duas formas, onde em uma delas apresenta-se a correspondência entre o corpo ordenado completo dos reais e a reta numérica, enquanto a outra apresenta a correspondência entre o corpo ordenado dos reais e os decimais.

O capítulo 4, contém as considerações finais acerca do trabalho desenvolvido.

CAPÍTULO 1

Fundamentos Básicos sobre Conjuntos e Álgebra Abstrata

1.1 Fundamentos Básicos sobre Conjuntos

Nesta secção não tratar-se-á dos aspectos rigorosos da teoria dos conjuntos e sim de alguns aspectos fundamentais de linguagem de conjuntos, os quais são base para o desenvolvimento deste trabalho. Para maiores detalhes sobre o assunto, ou mesmo, para encontrar alguns dos resultados apresentados nessa secção, indicam-se as referências [8], [12], [13] e [15].

1.1.1 Noções básicas de Conjuntos

Um conjunto é uma coleção de objetos, denominados seus elementos, a relação binária entre um objeto e o conjunto é de pertinência, ou seja:

1) Se um objeto **a** é um dos elementos que compõem o conjunto A, dizemos que **a** pertence ao conjunto A e escreve-se $\mathbf{a} \in A$;
2) Se um objeto **a** não é um dos elementos que compõem o conjunto A, dizemos que **a** não pertence ao conjunto A e escreve-se $\mathbf{a} \notin A$.

Exemplo 1.1 ***Conjunto dos Números Naturais***

A coleção dos números naturais 1,2,3,..., representada pelo simbolo $\mathbb{N}$ *é um exemplo de conjunto. A teoria sobre os números naturais parte dos três axiomas abaixo, conhecidos como axiomas de Peano.*

(A_1) *Todo número natural possui um sucessor que também é natural. E ainda, números naturais distintos possuem sucessores distintos;*

(A_2) *Existe um único número natural, denotado por 1, que não é sucessor de nenhum outro;*

(A_3) *(Princípio da Indução) Se um conjunto, constituído apenas por números naturais, contém o número 1 e também o sucessor de cada um de seus elementos, então esse conjunto contém todos os números naturais.*

Vale destacar que o terceiro axioma fornece uma ferramenta muito eficaz na matemática, conhecida como Princípio da Indução [13, *pg*.34]. *Pode-se representar os conjuntos dos números naturais através da seguinte notação:* $\mathbb{N} = \{1,2,3,4,...\}$.

Em matemática um conjunto pode ser caracterizado, por uma propriedade comum a cada um dos seus elementos ou ainda, listando todos os seus elementos.

Exemplo 1.2 *Seja o conjunto P dos números naturais pares, esse conjunto pode ser bem representado de qualquer uma das formas abaixo:*

- *P={*$x \in \mathbb{N}$ *; x é par };*
- *P={2,4,6,8,10,...}.*

Também em matemática os elementos dos conjuntos não são necessariamente números, podendo ser figuras geométricas, pessoas, etc.

Exemplo 1.3 *Como, por exemplo, o conjunto R dos poliedros regulares de Platão: R={tetraedro, hexaedro, octaedro, dodecaedro, icosaedro}.*

Definição 1.1 *Conjunto vazio que é representado por* $\emptyset$ *ou* $\{\}$ *é um conjunto que não possui elementos.*

Exemplo 1.4 *Segue-se alguns exemplos de conjuntos vazios:*

a) Seja A = {x; $x^2 = 9$ *e x é par}, então A=*$\emptyset$*;*
b) Seja B, o conjunto de brasileiros que possuem altura superior a 4 metros, então B=$\emptyset$.

Dados dois conjuntos A e B, a relação entre eles é de inclusão, diz-se que A é subconjunto de B, se todos elementos de A são também elementos de B, ou seja, A está contido em B, indicando com a notação $A \subset B$, ou ainda, pode-se afirmar que B contém A, indicado pela notação $B \supset A$.

Exemplo 1.5 *Sejam* $A = \{a,b,c,d\}$, $B = \{e,f,g,h\}$ *e* $C = \{a,b,c,d,e,f,g\}$. *Então* $A \subset C$ *(ou* $C \supset A$ *), pois todo elemento do conjunto A é também elemento do conjunto C. Entretanto, B não está contido em C , pois o elemento* $h \in B$ *e* $h \notin C$.

1.1.2 Operações entre Conjuntos

Quando se fala das operações entre conjunto é interessante salientar que uma ferramenta matemática bastante útil na visualização dessas operações é o diagrama de Venn. A ideia é a seguinte: primeiro para representar o conjunto de todos os elementos considerados traça-se um retângulo de dimensões arbitrárias. Depois, para cada subconjunto próprio do universo que o retângulo representa traça-se uma curva fechada e convexa, no interior desse retângulo, por exemplo:

Seja U o universo considerado e sejam A e B subconjuntos próprios de U, então a relação $A \subset B$ é representada na Figura 1.1.

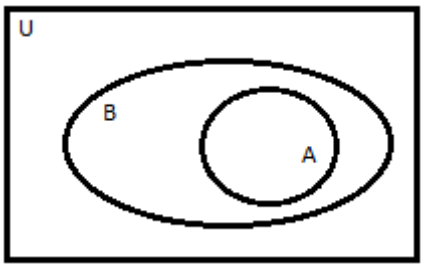

Figura 1.1: *Diagrama de Venn representando a situação $A \subset B$.*

Definição 1.2 *Dados dois conjuntos A e B, a reunião dos conjuntos A e B é o conjunto $A \cup B$, formado pelos elementos de A mais os elementos de B, portanto:*

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

O "ou"acima é diferente do usado no senso comum, o "ou" em matemática, no caso acima, significa que pertence a pelo menos um dos conjuntos sem excluir a possibilidade de pertencer ao mesmo tempo aos dois.

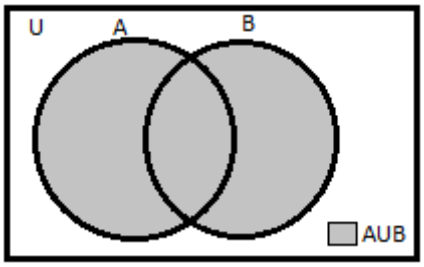

Figura 1.2: *Diagrama de Venn representando o conjunto $A \cup B$.*

Exemplo 1.6 *Sejam $A = \{1,3,5,7,9,10\}$ e $B = \{2,4,6,8,10\}$. Então, a reunião dos conjuntos A e B é o conjunto $A \cup B = \{1,2,3,4,5,6,7,8,9,10\}$.*

Definição 1.3 *Dados dois conjuntos A e B, a interseção dos conjuntos A e B é o conjunto $A \cap B$, formado pelos elementos que pertencem simultaneamente aos conjuntos A e B, portanto:*

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

Se A e B não possuem nenhum elemento em comum, então $A \cap B = \emptyset$. Neste caso, afirma-se que A e B são conjuntos disjuntos.

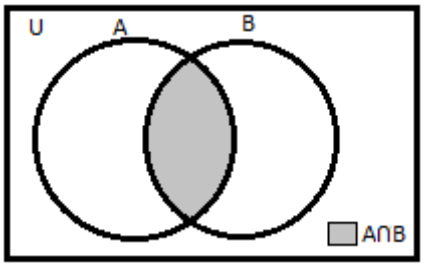

Figura 1.3: *Diagrama de Venn representando o conjunto $A \cap B$.*

Exemplo 1.7 *Sejam* $A=\{1,3,5,7,9,10\}$ *e* $B=\{2,4,6,8,10\}$. *Então,* $A \cap B=\{10\}$.

Definição 1.4 *Dados dois conjuntos A e B, a diferença dos conjuntos A e B é o conjunto $A - B$, formado pelos elementos que pertencem a A e não pertencem a B, portanto:*

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

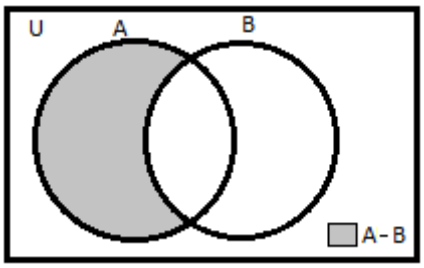

Figura 1.4: *Diagrama de Venn representando o conjunto diferença $A - B$.*

Exemplo 1.8 *Sejam* $A=\{1,3,5,7,9,10\}$ *e* $B=\{2,4,6,8,10\}$. *Então* $A-B=\{1,3,5,7,9\}$.

Definição 1.5 *Dados dois conjuntos A e B, o produto cartesiano dos conjuntos A e B é o conjunto $A \times B$, onde seus elementos são todos pares ordenados (a,b) cuja a primeira coordenada pertence a A e a segunda a B.*

$$A \times B = \{(a,b); a \in A \text{ e } b \in B\}.$$

Exemplo 1.9 *Sejam* $A=\{1,3,5\}$ *e* $B=\{2,10\}$. *Então:*

$$A \times B = \{(1,2),(1,10),(3,2),(3,10),(5,2),(5,10)\}.$$

1.1.3 Noções básicas de Funções

Definição 1.6 *Um função f de um conjunto A em um conjunto B é uma regra que a cada elemento $x \in A$ associa um único elemento $y = f(x) \in B$, onde f(x) é denominado o valor de f no elemento x. O conjunto A é chamado domínio da função f, e o conjunto B é chamado contradomínio. A notação de uma função f de um conjunto A em um conjunto B é dada por:*

$$f: A \to B.$$

O conjunto dos elementos $y \in B$ tais que existem pelo menos um $x \in A$ tal que $f(x) = y \in B$ é chamado imagem de A pela função f e é designado por f(A).

Exemplo 1.10 *Sejam S o conjunto dos polígonos do plano, $\mathbb{R}$ o conjunto dos números reais e $f: S \to \mathbb{R}$ a função que associa a cada polígono x sua área f(x).*

Definição 1.7 *Uma função $f: A \to B$ tal que f(A)= B, ou seja, o conjunto imagem coincide com o contradomínio é chamada de sobrejeção ou função sobrejetiva.*

Exemplo 1.11 *Seja $f: \mathbb{R} \to \mathbb{R}$ definida por $f(x)=x^2$, então f não é sobrejetora, pois o conjunto imagem de f não contém números negativos. No entanto, a função identidade $i : \mathbb{Z} \to \mathbb{Z}$, definida por i(x) = x é sobrejetiva, pois cada número inteiro é levado por i nele mesmo. Logo, o conjunto imagem de i é igual ao seu contradomínio, ou seja, $i(\mathbb{Z})=\mathbb{Z}$.*

Definição 1.8 *Uma função $f: A \to B$ é uma injeção ou função injetiva se, para todo $x_1, x_2 \in A$, com $x_1 \neq x_2$, tem-se $f(x_1) \neq f(x_2)$, ou seja, f leva elementos distintos de A em elementos distintos de B, ou ainda, se $f(x_1) = f(x_2)$ implica que $x_1 = x_2$.*

Exemplo 1.12 *A função identidade $i: \mathbb{Z} \to \mathbb{Z}$, definida por i(x) = x é injetiva. De fato, se $i(x_1) = i(x_2) \Rightarrow x_1 = x_2$. Por outro lado, se for considerada a função $f: \mathbb{Z} \to \mathbb{Z}$, definida por $f(x)=x^2$. Então f não é injetiva, pois f(-2) = f(2), no entanto, $-2 \neq 2$.*

Definição 1.9 *Uma função $f: A \to B$ é uma bijeção ou função bijetiva se, é ao mesmo tempo uma injeção e uma sobrejeção.*

Exemplo 1.13 *A função identidade $i: \mathbb{Z} \to \mathbb{Z}$, definida por $i(x) = x$ é bijetora, pois dos Exemplos 1.11 e 1.12 segue-se que i é uma função injetiva e sobrejetiva. Por outro lado, se considerada a função $f : \mathbb{Z} \to \mathbb{Z}$, definida por $f(x)=x^2$. Segue-se do Exemplo 1.12 que f não se trata de uma função injetiva, consequentemente nem bijetiva.*

1.1.4 Conjuntos Finitos, Infinitos e Enumeráveis

Conjuntos Finitos

Definição 1.10 *Um conjunto X denomina-se finito quando ocorre um dos casos:*

a) É vazio;
b) Existe, para algum $n \in \mathbb{N}$, uma bijeção $f : I_n \to X$, onde I_n é o conjunto {1,2,3,...,n} dos números naturais $\mathbb{N}$ de 1 até n.

No primeiro caso, diz-se que o conjunto X é vazio, já no segundo caso, que o conjunto X tem n elementos ou que tem número cardinal n. Informalmente, a correspondência $f : I_n \to X$, chama-se uma contagem do conjunto X.

Lema 1.1 *Se existe uma bijeção $f : X \to Y$, então dado $a \in X$ e $b \in Y$ existe uma bijeção $g : X \to Y$ tal que $g(a) = b$.*

Prova. Se $f(a) = b$, nada a provar. No entanto, se $f(a) \neq b$, como f é sobrejetiva, existe $f^{-1}(b) \in X$ tal que $f(f^{-1}(b)) = b$, define-se a bijeção $g : X \to Y$ pondo: $g(x) = f(x)$ se $x \neq a$ e $x \neq f^{-1}(b)$, enquanto, $g(a) = b$ e $g(f^{-1}(b)) = f(a)$. □

Teorema 1.1 *Seja A um subconjunto de I_n, se existir uma bijeção $f : I_n \to A$, então $I_n = A$.*

Prova. A prova decorre-se por indução em n. Para $n = 1$, tem-se que existe uma bijeção $f : I_1 \to A$, o que implica que $f(1) = 1$, ou seja, $A = I_1 = \{1\}$. Agora, suponha que o resultado seja válido para um certo número n e considere uma bijeção $f : I_{n+1} \to A$. Fixando $a = f(n+1)$, a restrição de f a I_n fornece uma bijeção $g : I_n \to A - \{a\}$, podendo ocorrer duas situações:

1ª) Se tiver $A - \{a\} \subset I_n$, então decorre-se da hipótese de indução que $A - \{a\} = I_n$, donde $a = n + 1$ e $A = I_{n+1}$.
2ª) Se não tiver $A - \{a\} \subset I_n$, então deve-se ter $n + 1 \in A - \{a\}$, sendo assim exite $b \in I_{n+1}$ tal que $f(b) = n + 1$. Logo, decorre-se do Lema 1.1, que pode-se definir uma bijeção $h : I_{n+1} \to A$ pondo $h(x) = f(x)$ se $x \neq b$ e $x \neq n + 1$, enquanto $h(b) = a$ e $h(n + 1) = n + 1$. Agora, a restrição de h a I_n fornece uma bijeção $m : I_n \to A - \{n + 1\}$, logo $A - \{n + 1\} \subset I_n$ e pela hipótese de indução decorre-se que $A - \{n + 1\} = I_n$, donde $A = I_{n+1}$.

Conclui-se assim a demonstração. □

Corolário 1.1 *Sejam f: $I_n \to X$ e g: $I_m \to X$ duas bijeções, então $m = n$.*

Prova. Considera-se apenas o caso em que $m \leq n$, já que os demais são análogos. Nesse caso tem-se que $I_m \subset I_n$. Pondo A=I_m, do Teorema 1.1, obtém-se I_m=I_n e, portanto, $m = n$. □

Teorema 1.2 *Se X é um conjunto finito, então todo subconjunto $Y \subset X$ é finito.*

Prova.

Basta considerar o caso em que $X = I_n$. Para $n = 1$, os únicos subconjuntos possíveis de I_1 são o próprio I_1 e $\emptyset$. Logo, $Y = I_1$ ou $Y = \emptyset$ os quais são finitos.

Suponhamos que o resultado seja verdadeiro para $X = I_n$ e verifiquemos que o resultado vale para $X = I_{n+1}$. De fato:

Se $Y \subset I_n \Rightarrow Y$ é finito pela hipótese de indução.

Agora, se $n+1 \in Y \Rightarrow Y - \{n+1\} \subset I_n \Rightarrow$ Existe a bijeção $\psi : I_p \to Y - \{n+1\}$, com $p \leq n$. Seja $\varphi : I_{p+1} \to Y$ a bijeção tal que

$$\varphi(x) = \begin{cases} \psi(x), & \text{se } x \in I_p, \\ n+1, & \text{se } x = p+1. \end{cases}$$

Isto implica que Y é finito com número de elementos $\leq p+1$. Como $p \leq n$, então $p+1 \leq n+1$.

Finalmente, como não pode existir uma bijeção $f : I_n \to Y$ de um conjunto finito I_n sobre uma parte própria $Y \subset I_n$ segue que se $Y \subset I_n$, com n elementos, então $Y = I_n$.

□

Exemplo 1.14 ***O conjunto dos poliedros regulares de Platão***

Dado o conjunto R={tetraedro, hexaedro, octaedro, dodecaedro, icosaedro} pode-se facilmente estabelecer uma bijeção com o conjunto I_5={1, 2, 3, 4, 5}. Seja $r : I_5 \to R$ essa bijeção, para defini-la basta escolher a imagem em R de r(1), r(2), r(3), r(4) e r(5) que pode ser feito de 5.4.3.2.1= 120 modos, logo pode-se construir ao todo 120 bijeções. Por exemplo, pondo r(1)=tetraedro, r(2)=hexaedro, r(3)=octaedro, r(4)=dodecaedro e r(5)=icosaedro, assim o conjunto R é finito e 5 é número cardinal do conjunto R, independendo das escolhas entre as 120 bijeções (contagens) possíveis.

Conjuntos Infinitos

Definição 1.11 *O conjunto X é infinito quando não é finito, ou seja, X é infinito quando não é vazio e nem existe, para algum $n \in \mathbb{N}$, uma bijeção f: $I_n \to X$, no qual I_n=$\{1, 2, 3, ..., n\}$ com $n \in \mathbb{N}$.*

Exemplo 1.15 *Segue alguns exemplos de conjuntos infinitos:*

1) *O conjunto* $\mathbb{N}$ = *{1, 2, 3, 4, ...} dos números naturais;*
2) *O conjunto* $\mathbb{Z}$ = *{0,*$\pm$*1,* $\pm$*2,* $\pm$*3,*$\pm$*4, ...} dos números inteiros;*
3) *O conjunto* $\mathbb{Q}$ = $\{\frac{a}{b}$*; a,* $b \in \mathbb{Z}$ *e* $b \neq 0$ *} dos números racionais;*
4) *O conjunto* $\mathbb{R}$ *dos números reais;*
5) *O conjunto* $\mathbb{C} = \{z = a + b \cdot i; a, b \in \mathbb{R}\}$ *dos números complexos.*

Teorema 1.3 *Se X é um conjunto infinito, então existe uma função injetiva* $f : \mathbb{N} \to X$.

Prova. Considerando os conjuntos não vazios $A_n \subset X$, com $n \in \mathbb{N}$. Pode-se escolher $x_1 \in A_1 = X$, pois A_1 não é vazio, e ponha $x_1 = f(1)$. Da mesma forma, escolhe-se $x_2 \in A_2 = X - \{f(1)\}$, sendo que A_2 não é vazio, pois X é infinito e colocando $x_2 = f(2)$. Considerando esse processo sucessivamente tem-se que $x_n \in A_n = X - \{f(1), f(2), ..., f(n-1)\}$, com A_n não vazio, pois X é infinito e agora defina a função f:$\mathbb{N} \to X$ tal que $f(n)$= x_n. Nessas condições f é injetiva. De fato, se $a \neq b$, considere apenas o caso $a < b$, pois o caso $b < a$ é análogo, então $f(a) \in \{f(1), f(2), ..., f(b-1)\}$ porém $f(b) \in X - \{f(1), f(2), ..., f(b-1)\}$, portanto $f(a) \neq f(b)$. □

Conjuntos Enumeráveis

Definição 1.12 *Um conjunto X é enumerável quando é finito ou quando existe uma bijeção com o conjunto dos números naturais* $\mathbb{N}$. *Seja f:*$\mathbb{N} \to X$ *essa bijeção, então f denomina-se uma enumeração de X, colocando f*(1)= x_1, *f*(2)=x_2, ..., *f*(*n*)=x_n, ... *Assim,* $X=\{x_1, x_2, ..., x_n, ...\}$. *Analogamente, se X for finito e não vazio, segue-se da Definição 1.10 que existe uma bijeção* $g : I_n \to X$, *com* $n \in \mathbb{N}$, *então uma enumeração de X pode ser definida por g, colocando g*(1)= x_1, *g*(2)=x_2, ..., *g*(*n*)=x_n. *Assim,* $X=\{x_1, x_2, ..., x_n\}$.

Exemplo 1.16 *O conjunto dos números naturais pares* $2.\mathbb{N} = \{2, 4, 6, 8, ...\}$ *é enumerável, basta tomar a bijeção* $f : \mathbb{N} \to 2.\mathbb{N}$ *definida por* $f(n) = 2.n$.

Exemplo 1.17 *O conjunto* $\mathbb{Z}$ *dos inteiros* $\{..., -3, -2, -1, 0, 1, 2, 3, ...\}$ *é enumerável, basta tomar a bijeção f:*$\mathbb{N} \to \mathbb{Z}$ *definida por* $f(1) = 0$, $f(2.n) = n$ *e* $f(2.n+1) = -n$.

Teorema 1.4 *Se X é enumerável e* $Y \subset X$, *então Y é enumerável.*

Prova. Se X é enumerável e finito, então decorre-se do Teorema 1.2, que $Y \subset X$ também é finito. Logo, da Definição 1.12 segue-se que Y é enumerável. Agora, se X é enumerável e infinito, então existe uma bijeção f:$\mathbb{N} \to X$, tal que $X = \{f(1), f(2), f(3), f(4), ...\}$.

Se $Y \subset X$ for finito, então Y é enumerável. No entanto, se $Y \subset X$ for infinito, deve-se encontrar uma bijeção $g : \mathbb{N} \to Y$. Seja $A = \{a \in \mathbb{N};\ f(a) \in Y\}$. Tem-se que $A \neq \emptyset$, pois $Y \neq \emptyset$. Como $A \subset \mathbb{N}$, exite a_1 que é o menor elemento de A. Defina $g(1) = f(a_1)$. Agora, considera-se o conjunto $A_1 = \{a \in \mathbb{N};\ f(a) \in Y \text{ e } a > a_1\}$, seja a_2 o menor elemento de A_1, e defina $g(2) = f(a_2)$. Considera-se, indutivamente o conjunto $A_n = \{a \in \mathbb{N}; f(a) \in Y \ e \ a > a_n\}$, seja a_{n+1} o menor elemento de A_n, e defina $g(n+1) = f(a_{n+1})$. Dessa forma, obtém-se a bijeção $g : \mathbb{N} \to Y$, tal que $Y = \{g(1), g(2), g(3), g(4), ..., \}$, portanto Y é enumerável. □

Corolário 1.2 *Seja $f : X \to Y$ uma função injetiva. Se Y é enumerável, então X também é enumerável.*

Prova. Como $f : X \to Y$ se trata de uma função injetora, tem-se que $f : X \to f(X)$, onde $f(X)$ é o conjunto imagem de X em relação a f, é uma bijeção. Como $f(X) \subseteq Y$ e Y pela hipótese é enumerável, decorre-se do Teorema 1.4 que $f(X)$ é enumerável e, portanto, X é enumerável. □

Corolário 1.3 *Seja $f : X \to Y$ uma função sobrejetiva. Se X é enumerável, então Y também é enumerável.*

Prova. Pelo fato de $f : X \to Y$ tratar-se de uma função sobrejetiva, então para cada $y \in Y$ existe pelo menos um $x \in X$ tal que $f(x) = y$, assim para cada y escolhe-se um único elemento x_y entre os x que satisfazem a relação $f(x) = y$. Dessa forma, defini-se uma função $g : Y \to X$ dada for $g(y) = x_y$, tal que $f(g(y)) = f(x_y) = y$ para todo $y \in Y$, assim g é uma função injetiva. Como por hipótese X é enumerável, decorre do Corolário 1.2 que Y é também um conjunto enumerável. □

Corolário 1.4 *Sejam X_1, X_2, X_3, ..., X_n, ... conjuntos enumeráveis, então a reunião $X = X_1 \cup X_2 \cup X_3 \cup ... \cup X_n \cup ...$ é enumerável.*

Prova. Considere que a reunião $X = X_1 \cup X_2 \cup X_3 \cup ... \cup X_n \cup ...$ de conjuntos enumeráveis sejam disjuntas dois a dois, pois caso contrário, basta considerar os conjuntos X_1, $X_2 - X_1$, $X_3 - (X_2 \cup X_1)$,..., cuja a união é também igual a X. Como os X_n são conjuntos enumeráveis, tem-se que:

$$X_1 = \{x_{11}, x_{12}, x_{13}, x_{14}, x_{15}, x_{16}, ..\}$$
$$X_2 = \{x_{21}, x_{22}, x_{23}, x_{24}, x_{25}, x_{26}, ..\}$$
$$X_3 = \{x_{31}, x_{32}, x_{33}, x_{34}, x_{35}, x_{36}, ..\}$$

$$\ldots$$
$$X_n = \{x_{n1}, x_{n2}, x_{n3}, x_{n4}, x_{n5}, x_{n6}, ..\}$$
$$\ldots$$

Para enumerar todos os elementos da reunião $X = X_1 \cup X_2 \cup X_3 \cup \ldots \cup X_n \cup \ldots$ basta considerar o seguinte processo:

(1) Os elementos da reunião de enumeráveis $X = X_1 \cup X_2 \cup X_3 \cup \ldots \cup X_n \cup \ldots$ são alinhados de forma que a linha L_i, ficam com aqueles elementos que pertencem ao conjunto enumerável X_i com $i = 1, 2, 3, ..$;

(2) Enumeram-se esses conjuntos, tomando o primeiro elemento como x_{11}, o segundo elemento como x_{21}, o terceiro elemento como x_{12} e assim por diante, conforme o sentido das setas do esquema representado na Figura 1.5.

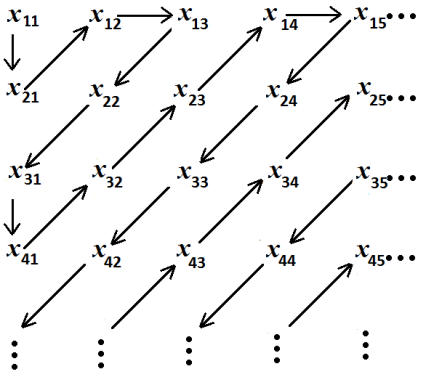

Figura 1.5: *Enumeração do conjunto* $X = X_1 \cup X_2 \cup \ldots \cup X_n \cup \ldots$.

Dessa forma, todos elemento de X estarão em correspondência com um número natural determinado, ficando assim estabelecida uma bijeção f: $\mathbb{N} \to X$. Da Definição 1.12, decorre-se que X é enumerável.

□

Exemplo 1.18 *O conjunto* $\mathbb{Q}^+$ *dos racionais positivos é enumerável. Basta para isso utilizar o método que pode ser obtido por meio dos seguintes passos:*

(1) Os racionais positivos, são alinhados de forma que a coluna R_i*, ficam com aqueles cujo o numerador seja i com* $i = 1, 2, 3, ..n, ...$*;*

(2) Enumeram-se esses racionais, tomando o primeiro elemento como $\frac{1}{1}$*, o segundo elemento como* $\frac{1}{2}$*, o terceiro elemento como* $\frac{2}{2}$ *e assim por diante, conforme o sentido das setas do esquema representado na Figura 1.6.*

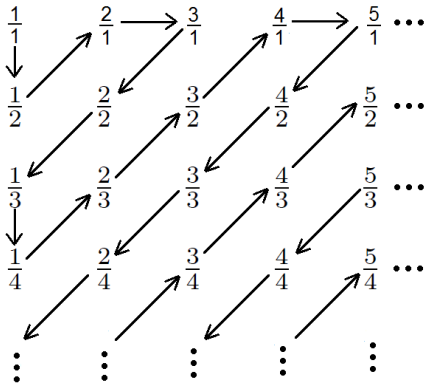

Figura 1.6: *Enumeração do conjunto* $\mathbb{Q}^+$.

Dessa forma, todos elementos do conjunto $\mathbb{Q}^+$ *estarão em correspondência com um número natural determinado. Assim, fica estabelecida uma sobrejeção* $f\colon \mathbb{N} \to \mathbb{Q}^+$ *e do Corolário 1.3, decorre-se que* $\mathbb{Q}^+$ *é enumerável. Logo, o conjunto dos números racionais* $\mathbb{Q}$ *também é um conjunto enumerável. De fato, pelo Corolário 1.3, tem-se que basta considerar a sobrejeção* $g\colon \mathbb{N} \to \mathbb{Q}$ *dada por:*

$$g(x) = \begin{cases} 0, & se\ x = 0, \\ f(n), & se\ x = 2 \cdot n - 1, \\ -f(n), & se\ x = 2 \cdot n. \end{cases}$$

1.2 Fundamentos Básicos de Álgebra Abstrata

Nesta secção tratar-se-á apenas dos aspectos necessários para o desenvolvimento deste trabalho relativos as definições de grupo, anel e corpo que são estruturas da álgebra que permitem a formalização conceitual de boa parte da matemática. Para maiores detalhes sobre o assunto, indicam-se as referências [4], [7], [10],[11], e [17].

1.2.1 Grupos

Ao longo da história nota-se que o conceito de grupo é um dos instrumentos de grande importância para a esquematização e organização de várias partes da matemática. Por exemplo, para o matemático francês Evariste Galois (1811-1832) ela foi essencial para que ele conseguisse por fim a questão da resolubilidade por radicais de equações de grau $n \geq 5$.

Definição 1.13 *Sejam G um conjunto não vazio munido de uma operação (ou lei de composição interna) denotada por* $*$*, tal que para cada a,b* $\in G$ *associa a um elemento* $a*b \in G$*. Diz-se G em relação* $*$*, ou simplesmente* $(G,*)$ *é um grupo se, e somente se, satisfazem as propriedades:*

(G_1) *ASSOCIATIVA*

Vale a propriedade associativa, ou seja:

$\forall\, a, b, c \in G,\ a*(b*c) = (a*b)*c;$

(G_2) *ELEMENTO NEUTRO*

Existe um elemento e de G, denominado elemento neutro tal que:

$\forall\, a \in G,\ a*e = e*a = a;$

(G_3) *ELEMENTO INVERSO*

Todo elemento de G é simetrizável em relação a $*$*, ou seja:*

$\forall\, a \in G,\ \exists\, a' \in G : a*a' = a'*a = e.$

Definição 1.14 *Defini-se um grupo* $(G,*)$ *como abeliano ou comutativo se, e somente se, G for comutativo em relação a operação* $*$*, ou seja:*

(G_4) *COMUTATIVO*

Dados quaisquer elementos $a,b \in G$*, vale a comutatividade, ou seja:*

$\forall\, a,b \in G,\ a*b = b*a.$

A respeito da notação $(G,*)$ para definir um grupo, quando não houver dúvidas em relação a operação $*$, esta será excluída da notação, assim usa-se apenas a G para denotar o grupo G.

Exemplo 1.19 ***Grupo aditivo dos inteiros***

Considere o conjunto dos números inteiros $\mathbb{Z}$=$\{0,\pm1,\pm2,\pm3,\pm4,\pm5,..\}$ *e a operação usual de adição, denotada por* $+$*, então o par* $(\mathbb{Z},+)$ *é um grupo, pois satisfaz as Propriedades* G_1*,* G_2 *e* G_3 *da Definição 1.13. Pelo fato, de também satisfazer a Propriedade* G_4 *da Definição 1.14, trata-se de um grupo comutativo ou abeliano.*

É interessante ressaltar que em um grupo $(G,*)$, quando o conjunto G é finito, diz-se que o par $(G,*)$ é um grupo finito.

Exemplo 1.20 ***($\mathbb{Z}_3$): grupo aditivo das classes de resto módulo 3***

Considere o conjunto $G = \{\overline{0},\overline{1},\overline{2}\}$ *e a operação usual de adição denotada por* $+$*, então o par* $(G,+)$ *é um grupo finito, pois satisfaz as Propriedades* G_1*,* G_2 *e* G_3 *da Definição 1.13 e G é um conjunto finito. Além disso, pelo fato de também satisfazer a Propriedade* G_4 *da Definição 1.14 se trata de um grupo comutativo ou abeliano. Para verificar que* $(G,+)$ *é um grupo comutativo basta considerar a tábua da operação* $+$ *no conjunto G:*

Tábua: $(G,+)$			
$+$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{0}$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{1}$	$\overline{1}$	$\overline{2}$	$\overline{0}$
$\overline{2}$	$\overline{2}$	$\overline{0}$	$\overline{1}$

Exemplo 1.21 ***Matrizes de ordem 2 com elementos inteiros***

Considere o conjunto de todas as matrizes de ordem 2 com elementos inteiros denotada por $M_2(\mathbb{Z})$ com a operação usual de adição entre matrizes, denotada aqui por $+$ e então, $(M_2(\mathbb{Z}),+)$ é um grupo comutativo, pois satisfaz as Propriedades G_1,G_2,G_3 e G_4 das Definições 1.13 e 1.14.

No entanto, ao considerar o conjunto $M_2(\mathbb{Z})$ com a operação usual de multiplicação entre matrizes, denotadas aqui por $\cdot$, a estrutura algébrica $(M_2(\mathbb{Z}),\cdot)$ não forma grupo, pois nem toda matriz de $M_2(\mathbb{Z})$ admite inverso multiplicativo, sendo assim não satisfaz a Propriedade G_3 da Definição 1.13.

1.2.2 Anéis e Anéis de Integridade

Anéis e Subanéis

Definição 1.15 *Seja A um conjunto não vazio munido de duas operações adição e multiplicação representadas respectivamente por $+$ e $\cdot$. A estrutura algébrica $(A,+,\cdot)$ é denominada anel se, e somente se, satisfaz as seguintes propriedades:*

(1) *O conjunto A é um grupo abeliano em relação a adição, ou seja, satisfaz as Propriedades G_1, G_2, G_3 e G_4 das Definições 1.13 e 1.14.*

(2) O conjunto A, em relação a multiplicação satisfaz as propriedades:

(M_1) *ASSOCIATIVA*
Vale a propriedade associativa, ou seja:
$\forall\ a, b, c \in A,\ a\cdot(b\cdot c) = (a\cdot b)\cdot c;$

(M_2) *A MULTIPLICAÇÃO É DISTRIBUTIVA EM RELAÇÃO À ADIÇÃO*
$\forall\ a, b, c \in A,\ a\cdot(b+c) = a\cdot b + a\cdot c\ .$

A respeito da notação $(A,+,\cdot)$ para definir um anel, quando não houver dúvidas em relação as operações $+$ e $\cdot$, opta-se pela exclusão dessas da notação, assim usa-se apenas a notação A para denotar o anel.

Exemplo 1.22 *$(\mathbb{Z},+,\cdot)$, $(\mathbb{Q},+,\cdot)$, $(\mathbb{R},+,\cdot)$ e $(\mathbb{C},+,\cdot)$ são anéis, onde $+$ e $\cdot$ são respectivamente as operações usuais de adição e multiplicação.*

Definição 1.16 *Seja $(A,+,\cdot)$ um anel e S um subconjunto não vazio de A. Diz-se que $(S,+,\cdot)$ é subanel de A se:*

(1) *o conjunto S é fechado para as operações $+$ e $\cdot$ de A, ou seja:*
$\forall\ a, b \in A \Rightarrow a+b \in S$ *e* $a\cdot b \in S;$

(2) *a estrutura $(S,+,\cdot)$ é também um anel, sendo que a adição e multiplicação são as mesmas do anel $(A,+,\cdot)$.*

Exemplo 1.23 ***Subanel*** $n\mathbb{Z}$***, com n inteiro não nulo.***

Considere o conjunto $n\mathbb{Z}=\{0,\pm 1\cdot n,\pm 2\cdot n,\pm 3\cdot n,\pm 4\cdot n,\pm 5\cdot n,...\}$ *com n sendo um inteiro não nulo e as operações de adição e multiplicação usuais entre os inteiros, tem-se que* $(n\mathbb{Z},+,\cdot)$ *é um subanel do anel* $(\mathbb{Z},+,\cdot)$.

Anéis Comutativos e Anéis com Unidade

Definição 1.17 *Considere o anel* $(A,+,\cdot)$*, diz-se que esse anel é comutativo se a multiplicação for comutativa, ou seja:*

$$\forall\ a,b\in A,\ a\cdot b=b\cdot a.$$

Definição 1.18 *O anel* $(A,+,\cdot)$ *é denominado um anel com unidade, se o mesmo contiver um elemento neutro para multiplicação, ou seja;*

$$\forall a\in A,\ \exists 1\in A;\ a\cdot 1=1\cdot a=a.$$

Exemplo 1.24 *Os anéis* $(\mathbb{Z},+,\cdot)$, $(\mathbb{Q},+,\cdot)$, $(\mathbb{R},+,\cdot)$ *e* $(\mathbb{C},+,\cdot)$ *são anéis comutativos, pois em todos a multiplicação é comutativa além de que, são anéis com unidade, pois têm o número 1 como unidade.*

Exemplo 1.25 *Os anéis* $M_n(A)$*, em que A indica* $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ *ou* $\mathbb{C}$*, se* $n>1$*, não são comutativos, pois em ambos casos não se tem obrigatoriamente* $A\cdot B=B\cdot A$*, ou seja, é possível encontrar matrizes A e B tais que* $A\cdot B\neq B\cdot A$*, para isso basta tomar como exemplo as matrizes:*

$$A=\begin{pmatrix} 1 & 1 & ... & 1\\ 0 & 1 & ... & 1\\ .... & .... & .... & ....\\ 0 & 0 & ... & 1 \end{pmatrix}\ e\ \ B=\begin{pmatrix} 1 & 0 & ... & 0\\ 1 & 1 & ... & 0\\ .... & .... & .... & ....\\ 1 & 1 & ... & 1 \end{pmatrix}.$$

No entanto, esses anéis são anéis com unidade, cuja a unidade desses é a matriz identidade

$$I_n=\begin{pmatrix} 1 & 0 & ... & 0\\ 0 & 1 & ... & 0\\ .... & .... & .... & ....\\ 0 & 0 & ... & 1 \end{pmatrix}.$$

Anéis de Integridade

Definição 1.19 *Se a e b são elementos não nulos de um anel* $(A,+,\cdot)$ *tais que* $a\cdot b=0$ *ou* $b\cdot a=0$*, sendo 0 o elemento neutro de A em relação a adição, diz-se que a e b são divisores próprios do zero em A.*

Exemplo 1.26 (Anel Z_4**)** *Considere o anel* $(Z_4,+,\cdot)$*, tem-se que* $\overline{2}$ *é um divisor próprio de zero em* Z_4 *, pois* $\overline{2}\cdot\overline{2}=\overline{0}$*, conforme a tábua de* Z_4 *abaixo:*

Tábua de Z_4				
$\cdot$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{2}$	$\overline{0}$	$\overline{2}$	$\overline{0}$	$\overline{2}$
$\overline{3}$	$\overline{0}$	$\overline{3}$	$\overline{2}$	$\overline{1}$

.

Definição 1.20 *Considere um anel comutativo com unidade* $(A,+,\cdot)$*, defini-se esse anel como anel de integridade ou domínio integridade se a seguinte afirmação for verdadeira:*

$$\forall\ a,b\in A,\ a\cdot b=0 \text{ ou } b\cdot a=0 \Rightarrow a=0 \text{ ou } b=0.$$

A afirmação acima é conhecida como a lei do anulamento do produto. Em outras palavras $(A,+,\cdot)$ *é um anel de integridade se, e somente se,* $(A,+,\cdot)$ *for um anel comutativo com unidade que não possui divisores próprios de zero.*

Exemplo 1.27 *Os anéis* $(\mathbb{Z},+,\cdot)$*,* $(\mathbb{Q},+,\cdot)$*,* $(\mathbb{R},+,\cdot)$ *e* $(\mathbb{C},+,\cdot)$ *são anéis de integridade.*

1.2.3 Corpo

Corpo

Conforme mencionado anteriormente, os anéis $(\mathbb{Z},+,\cdot)$ e $(\mathbb{Q},+,\cdot)$ são ambos anéis de integridade. Seja $U(A)$ o conjunto formado pelos elementos de A que possuem simétrico multiplicativo então: $U(\mathbb{Z})=\{-1,1\}$ e $U(\mathbb{Q})=\mathbb{Q}-\{0\}$.

Note que enquanto o anel $(\mathbb{Z},+,\cdot)$ possui apenas dois elementos que possuem inversos multiplicativos, no anel $(\mathbb{Q},+,\cdot)$ todo número racional não nulo admite simétrico multiplicativo, tal diferença motiva a definição:

Definição 1.21 *Um anel* $(K,+,\cdot)$ *comutativo com unidade recebe o nome de corpo se todo elemento não nulo de K admite simétrico multiplicativo, ou seja:*

$$\forall\ a\in K,\ a\neq 0 \Rightarrow \exists\ b\in K;\ a\cdot b = 1.$$

A respeito da notação $(K,+,\cdot)$ para definir um corpo, quando não houver dúvidas em relação as operações $+$ e $\cdot$, estas serão excluídas da notação, assim usa-se-á a notação K para definir corpo.

Exemplo 1.28 *Os anéis numéricos* $(\mathbb{Q},+,\cdot)$, $(\mathbb{R},+,\cdot)$ *e* $(\mathbb{C},+,\cdot)$ *são corpos, pois em ambos todos os seus elementos não nulos admitem inversos multiplicativos. No entanto, o anel* $(\mathbb{Z},+,\cdot)$ *não é um corpo pois, apenas os seus elementos* 1 *e* -1 *admitem inversos multiplicativos.*

Proposição 1.1 *Se* $(K,+,\cdot)$ *é um corpo, então* $(K,+,\cdot)$ *é também um anel de integridade.*

Prova. Sendo $(K,+,\cdot)$ um corpo, para mostrar que este também é um anel de integridade deve-se evidenciar que o mesmo satisfaz a lei do anulamento do produto, citada na Definição 1.20. Sejam $a,b \in K$ tais que $a \cdot b = 0$. Supondo, por exemplo, que $b \neq 0$, logo b é inversível, ou seja, existe $b^{-1} \in K$ tal que $b \cdot b^{-1} = 1$. Multiplicando os dois membros da igualdade $a \cdot b = 0$ por b^{-1} tem-se: $a \cdot b \cdot b^{-1} = 0.b^{-1} = 0$. Como $b \cdot b^{-1} = 1$ então: $a \cdot b \cdot b^{-1} = a \cdot 1 = a = 0$, ou seja $a = 0$. Analogamente, mostra-se que, quando $a \neq 0$, então $b = 0$. Logo o produto de dois fatores de K não pode ser nulo sem que um deles não o seja, o que demonstra que $(K,+,\cdot)$ é um anel de integridade. □

A recíproca da Proposição 1.1 não é verdadeira, pois conforme citado no Exemplo 1.28, o anel $(\mathbb{Z},+,\cdot)$ é um anel de integridade mas não é um corpo.

Proposição 1.2 *Seja* $(K,+,\cdot)$ *um corpo, então:*

(1) *As seguintes propriedades decorrem-se das Propriedades* G_1, G_2, G_3 *e* G_4 *das Definições 1.13 e 1.14:*

   a) *O elemento neutro aditivo é único;*
   b) *Para todo* $x \in K$, *o seu simétrico* $(-x)$ *é único e além disso tem-se que* $-(-x) = x$;
   c) *Vale a lei do corte, ou seja:*
   $\forall\, a,b,c \in A, b+c = a+c \Rightarrow b = c.$

(2) *As seguintes propriedades decorrem-se da Propriedade* M_1 *da Definição 1.15 e das Definições 1.17, 1.18 e 1.21:*

   a) *O elemento neutro multiplicativo é único;*
   b) *Para todo* $x \in K$, $x \neq 0$, *o seu inverso multiplicativo* x^{-1} *é único e além disso,* $(x^{-1})^{-1} = x$;
   c) *Vale a lei do corte, ou seja:*
   $\forall\, a,b,c \in A, a \cdot b = a \cdot c \Rightarrow b = c.$

Corpo Ordenado

Definição 1.22 *Um corpo $(K,+,\cdot)$ é ordenado se nele está contido um subconjunto próprio $P \subset K$, que satisfaz as seguintes condições:*

- (P_1) *Dados $x,y \in P$, tem-se: $x+y \in P$ e $x \cdot y \in P$, ou seja, P é fechado em relação a adição " $+$ " e a multiplicação " $\cdot$ ";*
- (P_2) *Dados $x \in K$, tem-se que exatamente uma das três alternativas ocorre: ou $x = 0$ ou $x \in P$ ou $-x \in P$, sendo que 0 é o elemento neutro da adição.*

Se $(K,+,\cdot)$ é um corpo ordenado, pode-se formar o conjunto $-P = \{-x; x \in P\}$ e assim obter:

$$K = P \cup \{0\} \cup -P.$$

Note que os conjuntos P, $\{0\}$ e $-P$ são dois a dois disjuntos.

Definição 1.23 *Sejam a e b elementos de um corpo ordenado $(K,+,\cdot)$ e $P \subset K$ é um subconjunto que satisfaz as Propriedades P_1 e P_2 da Definição 1.22. Diz-se que a " é menor do que " b, denotado por $a < b$ quando, $b-a \in P$. Diz-se a " é maior do que " b, denotado por $a > b$, quando $a-b \in P$.*

As relação $a < b$ e $a > b$ são as relações de ordem em $(K,+,\cdot)$.

Proposição 1.3 *A relação de ordem $a < b$ em $(K,+,\cdot)$ goza das seguintes propriedades:*

- (O_1) *TRANSITIVIDADE*
  $\forall\, a,b,c \in K$, $a < b$ *e* $b < c \Rightarrow a < c$;
- (O_2) *TRICOTOMIA*
  Dados $a,b \in K$, tem-se que exatamente uma das três alternativas ocorre: ou $a = b$ ou $a < b$ ou $b < a$;
- (O_3) *MONOTONICIDADE DA ADIÇÃO*
  $\forall\, a,b,c \in K$, $a < b \Rightarrow a+c < b+c$;
- (O_4) *MONOTONICIDADE DA MULTIPLICAÇÃO*
  $\forall\, a,b,c \in K$ *com* $0 < c$, $a < b \Rightarrow a \cdot c < b \cdot c$;
  No entanto se: $\forall\, a,b,c \in K$ *com* $c < 0$, $a < b \Rightarrow b \cdot c < a \cdot c$.

Prova. Considera-se $a,b,c \in K$ e o subconjunto $P \subset K$ que satisfaz as Propriedades P_1 e P_2 da Definição 1.22 então:

- (O_1) Como $a < b$ e $b < c$ então $(b-a),(c-b) \in P$. Logo, $(b-a)+(c-b) \in P$. Como $(b-a)+(c-b) = (c-a)$, decorre-se que $(c-a) \in P$ e portanto $a < c$.

(O_2) Considere $a,b \in K$ e sendo K um corpo ordenado, então ocorre um e somente um dos três casos abaixo:
(i) $a-b=0 \Rightarrow a=b$;
(ii) $a-b \in P \Rightarrow b<a$;
(iii) $-(a-b) \in P \Rightarrow b-a \in P \Rightarrow a<b$.

(O_3) Sendo $a<b$, então $b-a \in P$. Como 0 é elemento neutro da adição e $0=c+(-c)$ tem-se que:

$$b+0-a \in P \Rightarrow b+c+(-c)-a \in P \Rightarrow b+c-(a+c) \in P \Rightarrow a+c<b+c.$$

(O_4) Considerando $a<b$, segue-se que $b-a \in P$. Há que se dividir em dois casos:

1º Caso: Se $0<c$, então $c \in P$. Logo,

$$(b-a)\cdot c \in P \Rightarrow b\cdot c - a\cdot c \in P \Rightarrow a\cdot c < b\cdot c.$$

2º Caso: Se $c<0$, então $-c \in P$. Logo,

$$(b-a)\cdot(-c) \in P \Rightarrow a\cdot c - b\cdot c \in P \Rightarrow b\cdot c < a\cdot c.$$

□

A relação de ordem $a>b$ em $(K,+,\cdot)$ de maneira análoga também satisfaz as Propriedades O_1,O_2, O_3 e O_4 da Proposição 1.3.

Exemplo 1.29 *O corpo $(\mathbb{Q},+,\cdot)$ é um corpo ordenado.*

De fato, considere o subconjunto dos números racionais positivos denotado por $\mathbb{Q}^+=\{\frac{a}{b};\ a,b \in \mathbb{N}\}$. Para provar que $(\mathbb{Q},+,\cdot)$ é um corpo ordenado deve-se verificar as Propriedades P_1 e P_2 dadas na Definição 1.22. Para isso considere dois elementos quaisquer $x,y \in \mathbb{Q}^+$, ou seja, $x=\frac{a}{b}$ e $y=\frac{c}{d}$ com a,b,c e $d \in \mathbb{N}$.

(P_1)

Tem-se que $x+y=\frac{a}{b}+\frac{c}{d}=\frac{a\cdot d+c\cdot b}{b\cdot d}$. Como $(a\cdot d+c\cdot b),b\cdot d \in \mathbb{N}$ então $x+y \in \mathbb{Q}^+$. Já para o produto $x\cdot y$ temos que $x\cdot y=\frac{a}{b}\cdot\frac{c}{d}=\frac{a\cdot c}{b\cdot d}$. Como $a\cdot c, b\cdot d \in \mathbb{N}$ então $x\cdot y \in \mathbb{Q}^+$. Logo $\mathbb{Q}^+$ é fechado com relação a adição e a multiplicação.

(P_2)

Sejam $\frac{a}{b} \in \mathbb{Q}$, segue-se que $a,b \in \mathbb{Z}$, com $b \neq 0$. Então, tem-se três possibilidades $a\cdot b=0$, $a\cdot b>0$ ou $a\cdot b<0$. No 1^o caso, $a=0$. Logo, $\frac{a}{b}=0$, visto que $b \neq 0$. Já o 2^o caso torna $\frac{a}{b} \in \mathbb{Q}^+$ e no 3^o caso, $-\frac{a}{b} \in \mathbb{Q}^+$.

Proposição 1.4 *Sejam $(K,+,\cdot)$ um corpo ordenado e $P \subset K$ um subconjunto que satisfaz as Propriedades P_1 e P_2 da Definição 1.22. Se $a \neq 0$ e $a \in K$, então $a^2 \in P$.*

Prova. Como $a \neq 0$, então da Propriedade P_2 segue-se que $a \in P$ ou $-a \in P$. Assim, da Propriedade P_1 segue-se-se que $a \cdot a \in P$ ou $(-a) \cdot (-a) \in P$. Como $a \cdot a = (-a) \cdot (-a)$, decorre-se que: $a \cdot a = a^2 \in P$. □

Proposição 1.5 *Se $(K, +, \cdot)$ é um corpo ordenado e $P \subset K$ é um subconjunto que satisfaz as Propriedades P_1 e P_2 da Definição 1.22, então o elemento neutro da multiplicação, denotado por 1, é um elemento de P.*

Prova. Como $(K, +, \cdot)$ é um corpo tem-se que os elementos neutros da adição e da multiplicação são distintos, ou seja, $1 \neq 0$. Suponha, por absurdo, que $1 \notin P$. Então, da Propriedade P_2 segue-se que $-1 \in P$. Assim, da Propriedade P_1 decorre-se que $(-1) \cdot (-1) = 1 \in P$, o que é uma contradição. Portanto, $1 \in P$. □

Exemplo 1.30 *O corpo $(\mathbb{C}, +, \cdot)$ não é ordenado pois, se fosse existiria $P \subset \mathbb{C}$ satisfazendo as Propriedades P_1 e P_2 da Definição 1.22. Como, 1 é o elemento neutro da multiplicação de $\mathbb{C}$, $i \in \mathbb{C}$ e $i \neq 0$ então $i \in P$ ou $-i \in P$. Se ocorresse $i \in P$ teria-se $i \cdot i = -1 \in P$ o que contraria a Proposição 1.5, pois da Propriedade P_2 teria-se que $1 \notin P$. Se ocorresse $-i \in P$ teria-se $(-i) \cdot (-i) = -1 \in P$, novamente uma contradição. Portanto, $(\mathbb{C}, +, \cdot)$ não pode ser um corpo ordenado.*

Corpo Ordenado Completo

Definição 1.24 *Seja $(K, +, \cdot)$ um corpo ordenado e $A \subset K$. A é limitado superiormente se existe um $c \in K$ tal que $x \leq c$, para todo $x \in A$, nesse caso c é denominado cota superior de A. A menor das cotas superiores de um conjunto A limitado superiormente é denominada supremo do conjunto A, denotado por sup(A).*

Definição 1.25 *Seja $(K, +, \cdot)$ um corpo ordenado e $A \subset K$. A é limitado inferiormente se existe um $c \in K$, tal que $x \geq c$, para todo $x \in A$, nesse caso c é denominado cota inferior do conjunto A. Já a maior das cotas inferiores de um conjunto A limitado inferiormente é denominada ínfimo do conjunto A, denotado por inf(A).*

Definição 1.26 *Seja $(K, +, \cdot)$ um corpo ordenado e $A \subset K$. Quando A for limitado superiormente e inferiormente, diz-se que A é um conjunto limitado.*

Exemplo 1.31 *Considere o conjunto $A = \{2 - \frac{1}{n}; n \in \mathbb{N}\} \subset \mathbb{R}$. Nesse conjunto tem-se que inf(A)=1 e sup(A)=2.*

Teorema 1.5 *Seja $(K, +, \cdot)$ um corpo ordenado infinito. Tem-se que as afirmações abaixo são equivalentes:*

1) $\mathbb{N} \subset K$ *não é limitado superiormente.*

2) Para quaisquer $a,b \in K$*, com* $a > 0$ *existe* $n \in \mathbb{N}$ *tal que* $b < n \cdot a$*.*

3) Para qualquer $a \in K$*, com* $a > 0$ *existe* $n \in \mathbb{N}$ *tal que* $0 < \frac{1}{n} < a$*.*

Prova.

(1)⇒ (2): como $\mathbb{N} \subset K$ não é limitado superiormente e K é um corpo ordenado infinito, dados $a,b \in K$, com $a > 0$, existem $a^{-1} \in K$ e $n \in \mathbb{N}$ tais que:

$$a^{-1} \cdot a = 1 \text{ e } b \cdot a^{-1} < n \Rightarrow b \cdot a^{-1} \cdot a < n \cdot a \Rightarrow b < n \cdot a.$$

(2) ⇒ (3): de (2) tem-se que dado um $1, a \in K$, com $a > 0$, existe um $n \in \mathbb{N}$ tal que $1 < a \cdot n$. E ainda, como K é um corpo ordenado infinito, existe $n^{-1} \in K$ tal que $n^{-1} > 0$ e $n \cdot n^{-1} = 1$. Então:

$$1 < a \cdot n \Rightarrow 1 \cdot n^{-1} < a \cdot n \cdot n^{-1} \Rightarrow 0 < \frac{1}{n} < a.$$

(3) ⇒ (1): de (3) tem-se que dado qualquer $b \in K$, com $b > 0$, existe um $n \in \mathbb{N}$ tal que $\frac{1}{n} < \frac{1}{b}$. E ainda, como K é um corpo ordenado infinito, segue-se que $\frac{1}{n} \cdot n = 1$ e $\frac{1}{b} \cdot b = 1$. Então:

$$\frac{1}{n} < \frac{1}{b} \Rightarrow \frac{1}{n} \cdot n \cdot b < \frac{1}{b} \cdot n \cdot b \Rightarrow b < n \Rightarrow n > b.$$

Logo, nenhum elemento em K pode ser cota superior de $\mathbb{N}$. Então, $\mathbb{N}$ não é limitado superiormente. □

Definição 1.27 *Se um corpo ordenado* $(K,+,\cdot)$ *satisfazer uma das propriedades do Teorema 1.5, diz-se que* $(K,+,\cdot)$ *é um corpo Arquimediano.*

Exemplo 1.32 *O conjunto dos números racionais* $\mathbb{Q}$ *é um corpo arquimediano. De fato, para qualquer* $r = \frac{a}{b} \in \mathbb{Q}$ *e* $r = \frac{a}{b} > 0$*, com* $a,b \in \mathbb{N}$*, existe* $n = b+1 \in \mathbb{N}$ *tal que* $0 < \frac{1}{b+1} < \frac{a}{b}$*. Logo, decorre-se da Propriedade (3) do Teorema 1.5 e da Definição 1.27 que* $\mathbb{Q}$ *é um corpo arquimediano.*

Definição 1.28 *Um corpo K é dito completo se todo o subconjunto não vazio* $A \subset K$*, que é limitado superiormente, possui supremo em K.*

Proposição 1.6 *Todo corpo ordenado completo é arquimediano.*

Prova. Suponha, por absurdo, que o corpo ordenado completo K não seja arquimediano, então $\mathbb{N} \subseteq K$ é limitado superiormente. Se $b \in K$ é uma cota superior de $\mathbb{N}$, então $n+1 \leq b$ para todo $n \in \mathbb{N}$, mas assim tem-se que $b-1$ é também uma cota de superior de $\mathbb{N}$. Como

$b-1 < b$ segue que $\mathbb{N}$ não tem supremo, o que contradiz o fato do corpo ser completo. □

A existência de um corpo ordenado completo pode ser verificada através da expansão dos números racionais para os números reais. Podendo ser feita de várias maneiras. Por exemplo, construindo os números reais através do processo de cortes de Dedekind, ou das sequências de Cauchy (devido a Cantor). No entanto, a existência de dois corpos ordenados completos totalmente distintos não é possível, pois no máximo eles se diferem apenas pela natureza de seus elementos, mas não da maneira que se comportam ([13], pp. 59-61). Então, com intuito de estudar as propriedades de um corpo ordenado e completo, pode-se optar em garantir sua existência através do Axioma 1.1.

Axioma 1.1 (Axioma do Supremo) *Todo subconjunto* $\mathbb{R}$ *que é não vazio e limitado superiormente possui supremo em* $\mathbb{R}$.

Exemplo 1.33 *Decorre da Definição 1.28 e do Axioma 1.1 que* $(\mathbb{R}, +, \cdot)$ *é um corpo*

CAPÍTULO 2

Números Reais

Neste capítulo inicialmente estuda-se o que significa afirmar que "$\mathbb{R}$ é um corpo ordenado e completo" dando ênfase as suas propriedades e consequências sob o ponto de vista das teorias de álgebra e de análise. Posteriormente será abordado a correspondência entre os reais e reta real e ainda a representação decimal dos números reais. Os resultados apresentados neste capítulo poderão ser encontrados em [1], [4], [6], [13], [16], [19] e [20].

2.1 Números Reais como um corpo ordenado e completo

2.1.1 O corpo dos reais

Como $(\mathbb{R},+,\cdot)$ se trata de um anel comutativo com unidade onde todo elemento não nulo possui inverso multiplicativo, ou seja, U($\mathbb{R}$)= $\mathbb{R}-\{0\}$, sendo U($\mathbb{R}$) o conjunto formado pelos elementos não nulos de $\mathbb{R}$ que possuem simétrico multiplicativo, decorre da Definição 1.21 que $(\mathbb{R},+,\cdot)$ é um corpo.

Tem-se que o conjunto $\mathbb{R}$ é munido de duas operações denominadas adição e multiplicação, representadas respectivamente por $+$ e $\cdot$. A adição faz corresponder a cada par $a, b \in \mathbb{R}$, sua soma $a+b \in \mathbb{R}$, enquanto a multiplicação faz com que esses elementos sejam associados ao seu produto $a \cdot b \in \mathbb{R}$.

A estrutura algébrica $(\mathbb{R},+,\cdot)$ satisfaz as seguintes propriedades:

(1) A estrutura $(\mathbb{R},+)$ é um grupo comutativo, ou seja, o conjunto $\mathbb{R}$ em relação a adição satisfaz as Propriedades G_1, G_2, G_3 e G_4 das Definições 1.13 e 1.14;

(2) O conjunto $\mathbb{R}$ em relação a operação multiplicação satisfaz as seguintes propriedades:

(C_1) ASSOCIATIVA

Vale a propriedade associativa, ou seja:

$\forall\, a,b,c \in \mathbb{R},\ a \cdot (b \cdot c) = (a \cdot b) \cdot c$;

(C_2) COMUTATIVO

Dados quaisquer elementos a e b de $\mathbb{R}$, vale a comutatividade, ou seja:

$\forall\, a,b \in \mathbb{R},\ a \cdot b = b \cdot a$;

(C_3) ELEMENTO NEUTRO

Existe um elemento 1 de $\mathbb{R}$, denominado elemento neutro tal que:

$\forall\, a \in \mathbb{R},\ a \cdot 1 = 1 \cdot a = a$;

(C_4) ELEMENTO INVERSO

Todo elemento não nulo de $\mathbb{R}$, admite simétrico em relação a operação $\cdot$, ou seja:

$\forall\, a \in \mathbb{R}$ e $a \neq 0,\ \exists\, a^{-1} \in \mathbb{R},\ a \cdot a^{-1} = a^{-1} \cdot a = 1$;

(3) Vale no conjunto $\mathbb{R}$ a distributividade da multiplicação em relação a adição.

(C_5) DISTRIBUTIVA

Para todos $a,b,c \in \mathbb{R}$, tem-se: $a \cdot (b+c) = a \cdot b + a \cdot c$.

Veja alguns exemplos de propriedades algébricas básicas de $\mathbb{R}$ que são consequências diretas do fato de $(\mathbb{R},+,\cdot)$ ser um corpo, tais propriedades podem ser deduzidas das propriedades que definem um corpo.

Propriedade 2.1 (Unicidade do elemento neutro) *Os elementos neutros da adição e da multiplicação do corpo* $(\mathbb{R},+,\cdot)$ *são únicos.*

Prova. Inicialmente para provar o caso do elemento neutro da adição suponha, por absurdo, que existam dois elementos neutros distintos 0 e $0^{'}$. Segue-se da Propriedade G_2 da Definição 1.13 que: para o elemento neutro 0, $\forall a \in \mathbb{R}$, $a+0=a$, pondo $a = 0^{'} \Rightarrow 0^{'}+0 = 0^{'}$, e por outro lado, para o elemento neutro $0^{'}$, $\forall a \in \mathbb{R}, a+0^{'} = a$, pondo $a = 0 \Rightarrow 0+0^{'} = 0$. Assim, da Propriedade G_4 da Definição 1.14 decorre que: $0^{'}+0 = 0+0^{'} \Rightarrow 0^{'} = 0$, contradição, pois por hipótese $0^{'} \neq 0$. Portanto, o elemento neutro da adição é único. De modo análogo, das Definições 1.17 e 1.18 conclui-se que o elemento neutro da multiplicação é também único. □

Propriedade 2.2 (Unicidade do simétrico) *Os simétricos em relação a adição e multiplicação de um número x do corpo* $(\mathbb{R},+,\cdot)$*, desde que existam, são únicos.*

Prova. Para provar o caso do simétrico em relação a adição suponha, por absurdo, que existam em $\mathbb{R}$ dois elementos simétricos aditivos distintos $(-a)$ e $(-a)^{'}$ do elemento $a \in \mathbb{R}$. Tem-se da Propriedade G_3 da Definição 1.13 que: $a+(-a) = 0$ e $a+(-a)^{'} = 0$. Assim, das Propriedades G_1 e G_2 da Definição 1.13 decorre-se que:

$$(-a) = (-a)+0 = (-a)+(a+(-a)^{'}) = ((-a)+a)+(-a)^{'} = 0+(-a)^{'} = (-a)^{'},$$

contradição, pois por hipótese $(-a) \neq (-a)'$. Portanto, o elemento simétrico da adição é único. De modo análogo, conclui-se a unicidade do elemento simétrico da multiplicação. □

Propriedade 2.3 (Lei do Corte para a adição) *Dados a, b e $c \in \mathbb{R}$, tem-se:*

$$a+b=a+c \Rightarrow b=c.$$

Prova. Como $a \in \mathbb{R}$, então decorre-se da Propriedade G_3 da Definição 1.13 que existe um elemento $(-a) \in \mathbb{R}$ tal que $a+(-a)=0$, para provar que vale a lei do corte para adição basta somar o elemento $(-a)$ em ambos membros da equação $a+b=a+c$, ou seja: $a+b+(-a)=a+c+(-a)$. Assim, das Propriedades G_2 e G_4 das Definições 1.13 e 1.14 decorre-se que:

$$a+b+(-a)=a+c+(-a) \Rightarrow a+(-a)+b=a+(-a)+c \Rightarrow 0+b=0+c \Rightarrow b=c.$$

□

Propriedade 2.4 (Lei do Corte para a multiplicação) *Dados a, b e $c \in \mathbb{R}$, com $a \neq 0$, tem-se que:*

$$a \cdot b = a \cdot c \Rightarrow b = c.$$

Prova. Como $a \in \mathbb{R}$ com $a \neq 0$, então decorre-se da Definição 1.21 que existe um elemento $a^{-1} \in \mathbb{R}$ tal que $a \cdot a^{-1} = 1$, para provar que vale a lei do corte para multiplicação basta multiplicar o elemento a^{-1} em ambos membros da equação $a \cdot b = a \cdot c$, ou seja:

$$a \cdot b \cdot a^{-1} = a \cdot c \cdot a^{-1}.$$

Assim, segue-se da Definição 1.17 que:

$$a \cdot b \cdot a^{-1} = a \cdot c \cdot a^{-1} \Rightarrow a \cdot a^{-1} \cdot b = a \cdot a^{-1} \cdot c \Rightarrow b = c.$$

□

Propriedade 2.5 (Elemento absorvente da multiplicação) *Existe $0 \in \mathbb{R}$ tal que para todo elemento $a \in \mathbb{R}$, tem-se que $a \cdot 0 = 0$.*

Prova. Seja $a \in \mathbb{R}$. Segue-se da Propriedade G_2 da Definição 1.13 e da Definição 1.18 que: $a+0=a$ e $a \cdot 1 = a$. Assim, da Propriedade M_2 da Definição 1.15 segue-se que: $a = a \cdot 1 = a \cdot (1+0) = a \cdot 1 + a \cdot 0 = a + 0$. Logo, pela lei do corte tem-se que: $a \cdot 0 = 0$. □

Propriedade 2.6 (Regras de sinais) *Qualquer que sejam a e $b \in \mathbb{R}$, tem-se que:*

1) $a \cdot (-b) = (-a) \cdot b = -(a \cdot b)$,
2) $(-a) \cdot (-b) = a \cdot b$.

Prova.

1) Sejam $a, b \in \mathbb{R}$. Decorre-se da Propriedade M_2 da Definição 1.15 e da Propriedade G_3 da Definição 1.13 que:

$$\begin{aligned}(-a) \cdot b + a \cdot b &= (-a + a) \cdot b \\ \Rightarrow (-a) \cdot b + a \cdot b &= (0) \cdot b \\ \Rightarrow (-a) \cdot b + a \cdot b &= 0 \\ \Rightarrow (-a) \cdot b &= -(a \cdot b).\end{aligned}$$

De modo análogo, conclui-se que $a \cdot (-b) = -(a \cdot b)$. Portanto:

$$a \cdot (-b) = (-a) \cdot b = -(a \cdot b).$$

2) Do item (1) decorre-se que:

$$(-a) \cdot (-b) = -[a \cdot (-b)] = -[-(a \cdot b)] = a \cdot b.$$

□

Propriedade 2.7 *A equação $a + x = b$ tem solução única.*

Prova. Seja $x = (-a) + b$, então: $a + x = a + ((-a) + b) = (a + (-a)) + b = 0 + b = b$. Logo $(-a) + b$ é solução da equação. Suponha, por absurdo, que existam duas soluções distintas x_1 e x_2 para equação, então: $a + x_1 = b$ e $a + x_2 = b \Rightarrow a + x_1 = a + x_2 \Rightarrow x_1 = x_2$, contradição, pois por hipótese $x_1 \neq x_2$. Portanto, a solução é única. □

Propriedade 2.8 *Se dois números reais a,b têm quadrados iguais, então $a = \pm b$.*

Prova. Sejam $a, b \in \mathbb{R}$ tal que $a^2 = b^2$, então da Propriedade G_3 da Definição 1.13 decorre-se a existência em $\mathbb{R}$ do simétrico aditivo de b^2, somando esse elemento em ambos membros da igualdade tem-se que:

$$a^2 + (-(b^2)) = b^2 + (-(b^2)) \Rightarrow a^2 + (-(b^2)) = 0.$$

Assim, $a^2 + (-(b^2)) = (a + b).(a - b) \Rightarrow (a + b).(a - b) = 0$. Como $(\mathbb{R}, +, \cdot)$ é um corpo decorre-se da Proposição 1.1 que o mesmo é um anel de integridade. Logo, não possui divisores próprios de zero. Portanto, $a + b = 0$ ou $a - b = 0 \Rightarrow a = b$ ou $a = -b$.

□

2.1.2 O corpo ordenado dos reais

O corpo $(\mathbb{R},+,\cdot)$ é um copo ordenado, pois conforme a Definição 1.22, existe um subconjunto próprio $\mathbb{R}^+ \subset \mathbb{R}$ tal que satisfaz as seguintes propriedades:

(1) Dados $x,y \in \mathbb{R}^+$, tem-se que: $x+y \in \mathbb{R}^+$ e $x\cdot y \in \mathbb{R}^+$, ou seja, $\mathbb{R}^+$ é fechado em relação a adição e a multiplicação;
(2) Dados $x \in \mathbb{R}$, ocorre exatamente uma das três alternativas: ou $x=0$ ou $x \in \mathbb{R}^+$ ou $-x \in \mathbb{R}^+$, onde 0 é o elemento neutro da adição.

Como consequência do fato acima, o conjunto dos números reais pode ser escrito como a união de três conjuntos dois a dois disjuntos, bastando indicar como $\mathbb{R}^- = \{-x; x \in \mathbb{R}^+\}$ e os elementos desse conjunto são denominados números negativos, assim:

$$\mathbb{R} = \mathbb{R}^- \cup \{0\} \cup \mathbb{R}^+.$$

Proposição 2.1 *O quadrado de um número real não nulo é positivo, ou seja:*

$$a \in \mathbb{R}, \text{ com } a \neq 0 \Rightarrow a^2 \in \mathbb{R}^+.$$

Prova. Pondo $K = \mathbb{R}$ e $P = \mathbb{R}^+$ o resultado decorre-se da Proposição 1.4. □

Sendo $(\mathbb{R},+,\cdot)$ um corpo ordenado então a relação de ordem $a < b$ ou $a > b$ em $\mathbb{R}$, conforme demonstrado na Proposição 1.3, satisfaz as propriedades: transitividade, tricotomia, monotonicidade da adição e a monotonicidade da multiplicação.

Como 1 é positivo, pois $1 = 1^2 \in \mathbb{R}^+$, segue-se que $1 < 1+1 < 1+1+1 < ...$ e assim, segue-se que $\mathbb{N} \subset \mathbb{R}$. Decorre-se de $\mathbb{N} \subset \mathbb{R}$, que para cada $n \in \mathbb{N} \Rightarrow -n \in \mathbb{R}$, tem-se ainda que $0 \in \mathbb{R}$, então $\{n; n \in \mathbb{N}\} \cup \{0\} \cup \{-n; n \in \mathbb{N}\} = \mathbb{Z} \subset \mathbb{R}$ e assim, segue-se que $\mathbb{Z} \subset \mathbb{R}$. Além do fato de $a,b \in \mathbb{Z}$, com $b \neq 0$ e $\mathbb{Z} \subset \mathbb{R} \Rightarrow b^{-1} \in \mathbb{R} \Rightarrow a.b^{-1} \in \mathbb{R}$, portanto, $\mathbb{Q} \subset \mathbb{R}$. Então, tem-se que $\mathbb{N} \subset \mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R}$.

Definição 2.1 (Valor absoluto de um número real) *A relação de ordem definida em* $\mathbb{R}$ *permite definir o valor absoluto ou módulo de um número* $x \in \mathbb{R}$*, como sendo,*

$$|x| = \begin{cases} -x, & \text{se } x \leq 0, \\ x, & \text{se } x > 0. \end{cases}$$

Da Definição 2.1 segue-se que para todo $x \in \mathbb{R}$ tem-se $|x| \in \mathbb{R}^+$ pois , se $x \geq 0$ nota-se que $|x| = x \geq 0$ e se $x < 0$, então $-x > 0$ e $|x| = -x > 0$. Em outras palavras $|x| = max\{-x,x\}$, ou seja, o módulo de x é igual ao maior dos dois números reais $-x$ e x. Portanto, para qualquer número real x, tem-se que:

$$|x| \geq x \text{ e } |x| \geq -x \Rightarrow |x| \geq x \text{ e } -|x| \leq x \Rightarrow -|x| \leq x \leq |x|.$$

Pode-se ainda definir $|x|$ como o único numero real positivo cujo o quadrado é igual a x^2.

Exemplo 2.1 *Dados os números reais 5, -7 e -π temos que:* $|5| = 5$, $|-7| = 7$ *e* $|-\pi| = \pi$.

Teorema 2.1 *Para quaisquer que sejam* $x, y \in \mathbb{R}$, *tem-se:*

1) $|x+y| \leq |x| + |y|$ *(Desigualdade Triangular);*
2) $|x.y| = |x|.|y|$*;*
3) $||x| - |y|| \leq |x-y|$.

Prova.

(1) Da Definição 2.1, segue-se que dados $x, y \in \mathbb{R}$, então: $|x| \geq x$ e $|y| \geq y$ somando essas desigualdades tem-se que $|x| + |y| \geq x + y$. De maneira análoga, conclui-se que $|x| \geq -x$ e $|y| \geq -y$ e que $|x| + |y| \geq -(x+y)$. Logo:

$$|x| + |y| \geq max\{x+y, -(x+y)\} = |x+y|.$$

Portanto, $|x+y| \leq |x| + |y|$.

(2) Da Definição 2.1, segue-se que para todo $x \in \mathbb{R}$ ocorre que $x^2 = (-x)^2 = |x|^2$, pois $|x|$ é um dos elementos x e $-x$. Logo, $|x \cdot y|^2 = (x \cdot y)^2 = x^2 \cdot y^2 = |x|^2 \cdot |y|^2 = (|x| \cdot |y|)^2$. Portanto, $|x \cdot y| = |x| \cdot |y|$.

(3) Decorre-se da Desigualdade Triangular, que:

$$|x| = |(x-y)+y| \leq |(x-y)| + |y| \Rightarrow |x| - |y| \leq |(x-y)|.$$

E ainda que:

$$|y| = |(y-x)+x| \leq |(y-x)| + |x| \Rightarrow |y| - |x| \leq |(y-x)| \Rightarrow -(|x| - |y|) \leq |(y-x)|.$$

Como $|(x-y)| = |(y-x)|$. Concluí-se que:

$$|x-y| \geq max\{|x| - |y|, -(|x| - |y|)\} = ||x| - |y||.$$

Portanto, $||x| - |y|| \leq |x-y|$.

□

2.1.3 Completeza dos reais

A afirmação que o corpo ordenado dos reais é completo significa conforme a Definição 1.28 que todo subconjunto não vazio $A \subset \mathbb{R}$ que é limitado superiormente possui um supremo em $\mathbb{R}$. Os teoremas e proposições a seguir decorrem diretamente do fato de $(\mathbb{R}, +, \cdot)$ ser um corpo ordenado completo.

Teorema 2.2 ($\mathbb{R}$ é arquimediano) *Para quaisquer $a, b \in \mathbb{R}$, com $a > 0$ existe $n \in \mathbb{N}$ tal que $b < n \cdot a$.*

Prova. O resultado decorre da Proposição 1.6, ou seja, todo corpo ordenado completo é arquimediano. □

Proposição 2.2 *Seja $b \in \mathbb{R}^+$, existe uma única solução real positiva da equação $x^2 = b$. Esta solução será denotada por $\sqrt{b}$.*

Prova. Prova da unicidade: Suponha que existam duas soluções $x_1, x_2 \in \mathbb{R}^+$ da equação $x^2 = b$, então: $x_1^2 = b$ e $x_2^2 = b \Rightarrow x_1^2 = x_2^2 \Rightarrow x_1^2 - x_2^2 = 0 \Rightarrow (x_1 + x_2) \cdot (x_1 - x_2) = 0$, como $x_1 + x_2 > 0$ então, $x_1 - x_2 = 0 \Rightarrow x_1 = x_2$.

Prova da existência: Considere os conjuntos $A = \{x \in \mathbb{R}^+; x^2 > b\}$ e $B = \{x \in \mathbb{R}^+; x^2 < b\}$. Seja $c = inf(A)$ e suponhamos, por absurdo, que $c^2 \neq b$, então $c \in A$ ou $c \in B$. Se $c \in A$ pode-se mostrar para n suficientemente grande que $c - \frac{1}{n} \in A$ o que contradiz o fato de c ser o ínfimo de A. Por outro lado, se $c \in B$ pode-se mostrar para n suficientemente grande que $c + \frac{1}{n} \in B$ o que contradiz o fato de c ser a maior das cotas inferiores de A. Portanto $c = b$. □

Proposição 2.3 *Não existe nenhum $x \in \mathbb{Q}$ tal que x^2=2.*

Prova. Seja $x \in \mathbb{Q}$ tal que $x^2 = 2$. Ao considerar $x = \frac{a}{b}$ com a e b primos entre si, ou seja, $x = \frac{a}{b}$ está na sua forma reduzida. Como $x^2 = (-x)^2$ basta provar para o caso em que $x > 0$, ou seja, $x = \frac{a}{b}$ com $a, b \in \mathbb{N}$ e a, b primos entre si. Como $x^2 = 2$, tem - se:

$$(\frac{a}{b})^2 = 2 \Rightarrow \frac{a^2}{b^2} = 2 \Rightarrow a^2 = 2 \cdot b^2.$$

Logo, a é par. Então, existe um $c \in \mathbb{N}$ tal que $a = 2 \cdot c$. Substituindo $a = 2 \cdot c$ na equação $x^2 = 2$ tem-se que:

$$(2 \cdot c)^2 = 2 \cdot b^2 \Rightarrow 4 \cdot c^2 = 2 \cdot b^2 \Rightarrow 2 \cdot c^2 = b^2 \Rightarrow b \text{ é par.}$$

Absurdo, pois a, b serem pares contradiz a hipótese deles serem primos entre si. Portanto, não existe nenhum número racional cujo o quadrado é 2. □

Definição 2.2 (Intervalos) *Dados a,b* $\in \mathbb{R}$ *coma* $< b$*, chama-se de intervalos a classe de subconjuntos de* $\mathbb{R}$ *abaixo:*

I_1) *(a,b)=*$\{x \in \mathbb{R};\ a < x < b\}$*;*
I_2) *[a,b]=*$\{x \in \mathbb{R};\ a \leq x \leq b\}$*;*
I_3) *[a,b)=*$\{x \in \mathbb{R};\ a \leq x < b\}$*;*
I_4) *(a,b]=*$\{x \in \mathbb{R};\ a < x \leq b\}$*;*
I_5) *(-∞,a)=*$\{x \in \mathbb{R};\ x < a\}$*;*
I_6) *(-∞,a]=*$\{x \in \mathbb{R};\ x \leq a\}$*;*
I_7) *[a,∞)=*$\{x \in \mathbb{R};\ x \geq a\}$*;*
I_8) *(a,∞)=*$\{x \in \mathbb{R};\ x > a\}$*;*
I_9) *(-∞, ∞)* $= \mathbb{R}$.

Os intervalos I_1, I_2, I_3 e I_4 são intervalos limitados, sendo que os símbolos " [" e "] " no intervalo, quando estão imediatamente ao lado de número $c \in \mathbb{R}$ significa que esse real pertence ao intervalo, enquanto o símbolo " (" ou ") " imediatamente ao lado de um número $c \in \mathbb{R}$ significa que o número não pertence ao intervalo. Os intervalos I_5, I_6, I_7, I_8 e I_9 são ilimitados, com exceção de I_9 que é representação da própria reta r. Se $a = b$ no intervalo I_2 o mesmo se reduz a único elemento, sendo, denominado assim de intervalo degenerado.

As Proposições 2.2 e 2.3 apontam o fato de existir pelo menos um número que pertence ao corpo ordenado dos reais e não pertence ao corpo ordenado dos racionais, tal número é denominado por $\sqrt{2}$. Esse fato dá ênfase a uma das consequências do corpo ordenado dos reais ser completo enquanto o dos racionais não. Como $\mathbb{Q} \subset \mathbb{R}$ levanta-se a possibilidade da existência de outro conjunto. Os próximos teoremas irão ajudar a reforçar essa existência.

Teorema 2.3 *Dada uma sequência decrescente* $I_1 \supset I_2 \supset I_3 \supset ... \supset I_n \supset ...$ *de intervalos limitados e fechados* $I_n = [a_n, b_n]$*, existe pelo menos um número real c tal que* $c \in I_n$ *para todo* $n \in \mathbb{N}$.

Prova. Para $n \in \mathbb{N}$ existe um intervalo $I_{n+1} \subset I_n$, ou seja:

$$a_1 \leq a_2 \leq ...a_n \leq ... \leq b_n \leq ...b_2 \leq b_1.$$

Considere os conjuntos $A = \{a_1, a_2, ..., a_n\}$ e $B = \{b_1, b_2, ..., b_n\}$, observe que ambos são limitados, pois no caso de A o a_1 é cota inferior e cada um dos b_n é uma cota superior, já no caso do conjunto B o b_1 é uma cota superior e cada um dos a_n é uma cota inferior. Sejam a, b, respectivamente, os supremo de A e o ínfimo de B. Como cada um dos b_n é cota superior de A, então $a \leq b_n$ para cada valor de n, assim como cada a_n é cota inferior de B então $a_n \leq b$ para cada n, portanto $a \leq b$, logo:

$$a_1 \leq a_2 \leq ...a_n \leq ... \leq a \leq b \leq ... \leq b_n \leq ...b_2 \leq b_1.$$

Concluí-se que o a e b pertencem a todos os intervalos I_n, ou seja, $[a,b] \subset I_n$ para cada n, o que significa que pelo menos um ponto pertence a todos os intervalos I_n (caso $a = b$) ou um intervalo está contido em todos intervalos I_n (caso $a \neq b$). Se considerar um $x < a = supA$, existe algum $a_n \in A$, tal que $x < a_n$, ou seja, $x \notin I_n$. Assim, nenhum $x < a$ pertenceria a todos intervalos I_n, com $n \in \mathbb{N}$. De modo análogo, conclui-se que nenhum $y > b$ pertenceria a todos intervalos I_n, com $n \in \mathbb{N}$. Portanto, apenas os elementos do intervalo $[a,b]$ pertencem a todos intervalos I_n, com $n \in \mathbb{N}$. □

Teorema 2.4 *O conjunto dos números reais não é enumerável*

Prova. Considere o conjunto enumerável $X = \{x_1, x_2, ..., x_n, ...\} \subset \mathbb{R}$, pode-se encontrar um número $x \notin X$. Considere um intervalo I_1=[a_1,b_1] com a_1, b_1 sendo números reais distintos, tal que $x_1 \notin I_1$, em seguida considere o intervalo I_2=[a_2,b_2] com a_2, b_2 sendo números reais distintos, tal que $x_2 \notin I_2$ e $I_2 \subset I_1$ e assim por diante indutivamente obtêm-se que $I_1 \supset I_2 \supset I_3 \supset ... \supset I_n$, onde I_n são intervalos limitados fechados e não-degenerado, com $x_i \notin I_i (1 \leq i \leq n)$, podendo ainda obter $I_{n+1} \subset I_n$ com $x_{n+1} \notin I_{n+1}$. Isso fornece a sequência decrescente $I_1 \supset I_2 \supset I_3 \supset ... \supset I_n \supset ...$ de intervalos limitados e fechados. Pelo Teorema 2.3, decorre-se que existe $c \in \mathbb{R}$ tal que $c \in I_1 \supset I_2 \supset I_3 \supset ... \supset I_n \supset ...$ e c é diferente de todos x_n, e portanto nenhum conjunto enumerável X pode conter todos os números reais.

□

Como o conjunto dos números racionais $\mathbb{Q} \subset \mathbb{R}$ é enumerável enquanto o dos números reais $\mathbb{R}$ não é enumerável, então existe um conjunto $(\mathbb{R} - \mathbb{Q})$ que é disjunto dos racionais, tal que $\mathbb{R} = \mathbb{Q} \cup (\mathbb{R} - \mathbb{Q})$. Pode-se concluir que esse conjunto $(\mathbb{R} - \mathbb{Q})$ não é enumerável, pois do contrário $\mathbb{R}$ seria enumerável (Corolário 1.4). A existência desse conjunto motiva a definição a seguir:

Definição 2.3 *Um número chama-se irracional se não é racional. O conjunto de todos os números irracionais é representado por* $\mathbb{I}$*, note que* $\mathbb{I} = (\mathbb{R} - \mathbb{Q})$.

Teorema 2.5 *Para todo número primo p positivo tem-se que* $\sqrt{p}$ *é irracional.*

Prova. Suponha, por absurdo, que $\sqrt{p} = \frac{a}{b}$ *seja racional, com* $m.d.c(a,b) = 1$ *(A notação* $m.d.c(a,b)$*, representa máximo divisor comum de a e b). Assim*

$$(\sqrt{p})^2 = (\frac{a}{b})^2 \Rightarrow a^2 = p \cdot b^2,$$

como $m.d.c(a,b) = 1$ então p divide a^2. Logo existe $k \in \mathbb{N}$ tal que $a = p \cdot k$. Substituindo $a = p \cdot k$ em $a^2 = p \cdot b^2$ obtém-se $(p \cdot k)^2 = p \cdot b^2 \Rightarrow b^2 = p \cdot k^2$ o que implica que $b = p \cdot m$, com $m \in \mathbb{N}$. Segue-se que a e b são divisíveis por p, contradição, pois $m.d.c(a,b) = 1$. Portanto, para todo número primo p positivo temos que $\sqrt{p}$ é irracional. □

2.2 Representação na reta dos números reais

Ao se considerar, representar geometricamente os números reais seria interessante iniciar a representação com alguns de seus subconjuntos, como por exemplo, o conjunto dos números inteiros e o dos racionais. Para isso deve-se escolher um elemento geométrico. Nessa secção será apresentado um modelo interessante para essa finalidade, tal modelo é o de uma reta.

2.2.1 Números inteiros sobre a reta

Considere uma reta r e nela marca-se um ponto O denominado origem. Esse ponto determina na reta r duas semirretas sendo uma delas associada aos números positivos enquanto a outra aos negativos. Sobre a semirreta positiva (considere, por exemplo, que essa seja a semirreta à direita de O) escolhe-se um ponto A_1 tal que a medida do segmento de reta OA_1 vai ser a unidade de comprimento, ou seja,

$$med(OA_1) = 1 unidade.$$

.

Definição 2.4 *Conclui-se que um segmento OA e o segmento padrão u são comensuráveis se existir algum segmento w que caiba n vezes em u e m vezes em OA. Nesse caso tem-se que a medida de OA é $\frac{m}{n}$, ou seja, $med(OA) = \frac{m}{n}$ e ainda a medida do segmento w será $\frac{1}{n}$. Se os segmentos OA e u não forem comensuráveis diz-se que esses são incomensuráveis.*

Para associar cada número inteiro a um ponto da reta, pode-se iniciar associando o número 0 ao ponto O, em seguida o número 1 ao ponto A_1, e definir a medida do segmento OA_1 como o comprimento padrão, depois o número 2 se associa ao ponto A_2 da reta r, ponto que se encontra uma unidade à direita de A_1, ou seja,

$$med(A_1,A_2) = 1 \cdot med(O,A_1) \text{ e } med(O,A_2) = 2 \cdot med(O,A_1).$$

Já o número 3 se associa ao ponto A_3 da reta r, ponto que se encontra uma unidade à direita de A_2, ou seja, $med(A_2,A_3) = 1 \cdot med(O,A_1)$ e $med(O,A_3) = 3 \cdot med(O,A_1)$, dessa forma consegue - se associar todos os números inteiros positivos (Figura 2.1).

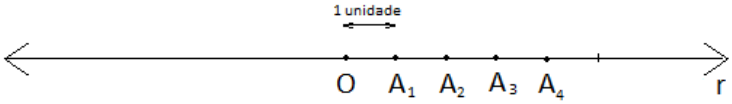

Figura 2.1: *Números inteiros positivos sobre a reta.*

De modo análogo, associam-se os números inteiros negativos a reta r. Primeiro marca-se na semirreta negativa (à esquerda da origem) o ponto A_{-1} de modo que $med(O,A_{-1}) = 1 \cdot med(O,A_1)$, em seguida o número -1 é associado a esse ponto, enquanto o número -2 é associado ao ponto da reta A_{-2} localizado uma unidade à esquerda de A_{-1}, já o número -3 é associado ao ponto da reta A_{-3} localizado 1 unidade à esquerda de A_{-2}, e assim por diante. Dessa forma consegue-se associar o conjunto $\mathbb{Z}$ a pontos da reta r (Figura 2.2), essa forma funciona pelo fato de qualquer um dos segmentos OA_n com $n \in \mathbb{Z} - \{0\}$ e o segmento OA_1 serem comensuráveis.

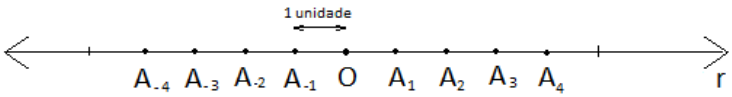

Figura 2.2: *Números inteiros sobre a reta.*

2.2.2 Números racionais sobre a reta

Pode-se observar que mesmo após representar números inteiros na reta r, faltam muitos pontos sobre a reta que não estão associados a nenhum número inteiro, como $\mathbb{Z} \subset \mathbb{Q}$, alguns desses pontos da reta podem ser associados aos pontos do conjunto $(\mathbb{Q} - \mathbb{Z})$.

Para associar números racionais positivos a pontos da reta r, primeiramente deve-se associar o número 0 ao ponto O da reta, em seguida dado o número racional $\frac{a}{b}$, com $a,b \in \mathbb{N}$, marca-se sobre o eixo positivo da reta o ponto A_a de forma que a $med(O,A_a) = a \cdot med(O,A_1)$, se $b = 1$ associa-se o número $\frac{a}{b}$ ao ponto A_a que coincidirá com um ponto já associado a um inteiro, no caso $a \in \mathbb{Z}$ (Figura 2.3), agora se $b > 1$, particiona-se o segmento OA_a em b segmentos iguais, marcando $b-1$ pontos sobre OA_a, sendo o ponto $A_{(a,b)}$ o ponto mais próximo de O, associando o número racional $\frac{a}{b}$ a esse ponto. Esse processo permite associar os números racionais positivos. Para o caso dos números racionais negativos faz-se uma construção análoga sobre a semirreta negativa.

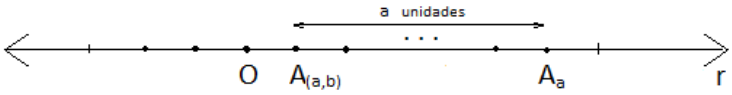

Figura 2.3: *Números racionais sobre a reta.*

2.2.3 Números não racionais na reta

Do Teorema 2.5, tem-se que para um p racional e primo o número $\sqrt{p}$ não é racional, seja um segmento OB de medida $\sqrt{p}$ e um segmento padrão OA_1 de medida racional então OA_1 e OB são segmentos incomensuráveis, logo os processos utilizados anteriormente para associar números inteiros e racionais a reta, não funcionam, em geral, para estes números. Para associar estes à reta usa-se um processo que tem como base o teorema abaixo:

Teorema 2.6 (Teorema de Pitágoras) *Seja ABC um triângulo retângulo em $\hat{A}$, então $BC^2 = AB^2 + AC^2$, ou seja, o quadrado do valor da hipotenusa é igual a soma dos quadrados dos valores dos catetos.*

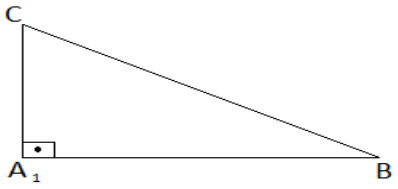

Figura 2.4: *Triângulo retângulo em $\hat{A}$.*

Inicialmente associa-se o número 0 ao ponto O da reta r, depois associa-se o número 1 ao ponto A_1 da semirreta positiva contida na reta r, depois considera-se um quadrado OA_1BC. Em seguida com o auxílio do compasso, fixa-se sua ponta seca em O e sua outra ponta em B traçando uma semicircunferência que intersecta a reta r em D_1, por construção tem-se que $med(O,D_1) = med(O,B)$. Como $med(O,A_1) = med(A_1,B) = 1$ (Figura 2.5), segue-se do Teorema de Pitágoras que $med(OD_1) = med(OB) = \sqrt{2}$, e por fim associa-se número $\sqrt{2}$ ao ponto D_1.

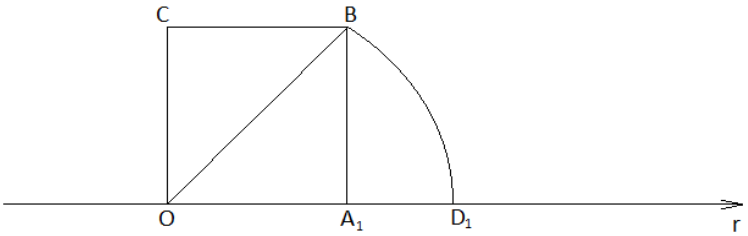

Figura 2.5: *Números não racionais sobre a reta r.*

Para associar o número $\sqrt{3}$ à reta r deve-se construir o retângulo OD_1B_1C (Figura 2.6), donde se obtém o triângulo retângulo OD_1B_1 cuja a hipotenusa OB_1 tem medida igual a $\sqrt{3}$. De forma análoga ao caso anterior, obtém-se um ponto D_2 em r tal que $med(OD_2) = \sqrt{3}$. E assim sucessivamente associam-se os números $\sqrt{4}$, $\sqrt{5}$, $\sqrt{6}$,... a pontos da reta r. Para associar os números $-\sqrt{2}$,$-\sqrt{3}$,$-\sqrt{4}$, $-\sqrt{5}$, $-\sqrt{6}$, ... basta repetir o processo só que considerando a semirreta negativa da reta r.

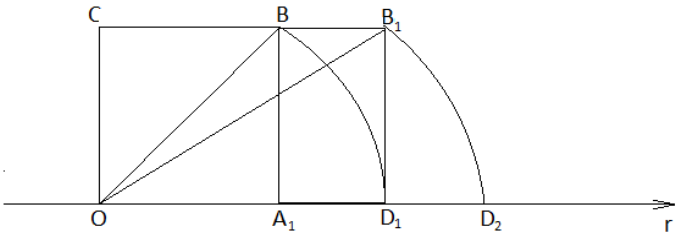

Figura 2.6: *Números não racionais sobre a reta r.*

2.2.4 Números reais na reta

Utilizando-se do axioma da construção de geometria Euclidiana é possível associar todos números reais aos pontos da reta r de maneira a não sobrar pontos sem ter correspondência em $\mathbb{R}$.

Axioma 2.1 *Existe uma correspondência biunívoca entre os pontos da reta e os números reais de forma que o valor absoluto da diferença entre os números associados é a distância entre os pontos correspondentes.*

Definição 2.5 *Seja r uma reta, em que é fixado um ponto O denominado a origem, que divide a reta r em duas semirretas onde em uma delas serão marcados os pontos associados a números reais positivos, enquanto na outra semirreta marcam-se os pontos associados a números reais negativos. Fixa-se também na semirreta positiva da reta r um ponto A, diferente de O, tomando-se o segmento OA como unidade de comprimento, o qual corresponderá ao número real 1, esta reta r é a reta numerada ou reta real.*

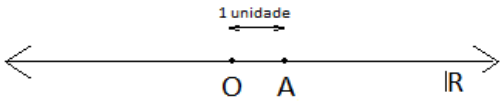

Figura 2.7: *Reta real.*

Devido a correspondência biunívoca entre os pontos da reta real e os números reais (conforme Axioma 2.1) pode-se optar a não se distinguir números reais e pontos da reta.

Definição 2.6 *A soma de dois números reais x e y, geometricamente se define através de uma traslação que conserva a direção e o sentido conforme indicado na Figura 2.8. Considera-se os seguintes casos:*

1) *Seja $x \in \mathbb{R}$ e $y \in \mathbb{R}^+$, então a soma $x+y$ é definida como o número real associado a extremidade final do segmento, orientado para a direita, com extremidade inicial em x, e comprimento com medida igual a medida do segmento associado a y;*
2) *Seja $x \in \mathbb{R}$ e $y \in \mathbb{R}^-$, então a soma $x+y$ é definido como o número real associado a extremidade final do segmento, orientado para a esquerda, com extremidade inicial em x, e comprimento com medida igual à medida do segmento associado a y.*

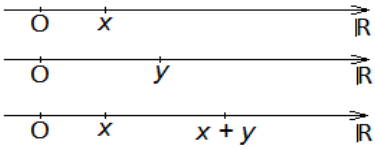

Figura 2.8: *Soma de dois reais positivos na reta real.*

Exemplo 2.2 (Representação geométrica da comutatividade aditiva em $\mathbb{R}$)
Consideraremos apenas a comutatividade da adição em $\mathbb{R}^+$, pois de maneira análoga representa-se os demais casos em $\mathbb{R}$. Então sejam $x, y \in \mathbb{R}^+$, da Definição 2.6 tem-se que a representação geométrica da comutatividade da adição em $\mathbb{R}^+$ é dada pela Figura 2.9:

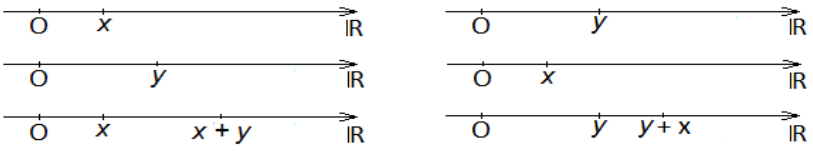

Figura 2.9: *Representação geométrica da comutatividade da adição em $\mathbb{R}^+$.*

Definição 2.7 *O produto de dois números reais positivos x e y, geometricamente é definido por meio da construção representada pela Figura 2.10:*

a) traça-se pela origem 0 uma reta s perpendicular a r, em seguida marca-se na reta real r os pontos 1, y , enquanto que na reta s marca-se o ponto x. Considere a reta t que passa por 1 e por x.
b) traça-se por y uma reta u paralela a reta t, então marca-se o ponto $P = u \cap s$, ou seja, o ponto de intersecção das retas s e u;
c) traça-se uma semicircunferência γ de origem em O e que passa por P, seja $Q = \gamma \cap r$. O número real associado ao ponto Q representa o produto dos números reais positivos x e y, ou seja, Q está associado ao número real $x \cdot y$.

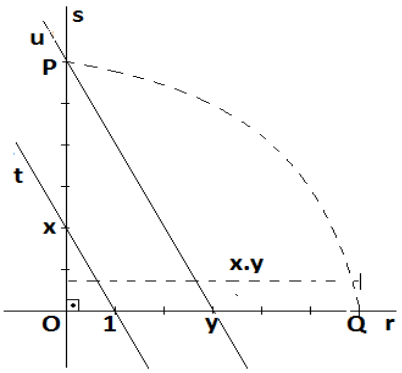

Figura 2.10: *Representação geométrica da multiplicação em* $\mathbb{R}^+$.

Para os demais casos possíveis de produto em $\mathbb{R}$*, basta modificar o sinal de* $x \cdot y$ *conforme a regra dos sinais:*

$$x < 0 \text{ e } y > 0 \Rightarrow -|x| \cdot |y|$$
$$x > 0 \text{ e } y < 0 \Rightarrow -|x| \cdot |y|$$
$$x < 0 \text{ e } y < 0 \Rightarrow +|x| \cdot |y|$$

De fato, o valor da medida do segmento OP indicado na Definição 2.7 é $x \cdot y$, pois os triângulos "$O1x$" e "OyP" são semelhantes pelo caso AAA (ângulo-ângulo-ângulo), logo:

$$\frac{y}{1} = \frac{OP}{x} \Rightarrow med(O,P) = x \cdot y.$$

Como P, Q pertencem a mesma semicircunferência então a medida de OP e OQ são iguais.

Exemplo 2.3 (Elemento neutro da multiplicação em $\mathbb{R}^+$**)** *Seja* $a \in \mathbb{R}^+$*, então* $a \cdot 1 = a$*. De fato, basta tomar na construção da Definição 2.7,* $x = a$ *e* $y = 1$*, os triângulos "*$O1x$*" e "*OyP*" são congruentes, logo o segmento* OQ *tem comprimento* a*, assim* $a \cdot 1 = a$*.*

Definição 2.8 (Representação na reta do valor absoluto em $\mathbb{R}$**)** *O valor absoluto de um número real* x *é representado na reta real como sendo o valor da distância entre o ponto* x *a* O*, sendo* O *a origem da reta numerada. Dados* $x, y \in \mathbb{R}$*, então* $|x-y| = |y-x|$ *é o valor das distâncias entre os pontos* x *e* y *da reta (Figura 2.11).*

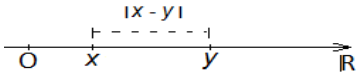

Figura 2.11: *Representação na reta do valor absoluto* $|x-y|$.

2.3 Representação decimal dos números reais

2.3.1 Expressões decimais e aproximações de números reais

Definição 2.9 *Seja k um inteiro positivo e considerando os inteiros a_1 ,a_2 ,a_3 , ... tais que $0 \leq a_i \leq 9$ (i = 1,2,3,...). Então o símbolo da forma α=k,$a_1a_2a_3....a_n...$ é denominado uma expressão decimal. Sendo o número k denominado parte inteira de α e os a_1 ,a_2 ,a_3 , ... são denominados dígitos.*

Exemplo 2.4 *São exemplos de expressões decimais:*

a) O resultado da divisão de 437 por 100, ou seja, $\frac{437}{100}$ = 4,37.

b) O resultado da divisão de 437 por 100, ou seja, $\frac{43}{1000}$ = 0,043.

c) O resultado da divisão de 10 por 9, ou seja, $\frac{10}{9}$ = 1,33333....

d) O resultado da divisão de 25 por 99, ou seja, $\frac{25}{99}$ = 0,25252525....

As expressões decimais que possuem um número finito de dígitos não nulos após a vírgula são denominadas de decimais finitos, enquanto os que possuem um número infinito de dígitos não nulos após a vírgula são denominadas de decimais infinitos.

Definição 2.10 *Toda fração cujo o denominador é uma potência de 10 é denominada fração decimal.*

Exemplo 2.5 *As frações $\frac{3}{10}, \frac{654}{100}, \frac{25}{1000}$ e $\frac{7}{10000}$ são exemplos de frações decimais.*

Os conjunto dos números reais $\mathbb{R}$ tem a propriedade de que para todo número real x, pode-se fazer uma aproximação tão boa quanto se deseja usando números racionais. De fato, seja k o maior inteiro positivo que é menor do que ou igual a parte inteira do número real x, então $k \leq x < k+1 \Rightarrow 0 \leq x-k < 1$, o erro da aproximação $x-k$ seria um número real que pertence ao intervalo $[0,1)$. Escrevendo $x-k$ = 0,$a_1a_2a_3....a_n...$ com $0 \leq a_i \leq 9$, o que significa que:

Ao considerar o número racional α_n, escrito na forma:

$$\alpha_n = a_n + a_{n-1} \cdot 10 + a_{n-2} \cdot 10^2 + a_{n-3} \cdot 10^3 + ... + a_2 \cdot 10^{n-2} + a_1.10^{n-1}.$$

Então $\frac{\alpha_n}{10^n} \leq x-k < \frac{\alpha_n+1}{10^n}$, assim $k + \frac{\alpha_n}{10^n}$ é uma boa aproximação, no sentido que o erro cometido de substituir x por α_n seria $|x-(k+\frac{\alpha_n}{10^n})|$ que é igual a um número não superior a $\frac{1}{10^n}$.

Definindo $\alpha_0 = k$, pode-se construir uma sequência não decrescente de números racionais $\alpha_0 \leq \alpha_1 \leq \alpha_2 \leq \alpha_3 \leq ... \leq \alpha_n \leq$ ... que serão valores cada vez mais próximos do número real x.

Define-se, então como limite dessa sequência de números racionais o número real x. O fato de sempre existir um número real x decorre de $\mathbb{R}$ ser um corpo ordenado completo.

Exemplo 2.6 *Considere o número real $x = 1$ e fazendo aproximações por números racionais α_n, assim:*

$\alpha_0 = 0$*, sendo 0 o maior inteiro* < 1.

$\alpha_1 = \dfrac{9}{10}$*, sendo 9 o maior dígito tal que* $0 + \dfrac{9}{10} \leq 1$. *Note que nesse caso o erro de aproximação é de* $1 - \dfrac{9}{10} = \dfrac{1}{10}$.

$\alpha_2 = \dfrac{9}{10} + \dfrac{9}{10^2}$*, sendo $a_2 = 9$ é o maior dígito tal que* $0 + \dfrac{9}{10} + \dfrac{9}{10^2} \leq 1$. *Note que nesse caso o erro de aproximação é de* $1 - \dfrac{9}{10} - \dfrac{9}{10^2} = \dfrac{1}{10^2}$.

E assim por diante, para um n suficientemente grande o valor do erro da aproximação de α_n é tão pequeno quanto se queira, como $\mathbb{R}$ é um corpo ordenado e completo, para um n suficientemente grande esse valor tende a zero, ou seja:

$$\frac{9}{10} + \frac{9}{10^2} + ... + \frac{9}{10^n} + ... = \sum_{n=1}^{\infty} \frac{9}{10^n} = 1.$$

2.3.2 Uma função sobrejetiva e "quase" injetiva.

Seja D o conjunto de todas as expressões decimais $0{,}a_1a_2a_3....a_n...$ pertencentes ao intervalo $[0,1)$, basta considerar apenas esse intervalo, pois as outras expressões decimais são facilmente obtidas mediante a translação conveniente de um número inteiro.

Defina-se a função $f : D \to \mathbb{R}$ dada pela expressão:

$$f(0,a_1a_2a_3....a_n...) = \frac{a_1}{10} + \frac{a_2}{10^2} + \frac{a_3}{10^3} + ... + \frac{a_n}{10^n} + ... = \sum_{n=1}^{\infty} \frac{a_n}{10^n}.$$

Como $\displaystyle\sum_{n=1}^{\infty} \frac{a_n}{10^n} \leq \sum_{n=1}^{\infty} \frac{9}{10^n} = 1$, então a série $\displaystyle\sum_{n=1}^{\infty} \frac{a_n}{10^n}$ é majorada pela série geométrica $\displaystyle\sum_{n=1}^{\infty} \frac{9}{10^n}$ (mais detalhes ver, [7]).

Exemplo 2.7 *Considere as expressões decimais α_1= 0,257 e α_2= 0,256999..., elas são levadas por f em:*

$$f(\alpha_1) = \frac{2}{10} + \frac{5}{10^2} + \frac{7}{10^3} \text{ e } f(\alpha_2) = \frac{2}{10} + \frac{5}{10^2} + \frac{6}{10^3} + \frac{9}{10^4} + \frac{9}{10^5} + \frac{9}{10^6} ...$$

Do exemplo acima, pode-se concluir que a função $f : D \to \mathbb{R}$ não é injetiva. Basta notar que $\dfrac{9}{10^4}, \dfrac{9}{10^5}, \dfrac{9}{10^6}, ...$ é uma progressão geométrica (PG), então decorre da fórmula de soma infinta dos termos de uma PG que:

$$f(\alpha_2) = \frac{2}{10} + \frac{5}{10^2} + \frac{6}{10^3} + \frac{9}{10^4} + \frac{9}{10^5} + \frac{9}{10^6} + ...$$

$$\Rightarrow f(\alpha_2) = \frac{2}{10} + \frac{5}{10^2} + \frac{6}{10^3} + \frac{\frac{9}{10^4}}{1 - \frac{1}{10}} \Rightarrow f(\alpha_2) = \frac{2}{10} + \frac{5}{10^2} + \frac{6}{10^3} + \frac{1}{10^3}$$

$$\Rightarrow f(\alpha_2) = \frac{2}{10} + \frac{5}{10^2} + \frac{7}{10^3} \Rightarrow f(\alpha_2) = f(\alpha_1)$$

Logo, $\alpha_1 \neq \alpha_2$ no entanto $f(\alpha_1) = f(\alpha_2)$, ou seja, f não é uma injeção.

A "quase" injetividade de f, ocorre pelo fato que o único caso em que expressões decimais distintas representam o mesmo número real ocorre se $0 \leq a_n \leq 8$, com $n \in \mathbb{N}$, $\alpha_1 = 0, a_1...a_n999...$ e $\alpha_2 = 0, a_1...(a_n + 1)000....$

De fato, como $f(\alpha_1) = \frac{a_1}{10} + \frac{a_2}{10^2} + ... + \frac{a_n}{10^n} + \frac{9}{10^{n+1}} + \frac{9}{10^{n+2}} + ...$, então:

$$f(\alpha_1) = \frac{a_1}{10} + \frac{a_2}{10^2} + ... + \frac{a_n}{10^n} + \frac{9}{10^n} \cdot (\frac{1}{10} + \frac{1}{10^2} + ...)$$

$$\Rightarrow f(\alpha_1) = \frac{a_1}{10} + \frac{a_2}{10^2} + ... + \frac{a_n}{10^n} + \frac{9}{10^n} \cdot (\frac{\frac{1}{10}}{1 - \frac{1}{10}})$$

$$\Rightarrow f(\alpha_1) = \frac{a_1}{10} + \frac{a_2}{10^2} + ... + \frac{a_n}{10^n} + \frac{9}{10^n} \cdot (\frac{1}{9})$$

$$\Rightarrow f(\alpha_1) = \frac{a_1}{10} + \frac{a_2}{10^2} + ... + \frac{a_n + 1}{10^n}.$$

E ainda, $f(\alpha_2) = \frac{a_1}{10} + \frac{a_2}{10^2} + ... + \frac{a_n + 1}{10^n}$. Logo, $f(\alpha_1) = f(\alpha_2)$, ou seja:

$$0, a_1...a_n999... \neq 0, a_1...(a_n + 1)00... \Rightarrow f(0, a_1...a_n999...) = f(0, a_1...(a_n + 1)00...).$$

Considerando D^* como sendo o conjunto formado por todas expressões decimais $\alpha = 0{,}a_1\ a_2\ a_3...$ das quais não tem todos elementos iguais a 9, a partir de uma certa ordem então, a função $f : D^* \to \mathbb{R}$ é injetiva.

Ao mostrar que a função f é sobrejetiva em $[0, 1)$ ocorre uma correspondência biunívoca $f : D^* \to [0, 1)$ ou seja $0, a_1a_2.... = \sum_{n=1}^{\infty} \frac{a_n}{10^n}$.

De fato, isso ocorre:

Seja $r \in [0, 1)$, decompondo $[0, 1)$ da seguinte forma: $[0, 1) = \bigcup_{i=0}^{9} [\frac{i}{10}, \frac{i+1}{10})$. Portanto r pertence a um, e só um desses subintervalos: $r \in I_1 = [\frac{a_1}{10}, \frac{a_1 + 1}{10})$. Agora se for considerada a decomposição $[\frac{a_1}{10}, \frac{a_1 + 1}{10}) = \bigcup_{i=0}^{9} [\frac{a_1}{10} + \frac{i}{10^2}, \frac{a_1}{10} + \frac{i+1}{10^2})$ novamente r pertence a um, e só um desses subintervalos: $r \in I_2 = [\frac{a_1}{10} + \frac{a_2}{10^2}, \frac{a_1}{10} + \frac{a_2 + 1}{10^2})$. E assim por diante. Pelo Teorema 2.3, existe pelo menos um número real $c \in I_n^*$, para todo $n \in \mathbb{N}$, no qual I_n^* é o intervalo fechado que tem as mesmas extremidades que I_n. Como $r \in I_n$, para todo $n \in \mathbb{N}$, segue-se que para n suficientemente grande a sucessão formada pelas

extremidades à esquerdas dos I_n tendem a r, e portanto, $r = \sum_{n=1}^{\infty} \frac{a_n}{10^n}$ e a decimal que toma para corresponder a r é $0{,}a_1a_2a_3$ ....

Devido a correspondência biunívoca $f{:}D^* \to [0,1)$ dada por:

$$f(0,a_1a_2....a_n...) = \frac{a_1}{10} + \frac{a_2}{10^2} + ... + \frac{a_n}{10^n} + ...$$

Pode-se optar em representar a expressão $f(0,a_1a_2....a_n...) = \frac{a_1}{10} + \frac{a_2}{10^2} + ... + \frac{a_n}{10^n} + ...$ por simplesmente $0,a_1a_2....a_n... = \frac{a_1}{10} + \frac{a_2}{10^2} + ... + \frac{a_n}{10^n} + ...$ Essa correspondência permite analisar e interpretar diversas propriedades do corpo ordenado completo dos reais de forma clara e concisa. Até mesmo em questões delicadas como, por exemplo, a questão da não enumerabilidade do conjunto dos números reais.

Exemplo 2.8 (A representação decimal da não enumerabilidade dos reais) *Do Teorema 2.4, segue-se que o conjunto dos números reais é não enumerável. De fato, usando o método da diagonal de Cantor, basta levar em consideração que o intervalo [0,1) é não enumerável. Suponha, por absurdo, que o intervalo [0,1) seja enumerável. Então, usando as expressões decimais pertencentes a D^* pode-se enumerar todos os números reais de [0,1) assim:*

$$\begin{gathered} 0,a_{11}a_{12}a_{13}a_{14}a_{15}... \\ 0,a_{21}a_{22}a_{23}a_{24}a_{25}... \\ 0,a_{31}a_{32}a_{33}a_{34}a_{35}... \ . \\ ... \\ 0,a_{n1}a_{n2}a_{n3}a_{n4}a_{n5}... \\ ... \end{gathered}$$

Construindo o número real $0,b_1b_2b_3b_4b_5...$ com $b_j \neq 9$ e $b_j \neq a_{jj}$, cujo $j \in \mathbb{N}$, observa-se que esse número não figura a lista acima, logo chega-se a uma contradição. Portanto, [0,1) é não enumerável, consequentemente o conjunto $\mathbb{R}$ também não.

Proposição 2.4 *O decimal finito é um número racional que pode ser representado por uma fração decimal.*

Prova. Seja $\alpha = 0,a_1a_2a_3....a_n$ a expressão decimal finita, então da função bijetiva $f : D^* \to [0,1)$ dada por $f(0,a_1a_2....a_n...) = \frac{a_1}{10} + \frac{a_2}{10^2} + ... + \frac{a_n}{10^n} + ...$ tem-se que:

$$\begin{gathered} f(\alpha) = \frac{a_1}{10} + \frac{a_2}{10^2} + ... + \frac{a_n}{10^n} \\ \Rightarrow f(\alpha) = \frac{a_1.10^{n-1} + a_2.10^{n-2} + ... + a_n.10^0}{10^n} \\ \Rightarrow f(\alpha) = \frac{a_1a_2...a_n}{10^n}. \end{gathered}$$

Como f é uma bijeção, pode-se adotar que: $\alpha = \frac{a_1 a_2 ... a_n}{10^n}$, ou seja, α=0,$a_1 a_2 .... a_n$ pode ser representado por uma fração decimal cuja potência do denominador é elevado a n (números de algarismos após a vírgula).

□

2.3.3 Dízimas periódicas simples e compostas.

Definição 2.11 *Uma dízima periódica simples é uma expressão decimal do tipo* α=*0,*$a_1 a_2 .... a_p a_1 a_2 .... a_p ...$ = *0,* $\overline{a_1 a_2 .... a_p}$ *na qual, os p primeiros dígitos imediatamente depois da vírgula formam um bloco de termos (chamado período) e a partir daí a expressão decimal é constituída da repetição desse bloco.*

Definição 2.12 *Uma dízima periódica composta é uma expressão decimal do tipo* α=*0,*$b_1 b_2 ... b_q$ $a_1 a_2 .... a_p a_1 a_2 .... a_p ...$= *0,*$b_1 b_2 ... b_q \overline{a_1 a_2 .... a_p}$ *que depois da vírgula tem uma parte que não se repete seguida por uma parte periódica.*

Teorema 2.7 (Transformação de dízimas periódicas em frações geratriz) *A dízima periódica = 0,*$b_1 b_2 ... b_q \overline{a_1 a_2 .... a_p}$ *de período* $a_1 .... a_p$ *é um número racional que pode ser escrito na forma*

$$\frac{b_1 ... b_q a_1 ... a_p - b_1 ... b_q}{9...90...0},$$

cujo denominador é um número com p noves e q zeros.

Prova. Seja $\alpha = 0, b_1 b_2 ... b_q a_1 a_2 .... a_p a_1 a_2 .... a_p ...$ então:

$$\begin{aligned}
\alpha &= \frac{b_1}{10} + \frac{b_2}{10^2} + ... + \frac{b_q}{10^q} + \frac{a_1}{10^{q+1}} + \frac{a_2}{10^{q+2}} + ... + \frac{a_p}{10^{q+p}} + ... \\
\Rightarrow \alpha &= \frac{b_1 b_2 ... b_q}{10^q} + \frac{a_1 a_2 ... a_q}{10^{q+p}} + \frac{a_1 a_2 ... a_q}{10^{q+2p}} + \frac{a_1 a_2 ... a_q}{10^{q+3p}} + ... \\
\Rightarrow \alpha &= \frac{b_1 b_2 ... b_q}{10^q} + \frac{a_1 a_2 ... a_q}{10^q} \cdot (\frac{1}{10^p} + \frac{1}{10^{2p}} + \frac{1}{10^{3p}} + ...)
\end{aligned}$$

Como $\frac{1}{10^p}$ + $\frac{1}{10^{2p}}$ + $\frac{1}{10^{3p}}$ + ... se trata da soma dos termos de uma P.G tem-se que $\frac{1}{10^p} + \frac{1}{10^{2p}} + \frac{1}{10^{3p}} + ... = \frac{1}{10^p - 1}$, assim:

$$\begin{aligned}
\alpha &= \frac{b_1 b_2 ... b_q}{10^q} + \frac{a_1 a_2 ... a_q}{10^q} \cdot (\frac{1}{10^p - 1}) \\
\Rightarrow \alpha &= \frac{b_1 ... b_q a_1 ... a_p - b_1 ... b_q}{10^q . (10^p - 1)} \\
\Rightarrow \alpha &= \frac{b_1 ... b_q a_1 ... a_p - b_1 ... b_q}{9...90...0},
\end{aligned}$$

cujo denominador $99..900...0 = 10^q.(10^p - 1)$ é um número com p noves e q zeros. □

Exemplo 2.9 *Seja o decimal* α = *0,23555..., então do teorema acima decorre que a sua representação em fração é dada por:* $\alpha = \frac{235-23}{900} = \frac{212}{900}$.

Corolário 2.1 *Seja* β = $0,b_1...b_nb_1...b_n...$ *uma dízima periódica simples, então* β *é igual a* $\frac{b_1...b_n}{9...9}$, *onde o denominador é um número constituído de n noves.*

Prova. Considere a dízima periódica simples $\alpha = 0,b_1...b_nb_1...b_n...$, decorre do Teorema 2.7 que : $\alpha = \frac{b_1b_2...b_n - 0}{99...9} \Rightarrow \alpha = \frac{b_1b_2...b_n}{99...9}$, cujo o denominador é um número constituído de n algarismos iguais a 9. □

Exemplo 2.10 *Seja o decimal* α = *0,235235235..., então segue-se do Corolário 2.1 tem-se que a sua representação em fração racional é dada por:* $\alpha = \frac{235}{999}$.

Corolário 2.2 *Toda dízima periódica simples é igual a uma fração irredutível cujo denominador não é divisível nem por 2 nem por 5.*

Prova. Seja α=$0,a_1a_2....a_pa_1a_2....a_p...$, uma dízima periódica simples de período $a_1a_2....a_p$, assim decorre do Teorema 2.7 que: $\alpha = \frac{a_1a_2....a_p - 0}{10^p - 1} = \frac{a_1a_2....a_p}{99...9}$, cujo o denominador $10^p - 1 = 99...9$ é um número constituído de p algarismos iguais a nove, logo não é divisível por 2 e nem por 5. Portanto, o denominador na forma irredutível de $\frac{a_1a_2....a_p}{99...9}$ também não é divisível por 2 e nem por 5. □

Corolário 2.3 *Uma dízima periódica composta com m termos não-periódicos é igual a uma fração irredutível cujo denominador é divisível por* 2^m *ou por* 5^m *, mas não por potências de 2 ou 5 cujo expoentes sejam maiores do que m.*

Prova. Seja α = α=$0,b_1b_2...b_m\ a_1a_2....a_pa_1a_2....a_p...$ essa dízima, então decorre do Teorema 2.7 que:

$$\alpha = \frac{b_1b_2...b_ma_1a_2....a_p - b_1b_2...b_m}{(10^p - 1).10^m}. \tag{2-1}$$

Como $10^p - 1 = 99...9$ é constituído de apenas p algarismos iguais a 9, tem-se que $m.d.c(10^p - 1, 10) = 1$. Já $10^m = 2^m.5^m$, então o denominador $(10^p - 1).10^m$ da fração (2-1) é divisível por 2^m e 5^m, mas não por potências 2^s ou 5^s, com $s > m$. Assim a forma irredutível da fração (2-1) também não é divisível por potências de 2 ou 5 cujo expoentes sejam maiores do que m. □

Conclusão

Conceitos e propriedades importantes da teoria de álgebra e de tópicos sobre conjuntos foram utilizados neste trabalho para definir os números reais como um corpo ordenado completo. Este contexto, traduz a intenção de oferecer uma alternativa à abordagem de números reais como uma simples extensão dos números racionais. Essa alternativa é a de que os números reais formam um corpo ordenado completo, visto que a ideia dos números reais, como extensão dos racionais, se faz importante para a percepção da existência do corpo dos reais. No entanto, ressalta-se que todas propriedades dos números reais decorrem do fato de formarem um corpo ordenado e completo.

A compreensão da abordagem sobre os números reais como corpo ordenado completo, apesar de minimizar o problema da circularidade deste tema, é uma questão delicada, pois para tal, se faz necessário o uso de estrutura axiomática de certa forma rigorosa, ao se considerar, por exemplo, um estudante a nível do ensino básico. Além do que, em geral, encontra-se dificuldades em construir situações concretas e cotidianas que realmente justifiquem a necessidade de expandir o estudo do conjunto dos números racionais para o estudo dos números reais. Para tentar minimizar essas dificuldades pode-se recorrer a própria história da evolução do conceito dos reais, da qual pode ser identificada ferramentas poderosas no aspecto de motivar e facilitar o estudo sobre os números reais.

Os problemas geométricos que os gregos já enfrentavam no período de 500 a 350 a.C. que envolviam medidas comensuráveis e incomensuráveis são exemplos disso, pois essas ideias permitem sistematizar uma correspondência entre os números reais e a reta, contribuindo assim para uma melhor compreensão e interpretação dos axiomas que fundamentam a base conceitual do corpo dos reais.

Através deste trabalho espera-se contribuir tanto com aqueles que se encontram numa formação em nível básico como aqueles que aspiram a uma formação acadêmica superior, baseado em conceitos matemáticos provindos, inicialmente, da álgebra, da análise e da matemática em geral. Em específico no caso do professor do ensino básico espera-se que, apesar de não ser aconselhado aplicar em sua totalidade no ensino básico os conceitos aqui discutidos, se tenha fornecido uma base conceitual que permita dar opções para que o mesmo possa construir estratégias pedagógicas de ensino referente a esse tema,

e que tais se demonstrem eficientes e significativas para o amadurecimento matemático de seus alunos.

Referências Bibliográficas

[1] ÁVILA, G. **Análise Matemática para Licenciatura**. Editora Edigard Blucher LTDA, São Paulo, 2001.

[2] BOYER, C. B. **História da Matemática**. Editora da Universidade de São Paulo, São Paulo, 1974.

[3] DA SILVA, A. L. V. **Números Reais no Ensino Médio: Identificando e Possibilitando Imagens Conceituais**. PhD thesis, PUC-Rio, Rio de Janeiro, 2001.

[4] DA SILVA, M. N. **O Corpo Completo dos Números Reais**. Ceará, 2009.

[5] DE ALENCAR FILHO, E. **Elementos de Análise Algébrica**. Nobel, São Paulo, 1964.

[6] DE FIGUEREDO, D. G. **Análise I**. Editora Universidade de Brasília Livros Técnicos e Científicos Editora S.A, 1975.

[7] DOMINGUES, H. H.; IEZZI, G. **Álgebra Moderna**. Atual Editora LTDA, São Paulo, 1982.

[8] GAMA, L. I. **Introdução à Teoria dos Conjuntos**. Insttituto Brasileiro de Geografia e Estatítica, Rio de Janeiro, 1941.

[9] GUNDLACH, B. H. **Números e Numerais**. Atual Editora LTDA, São Paulo, 2001.

[10] KUROSCH, A. G. **Curso de Álgebra Superior**. Mir, Moscou, 1968.

[11] LANG, S. **Estruturas Algébricas**. Livro Técnico S.A, Rio de Janeiro, 1972.

[12] LIMA, E. L. **Álgebra Linear**. Impa, Rio de Janeiro, 2004.

[13] LIMA, E. L. **Análise Real volume 1: Funções de Uma Variável**. Impa, Rio de Janeiro, 2011.

[14] LIMA, E. L.; CARVALHO, P. C. P.; WAGNER, E.; MORGADO, A. C. **A Matemática do Ensino Médio**. SBM, Rio de Janeiro, 2006.

[15] LIPSCHUTZ, S. **Teoria y Problemas de Teoria de Conjuntos y Temas Afines.** Libros McGraw - Hill de México, S.A, México, 1970.

[16] LOPES, P. C. R. **Construções dos números reais**. Mestrado, Universidade da Madeira, 2006.

[17] MESERVE, B. E. **Conceptos Fundamentales de Algebra**. Universidad de Chile, Santiago, 1965.

[18] MORGADO, A. C.; JÚDICE, E. D.; WAGNER, E.; LIMA, E. L.; DE CARVALHO, J. B. P.; CARNEIRO, J. P. Q.; GOMES, M. L. M.; CARVALHO, P. C. P. **Exame de Textos: Análise de Livros de Matemática para o Ensino Médio**. SBM, Rio de Janeiro, 2001.

[19] NETO, A. C. M. **Tópicos de Matemática Elementar, Números Reais**. SBM, Rio de Janeiro, 2012.

[20] OQUENDO, H. P. **Análise na Reta - Notas de Aula**. Curitiba-PR, 2012.