INSTITUTO DE MATEMÁTICA

Universidade Federal do Rio de Janeiro

UFRJ

Construção dos Números Reais: do Saber de Conteúdo ao Saber Pedagógico de Conteúdo

Jairo Riguetti Godinho Dutra

Rio de Janeiro, Brasil

2 de agosto de 2024

Construção dos Números Reais: do Saber de Conteúdo ao Saber Pedagógico de Conteúdo

Jairo Riguetti Godinho Dutra

Dissertação de mestrado apresentada ao Programa de Pós-graduação em Matemática em Rede Nacional da Sociedade Brasileira de Matemática através do Instituto de Matemática e Estatística da Universidade Federal do Rio de Janeiro, como parte dos requisitos necessários à obtenção do título de Mestre em Matemática.

Universidade Federal do Rio de Janeiro

Instituto de Matemática e Estatística

Programa de Pós-Graduação em Matemática em Rede Nacional

Orientador: Prof. Dr. Nei C. S. Rocha

Rio de Janeiro, Brasil

2 de agosto de 2024

CIP - Catalogação na Publicação

Mengano, Fulano
M962t Titulo / Fulano Mengano. -- Rio de Janeiro, 2019.
101 f.

Orientador: Fulanaorientadora Menganaorientadora.
Coorientador: Fulanacoorientadora Menganacoorientadora.
Tese (doutorado) - Universidade Federal do Rio de Janeiro, Instituto de Matemática, Programa de Pós Graduação em Matemática, 2019.

1. análise. 2. álgebra. 3. geometria. I. Menganaorientadora, Fulanaorientadora, orient. II. Menganacoorientadora, Fulanacoorientadora, coorient. III. Título.

Elaborado pelo Sistema de Geração Automática da UFRJ com os dados fornecidos pelo(a) autor(a), sob a responsabilidade de Miguel Romeu Amorim Neto - CRB-7/6283.

Jairo Riguetti Godinho Dutra

Construção dos Números Reais: do Saber de Conteúdo ao Saber Pedagógico de Conteúdo

Dissertação de mestrado apresentada ao Programa de Pós-graduação em Matemática em Rede Nacional da Sociedade Brasileira de Matemática através do Instituto de Matemática e Estatística da Universidade Federal do Rio de Janeiro, como parte dos requisitos necessários à obtenção do título de Mestre em Matemática.

Trabalho aprovado por

Prof. Dr. Nei C. S. Rocha
Orientador

Professor

Professor

Rio de Janeiro, Brasil
2 de agosto de 2024

Este trabalho é dedicado às crianças adultas que,
quando pequenas, sonharam em se tornar cientistas.

Agradecimentos

agradecimentos principais

Resumo

Este trabalho aborda os principais conjuntos numéricos estudados na Educação Básica no Brasil, com foco no conjunto dos números reais e pretende servir de base e incentivo ao estudo e aprofundamento deste tema por parte dos professores matemática que atuam neste nível de ensino. A abordagem buscou ser, sempre que possível, construtiva. Porém, para não tornar a leitura demasiadamente pesada e cansativa os conjuntos dos números naturais ($\mathbb{N}$) e dos números inteiros ($\mathbb{Z}$), foram apresentados de forma axiomática, mas a partir daí, todos os resultados tratados foram demonstrados. Para introduzir o conjunto dos números racionais ($\mathbb{Q}$), foi utilizada uma noção intuitiva muito comum nos ensinos fundamental e médio, a saber, a ideia de tomar partes de uma unidade dividida em partes iguais. Porém, quando necessário, abandonou-se a intuição para dar lugar às formalizações. Já a apresentação do conjunto dos números reais ($\mathbb{R}$) foi absolutamente formal e construtiva, pois o foco do trabalho é o completo entendimento desse conjunto. Isso porque, muitas vezes a compreensão de $\mathbb{R}$ não é simples, sendo esse um ponto sensível no ensino de conjuntos numéricos na Educação Básica.

Palavras-chave: números, conjuntos numéricos, formalização, axiomas, propriedades.

Abstract

This thesis addresses the main numerical sets studied in Basic Education in Brazil, and aims to contribute for the study and deepening of this theme by mathematics teachers who work at this level of education. The approach sought to be, whenever possible, constructive. But not to make the reading too heavy and tiring the sets of natural numbers ($\mathbb{N}$) and integers ($\mathbb{Z}$) were presented in an axiomatic way. But from there on, all the results were demonstrated. In order to introduce the set of rational numbers ($\mathbb{Q}$), we made use of an intuitive notion very common in elementary and middle school, namely the idea of taking parts of a unit that was divided into equal parts. But when necessary, the intuition was abandoned to give way to the necessary formalizations. On the other hand, the presentation of the set of real numbers ($\mathbb{R}$) was absolutely formal and constructive, because the focus of the work is on the thorough understanding of this set, since very often the understanding of ($\mathbb{R}$) is not simple, this being a sensitive point in the teaching of numerical sets in Basic Education.

Keywords: numbers, numerical sets, formalization, axioms, properties.

Lista de ilustrações

Figura 1 – Quadrado unitário. 64
Figura 2 – Função Alternada. 93

Lista de tabelas

Tabela 1 – Função Alternada 93
Tabela 2 – Organização das frações positivas numa matriz infinita. 95

Sumário

1 NÚMEROS NATURAIS . . . 19
1.1 Axiomas de Peano . . . 20
1.2 Adição . . . 21
1.3 Multiplicação . . . 23
1.4 Relação de Ordem . . . 25
1.5 Uma Via Alternativa . . . 29

2 NÚMEROS INTEIROS . . . 31
2.1 Adição . . . 33
2.2 Multiplicação . . . 33
2.3 Subtração . . . 35
2.4 Relação de Ordem . . . 36
2.5 Resolução de Equações em $\mathbb{Z}$ . . . 42

3 NÚMEROS RACIONAIS . . . 45
3.1 Adição . . . 48
3.2 Multiplicação . . . 51
3.3 Subtração . . . 53
3.4 Divisão . . . 54
3.5 Relação de Ordem . . . 55
3.5.1 $\mathbb{Q}$ é um Corpo Ordenado . . . 59
3.6 A Densidade de $\mathbb{Q}$ . . . 60
3.7 Existência de Incomensuráveis . . . 62

4 NÚMEROS REAIS . . . 65
4.1 A Deficiência de $\mathbb{Q}$ . . . 65
4.2 Cortes de Dedekind . . . 67
4.3 A Construção de Dedekind . . . 69
4.3.1 Adição de Cortes . . . 71
4.3.2 Relação de Ordem entre Cortes . . . 74
4.3.3 Multiplicação de Cortes . . . 77
4.4 O Conjunto dos Números Reais . . . 82
4.5 Um Corpo Ordenado Completo . . . 83
4.6 Axioma do Supremo . . . 85
4.7 Outra Abordagem Além de Dedekind . . . 86

5 SUGESTÕES PARA ABORDAR O CONJUNTO DOS NÚMEROS REAIS NO ENSINO MÉDIO 89
5.1 Considerações Iniciais 89
5.2 Recontar a História 90
5.3 Enumerabilidade 91
5.3.1 $\mathbb{Z}$ é enumerável 92
5.3.2 $\mathbb{Q}$ é enumerável 94
5.4 Outros Conjuntos Enumeráveis 96
5.4.1 $X_{n+\sqrt{p}}$ é enumerável 97
5.4.2 $X_{n\sqrt{p}}$ é enumerável 97
5.5 Tamanho de $\mathbb{R}$ 98
5.6 $\mathbb{R}$ é ou não é enumerável? 98

6 CONSIDERAÇÕES FINAIS 101

REFERÊNCIAS 103

APÊNDICES 105

APÊNDICE A – NÃO EXISTE NÚMERO RACIONAL CUJO QUADRADO SEJA UM NÚMERO PRIMO 107

APÊNDICE B – O CONJUNTO DOS NÚMEROS PRIMOS É INFINITO 109

1 Números Naturais

Os números naturais sempre estiveram relacionados ao processo de contagem, inclusive este é o primeiro contato de muitos estudantes com este conjunto numérico. O método de associar os números naturais a objetos concretos, como a quantidade de brinquedos de uma criança, a quantidade de carteiras em uma sala de aula ou a quantidade de bolinhas de gude que cabem dentro de um pote é uma maneira eficaz para desenvolver a ideia de número natural no imaginário dos alunos.

Entretanto para fins matemáticos, isto é, para o desenvolvimento de um encadeamento lógico de ideias, uma noção intuitiva e informal não é suficiente. Um processo comum em Matemática é a demonstração de teoremas, isto é, a justificação lógica de afirmações a partir de outras afirmações já tidas como irrefutáveis. O princípio de toda essa cadeia de afirmações se dá por meio de teoremas já demonstrados utilizando-se apenas conceitos primitivos[1] e axiomas.

Um axioma é uma afirmação que não é simples o suficiente para ser considerada um conceito primitivo, porém também não pode ser demonstrada por meio das noções básicas assumidas numa determinada teoria. Um axioma muito famoso na Matemática é o Quinto Postulado de Euclides[2]. Durante muito tempo matemáticos proeminentes de diversas épocas tentaram demonstrá-lo sem sucesso. Até que depois de mais de dois mil anos de tentativas Beltrami[3] provou definitivamente que o quinto postulado de Euclides não podia ser demonstrado e, portanto, era de fato, um axioma.

Quanto ao conjunto dos números naturais há pelo menos duas maneiras conhecidas em Matemática para sua formalização. Uma delas é uma abordagem construtiva via Teoria dos Conjuntos que pode ser encontrada em (HALMOS, 2001), a outra é a bastante difundida e conhecida formalização através dos Axiomas de Peano[4].

Neste trabalho a formalização utilizada será a dada por Giuseppe Peano. Ao mesmo tempo, sempre que conveniente as afirmações, definições e operações serão relacionadas com as noções intuitivas adquiridas desde a escola básica a fim de que seja possível estabalecer uma ponte entre o formalismo matemático e os conceitos aprendidos de forma empírica. Tal postura reforça a intenção deste trabalho de servir como uma ferramenta de reflexão a respeito dos conjuntos numéricos para professores da Educação Básica.

---

1 Conceito Primitivo são objetos que não se definem.

2 Euclides de Alexandria foi um matemático e escritor grego que ficou conhecido como o pai da Geometria devido ao seu trabalho entitulado Os Elementos.

3 Eugenio Beltrami foi um matemático italiano formado em Engenharia Ferroviária pela Universidade de Paiva.

4 Giuseppe Peano foi um Matemático italiano considerado um dos fundadores da Lógica Matemática e da Teoria dos Conjuntos.

Destaca-se que este trabalho não pretende lidar com teorias matemáticas demasiadamente abstratas, a profundidade escolhida para tratar os temas varia de acordo com a necessidade. Isto é, o aprofundamento nos conceitos e teorias matemáticas será o suficiente para explicar satisfatoriamente os tópicos abordados.

A fim de conectar o importante conceito de sucessor de um número natural à noção intuitiva de somar uma unidade, é razoável admitr que ao aprender a contar uma criança parece não ter problemas em aceitar que sempre é possível acrescentar mais um elemento à coleção de objetos que se está contando. Esta noção intuitiva de "acrescentar mais um" está presente nos axiomas de Giuseppe Peano e tem como desfecho a definição de soma de dois números naturais.

1.1 Axiomas de Peano

O conjunto do números naturais será denotado pela letra $\mathbb{N}$. Giuseppe Peano caracterizou tal conjunto através dos seguintes axiomas:

1. Todo número natural tem um único sucessor, que também é um número natural.
2. Números naturais diferentes tem sucessores diferentes.
3. Existe um único número natural, designado por 0 que não é sucessor de nenhum outro.
4. Seja X um conjunto de números naturais, isto é, X é um subconjunto de $\mathbb{N}$. Se $0 \in X$ e se, além disso, o sucessor de cada elemento de X ainda pertence a X, então $X = \mathbb{N}$.

O axioma 4 é conhecido como **Axioma da Indução** ele serve como base para diversas demonstrações a respeito de inúmeras propriedades do números naturais, e com algumas adaptações a respeito dos números inteiros também.

Observação 1. *Há divergência a respeito de ser ou não o número* 0 *um número natural. Dessa forma, para alguns autores o conjunto dos números naturais se inicia no número* 1*. Tal discordância não acarreta em erros ou problemas estruturais nas definições e teoremas, trata-se mais de uma questão de conveniência e gosto. Neste trabalho o conjunto do números naturais começa com o número* 0*.*

Como será visto na seção 1.2 o ato ou a operação de tomar o sucessor de um número natural está intimamente ligado à operação de adição. Mais do que isso, tomar o sucessor de um número natural equivale a adicionar a esse número uma unidade. O sucessor de um número natural arbitrário n será representado pelo símbolo $n^\star$.

1.2 Adição

Não é raro encontrar na Matemática definições dadas de forma recursiva[5]. A definição da operação de adição entre números naturais é uma delas.

Definição 1. *A adição de dois números naturais m e n, é designada por $m+n$ e definida do seguinte modo:*

$$\begin{cases} m+0=m \\ m+n^\star=(m+n)^\star \end{cases}$$

Na operação de adição entre dois números naturais quaisquer m e n, esses números são chamados de *parcelas* e o número $m+n$ é chamado de *soma*.

Considerando um número natural arbitrário n, a definição 1 permite concluir que o resultado da adição de n com 0 é o próprio número natural n: $n+0=n$.

Além disso, fornece também a soma de n com o sucessor de 0: $n+0^\star=(n+0)^\star=n^\star$. Ou seja, a soma de um número natural qualquer com o sucessor de 0 é o sucessor do natural arbitrário tomado inicialmente.

A partir daí, pode-se inferir que $n+(0^\star)^\star=(n+0^\star)^\star=(n^\star)^\star$ ou ainda $n+((0^\star)^\star)^\star=(n+(0^\star)^\star)^\star=((n^\star)^\star)^\star$, isto é, dado $n\in\mathbb{N}$ tem-se $n=(0^\star)^{\star\cdots\star}$ para um número finito p $(p\in\mathbb{N})$ de sucessores de 0. Em outras palavras qualquer número natural pode se alcançado aplicando-se a operação de tomar o sucessor de 0 uma quantidade suficiente de vezes. Então

$$m+n=m+(0^\star)^{\star\cdots\star}=(m+0^\star)^{\star\cdots\star}=(m^\star)^{\star\cdots\star} \tag{1.1}$$

Portanto, $m+n$ está definido para todo $m,n\in\mathbb{N}$, isto é, a cada dois números naturais m e n é associado outro número, também natural, chamado soma $m+n$.

Nota-se que utilizando o conceito de sucessor, pode-se somar quaisquer dois números naturais!

Definição 2. *O número natural que é o sucessor de* 0 *será indicado por* 1*, isto é,* $1=0^\star$*, o sucessor do sucessor de* 0 *será indicado por* 2*, ou seja,* $2=1^\star=(0^\star)^\star$*, o sucessor do sucessor do sucessor de* 0 *será indicado por* 3*, a saber* $3=2^\star=((0^\star)^\star)^\star$ *e assim por diante.*

Como essa notação o conjunto dos números naturais pode ser escrito da seguinte forma

$$\mathbb{N}=\left\{0,0^\star,(0^\star)^\star,((0^\star)^\star)^\star,\cdots\right\}=\{0,1,2,3,\cdots\}$$

[5] Que vai até o infinito.

Proposição 1. *Para todo número natural n, tem-se $n^\star = n + 1$ e $n^\star = 1 + n$. Portanto, $n + 1 = 1 + n$.*

Demonstração. Para a primeira igualdade, tem-se: $n + 1 = n + 0^\star = (n + 0)^\star = n^\star$. Para a segunda igualdade seja o conjunto $A = \{n \in \mathbb{N}; n^\star = 1 + n\}$. Decorre da definição de adição de dois números naturais que $0 \in A$, pois $0^\star = 1 = 1 + 0$.

Seja $n \in A$, mostra-se que $n^\star \in A$. De fato, como $n^\star = 1 + n$, tem-se que $(n^\star)^\star = (1 + n)^\star = 1 + n^\star$, isto é, $n^\star \in A$. Assim pelo axioma 4, obtem-se $A = \mathbb{N}$. QED

Antes de demonstrar as propriedades já conhecidas da adição de números naturais, vale ressaltar que a definição formal de soma por meio do processo de tomar o sucessor iteradas vezes está de acordo com a noção intuitiva da escola básica. Por exemplo, quando uma criança, nos seus primeiros anos de escola, deseja encontrar a soma $3+2$ não é raro ver a criança representando com o dedos o número 3 e tomar o sucessor duas vezes, também com os dedos, para chegar na soma.

Teorema 1. *Sejam m, n e p números naturais arbitrários. São verdadeiras as seguintes afirmações:*

1. *Propriedade associativa da adição: $m + (n + p) = (m + n) + p$.*
2. *Existência do elemento neutro da adição: $n + 0 = n = 0 + n$.*
3. *Propriedade comutativa da adição: $m + n = n + m$.*
4. *Lei do cancelamento da adição: $m + p = n + p \Rightarrow m = n$.*
5. *Anulamento da adição: $m + n = 0 \Rightarrow m = n = 0$.*

Demonstração.

1. Sejam fixados, porém abitrários os naturais m e n e seja também o conjunto $A_{(m,n)} = \{p \in \mathbb{N} \mid m + (n + p) = (m + n) + p\}$ de todos os naturais que são associativos com m e n. Pela definição de adição tem-se que $0 \in A_{(m,n)}$, pois $m + (n + 0) = (m + n) + 0$. Tome $k \in A_{(m,n)}$, então $m + (n + k^\star) = m + (n + k)^\star = (m + (n + k))^\star = ((m + n) + k)^\star = (m + n) + k^\star$, ou seja, $k^\star \in A_{(m,n)}$. Logo pelo axioma da indução $A_{(m,n)} = \mathbb{N}$ e a adição é associativa em $\mathbb{N}$.

2. Da definição de adição segue que $n+0 = n$. Seja agora o conjunto $E_0 = \{n \in \mathbb{N} \mid n = 0 + n\}$. Da definição de adição decorre que $0 \in E_0$, pois $0 = 0 + 0$. Tome $k \in E_0$, então $0 + k^\star = (0 + k)^\star = k^\star$, ou seja, $k^\star \in E_0$. Logo pelo axioma da indução $E_0 = \mathbb{N}$ e 0 é o elemento neutro da adição.

3. Seja fixado, porém abitrário o natural m e seja o conjunto $C_m = \{n \in \mathbb{N} \mid n + m = m + n\}$ de todos os naturais que comutam com m. Pela definição de adição tem-se que $0 \in C_m$, pois por (2), $n + 0 = 0 + n$. Tome $k \in C_m$, então pela proposição 1 $k^\star + m = (k + 1) + m = k + (1 + m) = k + (m + 1) = (k + m) + 1 = (m + k) + 1 = (m + k)^\star = m + k^\star$, ou seja, $k^\star \in C_m$. Logo pelo axioma da indução $C_m = \mathbb{N}$ e a adição é comutativa em $\mathbb{N}$.

4. Sejam fixados, porém abitrários os naturais m e n e seja também o conjunto $B_{(m,n)} = \{p \in \mathbb{N} \mid m + p = n + p \Rightarrow m = n\}$ de todos os naturais para os quais vale a lei do cancelamento da adição com m e n. Pela definição de adição tem-se que $0 \in B_{(m,n)}$, pois $m+0 = n+0 \Rightarrow m = n$, já que $m+0 = m$ e $n+0 = n$ Tome $k \in B_{(m,n)}$, então pela proposição 1 $m+k^\star = n+k^\star \Leftrightarrow m+(k + 1) = n+(k + 1) \Leftrightarrow m+(1 + k) = n + (1 + k) \Leftrightarrow (m + 1) + k = (n + 1) + k \Leftrightarrow m + 1 = n + 1 \Leftrightarrow m^\star = n^\star \Leftrightarrow m = n$, ou seja, $k^\star \in B_{(m,n)}$. Logo pelo axioma da indução $B_{(m,n)} = \mathbb{N}$ e vale a lei do cancelamento da adição em $\mathbb{N}$.

5. Suponha por absurdo que se tenha $m + n = 0$, mas que pelo menos um deles seja diferente de zero. Sem perda de generalidade suponha $n \neq 0$, então existe um natural p tal que $p^\star = n$. Assim $0 = m+n = m+p^\star = (m + p)^\star$. Ou seja, zero é o sucessor de algum número natural, o que é um absurdo, pois zero é o único número natural que não é sucessor de nenhum outro. Portanto, se $m + n = 0$ devem ser, necessariamente, $m = n = 0$.

QED

1.3 Multiplicação

Assim como a definição da adição, a operação de multiplicação de dois números naturais é dada recursivamente.

Definição 3. *A multiplicação de dois números naturais m e n é designada por $m \cdot n$ e definida do seguinte modo:*

$$\begin{cases} m \cdot 0 = 0 \\ m \cdot n^\star = m \cdot n + m \end{cases} \equiv \begin{cases} m \cdot 0 = 0 \\ m \cdot (n + 1) = m \cdot n + m \end{cases}$$

Na operação de multiplicação entre dois números naturais quaisquer m e n, esses números são chamados de *fatores* e o número $m \cdot n$ é chamado de *produto*.

Assim como ocorreu com a definição de adição, a definição 3 fornece o resultado da operação de multiplicação de um número natural arbitrário n com o 0: $n \cdot 0 = 0$.

Por motivos de simplicidade será adotada a notação mn para representar a multiplicação dos números m e n, ou seja, $mn = m \cdot n$.

Assim como ocorreu na definição de adição, se faz necessário verificar se a operação de multiplicação entre dois números naturais é uma operação *bem definida*[6]. Para tanto sejam o número natural fixado, porém arbitrário, m e o conjunto $P_m = \{n \in \mathbb{N}; mn \in \mathbb{N}\}$. Verifica-se que $0 \in P_m$, pois $m \cdot 0 = 0 \in \mathbb{N}$. Tomando um $k \in P_m$ tem-se que $mk \in \mathbb{N}$ e, portanto, $m(k+1) = mk + m \in \mathbb{N}$. Em outras palavras, o natural 0 pertence ao conjunto P_m e o fato de um natural qualquer k pertencer ao conjunto P_m implica que o seu sucessor $k+1$ também pertence ao conjunto P_m. Como m foi tomado arbitrário, segue do princípio da indução que $P_m = \mathbb{N}$ e a operação de multiplicação está bem definida no conjunto dos números naturais.

Proposição 2 (Propriedade Distributiva)**.** *Sejam m, n e p números naturais arbitrários. Valem as seguintes igualdades: $m(n+p) = mn + mp$ e $(m+n)p = mp + np$.*

Demonstração. Sejam fixados, porém abitrários os naturais m e n e seja também o conjunto $P_{(m,n)} = \{p \in \mathbb{N} \mid m(n+p) = mn + mp\}$ de todos os naturais que podem ser distribuídos em relação à soma $m + n$. Segue da existência do elemento neutro da adição que $mn = m(n+0)$ e da definição de multiplicação que $mn + m \cdot 0 = mn$, portanto $m(n+0) = mn + m \cdot 0$, logo $0 \in P_{(m,n)}$. Tome $k \in P_{(m,n)}$, então $m(n+k^\star) = m(n+(k+1)) = m((n+k)+1) = m(n+k) + m = (mn+mk) + m = mn + (mk+m) = mn + (m(k+1)) = mn + mk^\star$, ou seja, $k^\star \in P_{(m,n)}$. Logo pelo axioma da indução $P_{(m,n)} = \mathbb{N}$ e a propriedade distributiva vale em $\mathbb{N}$.

De forma análoga, usando indução sobre p, mostra-se que $(m+n)p = mp + np$. QED

Novamente como ocorreu para a adição o teorema 2 reune propriedades já conhecidas da multiplicação de números naturais.

Teorema 2. *Sejam m, n e p números naturais arbitrários. São verdadeiras as seguintes afirmações:*

1. *Propriedade associativa da multiplicação: $m(np) = (mn)p$.*
2. *Propriedade comutativa da multiplicação: $mn = nm$.*
3. *Existência do elemento neutro da multiplicação $n \cdot 1 = n = 1 \cdot n$.*
4. *Anulamento da multiplicação: $mn = 0 \Rightarrow m = 0$ ou $n = 0$.*

Demonstração.

[6] Uma operação é dita bem definida quando o resultado da operação entre dois elementos de um conjunto A ainda é um elemento de A.

1. Sejam fixados, porém abitrários os naturais m e n e seja também o conjunto $A_{(m,n)} = \{p \in \mathbb{N} \mid m\,(np) = (mn)\,p\}$ de todos os naturais que são associativos com m e n. Pela definição de multiplicação tem-se que $0 \in A_{(m,n)}$, pois $m\,(n \cdot 0) = m \cdot 0 = 0 = (mn)\,0$. Tome $k \in A_{(m,n)}$, então $m\,(nk^\star) = m\,(n\,(k+1)) = m\,(nk+n) = m\,(nk) + mn = (mn)\,k + mn = (mn)\,(k+1) = (mn)\,k^\star$, ou seja, $k^\star \in A_{(m,n)}$. Logo pelo axioma da indução $A_{(m,n)} = \mathbb{N}$ e a multiplicação é associativa em $\mathbb{N}$.

2. Inicialmente seja o conjunto $C_0 = \{n \in \mathbb{N} \mid 0 = 0 \cdot n\}$ de todos os naturais que multiplicados por 0, nesta ordem, resultam em 0. Segue da definição de multiplicação que $0 \in C_0$, pois $0 = 0 \cdot 0$. Tome $k \in C_0$, da definição de multiplicação segue que $0 = 0 + 0 = 0 \cdot k + 0 = 0\,(k+1) = 0 \cdot k^\star$, ou seja, $k^\star \in C_0$. Logo pelo axioma da indução $C_0 = \mathbb{N}$ e todos os números nacionais comutam com o zero. Seja agora fixado, porém abitrário o natural m e seja também o conjunto $C_m = \{n \in \mathbb{N} \mid nm = mn\}$ de todos os naturais que comutam com m. Pelo que foi demonstrado $0 \in C_m$, pois $0 \cdot m = 0 = m \cdot 0$. Tome $k \in C_m$, então $mk^\star = m\,(k+1) = mk + m = km + m = (k+1)\,m = k^\star m$, ou seja, $k^\star \in C_m$. Logo pelo axioma da indução $C_m = \mathbb{N}$ e a multiplicação é comutativa em $\mathbb{N}$.

3. De fato, $n \cdot 1 = n$, pois $n \cdot 1 = n \cdot (0+1) = n \cdot 0 + n = 0 + n = n$. Seja agora o conjunto $E_1 = \{n \in \mathbb{N} \mid n = 1 \cdot n\}$. De (2) decorre que $0 \in E_1$, pois $0 = 1 \cdot 0$. Tome $k \in E_1$, então $k^\star = k + 1 = 1 \cdot k + 1 = 1\,(k+1) = 1 \cdot k^\star$, ou seja, $k^\star \in E_1$. Logo pelo axioma da indução $E_1 = \mathbb{N}$ e 1 é o elemento neutro da multiplicação.

4. Suponha por absurdo que sejam ambos m e n diferentes de zero, mas que seja $mn = 0$. Como $n \neq 0$ existe $0 \neq p \in \mathbb{N}$ tal que $n = p^\star = p + 1$, portanto, $0 = mn = mp^\star = m\,(p+1) = mp + m$. Mas essa cadeia de igualdades é um absurdo, pois segundo o item (5) do teorema 1 a soma de dois naturais só é zero quando ambos são zero. Logo pelo menos um entre m e n deve ser igual a zero.

QED

1.4 Relação de Ordem

Intuitivamente é fácil decidir qual dos números 2 ou 7 é o maior. Entretanto, é necessária uma maneira formal de comparar números naturais. Por isso a definição 4 estabelece um critério para essa comparação.

Definição 4. *Dados m e $n \in \mathbb{N}$ diz-se que "m é menor do que ou igual a n" quando existe $p \in \mathbb{N}$ tal que $m + p = n$.*

Simbolicamente

$$m \leq n \Leftrightarrow \exists\, p \in \mathbb{N}; m + p = n.$$

Não raramente a expressão *"m é menor do que ou igual a n"* é substituída pela expressão *"m é menor ou igual a n"*. Esta expressão além de ser gramaticalmente incorreta não transmite a ideia matemática de relação de ordem. Entretanto é uma expressão comumente utilizada por professores e estudantes de matemática.

Quando $m \leq n$ pode-se escreve também $n \geq m$ para representar a mesma relação e tal notação é lida como *"n é maior do que ou igual a m"*.

Fixando a notação $\mathbb{N}^*$ para o conjunto dos números naturais sem o zero, isto é, $\mathbb{N}^* = \{1, 2, 3, \cdots\}$. Pode-se definir uma relação de ordem mais restrita do que a relação 4.

Definição 5. *Dados m e $n \in \mathbb{N}$ diz-se que "m é menor do que n" quando existe $p \in \mathbb{N}^*$ tal que $m + p = n$.*

Simbolicamente

$$m < n \Leftrightarrow \exists\ p \in \mathbb{N}^*; m + p = n.$$

Assim como para a relação *"menor do que ou igual a"*, há, para a relação *"menor do que"*, uma escrita equivalente, a saber, $m < n$ é equivalente a $n > m$ a última sendo lida como *"n é maior do que m"*.

São elencados a seguir alguns teoremas importantes a respeito da relação de ordem no conjunto dos números naturais.

Teorema 3 (Propriedades da Relação de Ordem)**.** *Sejam m, n e $p \in \mathbb{N}$. Valem:*

1. *Reflexividade: $m \leq m$.*
2. *Antissimetria: Se $m \leq n$ e $n \leq m \Rightarrow m = n$.*
3. *Transitividade: Se $m \leq n$ e $n \leq p \Rightarrow m \leq p$.*

Demonstração.

1. Basta observar que $m + 0 = m$.
2. Se $m \leq n$ existe $k \in \mathbb{N}$ tal que $m + k = n$ e se $n \leq m$ existe $j \in \mathbb{N}$ tal que $n + j = m$, logo $n + (j + k) = n \Rightarrow j + k = 0$, mas pelo item (5) do teorema 1 $j + k = 0 \Leftrightarrow j = k = 0$ mostrando que $m = m + 0 = n$.
3. Se $m \leq n$ existe $k \in \mathbb{N}$ tal que $m + k = n$ e se $n \leq p$ existe $j \in \mathbb{N}$ tal que $n + j = p$, então $m + (k + j) = p$ o que é equivalente a dizer que $m \leq p$.

QED

Teorema 4 (Compatibilidade da relação de ordem com as operações em $\mathbb{N}$)**.** *Sejam m, n e $p \in \mathbb{N}$. São válidas as seguintes implicações:*

1. $m \leq n \Rightarrow m + p \leq n + p$.

2. $m \leq n \Rightarrow mp \leq np$.

Demonstração.

1. Se $m \leq n$ existe $k \in \mathbb{N}$ tal que $m + k = n$ segue daí que $n + p = (m + k) + p = m + (k + p) = m + (p + k) = (m + p) + k$, logo $m + p \leq n + p$.

2. Se $m \leq n$ existe $k \in \mathbb{N}$ tal que $m + k = n$ segue daí que $np = (m + k)\, p = mp + kp$, logo $mp \leq np$.

QED

Teorema 5. *Sejam $m, n \in \mathbb{N}$. Então $m < n$ se, e somente se, $m + 1 \leq n$.*

Demonstração. Se $m < n$ existe $k \in \mathbb{N}^*$ tal que $m + k = n$. Como $p \neq 0$ existe $q \in \mathbb{N}$ tal que $p = q^\star = q + 1$. Logo $n = m + k = m + (q + 1) = m + (1 + q) = (m + 1) + q$, ou seja, $m + 1 \leq n$.

Reciprocamente se $m + 1 < n$ existe $k \in \mathbb{N}$ tal que $n = (m + 1) + k = m + (1 + k)$. Como $(1 + k) \neq 0$ segue que $m < n$. QED

Uma importante consequência da definição da relação de ordem dada em 5 no conjunto dos números naturais é apresentada no teorema 6.

Teorema 6 (Lei da Tricotomia em $\mathbb{N}$)**.** *Para quaisquer $m, m \in \mathbb{N}$, tem-se que uma, e apenas uma, das relações segiuntes ocorre:*

1. $m < n$.

2. $m = n$.

3. $m > n$.

Demonstração. Por definição não podem ocorrer simultaneamente (1) e (2) e também (2) e (3). Se (1) e (3) ocorressem ao mesmo tempo existiriam $k, q \in \mathbb{N}^*$ tais que $n = m + k$ e $m = n + q$ de onde se obteria $n + 0 = n = (m + k) = (n + q) + k = n + (q + k)$. Cancelando n seria $q + k = 0$, pelo item (5) do teorema 1 $k = q = 0$, oque é uma contradição. Portanto, (1) e (3) também não ocorrem simultaneamente.

Seja agora o conjunto $T = \{x \in \mathbb{N} \mid x = m \text{ ou } x > m \text{ ou } x < m\}$ onde m um natural fixo e arbitrário. Zero pertence a T, pois ou $0 = m$ ou $0 \neq m$ e no segundo caso $0 < m$, pois $m = 0 + m$. Tome $k \in T$, existem três possibilidades:

1. $k = m$. Neste caso, $k + 1 = m + 1$, de onde $k + 1 > m$ e, portanto, $k + 1 \in T$.

2. $k > m$. Neste caso, existe $p \in \mathbb{N}^*$ tal que $k = m + p$. Então $k + 1 = (m + p) + 1 = m + (p + 1)$, de onde $k + 1 > m$ e, daí, $k + 1 \in T$.

3. $k < m$. Neste caso, existe $p \in \mathbb{N}^*$ tal que $m = k + p$. Como $p \neq 0$, então $p = p' + 1$, $p' \in \mathbb{N}$. Logo $m = k + (p' + 1) = k + (1 + p') = (k + 1) + p'$. Se $p' = 0$, então $m = k + 1$ e $k + 1 \in T$. Se $p' \neq 0$, então $m > k + 1$ e $k + 1 \in T$.

Assim, pelo axioma da indução, $T = \mathbb{N}$. QED

O teorema a seguir é muito importante, pois a partir dele podem ser demonstrados muitos resultados relevantes dos conjuntos numéricos, entre eles esta a Propriedade Arquimediana que vai ser mostrar muito importante ao longo do texto.

Teorema 7 (Princípio da Boa Ordenação)**.** *Todo subconjunto não vazio de* $\mathbb{N}$ *possui um menor elemento.*

Demonstração. Seja S um subconjunto não vazio de $\mathbb{N}$ e considere o conjunto $M = \{n \in \mathbb{N} \mid n \leq x \ \forall x \in S\}$. É claro que $0 \in M$, pois $0 \leq n \ \forall n \in \mathbb{N}$. Como $S \neq \emptyset$ se pode tomar $s \in S$. Então $s + 1 \notin S$, pois $s + 1$ não é menor ou igual a s, assim, $M \neq \mathbb{N}$. Como $0 \in M$ e $M \neq \mathbb{N}$ deve existir $m \in M$ tal que $m + 1 \notin M$, pois caso sontrário, pelo axioma da indução seria M igual a $\mathbb{N}$. Tal m é o menor elemento de S, isto é, $m = \min(S)$! Como $m \in M$, $m \leq x \ \forall x \in S$. Falta verificar que $m \in S$. Para isso suponha por absurdo que $m \notin S$, então $m < x \ \forall x \in S$. Pelo teorema 5 seria $m + 1 \leq x \ \forall x \in S$, de onde resultaria $m + 1 \in M$, o que é uma contradição, pois m foi escolhido de modo que $m + 1 \notin M$. Portanto, $m \in S$ e é o seu menor elemento. QED

Teorema 8. *Para todo número natural* n *vale que* $n < n^\star$. *Em particular* $0 < 1$.

Demonstração. Basta observar que que $1 \in \mathbb{N}^*$ e que $n^\star = n+1$ que decorre imediatamente da definição de ordem que $n < n + 1 = n^\star$. QED

Teorema 9. *Se* $m, n \in \mathbb{N}$ *tais que* $m \leq n \leq m + 1$ *então* $n = m$ *ou* $n = m + 1$.

Demonstração. Suponha, por absurdo, que existe p natural entre m e $m + 1$ que seja diferente destes. Defina o conjunto $S = \{k \in \mathbb{N} \mid m < k < m + 1\}$, que é não vazio, pois $p \in S$. Como $S \subset \mathbb{N}$, pelo Princípio da Boa Ordenação existe $q \in S$ tal que $q \leq k \ \forall k \in S$. Por estar em S segue que $0 < q < 1$. Ou seja, pela definição da relação $<$, existem $c_1, c_2 \in \mathbb{N}$ tais que $q = 0 + c_1$ e $1 = q + c_2$. Multiplicando essas igualdades por q se obtém $q^2 = 0 + c_1 q$ e $q = q^2 + c_2 q$ e, como $c_1 q, c_2 q \in \mathbb{N}^*$, o que implica em $0 < q^2 < q < 1$. Mas isso é um absurdo, pois $q^2 \in S$ e é menor do que q. Logo não existe nenhum número

natural estritamente entre n e $n+1$. Ou, em outras palavras, não existe nenhum número natural entre n e o seu sucessor. QED

Corolário 9.1. *Se $n \in \mathbb{N}$ e $0 \leq n \leq 1$ então $n = 0$ ou $n = 1$.*

Demonstração. Basta fazer $m = 0$ na demonstração do teorema 9. QED

Teorema 10 (Propriedade Arquimediana)**.** *Sejam $a, b \in \mathbb{N}$ com $a \neq 0$, existe um $n \in \mathbb{N}$ tal que $b < na$.*

Demonstração. Se $a = 1$ basta fazer $n = b + 1$ que $b < (b+1) \cdot 1 = na$.

Se $b = 0$ basta fazer $n = 1$, pois $a \neq 0$ então $b = 0 < 1 \cdot a = na$.

Agora se $b \neq 0$ e $a \neq 1$ como $a \neq 0$ decorre de 8 e da transitividade da ordem que $1 < a$. Note que $1 < a \Rightarrow \exists c \in \mathbb{N}^*$ com $a = 1 + c \Rightarrow ba = b + bc$, note ainda que $bc \neq 0$. Basta então fazer $n = b$, pois da igualdade $ba = b + bc$ segue que $b < ba = na$. QED

1.5 Uma Via Alternativa

Na construção do conjunto dos números naturais foram considerados quatro axiomas, dentre eles o axioma da Indução, e a partir daí foram demonstrados alguns teoremas. Entre os teoremas demonstrados está o Princípio da Boa Ordenação, ou seja, o Princípio da Boa Ordenação foi obtido como uma consequência do Princípio da Indução e dos demais axiomas. Um fato interessante, que pode ser visto em (FERREIRA, 2013), é o seguinte: assumindo os três primeiros axiomas de Peano juntamente com o Princípio da Boa Ordenação pode-se provar o Princípio da Indução. Isso significa que o Princípio da Indução e o Princípio da Boa Ordenação são matematicamente equivalentes. Isto é, assumindo os três primeiros axomas de Peano e um dos princípios, o outro pode ser demonstrado como um teorema e, mais do que isso o conjunto numérico obtido com essa nova lista de axiomas é exatamente o mesmo com as mesmas propriedades.

2 Números Inteiros

Neste ponto o professor de Matemática deve estar sentindo falta de duas operações aritméticas recorrentes nas salas de aula da Educação Básica, a saber, as operações de subtração e de divisão. Ao longo do texto serão apresentadas as justificativas para a escolha de não apresentar essas operações ao abordar o conjunto dos números naturais. Ademais, considerando as devidas ressalvas a respeito de onde estão sendo definidas as operações, a subtração pode ser entendida como uma adição e a divisão pode ser entendida como uma multiplicação.

Destaca-se que ao definir as operações de adição e multiplicação de números naturais, tomou-se o cuidado de verificar se estas estavam bem definidas naquele conjunto. Isto é, foi comprovado que, com as definições dada, a soma e o produto de dois numeros naturais ainda eram números naturais. Ou em outras palavras ficou demonstrado que as operações de adição e multiplicação são operações fechadas e $\mathbb{N}$. Simbolicamente: dados $m, n \in \mathbb{N}$ tem-se que $m + n, mn \in \mathbb{N}$.

O principal motivo para não se definir a operação de subtração no conjunto do números naturais é o fato desta não ser uma operação fechada em $\mathbb{N}$. Por exemplo, sabe-se da experiência matemática, inclusive aquela da escola básica, que ao subtrair o natural 5 do natural 3 se obtém como resultado o número -2, e que este não é um número natural.

Na Matemática atual todos os conjuntos numéricos conhecidos podem ser formalizados através de axiomas ou, com exceção do conjuntos dos números naturais, podem ser construídos algebriamente a partir de outro conjunto já conhecido. Com os conjunto dos números inteiros não é diferente. Tal conjunto pode ser formalmente construído a partir do conjunto do números naturais, como sendo o conjunto das classes de equivalência do conjunto $\mathbb{N} \times \mathbb{N}$ com respeito a uma certa relação de equivalência $\sim$. Dito de outra forma o Conjunto dos Números Inteiros, denotado pela letra $\mathbb{Z}$[1] pode ser obtido da seguinte forma $\mathbb{Z} = {}^{\mathbb{N}\times\mathbb{N}}/_{\sim}$, isto é, $\mathbb{Z}$ é o conjunto quociente[2] de $\mathbb{N} \times \mathbb{N}$ com respeito à relação de equivalência $\sim$. O primeiro a utilizar a letra $\mathbb{Z}$ para representar nos números inteiros foi o matemático Landau[3].

Tal construção, apesar de muito bela, utiliza conceitos de matemática de nível superior como relação de equivalência, classe de equivalência e conjunto quociente. Desenvolver esta construção fugiria dos propósitos deste trabalho, que é apresentar ao professor de matemática da educação básica uma fundamentação teórica a respeito dos conjuntos

[1] Devido a palavra alemã Zahl, que significa número.
[2] Conjunto formado pelas classes de equivalência.
[3] Edmund Georg Hermann Landau foi um matemático alemão com contribuições nas áreas de Teoria dos Números e Análise Complexa.

numéricos, em especial o conjunto dos números reais, que dê sentido a esses conjuntos e que permita ao professor ter domínio do tema.

Dessa forma não será feita aqui a apresentação formal da construção de $\mathbb{Z}$ por meio de classes de equivalência. Ao contrário, assim como foi feito na apresentação do conjunto dos números naturais, será dada uma lista de axiomas e, a partir dela serão desenvolvidos pontos importantes a respeito dos números inteiros. A lista de axiomas assumida aqui para caracterizar o conjunto dos números inteiros é um tanto mais extensa do que aquela necessária para descrever os números naturais. Inclusive a lista assumida neste texto não é a menor possível. Isso porque pretenede-se evitar o excesso de proposições e demonstrações, mas ao mesmo tempo pretende-se dar certo formalismo à noção intuitiva de número inteiro já existente no imaginário dos leitores. Os interessados em apreciar o desenvolvimento lógico baseado nas afirmações mínimas necessárias podem consultar (FERREIRA, 2013) onde a construção formal de $\mathbb{Z}$ é feita de forma muito didática.

Vale ressaltar que não é possível evitar completamente noções e conceitos da matemática de nível superior. Não raramente, para completo entendimento do texto, são requeridos conceitos mais comuns nos cursos de graduação. Esses conceitos entretanto são de conhecimento daqueles que passaram por um curso de licenciatura em Matemática. O que se tenta fazer aqui é poupar o professor de coneitos que demandam estudo e conhecmento mais aprofundados.

Como exemplificado dados dois números naturais m e n nem sempre a *diferença*[4] $m - n$ é um número natural. O que se deseja com o conjunto dos números inteiros é completar o conjunto dos números naturais de modo a corrigir essa falha. Isto é, deseja-se subtrair quais dois números, independentemente da relação de ordem entre eles, e encontrar um resultado que ainda seja um número. Para tanto, dado um número natural qualquer n, utiliza-se o símbolo $-n$ para representar o número $0 - n$. Assim $-1 = 0 - 1$, $-2 = 0 - 2$, $-3 = 0 - 3$ e assim em diante, além disso, $-1 = 0 - 1 = 1 - 2 = 2 - 3 = 3 - 4 = \cdots$, o seja, o número -1 pode ser obtido por meio de diferenças de números naturais, de mais de uma maneira. Generalizando essa ideia, o número $-n$ também pode ser obtido de diversas maneiras, a saber, $-n = k - (k + n)$ para quaisquer n e k naturais.

O símbolo $-n$ é dito ser número simétrico do número n. Acrescentando estes novos números ao conjunto dos números naturais cria-se um novo conjunto numérico, a saber, o conjunto dos números inteiros.

$$\mathbb{Z} = \{\cdots, -4, -3, -2 - 1, 0, 1, 2, 3, \cdots\}.$$

Observa-se que, o conjunto dos números naturais está incluído nos conjunto dos números inteiros, ou dito de outra forma o conjunto do naturais é um subconjunto do

[4] Diferença é o nome dado ao resultado da operação de subtração.

conjunto dos inteiros. Isto é, $\mathbb{N} \subset \mathbb{Z}$ e mais do que isso, esses dois conjuntos não são iguais, pois, por exemplo, o número -10 pertence ao conjunto dos números inteiros, porém não pertence ao conjunto dos números naturais.

2.1 Adição

Asssim como no conjunto dos números naturais, no conjunto dos números inteiros está bem definida uma operação binária chamada adição que a cada dois números inteiros $a, b \in \mathbb{Z}$ relaciona um novo número inteiro $a + b \in \mathbb{Z}$ denominado *soma* das *parcelas* a e b.

Para caracterizar a operação de adição no conjunto $\mathbb{Z}$ de forma que as propriedades da adição de números naturais continuem válidas devem ser aceitas como axiomas as seguintes propriedades:

Axiomas de Adição. *Dados a, b e $c \in \mathbb{Z}$ valem as afirmações:*

1. *Propriedade associativa da adição: $a + (b + c) = (a + b) + c$.*
2. *Propriedade comutativa da adição: $a + b = b + a$.*
3. *Existência do elemento neutro da adição: $a + 0 = a = 0 + a$.*
4. *Existência do elemento simétrico (inverso aditivo) da adição: Existe $-a \in \mathbb{Z}$ único, tal que $a + (-a) = 0 = (-a) + a$.*

Para cracterizar completamente o conjunto dos números inteiros ainda são necessários os axiomas de multiplicação e o axioma de distributividade, entretanto apenas com os axiomas de adição já é possível, como mostra a proposição 3, verificar que vale também no conjunto dos números inteiros a lei do cancelamento da adição.

Proposição 3 (Lei do cancelamento da adição)**.** *Para quaisquer a, b e $c \in \mathbb{Z}$ tem-se que, se $a + c = b + c \Rightarrow a = b$.*

Demonstração. Para verificar esta igualdade, basta utilizar o quarto axioma da operação de adição e somar o simétrico c em ambos os lados da igualdade $a + c = b + c$ e depois utilizar o primeiro axioma da adição, o axioma da associatividade. Fazendo isso se obtém $a + c = b + c \Leftrightarrow a + c + (-c) = b + c + (-c) \Leftrightarrow a + 0 = b + 0 \Leftrightarrow a = b$. QED

2.2 Multiplicação

Igualmente define-se no conjunto dos números inteiros a operação binária chamada multiplicação que a cada dois números inteiros $a, b \in \mathbb{Z}$ relaciona um novo número inteiro $ab \in \mathbb{Z}$ denominado *produto* dos *fatores* a e b.

Para caracterizar a operação de multipplicação no conjunto $\mathbb{Z}$ de forma que as propriedades da multiplicação de números naturais continuem válidas devem ser aceitas como axiomas as seguintes propriedades:

Axiomas de Multiplicação. *Dados a, b e $c \in \mathbb{Z}$ valem as afirmações:*

1. *Propriedade associativa da multiplicação: $a\,(bc) = (ab)\,c$.*
2. *Propriedade comutativa da multiplicação: $ab = ba$.*
3. *Lei do cancelamento da multiplicação: Se $a \neq 0$ e $ac = bc \Rightarrow a = b$.*
4. *Existência do elemento neutro da multiplicação: $a \cdot 1 = a = 1 \cdot a$.*

Por fim para caracterização completa do conjunto dos números inteiros, contendo o conjuntos dos números naturais de forma que continuam válidas todas as suas propriedades, é preciso assumir como axioma a distributividade da multiplicação em relação à adição.

Axioma de Distributividade. *Dados a, b e $c \in \mathbb{Z}$ vale: $a\,(b + c) = ab + ac$.*

De posse deste grupo de axiomas pode-se provar as demais regras conhecidas das operações com números inteiros. Para finalizar a seção serão elencadas e demosntradas algumas dessas regras.

Proposição 4. *Para todo inteiro a, tem-se:*

1. $a \cdot 0 = 0$.
2. $(-1) \cdot a = -a$.

Demonstração.

1. Usando a distributividade tem-se que $a \cdot 0 + a \cdot 0 = a\,(0 + 0) = a \cdot 0 = a \cdot 0 + 0$. Ou seja, $a \cdot 0 + a \cdot 0 = a \cdot 0 + 0$. Agora usando a proposição 3, segue-se que $a \cdot 0 = 0$.
2. Usando os axiomas da existência do simétrico, existência do neutro da multiplicação, da distributividade e a propriedade do cancelamento: $-a + a = 0 = 0 \cdot a = (-1 + 1) \cdot a = (-1) \cdot a + 1 \cdot a = (-1) \cdot a + a \Leftrightarrow -a = (-1) \cdot a$.

QED

Proposição 5 (Propriedade do Anulamento da Multiplicação)**.** *Dados $a, b \in \mathbb{Z}$ se $ab = 0 \Rightarrow a = 0$ ou $b = 0$.*

Demonstração. Se $ab = 0$, usando o primeiro item da proposição 4, pode-se escrever $ab = a \cdot 0$. Se $a = 0$, a demosntração está feita. Se $a \neq 0$ usando o axioma do cancelamento da multiplicação $ab = 0 = a \cdot 0 \Leftrightarrow b = 0$.

QED

Proposição 6. *Vale que* $(-1)(-1) = 1$.

Demonstração. Considere a igualdade $0 = (-1) \cdot 0 = (-1)(1 + (-1))$. Da distributividade segue $0 = (-1) \cdot 1 + (-1)(-1) = -1 + (-1)(-1)$, então $0 + 1 = -1 + 1 + (-1)(-1)$. De onde segue que $1 = (-1)(-1)$. QED

Proposição 7 (Regra de Sinais)**.** *Dados* $a, b \in \mathbb{Z}$ *vale:*

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

Demonstração.

1. Usando a existência e a unicidade do elemento simétrico e a lei do cancelamento da adição: $-(-a) + (-a) = 0 = a + (-a) \Leftrightarrow -(-a) = a$
2. Do segundo item da proprosição 4 e pelo axioma de associatividade decorre que $(-a)\, b = ((-1)\, a)\, b = (-1)\, ab = a\,(-1)\, b = a\,(-b) = a\,(-1)\, b = (-1)\,(ab) = -(ab)$.
3. Do que foi demonstrado até aqui segue $(-a)(-b) = ((-1)\, a)\,((-1)\, b) = (-1)(-1)\, ab = 1 \cdot ab = ab$.

QED

2.3 Subtração

Definição 6. *Dados* $a, b \in \mathbb{Z}$*, define-se a subtração de* a *por* b *como*

$$a - b = a + (-b)\,.$$

Ou seja, subtrair b *de* a *é o mesmo que adicionar* a *ao inverso aditivo de* b.

Nota-se que a operação de subtração não é associativa, comutativa tampouco possui elemento neutro. Pois $10 = 5 - (7 - 12) \neq (5 - 7) - 12 = -14$, $2 = 8 - 6 \neq 6 - 8 = -2$.

O candidato a elemento neutro da subtração seria o número 0, mas $0 - a = -a \neq a = a - 0 \ \forall a \in \mathbb{Z}$.

A proposição 8 reúne algumas propriedades satisfeitas pela operação de subtração.

Proposição 8. *Dados a, b e $c \in \mathbb{Z}$ vale:*

1. $(a - b) + b = a$.
2. $-(a + b) = (-a) + (-b) = -a - b$.
3. $-(a - b) = b - a$.
4. $a(b - c) = ab - ac$.

Demonstração.

1. $(a - b) + b = a + (-b) + b = a + 0 = a$.
2. $-(a + b) = (-1)(a + b) = (-1)a + (-1)b = (-a) + (-b) = -a - b$.
3. $-(a - b) = (-1)(a + (-b)) = (-1)a + (-1)(-b) = -a + (-(-b)) = -a + b = b - a$.
4. $a(b - c) = a(a + (-c)) = ab + a(-c) = ab - ac$.

QED

2.4 Relação de Ordem

A fim de estabeler uma relação de ordem em $\mathbb{Z}$ se faz necessário antes definir alguns subconjuntos importantes do conjunto dos inteiros. Assim como foi feito para o conjunto dos números naturais, o conjunto $\mathbb{Z}^*$ representa o conjunto dos números inteiros não nulos. Além disso, $\mathbb{Z}_+$ será chamado do conjunto dos inteiros não negativos, $\mathbb{Z}_-$ será chamado do conjunto dos inteiros não positivos, $\mathbb{Z}_+^*$ é o conjunto dos inteiros positivos e $\mathbb{Z}_-^*$ é o conjunto dos inteiros negativos. Os elementos de cada um desses subconjuntos de $\mathbb{Z}$ são explicitados em símbolos:

$$\mathbb{Z}^* = \{\cdots, -3, -2, -1, 1, 2, \cdots\}$$

$$\mathbb{Z}_+ = \{0, 1, 2, 3, 4, \cdots\}$$

$$\mathbb{Z}_- = \{\cdots, -4, -3, -2, -1, 0\}$$

$$\mathbb{Z}_+^* = \{1, 2, 3, 4, \cdots\}$$

$$\mathbb{Z}_-^* = \{\cdots, -4, -3, -2, -1\}$$

Com esta notação conclui-se que $\mathbb{N} = \mathbb{Z}_+$, portanto, as operações de adição e de multiplicação são fechadas em $\mathbb{Z}_+$, pois elas são na verdade as operações de adição e multiplicação em $\mathbb{N}$, que são operações fechadas naquele conjunto. Também se observa que $\mathbb{Z}$ é a união disjunta dos conjuntos $\mathbb{Z}_-^*$, $\{0\}$ e $\mathbb{Z}_+^*$ Isto é, $\mathbb{Z}$ é a união destes três conjuntos e não há interseção entre pares desses conjuntos. Simbolicamente tem-se: $\mathbb{Z} = \mathbb{Z}_-^* \cup \{0\} \cup \mathbb{Z}_+^*$ e $\mathbb{Z}_-^* \cap \{0\} = \emptyset$, $\{0\} \cap \mathbb{Z}_+^* = \emptyset$ e $\mathbb{Z}_-^* \cap \mathbb{Z}_+^* = \emptyset$

Definição 7. *Dados $a, b \in \mathbb{Z}$ diz-se que "a é menor do que ou igual a b" quando $b - a$ pertence a $\mathbb{Z}_+$.*

Simbolicamente

$$a \leq b \Leftrightarrow b - a \in \mathbb{Z}_+.$$

A expressão $a \leq b$ é equivalente a expressão $b \geq a$ que se lê da seguinte forma: "*b é maior do que ou igual a a*".

Há ainda uma maneira de estabelecer uma ordem em $\mathbb{Z}$ de forma que a definição se assemelhe àquela dada para os números naturais. Diz-se que $a \leq b \Leftrightarrow \exists\, c \in \mathbb{Z}_+; a + c = b$, basta tomar $c = b - a$.

Substituindo-se $\mathbb{Z}_+$ por $\mathbb{Z}_+^*$ na definição 7, obtém-se uma relação de ordem mais restritiva que é a relação *"menor do que"*. Esta relação é dita mais restritiva, pois exclui a possibilidade de serem iguais os números comparados.

Definição 8. *Dados $a, b \in \mathbb{Z}$ diz-se que "a é menor do que b" quando $b - a$ pertence a $\mathbb{Z}_+^*$.*

Simbolicamente

$$a < b \Leftrightarrow b - a \in \mathbb{Z}_+^*.$$

Analogamente dizer que *a é menor do que b* é equivalente a dizer que *b é maior do que a*, que matematicamente se escrever: $b > a$.

Assim como foi feito para a relação de ordem definida em $\mathbb{N}$ os teoremas a seguir compreendem fatos importantes sobre a relação de ordem agora definida em $\mathbb{Z}$.

Teorema 11 (Propriedades da Relação de Ordem)**.** *Sejam a, b e $c \in \mathbb{Z}$. Valem:*

1. *Reflexividade: $a \leq a$.*
2. *Antissimetria: Se $a \leq b$ e $b \leq a \Rightarrow a = b$.*

3. *Transitividade: Se* $a \leq b$ *e* $b \leq c \Rightarrow a \leq c$.

Demonstração.

1. Basta observar que $a - a = 0 \in \mathbb{Z}_+$.

2. Se $a \leq b$, por definição, $b-a \in \mathbb{Z}_+$, da mesma forma se $b \leq a$, por definição, $a-b \in \mathbb{Z}_+$. Como a operação de adição é fechada em $\mathbb{Z}_+$ tem-se que $(b-a)+(a-b) \in \mathbb{Z}_+$. Mas $(b-a)+(a-b) = b-a+a-b = b-0-b = b-b = 0$ e pelo item (5) do teorema 1 a soma de dois naturais é zero se, e somente se, ambos forem simultaneamente zero, logo $b-a = a-b = 0$, donde se conclui que $a = b$.

3. Se $a \leq b$ e $b \leq c$, por definição, $b-a \in \mathbb{Z}_+$ e $c-b \in \mathbb{Z}_+$, pelo fechamento da operação de adição em $\mathbb{N}$ segue que $b-a+c-b = c-a \in \mathbb{Z}_+$. Logo $a \leq c$.

QED

Teorema 12. *Sejam* $a, b \in \mathbb{Z}$. *São válidas as seguintes implicações:*

1. *Se* $0 < a$ *e* $0 < b \Rightarrow 0 < ab$.

2. *Se* $a < 0$ *e* $b < 0 \Rightarrow 0 < ab$.

3. *Se* $0 < a$ *e* $b < 0 \Rightarrow ab < 0$.

Demonstração.

1. Este item decorre diretamente do fechamento da multiplicação em $\mathbb{Z}_+ = \mathbb{N}$ e da Propriedade do Anulamento da Multiplicação, a proposição 5. Se $0 < a$ e $0 < b$ segue que $a - 0 = a$ e $b - 0 = b$ pertencem ambos a $\mathbb{Z}_+^*$, por definição. Logo $ab \in \mathbb{Z}_+^*$, pois $\mathbb{Z}_+^* \subset \mathbb{Z}_+$, mas $ab - 0 = ab$, ou seja, $ab - 0 \in \mathbb{Z}_+^*$ ou $0 < ab$.

2. Se $a < 0$ e $b < 0$ segue, por definição, que $0-a = -a$ e $0-b = -b$ pertencem ambos a $\mathbb{Z}_+^*$. Portanto, pelo fechamento da multiplicação no conjunto dos números naturais e pela proposição 5, $-a \cdot -b \in \mathbb{Z}_+^*$. E pelo item (3) da proposição 7 $-a \cdot -b = ab$. Logo $ab \in \mathbb{Z}_+^*$ o que é o mesmo que $0 < ab$.

3. Se $0 < a$ e $b < 0$ segue, por definição, que $a - 0 = a$ e $0 - b$ pertencem ambos a $\mathbb{Z}_+^*$. Assim, pelo fechamento da multiplicação em $\mathbb{Z}_+$ e pela proposição 5 tem-se que $a\,(b-0) = ab - a \cdot 0 = ab - 0 \in \mathbb{Z}_+^*$. Ou seja, $0 < ab$.

QED

Proposição 9. *Se* $a \in \mathbb{Z}$ *tal* $a < 0$, *então* $0 < -a$.

Demonstração. Se $a < 0$, da definição da ordem estrita, $0-a = -a \in \mathbb{Z}_+^*$. Mas $-a = -a-0$, ou seja, $0 < -a$. QED

Proposição 10. *Todo inteiro positivo é maior do que zero e todo inteiro negativo é menor do que zero.*

Demonstração. Se a é um inteiro positivo, por definição, $a \in \mathbb{Z}_+^*$, mas $a = a - 0$, logo $a - 0 \in \mathbb{Z}_+^*$, portanto, $0 < a$. Analogamente, se a é um inteiro negativo, da proposição 9, $-a \in \mathbb{Z}_+^*$, mas $-a = 0 - a$, logo $0 - a \in \mathbb{Z}_+^*$, portanto, $a < 0$. QED

Teorema 13. *Dados a, b e $c \in \mathbb{Z}$, são válidas as implicações:*

1. $a < b \Leftrightarrow a + c < b + c$.
2. *Se* $a < b$ *e* $0 < c \Rightarrow ac < bc$.
3. *Se* $a < b$ *e* $c < 0 \Rightarrow bc < ac$.

Demonstração.

1. Se $a < b$ pela definição de ordem $b - a \in \mathbb{Z}_+^*$ e $b - a = b + 0 - a = b + c - c - a = b + c - (a + c)$, ou seja, $b + c - (a + c) \in \mathbb{Z}_+^*$ e $a + c < b + c$.
2. Se $a < b$ e $0 < c$, pela definição de ordem $(b - a), c \in \mathbb{Z}_+^*$, logo $c(b - a) \in \mathbb{Z}_+^*$, pois pelo teorema 12 $c(b - a) \in \mathbb{Z}_+$ e pela proposição 5, o produto de dois inteiros só é zero, quando pelo menos um dos fatores é zero. Mas $c(b - a) = bc - ac$. Ou seja, $bc - ac \in \mathbb{Z}_+^*$ o que mostra que $ac < bc$.
3. Se $a < b$ e $c < 0$, pela definição de ordem $(b - a), (0 - c) \in \mathbb{Z}_+^*$, logo $(0 - c)(b - a) \in \mathbb{Z}_+^*$, pois pelo teorema 2.4 $(b - a), (0 - c) \in \mathbb{Z}_+$ e pela proposição 5, o produto de dois inteiros só é zero, quando pelo menos um dos fatores é zero. Mas $(0 - c)(b - a) = -c(b - a) = -bc + ac = ac - bc$. Ou seja, $ac - bc \in \mathbb{Z}_+^*$ o que mostra que $bc < ac$.

QED

Observação 2. *A relação de ordem "menor do que ou igual a" representada pelo símbolo $\leq$ também é compatível com as operações de adição e multiplicação como no teorema 2.4. A demosntração é feita de forma análoga.*

Teorema 14. *Dados $a, b, c, d \in \mathbb{Z}$. Se $a \leq b$ e $c \leq d$ então $a + c \leq b + d$.*

Demonstração. Se $a \leq b$ e $c \leq d$ tem-se que $(b - a), (d - c) \in \mathbb{N}$ logo $\mathbb{N} \ni (b - a) + (d - c) = (b + d) - (a + c)$, isto é, $a + c \leq b + d$. QED

Assim como aconteceu para números naturais, no conjunto dos números inteiros a relação de ordem *"menor do que"* tem uma propriedade muito importante que está descrita na proposição 11.

Proposição 11 (Lei da Tricotomia em $\mathbb{Z}$)**.** *Para quaisquer $a, b \in \mathbb{Z}$, tem-se que uma, e apenas uma, das relações segiuntes ocorre:*

1. $a < b$.
2. $a = b$.
3. $a > b$.

Demonstração. Por definição não podem ocorrer simultaneamente (1) e (2) e também (2) e (3). Se (1) e (3) ocorressem ao mesmo tempo seriam $(a-b), (b-a)$ ambos elementos de $\mathbb{Z}_+^*$ e, consequentemente, seria também um elemento de $\mathbb{Z}_+^*$ o número $a-b+b-a=0$. Mas isso não ocorre, pois $0 \notin \mathbb{Z}_+^*$. Portanto, (1) e (3) também não ocorrem simultaneamente. Agora como $\mathbb{Z}$ é a união disjunta de $\mathbb{Z}_-^*$, $\{0\}$ e $\mathbb{Z}_+^*$, se $a-b \in \mathbb{Z}$, deve necessariamente ocorrer $a-b \in \mathbb{Z}_-^*$ ou $a-b \in \{0\}$ ou $a-b \in \mathbb{Z}_+^*$. QED

É possível definir para certos subconjuntos do conjunto dos números inteiros uma proposição similar ao Princípio da Boa Ordenação definida para o conjunto dos números naturais. Mas para isso são necessárias algumas definições.

Definição 9. *Diz-se que um subconjunto $A \in \mathbb{Z}$ é limitado inferiormente quando existe inteiro k tal que $k \leq a$ para todo $a \in A$. O elemento k quando existe, é chamado de cota inferior do subconjunto A. Se a cota inferior está no conjunto A, dizemos que k é o menor elemento de A.*

Teorema 15 (Princípio do Menor Inteiro)**.** *Todo subconjunto não vazio de $\mathbb{Z}$ limitado inferiormente possui um menor elemento.*

Demonstração. Seja S um subconjunto não vazio de $\mathbb{Z}$ limitado inferiormente. Como S é limitado inferiormente existe $a \in \mathbb{Z}$ tal que $a \leq n$ para todo $n \in S$. então se pode concluir então que o conjunto $R = \{n - a \mid n \in S\}$ é não vazio, pois S é não vazio. Mais do que isso, os elementos de R são todos não negativos, ou seja, $R \subset \mathbb{N}$. Logo existe R possui um menor elemento m_0. Tem-se que $m_0 = n_0 - a$, com $n_0 \in S$ é o menor elemento de S.De fato, se existir $S \ni n_1 < n_0$ acontece $R \ni n_1 - a < n_0 - a$, o que é uma contradição, pois $n_0 - a$ é o menor elemento de R. QED

Com o Princípio do Menor Inteiro pode-se provar uma proposição que pode ser considerada como uma generalização do Axioma da Indução. Vale também para

subconjuntos limitados inferiormente de números inteiros um método de demosntração semelhante ao método teorizado por Giuseppe Peano, e esse é o assunto do teorema 16.

Teorema 16 (Princípio da Indução sobre os Inteiros)**.** *Seja L é um subconjunto não vazio de $\mathbb{Z}$ limitado inferiormente e α seu menor elemento e seja também $\mathcal{P}$ uma proposição válida para α. Nestas condições, se a validade de $\mathcal{P}$ para cada $n \in L$ implicar na validade de $\mathcal{P}$ para $n+1$, então a proprosição $\mathcal{P}$ é válida para todo $n \in L$.*

Demonstração. O conjunto L pode ser descrito da seguinte forma: $L = \{n \in \mathbb{Z} \mid \alpha \leq n\}$. Seja S o conjunto dos elementos de L tais que a proposição $\mathcal{P}$ não é válida, ou seja, $S = \{m \in L \mid \mathcal{P}(m) \text{ é falsa}\}$. Suponha, por absurdo, que $S \neq \emptyset$. Como $S \neq \emptyset$ e S é limitado inferiomente, pelo Princípio do Menor Inteiro S possui um menor elemento $\beta \in S$. Mas α é o menor elemento de L e, portanto, $\alpha \leq \beta$. Mas, por hipótese $\mathcal{P}(\alpha)$ é verdadeira, logo $\alpha \notin S$, logo $\alpha \neq \beta$. Assim $\alpha \leq \beta - 1 \leq \beta$. Como β é o menor elemento de S, a proposição $\mathcal{P}$ vale para $\beta - 1$. Dessa forma, pela hipóstese $\mathcal{P}$ vale para $(\beta - 1) + 1 = \beta$, o que é uma contradição. Logo $S = \emptyset$. QED

Teorema 17. *Não existe nenhum número inteiro n tal que $0 < n < 1$.*

Demonstração. Suponha por absurdo que exista n com essa propriedade. Logo, o conjunto $S = \{k \in \mathbb{Z} \mid 0 < k < 1\}$ é não vazio e limitado inferiormente. Portanto, por 15, S possui um menor elemento a, com $0 < a < 1$. Multiplicando as desigualdades por a segue que $0 < a^2 < a < 1$, logo $a^2 \in S$ e $a^2 < a$, uma contradição. Portanto, $S = \emptyset$. QED

Corolário 17.1. *Dado um número inteiro qualquer n, não existe nenhum número inteior m tal que $n < m < n + 1$.*

Demonstração. Suponha, por absurdo, que exista um inteiro m satisfazendo as desigualdades $n < m < n + 1$, logo $0 < m - n < 1$, o que é uma contradição pelo teorema 17 QED

Para dar uma demonstração sucinta, sem a necessidade de analisar vários casos, da importante Propriedade Arquimediana dos inteiros, é necessário definir antes a noção de *valor absoluto*.

Definição 10. *Seja $a \in \mathbb{Z}$ define-se* $|a| = \begin{cases} a, & \text{se } a \geq 0 \\ -a, & \text{se } a < 0 \end{cases}$.

Da definição 10 segue imediatamente que para todo $a \in \mathbb{Z}$, tem-se $|a| \geq 0$, e $|a| = 0$ se, e somente se, $a = 0$. O número inteiro $|a|$ é chamado de *módulo* de a ou de *valor absoluto de a*.

Além disso, se $a > 0$ e $b > 0$, segue-se que $ab > 0$ e que $|a| = a$ e $|b| = b$, então $|a|\,|b| = ab$. Mas como $ab > 0$, por definição $|ab| = ab$, ou seja, $|ab| = |a|\,|b|$.

Porém, se $a > 0$ e $b < 0$, segue-se que $ab < 0$ e, portanto, $-ab > 0$ e que $|a| = a$ e $|b| = -b$, então $|a|\,|b| = a\,(-b) = -ab$. E como $-ab > 0$, por definição $|ab| = -ab$, ou seja, $|ab| = |a|\,|b|$.

Também, se $a < 0$ e $b > 0$, segue-se que $ab < 0$ e, portanto, $-ab > 0$ e que $|a| = -a$ e $|b| = b$, então $|a|\,|b| = (-a)\,b = -ab$. E como $-ab > 0$, por definição $|ab| = -ab$, ou seja, $|ab| = |a|\,|b|$.

Ainda, se $a < 0$ e $b < 0$, segue-se que $ab > 0$ e que $|a| = -a$ e $|b| = -b$, então $|a|\,|b| = (-a)\,(-b) = ab$, por definição $|ab| = ab$, ou seja, $|ab| = |a|\,|b|$.

Finalmente, se $a = b = 0$, segue-se que $|ab| = |0| = 0 = 0 \cdot 0 = |0|\,|0| = |a|\,|b|$. Ou seja, para quaisquer que sejam $a, b \in \mathbb{Z}$ tem-se que $|ab| = |a|\,|b|$.

Proposição 12. *Se $a, b \in \mathbb{Z}$, com $a \neq 0$, então $|ab| \geq |b|$.*

Demonstração. Como $a \neq 0$ se tem que $|a| \neq 0$ e pelo teorema 17 $|a| \geq 1$. Logo $|ab| = |a|\,|b| \geq |b|$ QED

Teorema 18 (Propriedade Arquimediana)**.** *Sejam $a, b \in \mathbb{Z}$ com $a \neq 0$, existe $n \in \mathbb{Z}$ tal que $b < na$.*

Demonstração. Como $a \neq 0$ se tem que $|a| \neq 0$ e pelo teorema 17 $|a| \geq 1$. Logo da proposição 12 $(|b| + 1)\,|a| \geq |b| + 1 > |b| \geq b$. Então pela desigualdade, basta tomar $n = |b| + 1$, se $a > 0$ e $n = -\,(|b| + 1)$, se $a < 0$. QED

Corolário 18.1. *$\mathbb{N}$ é ilimitado em $\mathbb{Z}$*

Demonstração. Se $b \in \mathbb{Z}$, necessariamente, $|b| \in \mathbb{N}$ e, portanto, $|b| + 1 \in \mathbb{N}$. Suponha por absurdo que o conjunto dos naturais seja limitado em $\mathbb{Z}$ e que b seja uma cota superior para $\mathbb{N}$. Pelo teorema 18 para todo $0 < a \in \mathbb{N}$ basta tomar $n = |b| + 1$ que se tem $b < na$. Como $a, n \in \mathbb{N}$ o produto $na \in \mathbb{N}$ o que contradiz a hipótese de ser b uma cota superior para $\mathbb{N}$. QED

2.5 Resolução de Equações em $\mathbb{Z}$

Historicamente um dos grandes propulsores para desenvolvimento da Aritmética e da Álgebra foi a busca por soluções de equações algébricas[5]. Com o desenvolvimento feito até agora é possível verificar que, dependendo do conjunto numérico considerado, uma equação pode ou não possuir solução.

[5] Uma equação algébrica é uma equação do tipo $a_n x^n + a_{n-1} x^{n-1} + \cdots + a_0 = 0$ onde os coeficientes são números inteiros.

Por exemplo, a equação $2x + 3 = 5$ possui solução em $\mathbb{N}$. É fácil comprovar que $x = 1$ é uma solução da equação, pois $2 \cdot 1 + 3 = 2 + 3 = 5$. Entretanto, a equação $2x + 3 = 1$ não possui solução no conjunto dos números naturais. Contudo se o universo das possíveis soluções for ampliado, e ao invés de buscar soluções em $\mathbb{N}$ considerar-se o conjunto $\mathbb{Z}$ como o espaço onde podem ser encontradas as soluções para a equação $2x + 3 = 1$, sem dificuldade conclui-se que $x = -1$ é uma solução válida, já que $2 \cdot (-1) + 3 = -2 + 3 = 1$.

Esses dois exemplos simples mostram que ampliar o conceito de número traz certas vantagens. De posse dos números inteiros pode-se resolver equações que antes não possuíam solução. Seguramente a passagem dos naturais aos inteiros trouxe muito mais benefícios do que apenas a possibilidade de soluções de novas equações. Muitas situações do cotidiano da humanidade passaram a poder serem modeladas e resolvidas através da Matemática. Um exemplo famoso é a utilização dos números negativos para representar *débitos* ou *dívidas*.

Para os propósitos deste trabalho é suficiente exemplificar que os conjuntos numéricos foram apresentando algumas deficiências, e devido a isso, ao longo da história foram sendo expandidos a fim de que essas falhas fossem sanadas. As duas equações discutidas mostram que não pertencem a $\mathbb{N}$ as soluções de todas as equações algébricas com coeficientes no conjunto dos números naturais e que $\mathbb{Z}$ completa $\mathbb{N}$ no sentido que possibilita a solução de novas equações. Uma pergunta natural que surge diante desse fato é: o conjunto $\mathbb{Z}$ permite a solução de qualquer equação algébrica com coeficientes em $\mathbb{N}$ ou em $\mathbb{Z}$ que se pode imaginar?

É fato bastante conhecido que a respota para essa pergunta é NÃO, por exemplo, a equação $5x + 1 = 0$ assim como a equação $-5x - 1 = 0$ não possuem solução no conjunto dos números inteiros. Essa deficiência do conjunto $\mathbb{Z}$ será a motivação para, mais uma vez, estender o conceito de número.

3 Números Racionais

Como exposto no final do capítulo 2, o conjunto dos números inteiros não contém as soluções de todas as equações com coeficientes inteiros que se pode imaginar. Longe disso, basta tomar uma equação do tipo $ax = b$ com $a, b \in \mathbb{Z}$, $a \neq 0$ e b não sendo um múltiplo de a, que é possível construir infinitas equações com coeficientes inteiros que não possuem solução em $\mathbb{Z}$.

Tendo como motivação, mais uma vez, o desejo de encontrar soluções para qualquer equação que possa ser construída com coeficientes sendo os números inteiros (ressalta-se que $\mathbb{N} \subsetneq \mathbb{Z}$), surge, novamente, a necessidade de ampliar a ideia daquilo que, em Mmatemática, é chamado de número. Não foi exclusivamente a procura por soluções de equações algébricas com coeficientes inteiros que impulsionou o desenvolvimento dos conjuntos numéricos, mas este é o argumento utilizado neste trabalho para dar sentido e servir de justificativa para estudar os vários conjuntos numéricos. O conjunto dos números racionais, por exemplo, começou a ser questionado quanto à sua completude com base numa descoberta a respeito de medição de segmentos e não solução de equações. Tal descoberta demonstrou a existência de segmentos *incomensuráveis*, isto é, segmentos que não podem ser medidos com uma mesma unidade. Foi essa descoberta a maior força motriz para o desenvolvimento do conjunto dos números racionais.

Assim como o conjunto dos números inteiros, o conjunto dos números racionais pode ser construído com todo rigor e formalidade matemática, por meio de classes de equivalência. Considerando o conjunto $\mathbb{Z} \times \mathbb{Z}^*$ e uma determinada relação de equivalência $\sim$ o conjunto dos números racionais, denotado pela letra $\mathbb{Q}$, é definido como $\mathbb{Q} = {}^{\mathbb{Z} \times \mathbb{Z}^*}/_{\sim}$. Ou seja, o conjunto dos números racionais é o conjunto quociente do conjunto $\mathbb{Z} \times \mathbb{Z}^*$ relativamente à relação de equivalência $\sim$. De novo, para um estudo por meio de estruturas algébricas, o leitor interessado pode consultar (FERREIRA, 2013).

Seguindo o espírito do texto, será utilizada uma noção intuitiva de *fração*[1] presente no ensino dos racionais na escola básica, e a partir dela será dada uma formalização matemática para a ideia de número racional. É intuitivo e muito frequente nos ensinos fundamental e médio, por exemplo, relacionar a fração $\frac{3}{6}$ com da divisão de uma pizza ou uma barra de chocolate (ou qualquer outro objeto tomado como unidade) em seis partes iguais da qual foram tomados três pedaços. Mais geralmente, a fração $\frac{p}{q}$ significa que foram tomadas p partes de um todo, (uma pizza uma barra de chocolate, um bolo) que foi dividido em q partes iguais. Além disso, o número que fica acima do traço da fração

[1] Na Educação Básica, ao se estudar números racionais, o significado da palavra fração é o mesmo que parte. Mas do que isso, é: pedaço de um objeto tomado como referência de unidade, que foi dividido em partes iguais.

chama-se numerador da fração e o número que fica abaixo do traço se chama denominador da fração.

A fração $\frac{3}{6}$ é diferente da fração $\frac{6}{12}$! A primeira significa que a unidade (a pizza) foi divida em seis partes iguais e foram tomadas 3 dessas partes. Já a segunda diz que a unidade foi divida em doze partes iguais e foram tomadas seis partes. Entretanto em ambas as frações a quantidade de pizza tomada, ou a quantidade da unidade separada é a mesma. Se o todo foi divido em seis partes iguais e três delas foram tomadas, na verdade foi separada a metade do todo, o mesmo acontecendo se o todo for divido em doze partes iguais e forem tomadas seis dessas partes. Estas duas frações são ditas *equivalentes* e isso significa que elas representam a mesma quantidade.

A ideia de número racional será relacionada às *quantidades* que são representadas por frações. Entretanto, antes de estabelecer essa relação é necessário fixar alguns fatos. O primeiro deles é que parece ser bastante intuitivo e não gerar dúvidas a comparação entre as frações $\frac{4}{5}$ e $\frac{2}{5}$. Pensando em termos da quantidade representada por cada uma das frações, é claro que a fração $\frac{4}{5}$ representa uma quantidade maior do que a quantidade representada pela fração $\frac{2}{5}$. Em outras palavras, sabe-se como comparar frações de mesmo denominador, isto é, para decidir qual dentre as frações $\frac{p}{q}$ e $\frac{m}{q}$ é a maior, bastar olhar para a relação de ordem entre p e m.

O segundo fato é que se uma pizza (uma unidade) foi divida em 2 partes iguais e dessas partes foi tomada 1 parte, a quantidade representada pela fração $\frac{1}{2}$ é exatamente a mesma representada pela fração $\frac{2}{4}$, que representa que a unidade foi dividida em 4 partes iguais e foram separadas 2 partes. Ou ainda, que esta mesma quantidade da unidade pode ser encontrada dividindo-se a pizza em 10 partes iguais e separando-se 5 partes, o que é representado pela fração $\frac{5}{10}$. Generalizando, a quantidade representada por uma fração $\frac{p}{q}$ é exatamente a mesma quantidade representada pela fração $\frac{np}{nq}$ onde $n \in \mathbb{N}^*$.

De agora em diante a fim de evitar a necessidade de se escrever explicitamente que se está referindo a uma quantidade representada por uma fração, ficará subetendido que a notação $\frac{p}{q}$ significa tal quantidade. Com isso, pensando nas quantidades representadas pelas frações pode-se escrever $\frac{1}{2} = \frac{2}{4} = \frac{5}{10} = \cdots$ para dizer que as frações envolvidas nas igualdades são equivalentes.

Postos esses fatos é possível decidir quando duas frações $\frac{p}{q}$ e $\frac{m}{n}$ representam a mesma contidade. Pelo que foi exposto

$$\frac{p}{q} = \frac{pn}{qn} \quad \text{e} \quad \frac{m}{n} = \frac{mq}{nq}.$$

Portanto,

$$\frac{p}{q} = \frac{m}{n} \Leftrightarrow \frac{pn}{qn} = \frac{mq}{nq} \Leftrightarrow pn = mq.$$

As ideias apresentadas até o momento são puramente intuitivas, não há rigor ou

formalidade matemática envolvidos nelas. Entretanto tais fatos constituem uma boa base para aceitação da relação equivalência entre frações. De fato, a conclusão alcançada por meio do raciocínio intuitivo, neste caso, é matematicamente correta, o que leva a uma definição:

Definição 11. *Dados* $p, q \neq 0, m, n \neq 0 \in \mathbb{Z}$ *as frações* $\frac{p}{q} = \frac{m}{n} \Leftrightarrow pn = mq$.

Observação 3. *Note que na definição 11 as restrições impostas sobre os números envolvidos são as seguintes: ambos numerador e denominador das frações devem ser números inteiros, ou seja, podem ser números positivos, negativos ou iguais a zero exceto os denominadores que devem ser, necessariamente, diferentes de zero.*

Isso implica que estão englobadas na definição 11 frações que não possuem sentido na noção intuitiva de dividir uma unidade em partes iguais e tomar algumas destas partes; como, por exemplo, frações como $\frac{7}{5}$*, pois o que significa dividir uma unidade em 5 partes iguais e tomar 7 destas partes? Ou ainda, frações como* $\frac{-8}{13}$, $\frac{5}{-7}$, $\frac{-4}{-9}$ *entre outras.*

Esse fato mostra que embora a busca por uma representação concreta de conceitos matemáticos se mostre bastante efeitiva em alguns casos, nem sempre tal representação é capaz de abarcar a totalidade das ideias envolvidas. Nem por isso se deve abrir mão do recurso da associação concreta ou palpável para entendimento dos conceitos matemáticos; apenas deve-se ter cuidado para entender até que ponto essa associação é útil e, principalmente não permitir que essa ligação limite o desenvolvimento das teorias matemáticas.

Dito isto, estão incluídas entre as frações aceitas, aquelas que não encontraram justificativa de existir na partição da unidade, isto é, frações envolvendo numerador igual a zero e numeradores e denominadores negativos. Tal inclusão se justifica pelo desenvolvimento da teoria.

Já foi mostrado que uma mesma quantidade pode ser representada por infinitas frações diferentes, porém equivalentes. Dada uma quantidade, o conjunto de todas as frações que representam esta quantidade será chamado de classe[2].

Um número racional é uma classe de frações equivalentes, isto é, dada uma quantidade r representada pela classe de frações equivalentes $\left\{\frac{p}{q}, \frac{2p}{2q}, \frac{3p}{3q}, \cdots, \frac{np}{nq}, \cdots\right\}$, chama-se de número racional a classe $\left\{\frac{p}{q}, \frac{2p}{2q}, \frac{3p}{3q}, \cdots, \frac{np}{nq}, \cdots\right\}$. Dito de outra forma o número racional r é a classe de todas as frações que representam a quantidade r, pode-se escrever $r = \left\{\frac{p}{q}, \frac{2p}{2q}, \frac{3p}{3q}, \cdots, \frac{np}{nq}, \cdots\right\}$.

Pelo fato de ser a equivalência entre frações uma relação de equivalência no sentido matemático da expressão, pode-se escrever também $r = \frac{a}{b}$ onde $\frac{a}{b}$ é qualquer uma das frações que representam a quantidade r, ou seja, $\frac{a}{b} \in \left\{\frac{p}{q}, \frac{2p}{2q}, \frac{3p}{3q}, \cdots, \frac{np}{nq}, \cdots\right\}$. Diz-se que $\frac{a}{b}$ é uma representação fracionária do número racional r.

[2] Aqui está se fazendo alusão à classe de equivalência da relação de equivalência entre frações.

O número zero racional é a classe $0 = \left\{\cdots, \frac{0}{-2}, \frac{0}{-1}, \frac{0}{1}, \frac{0}{2}, \frac{0}{3}, \cdots\right\}$, ele é o único número racional que possui representação fracionária tanto com numerador e denominador com mesmos sinais quanto com sinais opostos.

Serão colecionados agora alguns resultados importantes a respeito dos números racionais.

Teorema 19. *Dois números racionais $r = \frac{p}{q}$ e $s = \frac{m}{n}$ são iguais se, e somente se, suas representações fracionárias são equivalentes. Ou, em outras palavras, se, e somente se, são a mesma classe.*

Demonstração. Se $r = s$ segue imediatamente que $\frac{p}{q} = \frac{m}{n}$ o que mostra que $\frac{p}{q}$ e $\frac{m}{n}$ são equivalentes.

Reciprocamente se $\frac{p}{q} = \frac{m}{n}$, seja $r = \frac{j}{k}$ então $\frac{j}{k} = \frac{p}{q}$ e por transitividade (da relação de equivalência) $\frac{m}{n} = \frac{j}{k}$, ou seja, $s = \frac{j}{k}$ e $r = s$. Demonstra-se exatamente da mesma forma que toda fração de s está em r. QED

Teorema 20. *Todo número racional pode ser representado por uma fração com denominador positivo.*

Demonstração. Dado um número racional r, seja $\frac{p}{q}$ um representante. Então, se $q > 0$ não há o que demonstrar, agora se $q < 0$ e como vale $p \cdot (-q) = (-p) \cdot q$, segue que $r = \frac{p}{q} = \frac{-p}{-q}$. Dessa forma, $\frac{-p}{-q}$ é uma fração com denominador positivo que representa r. QED

Finalmente fixando a notação $\mathbb{Q}$ para representar o conjunto dos números racionais e entendendo que os elementos deste conjunto são as quantidades representadas pelas frações de números inteiros, pode-se usar o seguinte abuso de linguagem para descrever de forma sucinta tal conjunto:

$$\mathbb{Q} = \left\{ \frac{p}{q} \mid p, q \in \mathbb{Z}, q \neq 0 \right\}.$$

Ou ainda, como sugere o teorema 20:

$$\mathbb{Q} = \left\{ \frac{p}{q} \mid p, q \in \mathbb{Z}, q > 0 \right\}.$$

3.1 Adição

Para estabelecer a adição de números racionais, mais uma vez será utilizada representação concreta associada à noção de número racional, isto é, a divisão de uma unidade (uma pizza, por exemplo) em partes iguais. Lembrando sempre que tal associação não contempla a totalidade do conceito matemático conhecido como número racional; porém serve muito bem ao propósito de introduzir e elucidar alguns pontos do tema.

Parece fácil aceitar que a quantidade representada pela operação de tomar 2 partes de uma pizza que foi dividia em 6 partes e em seguida tomar mais 3 partes dessa mesma pizza é a mesma quantidade, ou a mesma fração da unidade representada pela fração $\frac{5}{6}$. Utilizando uma notação simbólica o que está sendo dito é:

$$\frac{2}{6} + \frac{3}{6} = \frac{5}{6}.$$

Buscando uma generalização diz-se que a adição de dois números racionais, ou de duas frações de mesmo denonimador se reduz à adição dos números inteiros presentes nos numeradores da frações envolvidas na adição. Se r e s são racionais tais que $r = \frac{p}{q}$ e $s = \frac{m}{q}$ então

$$r + s = \frac{p}{q} + \frac{m}{q} = \frac{p+m}{q}.$$

A pergunta que resta agora é: como definir a adição de frações com denominadores diferentes? A resposta para esta pergunta se baseia na noção de frações equivalentes. Dados os racionais $r = \frac{p}{q}$ e $s = \frac{m}{n}$ basta buscar frações equivalentes que representam, respectivmente, r e s que tenham mesmo denominador e então efetuar a adição.

Pelo que foi desenvolvido $r = \frac{p}{q} = \frac{pn}{qn}$ e $s = \frac{m}{n} = \frac{mq}{nq}$, dessa forma

$$r + s = \frac{p}{q} + \frac{m}{n} = \frac{pn}{qn} + \frac{mq}{nq} = \frac{pn + mq}{nq}.$$

Resumindo o que foi dito, dados os racionais r e s representados, respectivamente, pelas frações $\frac{p}{q}$ e $\frac{m}{n}$, isto é, $r = \frac{p}{q}$ e $s = \frac{m}{n}$, a soma $r+s$, que também é um número racional, tem como uma representação fracionária a fração dada por $\frac{pn+mq}{nq}$, ou seja, $r + s = \frac{pn+mq}{nq}$.

Em todo texto, sempre que foi definida uma operação, tomou-se o cuidado de verificar se tal operação estava *bem definida*. Até este ponto, a expressão estar bem definida significou investigar se o resultado da operação, isto é, a soma, a multiplicação ou a diferença entre os números envolvidos ainda era um elemento do conjunto numérico abordado. Para a adição de números racionais não será diferente. Entretanto, o significado de uma operação estar bem definida neste conjunto é outro, uma vez que com a definição dada é claro que a soma de duas frações ainda é uma fração. Está sendo entendido por fração o quociente e dois números inteiros, então se $m, n \neq 0, p, q \neq 0 \in \mathbb{Z}$ decorre das propriedades com números inteiros que $pq + mq \in \mathbb{Z}$ e que $0 \neq nq \in \mathbb{Z}$ e, portanto, $\frac{pn+mq}{nq}$ é uma fração, ou seja, representa um número racional.

Da forma como foi definido, um número racional pode ser representado por mais de uma fração, então ter uma operação bem definida neste conjunto significa dizer que independentemente da representação fracionária escolhida o resultado da operação é o mesmo. Isto é, a soma $r + s$ independe das representações fracionárias escolhidas para representar r e s. Este é o conteúdo da proposição 13.

Proposição 13. *Sejam os racionais* $r = \frac{p}{q} = \frac{P}{Q}$ *e* $s = \frac{m}{n} = \frac{M}{N}$. *Então ambas as frações* $\frac{pn+mq}{nq}$ *e* $\frac{PN+MQ}{NQ}$ *representam o mesmo número racional* $r + s$.

Demonstração. Como as frações $\frac{p}{q}$ e $\frac{P}{Q}$ representam o mesmo número racional r, elas são frações equivalentes e, portanto $pQ = Pq$. Analogamente, $mN = Mn$. Disso decorre: $(pn + qm)\,QN = pQnN + qQmN = PqnM + qQMn = (PN + QM)\,qn$. Ou seja, $\frac{pn+mq}{nq} = \frac{PN+MQ}{NQ}$ e ambas representam o mesmo racional $r + s$. QED

Já tendo desenvolvido, com base em axiomas, as teorias dos números naturais e dos números inteiros pode-se enunciar como uma proposição e, portando, serem demonstradas as propriedades satisfeitas pela operação de adição em $\mathbb{Q}$.

Proposição 14 (Propriedades da Adição)**.** *Sejam os racionais* $r = \frac{p}{q}$ $s = \frac{m}{n}$ *e* $t = \frac{j}{k}$, *são válidas:*

1. *Propriedade associativa da adição:* $r + (s + t) = \frac{p}{q} + \left(\frac{m}{n} + \frac{j}{k}\right) = \left(\frac{p}{q} + \frac{m}{n}\right) + \frac{j}{k} = (r + s) + t$.
2. *Propriedade comutativa da adição:* $r + s = \frac{p}{q} + \frac{m}{n} = \frac{m}{n} + \frac{p}{q} = s + r$.
3. *Existência do elemento neutro da adição:* $\frac{p}{q} + \frac{0}{1} = \frac{p}{q} = \frac{0}{1} + \frac{p}{q}$, $(r + 0 = r = 0 + r)$.
4. *Existência do elemento simétrico (inverso aditivo) da adição: Existe* $-r = -\frac{p}{q} \in \mathbb{Q}$ *único, tal que* $\frac{p}{q} + \left(-\frac{p}{q}\right) = 0 = \left(-\frac{p}{q}\right) + \frac{p}{q}$, $(r - r = 0 = -r + r)$.
5. *Lei do cancelamento da adição:* $\frac{p}{q} + \frac{m}{n} = \frac{p}{q} + \frac{j}{k} \Rightarrow \frac{m}{n} = \frac{j}{k}$, $(r + s = r + t \Rightarrow s = t)$.

Demonstração.

1. $r+(s+t) = \frac{p}{q}+\left(\frac{m}{n} + \frac{j}{k}\right) = \frac{p}{q}+\frac{mk+jn}{nk} = \frac{pnk+q(mk+jn)}{qnk} = \frac{pnk+qmk+qjn}{qnk} = \frac{(pn+qm)k+qnj}{qnk} = \frac{pn+qm}{qn} + \frac{j}{k} = \left(\frac{p}{q} + \frac{m}{n}\right) + \frac{j}{k} = (r + s) + t$.
2. $r + s = \frac{p}{q} + \frac{m}{n} = \frac{pn+mq}{qn} = \frac{mq+pn}{nq} = \frac{m}{n} + \frac{p}{q} = s + r$.
3. $\frac{p}{q} + \frac{0}{1} = \frac{p\cdot 1+q\cdot 0}{p\cdot 1} = \frac{p}{q}$.
4. $\frac{p}{q} + \left(-\frac{p}{q}\right) = \frac{p}{q} + \frac{-p}{q} = \frac{pq-pq}{pq} = \frac{0}{pq} = 0$.
5. $\frac{p}{q} + \frac{m}{n} = \frac{p}{q} + \frac{j}{k} \Leftrightarrow \frac{-p}{q} + \frac{p}{q} + \frac{m}{n} = \frac{-p}{q} + \frac{p}{q} + \frac{j}{k} \Leftrightarrow 0 + \frac{m}{n} = 0 + \frac{j}{k} \Rightarrow \frac{m}{n} = \frac{j}{k}$.

QED

Observação 4. *Da definição de adição entre frações pode-se concluir que o simétrico do racional* $\frac{p}{q}$ *pode ser escrito como* $\frac{-p}{q}$, *pois dado um número racional o seu simétrico é outro número racional tal que, quando adicionado a ele, obtém-se como soma o número zero.*

Ora, $\frac{p}{q} + \frac{-p}{q} = \frac{pq-pq}{q^2} = \frac{0}{q^2} = 0$. *Logo* $-\frac{p}{q} = \frac{-p}{q}$. *Além disso, se* $q < 0$, *segue-se que* $-q > 0$, *e do teorema 20 todo racional pode ser representado por uma fração com denominador positivo; portanto,* $-\frac{p}{q} = \frac{-p}{q} = \frac{p}{-q}$.

3.2 Multiplicação

Mais uma vez será utilizada a analogia da quantidade tomada, separada ou reservada de uma unidade (uma pizza, por exemplo) ser representada por uma fração, para dar sentido, mesmo que apenas inicialmente, à multiplicação de dois números racionais.

Mais uma vez parece não ser difícil aceitar que, supondo uma unidade divida em 6 pedaços iguais, tomar ou separar um desses pedaços e em seguida outro, em símbolos, equivale a $\frac{1}{6} + \frac{1}{6} = \frac{2}{6}$. Entretanto, tomar seguidamente um pedaço da unidade e em seguida outro pedaço é o mesmo que tomar dois pedaços iguais de uma única vez, ou é o mesmo que

$$2 \cdot \frac{1}{6} = \frac{2}{6}.$$

De modo geral dado $n \in \mathbb{N}$

$$n \cdot \frac{p}{q} = \frac{np}{q}.$$

Neste ponto há duas opções: ou procura-se uma interpretação concreta, como a da divisão da pizza, por exemplo, para justificar a definição da operação de multiplicação (e as demais operações) entre frações, ou simplesmente se apresenta a definição historicamente usada, ressaltando que tal definição prevaleceu e continua a prevalecer, pois possibilita o desenvolvimento frutífero das relações entre os números racionais.

O professor de Matemática deve saber que há uma certa liberdade ao se definir uma operação matemática; portanto, a multiplicação entre números racionais pode ser definida uma forma diferente daquela tradicionalmente usada. O que deve ser questionado é: tal definição trará consigo bons frutos? Proporciona novas descobertas interessantes?

A História da Matemática mostra que a definição de multiplicação de números racionais tradicionalmente usada é bastante fértil, por isso será adota a seguinte postura: aceita-se a definição da operação de multiplicação e a partir daí se analisam os resultados a partir dela.

Dito isso, dados $n \in \mathbb{Z}$, $r = \frac{p}{q}, s = \frac{m}{n} \in \mathbb{Q}$, a multiplicação de um racional por um número inteiro é definida como

$$n \cdot \frac{p}{q} = \frac{np}{q},$$

e a multiplicação de duas frações e definida como

$$r \cdot s = \frac{p}{q} \cdot \frac{m}{n} = \frac{pm}{qn}.$$

Ao resultado da multiplicação entre dois números racionais chama-se *produto*.

Assim como feito para a soma, a proposição 15 verifica que o produto de racionais está bem definido, no sentido que independe da representação fracionária escolhida.

Proposição 15. *Sejam os racionais* $r = \frac{p}{q} = \frac{P}{Q}$ *e* $s = \frac{m}{n} = \frac{M}{N}$*, então ambas as frações* $\frac{pm}{nq}$ *e* $\frac{PM}{NQ}$ *representam o mesmo número racional* $r \cdot s$*.*

Demonstração. Como as frações $\frac{p}{q}$ e $\frac{P}{Q}$ representam o mesmo número racional r, elas são frações equivalentes e, portanto $pQ = Pq$. Analogamente, $mN = Mn$. Disso decorre: $pmNQ = pQmN = PqMn = PMnq$. Ou seja, $\frac{pm}{nq} = \frac{PM}{NQ}$ e ambas representam o mesmo racional $r \cdot s$. QED

Já a proposição 16 verifica as propriedades satisfeitas pela operação de multiplicações entre os racionais.

Proposição 16 (Propriedades da Multiplicação)**.** *Sejam os racionais* $r = \frac{p}{q}$ $s = \frac{m}{n}$ *e* $t = \frac{j}{k}$*, são válidas:*

1. *Propriedade associativa da multiplicação:* $r \cdot (s \cdot t) = \frac{p}{q} \cdot \left(\frac{m}{n} \cdot \frac{j}{k}\right) = \left(\frac{p}{q} \cdot \frac{m}{n}\right) \cdot \frac{j}{k} = (r \cdot s) \cdot t$.
2. *Propriedade comutativa da multiplicação:* $r \cdot s = \frac{p}{q} \cdot \frac{m}{n} = \frac{m}{n} \cdot \frac{p}{q} = s \cdot r$.
3. *Existência do elemento neutro da multiplicação:* $\frac{p}{q} \cdot \frac{1}{1} = \frac{p}{q} = \frac{1}{1} \cdot \frac{p}{q}$, $(r \cdot 1 = r = 1 \cdot r)$.
4. *Existência do elemento inverso da multiplicação: Se* $r \neq 0$ *existe* $r^{-1} = \left(\frac{p}{q}\right)^{-1} \in \mathbb{Q}$ *único, tal que* $\frac{p}{q} \cdot \left(\frac{p}{q}\right)^{-1} = 1 = \left(\frac{p}{q}\right)^{-1} \cdot \frac{p}{q}$, $(r \cdot r^{-1} = 1 = r^{-1} \cdot r)$.
5. *Lei do cancelamento da multiplicação: Se* $\frac{p}{q} \neq 0$ *então* $\frac{p}{q} \cdot \frac{m}{n} = \frac{p}{q} \cdot \frac{j}{k} \Rightarrow \frac{m}{n} = \frac{j}{k}$, $(r \cdot s = r \cdot t \Rightarrow s = t)$.

Demonstração.

1. $r \cdot (s \cdot t) = \frac{p}{q} \cdot \left(\frac{m}{n} \cdot \frac{j}{k}\right) = \frac{p}{q}\left(\frac{mj}{nk}\right) = \frac{pmj}{qnk} = \left(\frac{pm}{qn}\right)\frac{j}{k} = \left(\frac{p}{q} \cdot \frac{m}{n}\right) \cdot \frac{j}{k} = (r \cdot s) \cdot t$.
2. $r \cdot s = \frac{p}{q} \cdot \frac{m}{n} = \frac{pm}{qn} = \frac{mp}{nq} = \frac{m}{n} \cdot \frac{p}{q} = s \cdot r$.
3. $\frac{p}{q} \cdot \frac{1}{1} = \frac{p \cdot 1}{q \cdot 1} = \frac{p}{q}$.
4. $\frac{p}{q} \cdot \left(\frac{p}{q}\right)^{-1} = \frac{p}{q} \cdot \frac{q}{p} = \frac{pq}{qp} = 1$.
5. $\frac{p}{q} \cdot \frac{m}{n} = \frac{p}{q} \cdot \frac{j}{k} \Leftrightarrow \frac{q}{p} \cdot \frac{p}{q} \cdot \frac{m}{n} = \frac{q}{p} \cdot \frac{p}{q} \cdot \frac{j}{k} \Leftrightarrow 1 \cdot \frac{m}{n} = 1 \cdot \frac{j}{k} \Rightarrow \frac{m}{n} = \frac{j}{k}$.

QED

Observação 5. *Da definição de multiplicação entre números racionais pode-se concluir que o inverso do racional* $\frac{p}{q}$ *pode ser escrito como* $\frac{q}{p}$*, pois dado um número racional o seu inverso é outro número racional tais que o porduto entre eles é o número um. Ora,* $\frac{p}{q} \cdot \frac{q}{p} = \frac{pq}{qp} = 1$*, logo* $\left(\frac{p}{q}\right)^{-1} = \frac{q}{p}$*. Além disso, decorre desse fato o único racional que não possui inverso é o zero, porque não está definida nenhuma fração cujo denominador é zero.*

Proposição 17 (Propriedade do Anulamento da Multiplicação)**.** *Dados* $r = \frac{p}{q}, s = \frac{m}{s} \in \mathbb{Q}$ *se* $rs = 0 \Rightarrow r = 0$ *ou* $s = 0$*.*

Demonstração. Se $rs = 0$, necessariamente, $\frac{p}{q} \cdot \frac{m}{n} = \frac{pm}{qn} = 0$, mas $\frac{pm}{qn} = 0 \Leftrightarrow pm = 0$, pois o denominador de uma fração nunca é zero. Então pela propriedade do anulamento da multiplicação em $\mathbb{Z}$ segue que $p = 0$ ou $m = 0$. Mas $p = 0 \Rightarrow r = 0$ e Mas $m = 0 \Rightarrow s = 0$ o que demonstra a proposição.

QED

Por fim, a proposição 18 relaciona as operações de adição e multiplicação entre números racinais.

Proposição 18 (Propriedade Distribuitva)**.** *Dados os racionais* $r = \frac{p}{q}$*,* $s = \frac{m}{n}$ *e* $t = \frac{j}{k}$*, vale:* $r \cdot (s + t) = \frac{p}{q} \cdot \left(\frac{m}{n} + \frac{j}{k}\right) = \frac{p}{q} \cdot \frac{m}{n} + \frac{p}{q} \cdot \frac{j}{k} = r \cdot s + r \cdot t$*.*

Demonstração. $r \cdot (s + t) = \frac{p}{q} \cdot \left(\frac{m}{n} + \frac{j}{k}\right) = \frac{p}{q} \cdot \left(\frac{mk+jn}{nk}\right) = \frac{p(mk+jn)}{qnk} = \frac{pmk+pjn}{qnk} = \frac{pmk}{qnk} + \frac{pjn}{qnk} = \frac{pm}{qn} + \frac{pj}{qk} = \frac{p}{q} \cdot \frac{m}{n} + \frac{p}{q} \cdot \frac{j}{k} = r \cdot s + r \cdot t$. QED

3.3 Subtração

Sempre que se deseja ampliar o conceito de número, é útil que as definições e propriedades estabelecidas nos conjuntos numéricos já existentes sejam mantidas, a fim de que a extensão do conceito traga novas possibilidades e não o contrário, ou seja, limite a teoria já existente. Desse modo, assim como foi feito no conjunto dos números inteiros, a *diferença* entre dois números racionais será definida em termos da adição.

Dados os racionais $r = \frac{p}{q}$ e $s = \frac{m}{n}$ a *diferença* $r - s$ é dada por $r + (-s)$. Ou seja,

$$r - s = \frac{p}{q} - \frac{m}{n} = \frac{p}{q} + \frac{-m}{n} = \frac{pn + (-mq)}{nq} = \frac{pn - mq}{nq}.$$

Novamente deseja-se verificar se a operação de subtração está bem definda, esse trabalho é feito pela proposição 19.

Proposição 19. *Sejam os racionais* $r = \frac{p}{q} = \frac{P}{Q}$ *e* $s = \frac{m}{n} = \frac{M}{N}$*, então ambas as frações* $\frac{pn-mq}{nq}$ *e* $\frac{PN-MQ}{NQ}$ *representam o mesmo número racional* $r - s$*.*

Demonstração. Como as frações $\frac{p}{q}$ e $\frac{P}{Q}$ representam o mesmo número racional r, elas são frações equivalentes e, portanto $pQ = Pq$. Analogamente, $mN = Mn$. Disso decorre: $(pn - qm)\,QN = pQnN - qQmN = PqnN - qQMn = (PN - QM)\,qn$. Ou seja, $\frac{pn-mq}{nq} = \frac{PN-MQ}{NQ}$ e ambas representam o mesmo racional $r - s$. QED

3.4 Divisão

Apesar de não ter sido mencionada ao abordar o conjunto dos números inteiros, a operação de divisão pode ser realizada naquele conjunto. Na verdade a divisão pode ser feita até mesmo no conjunto dos números naturais. O motivo pelo qual a divisão não foi mencionada anteriormente é o fato desta não ser uma operação fechada naqueles conjuntos. Isto é, dados dois números naturais m, n nem sempre o *quociente* $m \div n$ é um número natural, tampouco dados dois números inteiros a, b nem sempre o quociente $a \div b$ é um número inteiro. Isso não acontece no conjunto dos números racionais. Dados dois racionais, é imediato concluir que o quociente entre eles é sempre um número racional. Isto é, o quociente entre dois números racionais possui uma representação fracionária, nos termos definidos neste texto, e por isso representa um número racional.

Mantendo a atitude de aceitar a definição tradicional das operações entre os racionais ao invés de ir buscar sentido numa representação concreta, desde que $0 \neq m \in \mathbb{Z}$ define-se a divisão $(r \div s)$ entre os números $r = \frac{p}{q}$ e $s = \frac{m}{n}$ como sendo o número racional t tal que $r = ts$. Em notação matemática:

$$\frac{p}{q} \div \frac{m}{n} = \frac{x}{y} \Leftrightarrow \frac{p}{q} = \frac{m}{n}\frac{x}{y}.$$

Fazendo $\frac{x}{y} = \frac{pn}{qm}$ verifica-se que $\frac{m}{n}\frac{pn}{qm} = \frac{p}{q}$, logo

$$\frac{p}{q} \div \frac{m}{n} = \frac{pn}{qm}.$$

Mais uma vez deseja-se verificar se a operação recém definida está bem definda no conjunto. Desta vez o serviço é feito pela proposição 20.

Proposição 20. *Sejam os racionais $r = \frac{p}{q} = \frac{P}{Q}$ e $s = \frac{m}{n} = \frac{M}{N}$, então ambas as frações $\frac{pn}{qm}$ e $\frac{PN}{QM}$ representam o mesmo número racional $r \div s$.*

Demonstração. Como as frações $\frac{p}{q}$ e $\frac{P}{Q}$ representam o mesmo número racional r, elas são frações equivalentes e, portanto $pQ = Pq$. Analogamente, $mN = Mn$. Disso decorre: $pnQM = PqnM = PqmN = qmPN$. Ou seja, $\frac{pn}{qm} = \frac{PN}{QM}$ e ambas representam o mesmo racional $r \div s$. QED

Com a definição da divisão no conjunto dos números racionais, as frações podem ser interpretadas como quociente de números inteiros e com essa interpretação é natural a

identificação de um número inteiro n com o número racional $\frac{n}{1}$. Com isso fica constatado que $\mathbb{Z} \subset \mathbb{Q}$, pois $n = 1 \cdot \frac{n}{1}$. Além disso, ficou demonstrado que a soma, a diferença, o produto e o quociente de números racionais possuem representação fracionária, logo são números racionais. Isso significa que as operações de adição, subtração, multiplicação e divisão são operações fechadas em $\mathbb{Q}$.

3.5 Relação de Ordem

Como foi demonstrado no teorema 20 todo número racional pode ser representado por uma fração com denominador positivo, e por isso, se pode escrever $\mathbb{Q} = \left\{\frac{p}{q} \mid p, q \in \mathbb{Z}, 0 < q\right\}$. Tendo como base essa definição do conjunto dos racionais definem-se os seguintes subconjuntos de $\mathbb{Q}$:

O conjunto das frações não nulas

$$\mathbb{Q}^* = \left\{\frac{p}{q} \mid \frac{p}{q} \in \mathbb{Q}, 0 \neq pq\right\}.$$

O conjunto das frações positivas

$$\mathbb{Q}_+^* = \left\{\frac{p}{q} \mid \frac{p}{q} \in \mathbb{Q}, 0 < pq\right\}.$$

O conjunto das frações não negativas

$$\mathbb{Q}_+ = \left\{\frac{p}{q} \mid \frac{p}{q} \in \mathbb{Q}, 0 \leq pq\right\}.$$

O conjunto das frações negativas

$$\mathbb{Q}_-^* = \left\{\frac{p}{q} \mid \frac{p}{q} \in \mathbb{Q}, pq < 0\right\}.$$

O conjunto das frações não positivas

$$\mathbb{Q}_- = \left\{\frac{p}{q} \mid \frac{p}{q} \in \mathbb{Q}, pq \leq 0\right\}.$$

Desse modo, um número racional $\frac{p}{q}$, com $q > 0$, será positivo quando $p > 0$. Além disso, uma fração só é zero quando $p = 0$ e finalmente uma fração só é negativa quando $p < 0$.

De posse destas definições é possível definir uma relação de ordem em $\mathbb{Q}$.

Definição 12. *Dados $r = \frac{p}{q}, s = \frac{m}{n} \in \mathbb{Q}$ com $0 < q, n$ diz-se que:*

- *r é menor do que ou igual a s, ou em símbolos, $\frac{p}{q} \leq \frac{m}{n} \Leftrightarrow \frac{m}{n} - \frac{p}{q} \in \mathbb{Q}_+$.*

- *r é menor do que s, ou em símbolos,* $\frac{p}{q} < \frac{m}{n} \Leftrightarrow \frac{m}{n} - \frac{p}{q} \in \mathbb{Q}_+^*$.

A definição 12 pode ser traduzida em termos da relação de ordem entre números inteiros, pois

$$\frac{p}{q} \leq \frac{m}{n} \Leftrightarrow \frac{m}{n} - \frac{p}{q} \in \mathbb{Q}_+.$$

Mas

$$\frac{m}{n} - \frac{p}{q} = \frac{mq - pn}{nq},$$

então,

$$\frac{p}{q} \leq \frac{m}{n} \Leftrightarrow \frac{mq - pn}{nq} \in \mathbb{Q}_+.$$

Porém

$$\frac{mq - pn}{nq} \in \mathbb{Q}_+ \Leftrightarrow mq - pn \in \mathbb{Z}_+ \Leftrightarrow pn \leq mq.$$

Assim, tem-se

$$\frac{p}{q} \leq \frac{m}{n} \Leftrightarrow pn \leq mq.$$

Analogamente

$$\frac{p}{q} < \frac{m}{n} \Leftrightarrow pn < mq.$$

Serão elencadas agora algumas propriedades satisfeitas pela relação de ordem em $\mathbb{Q}$. Estas proposições são necessárias para mostrar que, assim como em $\mathbb{Z}$, a relação de ordem *"menor do que ou igual a"* definida em $\mathbb{Q}$ é reflexiva, antissimétrica e transitiva.

Proposição 21. *Todo racional positivo r pode ser representado por uma fração com numerador e denominador ambos positivos.*

Demonstração. Seja $r = \frac{p}{q}$; sem perda de generalizada, pelo teorema 20, pode-se supor $q > 0$. Do teorema 12, segue-se que se $p > 0$, necessariamente, $0 < pq$ e, por definição, $r \in \mathbb{Q}_+^*$. QED

Proposição 22. *As operações de adição e de multiplicação são fechadas em $\mathbb{Q}_+$; e mais do que isso, dados $r, s \in \mathbb{Q}_+$, $r + s = 0 \Leftrightarrow r = s = 0$.*

Demonstração. Sejam $r = \frac{p}{q}$ e $s = \frac{m}{n}$ elementos de $\mathbb{Q}_+$. Sem perda de generalidade, pelo teorema 20, pode-se supor que $q > 0$ e $n > 0$ e pelo teorema 12, $0 < qn$. Se $p < 0$, $r \notin \mathbb{Q}_+$, não há o que demonstrar, assim como se $m < 0$, $s \notin \mathbb{Q}_+$, não há o que demonstrar, então $p > 0$ e $m > 0$ e segue-se daí que $0 < pn$ e $0 < qm$.

Assim, por 13 segue-se que $0 < pn + mq$ e, consequentemente, $0 < (pn + mq)\, qn$. Mas é claro que $0 < (pn + mq)\, qn \Rightarrow 0 \leq (pn + mq)\, qn$, mostrando que $r + s \in \mathbb{Q}_+$.

Da mesma forma, por 12 segue-se $0 < pm$ e, consequentemente, $0 < pmpn$, o que implica em $0 \leq pmqn$, mostrando que $r \cdot s \in \mathbb{Q}_+$. E pela propriedade do anulamento da multiplicação de números racionais $r \cdot s = 0 \Leftrightarrow r = s = 0$.

Suponha agora, por absurdo, que sejam $r, s \in \mathbb{Q}_+$, $r \neq 0 \neq s$ e $r + s = 0$. Logo, $r, s \in \mathbb{Q}_+^* \subset \mathbb{Q}_+$ e pela proposição 21, $p, q, m, n > 0$. Dessa forma, $\frac{p}{q} + \frac{m}{n} = \frac{pn+qm}{qn} = 0$, mas $\frac{pn+qm}{qn} = 0 \Leftrightarrow pn + qm = 0$. Como $p, q, m, n > 0$, pn e qm são naturais e, portanto, pelo anulamento da adição dos naturais $pn = qm = 0$. Por definição de fração $q \neq 0 \neq n$, então pelo anulamento da multiplicação dos naturais, $p = m = 0$, o que é uma contradição. Dessa forma, a única maneira de se obter $r + s = 0$ é sendo $r = s = 0$. QED

A proposição 23 afirma que a relação de ordem em $\mathbb{Q}$ tem propriedades semelhantes à relação de ordem em $\mathbb{Z}$.

Proposição 23 (Propriedades da Relação de Ordem)**.** *Sejam $r = \frac{p}{q}, s = \frac{m}{n}$ e $t = \frac{j}{k} \in \mathbb{Q}$. Valem:*

1. *Reflexividade: $r \leq r$.*
2. *Antissimetria: Se $r \leq s$ e $s \leq r \Rightarrow r = s$.*
3. *Transitividade: Se $r \leq s$ e $s \leq t \Rightarrow r \leq t$.*

Demonstração.

1. Basta observar que $r - r = 0 \in \mathbb{Q}_+$.
2. Se $r \leq s$, por definição, $s - r \in \mathbb{Q}_+$, da mesma forma se $s \leq r$, por definição, $r - s \in \mathbb{Q}_+$. Como a operação de adição é fechada em $\mathbb{Q}_+$ tem-se que $(s - r) + (r - s) \in \mathbb{Q}_+$. Mas $(s - r) + (r - s) = s - r + r - s = s - 0 - s = s - s = 0$ e pela proposição 22 a soma de dois racionais não negativos é zero se, e somente se, ambos forem simultaneamente zero, logo $s - r = r - s = 0$, donde se conclui que $r = s$.
3. Se $r \leq s$ e $s \leq t$, por definição, $s - r \in \mathbb{Q}_+$ e $t - s \in \mathbb{Q}_+$, pelo fechamento da operação de adição em $\mathbb{Q}_+$ segue que $s - r + t - s = t - r \in \mathbb{Q}_+$. Logo $r \leq t$.

QED

A relação de ordem no conjunto dos números racionais é compatível com as operações de adição e multiplicação. A proposição 24 mostra isso.

Proposição 24 (Compatibilidade da relação de ordem com as operações em $\mathbb{Q}$)**.** *Dados r, s e $t \in \mathbb{Q}$, são válidas as implicações:*

1. $r < s \Leftrightarrow r + t < s + t$.
2. *Se* $r < s$ *e* $0 < t \Rightarrow rt < st$.
3. *Se* $r < s$ *e* $t < 0 \Rightarrow st < rt$.

Demonstração.

1. Se $r < s$, pela definição de ordem $s - r \in \mathbb{Q}_+^*$ e $s - r = s + 0 - r = s + t - t - r = s + t - (r + t)$, ou seja, $s + t - (r + t) \in \mathbb{Q}_+^*$ e $r + t < s + t$.
2. Se $r < s$ e $0 < t$, pela definição de ordem $(s - r), t \in \mathbb{Q}_+^*$, logo $t(s - r) \in \mathbb{Q}_+^*$, pela proposição 22. Mas $t(s - r) = ts - tr$. Ou seja, $rt - st \in \mathbb{Q}_+^*$ o que mostra que $rt < st$.
3. Se $r < s$ e $t < 0$, pela definição de ordem $(s - r), (0 - t) \in \mathbb{Q}_+^*$, logo $(0 - t)(s - r) \in \mathbb{Q}_+^*$, pela proposição 22. Mas $(0 - t)(s - r) = -t(s - r) = rt - st$. Ou seja, $rt - st \in \mathbb{Q}_+^*$ o que mostra que $st < rt$.

QED

Proposição 25. *Se* $r \in \mathbb{Q}$ *tal* $r < 0$*, então* $0 < -r$.

Demonstração. Se $r < 0$, da definição da ordem estrita, $0 - r = -r \in \mathbb{Z}_+^*$. Mas $-r = -r - 0$, ou seja, $0 < -r$. QED

Proposição 26. *Todo racional positivo é maior do que zero e todo racional negativo é menor do que zero.*

Demonstração. Se r é um racional positivo, por definição, $r \in \mathbb{Q}_+^*$, mas $r = r - 0$, logo $r - 0 \in \mathbb{Q}_+^*$, portanto, $0 < r$. Analogamente se r é um racional negativo, da proposição 25, $-r \in \mathbb{Q}_+^*$, mas $-r = 0 - r$, logo $0 - r \in \mathbb{Q}_+^*$, portanto, $r < 0$. QED

Valem também em $\mathbb{Q}$ a tricotomia a a Propriedade Arquimediana, que são tema das proposições 27 e 28.

Proposição 27 (Lei da Tricotomia em $\mathbb{Q}$)**.** *Para quaisquer* $r, s \in \mathbb{Q}$*, tem-se que uma, e apenas uma, das relações segiuntes ocorre:*

1. $\frac{p}{q} < \frac{m}{n}$
2. $\frac{p}{q} = \frac{m}{n}$
3. $\frac{p}{q} > \frac{m}{n}$

Demonstração. Decorre diretamente da tricotomia em $\mathbb{Z}$, porque $pn < qm \Rightarrow \frac{p}{q} < \frac{m}{n}$, $pn = qm \Rightarrow \frac{p}{q} = \frac{m}{n}$ e $pn > qm \Rightarrow \frac{p}{q} > \frac{m}{n}$. QED

Proposição 28 (Propriedade Arquimediana)**.** *Dados $r, s \in \mathbb{Q}$ com $s \neq 0$, existe $n \in \mathbb{Z}$ tal que $r < ns$.*

Demonstração. Todo racional pode ser escrito com uma representação fracionária com denominador positivo. Então sejam $r = \frac{p}{q}$ com $0 < q$ e $r = \frac{j}{k}$ com $0 < k$. Assim, o que precisa ser provado é $\frac{p}{q} < n\frac{j}{k}$, o que é equivalente a $pk < njq$.

Se $r = 0$ e $0 < s$, basta tomar $n = 1$ que se tem $r = 0 < s = 1 \cdot s = ns$. Agora se $r = 0$ e $0 > s$, basta tomar $n = -1$ que se tem $r = 0 < -s = (-1) \cdot (-a) = ns$.

Se $0 < r = \frac{p}{q} \Rightarrow 0 < p$ e como $0 < k$ segue-se que $0 < pk$. E se $0 < s = \frac{j}{k} \Rightarrow 0 < j$ e como $0 < q$ segue-se que $0 < jq$. Mas $0 < jq \Rightarrow 1 \leq jq \Rightarrow 1 < 2jq$. Multiplicando ambos os membros da inequação por $pk > 0$ segue-se que $pk < 2pkjq$. Então basta tomar $n = 2pk$ para ver que $pk < njq \Leftrightarrow \frac{p}{q} < n\frac{j}{k} \Leftrightarrow r < ns$.

Se $0 < r = \frac{p}{q} \Rightarrow 0 < p$ e como $0 < k$ segue-se que $0 < pk$. E se $0 > s = \frac{j}{k} \Rightarrow 0 > j$ e como $0 < q$ segue-se que $0 > jq$, o que implica em $0 < -jq$. Mas $0 < -jq \Rightarrow 1 \leq -jq \Rightarrow 1 < -2jq$. Multiplicando ambos os membros da inequação por $pk > 0$ segue-se que $pk < -2pkjq$. Então basta tomar $n = -2pk$ para ver que $pk < njq \Leftrightarrow \frac{p}{q} < n\frac{j}{k} \Leftrightarrow r < ns$.

Se $0 > r = \frac{p}{q} \Rightarrow 0 > p$ e como $0 < k$ segue-se que $0 > pk$. E se $0 > s = \frac{j}{k} \Rightarrow 0 > j$ e como $0 < q$ segue-se que $0 > jq$. Mas $1 > 0 > jq \Rightarrow 1 > jq$. Multiplicando ambos os membros da inequação por $pk < 0$ segue-se que $pk < pkjq$. Então basta tomar $n = pk$ para ver que $pk < njq \Leftrightarrow \frac{p}{q} < n\frac{j}{k} \Leftrightarrow r < ns$.

Se $0 > r = \frac{p}{q} \Rightarrow 0 > p$ e como $0 < k$ segue que $0 > pk$. E se $0 < s = \frac{j}{k} \Rightarrow 0 < j$ e como $0 < q$ segue que $0 < jq$ o que implica em $0 > -jq$. Mas $0 > -jq \Rightarrow 1 > 0 > -jq \Rightarrow 1 > -jq$. Multiplicando ambos os membros da inequação por $pk < 0$ segue que $pk < -pkjq$, então basta tomar $n = -pk$ para ver que $pk < njq \Leftrightarrow \frac{p}{q} < n\frac{j}{k} \Leftrightarrow r < ns$. QED

3.5.1 $\mathbb{Q}$ é um Corpo Ordenado

Um conjunto A, com pelo menos dois elementos, é dito um anel[3] se neste conjunto estão definidas duas operações: uma operação denotada por $(+)$ chamada de *adição* e a outra denotada por $(\cdot)$ chamada *multiplicação*. A adição é uma operação associativa, comutativa, possui elemento neutro e possui elemento simétrico; a multiplicação é uma operação associativa e, além disso, vale a distributividade da multiplicação em relação à adição.

[3] Um anel é uma estrutura algébrica, isto é, um conjunto sobre o qual estão definidas uma ou mais operações que satisfazem certas propriedades.

Com esta definição é possível concluir que $\mathbb{N}$ não é um anel, pois neste conjunto nenhum elemento possui elemento simétrico, porém os conjuntos $\mathbb{Z}$ e $\mathbb{Q}$ são anéis.

Ademais, quando a operação de multiplicação de um anel é comutativa diz-se que o anel é um *anel comutativo*. Também quando num anel existe um elemento neutro para a operação de multiplicação diz-se que tal conjunto é um *anel com unidade*. Os conjuntos $\mathbb{Z}$ e $\mathbb{Q}$ são ambos anéis comutativos com unidade.

Um elemento a de um anel com unidade A é dito ser inversível se, e somente se, existe $a' \in A$ tal que $a \cdot a' = 1 = a' \cdot a$. No conjunto $\mathbb{Z}$ os únicos elementos inversíveis são os números -1 e 1, pois $-1 \times -1 = 1$ e $1 \times 1 = 1$.

Por fim, um anel comutativo com unidade é dito ser um *corpo* se, e somente se, todo elemento não nulo é inversível. Como visto na observação 5 todo racional não nulo $r = \frac{p}{q}$ possui um inverso $r' = \frac{q}{p}$ que também é um racional. Portando, $\mathbb{Q}$ é um corpo, e mais do que isso, de todos os conjuntos numéricos discutidos até este ponto ele é o único que satisfaz essa definição.

Em outras palavras, um corpo é um conjunto no qual estão definidas as operações de adição e multiplicação e ambas são associativas, comutativas, possuem elemento neutro, possuem elemento oposto (que para a adição é chamado de simétrico e para a multiplicação é chamado do inverso) e vale a distributividade da multiplicação em relação à adição.

Se em um corpo se pode definir uma ordem que seja compatível com as operações de adição e de multiplicação se diz que este corpo é um corpo ordenado. A proposição 24 mostra que a relação de ordem *"menor do que"* definida em $\mathbb{Q}$ é compatível com as operações lá definidas. Logo o conjunto dos números racionais com as operações de adição e multiplicação usualmente definidas é um corpo ordenado. Costuma-se utilizar a notação $[\mathbb{Q}, +, \cdot, <]$ para indicar este fato.

3.6 A Densidade de $\mathbb{Q}$

Em 3.5.1 foram introduzidas algumas definições da álgebra a fim de caracterizar o conjunto dos números racionais como um corpo ordenado. Isso foi feito seguindo o espírito adotado durante todo o trabalho: o professor de Matemática da educação básica deve conhecer de forma mais aprofundada os assuntos que vai lecionar, para assim ter domínio do conteúdo e ser capaz de elaborar boas estratégias didádicas sobre os temas. Os interessados em Álgebra podem consultar (GARCIA, 2018) para um estudo mais profundo.

Entretanto, mesmo fixando a atenção nos conjuntos abordados até o momento apenas como conjuntos numéricos, as diferenças entre o conjunto dos números racionais e os demais conjuntos é bem maior do que pode parecer a primeira vista. Uma importante diferença característica de $\mathbb{Q}$ que não está presente em $\mathbb{Z}$ e tampouco em $\mathbb{N}$ é dada pelo

teorema 21. Para provar tal teorema é necessário primeiro verificar o lema 1.

Lema 1. *Se s e t são dois racionais quaisquer tais que $t > 0$, então $s - t < s$.*

Demonstração. É claro que $s-(s-t) = s-s+t = t \in \mathbb{Q}_+^*$, daí segue que $s-t < s$. QED

Teorema 21. *Sejam $r, s \in \mathbb{Q}$ tais que $r < s$, então existem infinitos racionais entre r e s.*

Demonstração. Sendo $r < s$ e fazendo $t = \frac{s-r}{n}$ com $n \in \mathbb{N}^*$ segue que $t > 0$, assim do lema 1 se pode concluir que $s - t = s - \frac{s-r}{n} < s$, mas $s - \frac{s-r}{n} < s \Leftrightarrow s - \frac{1}{n}(s-r) < s \Leftrightarrow r - r + s - \frac{1}{n}(s-r) < s \Leftrightarrow r - \frac{n}{n}r + \frac{n}{n}s - \frac{1}{n}(s-r) < s \Leftrightarrow r + \frac{n}{n}(s-r) - \frac{1}{n}(s-r) < s \Leftrightarrow r + \frac{n(s-r)}{n} - \frac{(s-r)}{n} < s \Leftrightarrow r + \frac{(n-1)(s-r)}{n} < s \Leftrightarrow r + (n-1)\frac{(s-r)}{n} < s$, ou seja, $r + (n-1)t < s$. Agora é claro que $r < r + t < r + 2t < r + 3t < \cdots < r + (n-1)t$. Portanto, $r < r+t < r+2t < r+3t < \cdots < r+(n-1)t < s$, isto é, os números racionais $r+t, r+2t, r+3t, \cdots, r+(n-1)t$ estão todos entre r e s. Como n é um natural arbitrário diferente de zero segue o teorema. QED

Observação 6. *A demonstração do teorema 21 só é possível, porque o conjunto dos racionais é um corpo, isto é, porque todo elemento não nulo de $\mathbb{Q}$ possui inverso em $\mathbb{Q}$. Ou, em outras palavras, a demonstração só é possível, porque a operação de divisão é fechada no conjunto dos números racionais. Tal fato não ocorre em $\mathbb{Z}$ muito menos em $\mathbb{N}$, pois não se pode garantir que o número $t = \frac{s-r}{n}$ é um número inteiro ou um número natural.*

Corolário 21.1. *Dados dois números racionais quaisquer r e s tais que $r < s$, a média aritmética entre eles $\frac{r+s}{2}$ é um número racional, tal que $r < \frac{r+s}{2} < s$.*

Demonstração. Basta fazer $n = 2$ na demonsteração do teorema 21. Fazendo isso segue que $r + t = r + \frac{s-r}{2} = r + \frac{s}{2} - \frac{r}{2} = \frac{r}{2} + \frac{s}{2} = \frac{r+s}{2}$. QED

Observação 7. *Quando a média aritmética de dois números inteiros $m < n$ existe, isto é, quando ela ainda é um número inteiro, também vale que $m < \frac{m+n}{2} < n$. Para provar isso basta observar que $m < n \Rightarrow m + m < m + n < n + n \Rightarrow m = \frac{m+m}{2} < \frac{m+n}{2} < \frac{n+n}{2} = n$. O mesmo valendo para o conjunto do números naturais. Para que isso seja verdade basta tomar m e n ambos simultaneamente ou pares ou ímpares.*

Com o exposto no teorema 21 o conjunto dos números racionais ganha uma característica importante, a saber, a propriedade de ser *denso*. Porém perde uma propriedade marcante existente no conjunto dos números naturais e nos subconjuntos de $\mathbb{Z}$ limitados inferiormente, nomeadamente, o Princípio da Boa Ordenação. Não é verdade que todo conjunto de números racionais limitado inferiormente possui um menor elemento. Por exemplo, o conjunto $\mathbb{Q}_+^*$ é limitado inferiormente, mas não possui um menor elemento. Zero é a maior das cotas inferiores deste conjunto e não pertence ao conjunto, assim sendo o menor elemento de $\mathbb{Q}_+^*$, se existir, deve ser positivo. Supondo que seja p este menor

elemento, tem-se que $0 < p$, mas pelo corolário 21.1 segue que $0 < \frac{p}{2} < p$, o seja, $\frac{p}{2}$ é um racional positivo e, portanto, pertence a $\mathbb{Q}_+^*$ que é menor do que p, logo p não é o menor elemento de $\mathbb{Q}_+^*$. Como p foi tomado arbitrário segue que $\mathbb{Q}_+^*$ não possui um menor elemento.

Um conjunto S de números racionais é dito *denso* em $\mathbb{Q}$ se entre dois elementos quaisquer e distintos de $\mathbb{Q}$ existirem infinitos elementos de S. Diante desta definição e do teorema 21 observa-se que $\mathbb{Q}$ é um conjunto denso. É possível afirmar também que $\mathbb{N}$ e $\mathbb{Z}$ não são densos e que nenhum conjunto finito de números racionais é denso.

Em resumo, a partir da definição de número racional o conjunto numérico criado, isto é o conjunto $\mathbb{Q}$, perde a propriedade de ser bem ordenado, mas ganha outra propriedade muito importante, a característica de ser denso.

3.7 Existência de Incomensuráveis

Durante todo este trabalho se tem buscado sistematicamente ampliar o conceito de número a fim de agregar novas possibilidades à Matemática. Por exemplo, a solução de novos modelos de equações, a modelagem de novos problemas práticos entre outras coisas.

Em 3.6 ficou demonstrada uma grande diferença entre o conjunto dos números racionais e o demais conjuntos numéricos vistos até agora. O fato de $\mathbb{Q}$ ser denso mostra que ele possui uma estrutura bastante diferente de $\mathbb{Z}$ e $\mathbb{N}$. Tendo como motivação essa nova propriedade existente somente no conjunto dos números racionais, corre-se o risco de acreditar que o conjunto $\mathbb{Q}$ é suficiente para todos os propósitos teóricos e práticos da Matemática. Entretanto isto não é uma verdade, e para mostrar isso será utilizada ideia de medida de um segmento de reta relacionada a um número racional.

Acontece que os números naturais surgem como uma resposta à necessidade de contar, os números inteiros como um modelo para representar débitos ou dívidas e os números racionais para representar quantidades não inteiras. Dentre as quantidades nem sempre inteiras que podem ser representadas pelos números racionais estão as medidas de segmentos.

Medir nada mais é do que comparar, sendo assim para medir um segmento de reta AB, basta escolher arbitrariamente um segmento u que servirá de segmento padrão (ou unidade) e a partir daí comparar AB e u. Para medir segmentos são necessários alguns axiomas da Geometria Euclidiana: por definição, a medida da unidade u é igual a 1, se o segmento AB é divido em n segmentos justapostos por $n-1$ pontos interiores então a medida AB será igual à soma das medidas desses n segmentos. Além disso, é também aceito como axioma que segmentos congruentes possuem a mesma medida. Se os n segmentos justapostos que compõem AB forem todos congruentes ao segmento unitário,

diz-se que u cabe n vezes em AB e a medida de AB é igual a n.

Como a escolha do segmento unitário é arbitrária nem sempre é possível encaixar o segmento u um número exato de vezes no segmento AB que se pretende medir. Quando isso acontece, um caminho a seguir é procurar um pequeno segmento v que caiba q vezes no segmento unitário u e p vezes no segmento AB. Quando o segmento v existe ele é então uma medida comum entre u e AB, e AB e u são ditos *comensuráveis*. Cabendo v em u uma quantidade igual a q vezes a medida de v é dada pela fração $\frac{1}{q}$ e, consequentemente, a medida de AB será $p \cdot \frac{1}{q} = \frac{p}{q}$.

Durante muito tempo os matemáticos acreditaram que dados dois segmentos de reta quaisquer eles sempre eram comensuráveis, ou seja, para quaisquer segmentos AB e CD, acreditava-se sempre ser possível encontrar um segmento EF que caberia q vezes em AB e p vezes em CD. Porém isso não é verdade!

Esta crença durou até que um membro da escola pitagórica observou que o lado e a diagonal de um quadrado são segmentos *incomensuráveis*. Isto é, não é possível encontrar um segmento que caiba um número exato de vezes q no lado e um número exato de vezes p na diagonal de um quadrado.

Existe uma demonstração utilizando argumentos geométricos e o método da exaustão para demosntrar esse fato; inclusive foi a demonstração dada pela escola pitagórica. Contudo utilizando conhecimentos de aritmética, é possível apresentar uma demosntração mais simples e esta é a demonstração apresentada aqui. Porém, antes é preciso destacar que o produto de dois números pares é um número par e que o produto de dois números ímpares é um número ímpar. Em particular o quadrado de número par é par e o quadrado de um inteiro ímpar é ímpar.

Em notação matemática $2n \times 2n = 2\,(2n^2)$ fazendo $m = 2n^2$ segue $2n \times 2n = 2\,(2n^2) = 2m$, da mesma forma $(2n+1) \times (2n+1) = 2\,(2n^2) + 2\,(2n) + 1 = 2\,(2n^2 + 2n) + 1$ fazendo $k = 2n^2 + 2n$ segue $(2n+1) \times (2n+1) = 2\,(2n^2 + 2n) + 1 = 2k + 1$.

Além disso, todo racional pode ser representado por uma fração irredutível. Por fração irredutível entende-se uma fração $\frac{p}{q}$ na qual p e q não possuem divisores em comum exceto o número 1.

Conhecendo esses fatos observe a figura 1 para comprovar a existência de segmentos incomensuráveis.

Se existisse um segmento v que coubesse q vezes em AB e p vezes na diagonal AC do quadrado $ABCD$, tomando AB como unidade, a medida de AC seria igual ao número racional representado pela $\frac{p}{q}$, e por definição, a medida de AB seria 1. Dessa forma, pelo teorema de Pitágoras seria $\left(\frac{p}{q}\right)^2 = 1^2 + 1^2 = 2$, isto é, existiria um número racional r representado pela fração irredutível $\frac{p}{q}$ tal que $r^2 = 2$. Daí segue que

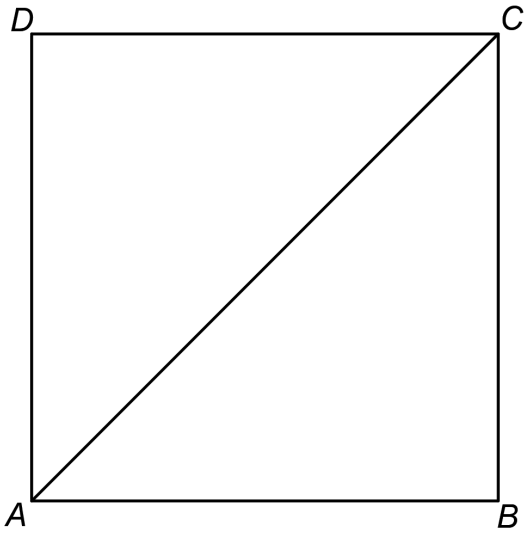

Figura 1 – Quadrado unitário.

$$\frac{p^2}{q^2} = 2 \Leftrightarrow p^2 = 2q^2 \tag{3.1}$$

O termo $2q^2$ é um inteiro par, pois é multiplo de 2, logo como $p^2 = 2q^2$, p^2 é um inteiro par e, consequentemente, p é um inteiro par. Pode-se então escrever $p = 2a$ onde $a \in \mathbb{Z}$. Substituindo p por $2a$ na equação 3.1 se obtém

$$(2a)^2 = 2q^2 \Leftrightarrow 4a^2 = 2q^2 \Leftrightarrow 2a^2 = q^2 \tag{3.2}$$

Analogamente o termo $2a^2$ é um inteiro par, pois é multiplo de 2, logo como $q^2 = 2a^2$, q^2 é um inteiro par e, consequentemente, q é um inteiro par. Ou seja, chegamos a conclusão de que p e q são ambos pares. Mas isso é uma contradição, pois p e q foram supostos inicialmente não possuírem divisores em comum. Esta contradição significa que o lado e a diagonal de um quadrado são incomensuráveis, ou em última análise que não existe número racional cujo quadrado é igual a 2. O que mosrta que o conjunto dos números racionais não é capaz de medir todos os segmentos de reta existentes.

4 Números Reais

4.1 A Deficiência de $\mathbb{Q}$

Nas seções precedentes ficou demonstrado que o conjunto $\mathbb{N}$ e que subconjuntos de $\mathbb{Z}$ limitados inferiormente são bem ordenados, isto é, possuem um menor elemento. Enquanto que o conjunto $\mathbb{Q}$ não possui essa propriedade, porém é um conjunto denso.

Existe um conceito que substitui o menor elemento de um conjunto quando este não existe. Este conceito é o *ínfimo*, o ínfimo de um conjunto limitado inferiormente é a maior das cotas inferiores desse conjunto. Por exemplo, o conjunto $S = \left\{\frac{1}{n} \mid n \in \mathbb{N}^*\right\}$ é claramente limitado inferiormente, pois qualquer número negativo é uma cota inferior para ele, mas não possui menor elemento. Entretanto o ínfimo de S é o número zero. Para verificar isso observa-se que zero é uma cota interior para S. Como zero é maior do que qualquer número negativo se α é o ínfimo de S deve ser, necessariamente, $\alpha \geq 0$. Supondo que $\alpha > 0$, pela propriedade arquimediana existe $n \in \mathbb{N}^*$ tal que $1 < n\alpha \Leftrightarrow \frac{1}{n} < \alpha$. Isso mostra que existe um elemento de S que é menor do que α, contradizendo o fato de ser α uma cota inferior para S. Portanto, $\alpha > 0$ não pode ser o ínfimo de S restando apenas a opção $\inf(S) = 0$. Quando um conjunto limitado inferiormente possui elemento mínimo é ele o ínfimo do conjunto.

Como visto na seção 3.5.1 o conjunto $\mathbb{Q}$ é um corpo ordenado, além disso da seção 3.6 segue que o conjunto dos números racionais é denso. Agora, diante da nova definição de ínfimo, uma pergunta pertinente é a seguinte: no corpo dos números racionais todo conjunto limitado inferiomente possui um ínfimo?

A resposta para essa pergunta é NÃO, e a existência de segmentos incomensuráveis é uma pista para mostrar isso. Para exemplificar este fato seja $X = \left\{r \in \mathbb{Q}_+^* \mid 2 < r^2\right\}$, note que este conjunto é limitado inferiormente, por exemplo por 0, pois todos os seus elementos são positivos. Será demonstrado que este conjunto não possui ínfimo.

Inicia-se mostrando que X não possui elemento mínimo. De fato, dado qualquer $r \in X$, tem-se $0 < r$ e $2 < r^2$. Pelo teorema 21 pode-se obter um número racional x tal que $0 < x < \frac{r^2-2}{2r}$. Logo $2rx < r^2 - 2 \Leftrightarrow 2 < r^2 - 2rx < r^2 - 2rx + x^2 = (r-x)^2$, isto é, $2 < (r-x)^2$. Além disso, $x < \frac{r^2-2}{2r} = \frac{r}{2} - \frac{1}{r} < \frac{r}{2} < r$ de onde segue que $r - x > 0$. Dessa forma, dado $r \in X$ arbitrário, é possível obter $r - x \in X$ com $r - x < r$. Dito de outra forma, dado qualquer racional r pertencente a X sempre é possível encontrar outro racional s menor do que o racional r que ainda é um elemento de X, por isso não existe elemento mínimo em X.

Para mostrar que o conjunto X não possui ínfimo será necessário lançar mão

de um conjunto auxiliar, mas para entender os argumentos que envolvem esse conjunto são necessárias algumas definições. Assim como certos conjuntos limitados inferiormente possuem um menor elemento, existe uma noção equivalente, a saber, o *maior elemento* para conjuntos que são *limitados superiormente*. Estes objetos são tema da definição 13.

Definição 13. *Diz-se que um subconjunto $A \in \mathbb{Z}$ é limitado superiormente quando existe inteiro k tal que $a \leq k$ para todo $a \in A$. O elemento k quando existe, é chamado de cota superior do subconjunto A. Se a cota superior está no conjunto A, dizemos que k é o maior elemento de A.*

Da mesma, forma para conjuntos limitados superiormente que não são bem ordenados, isto é, que não possuem um maior elemento define-se o *supremo* que é a menor das cotas superiores deste conjunto.

Voltando ao conjunto X, trilhando o caminho para mostra que este conjunto não possui ínfimo, considera-se o conjunto auxiliar $Y = \{s \in \mathbb{Q}_+ \mid s^2 < 2\}$. Este conjunto é limitado superiormente. Por exemplo, o número 2 é uma cota superior para Y, pois $s^2 < 2 < 4 = 2^2 \Rightarrow s^2 < 2^2$ e como $s \geq 0$ e $2 > 0$, para todo $s \in Y$, $s^2 < 2^2 \Rightarrow s < 2$. Assim como X é limitado inferiormente e não possui ínfimo, Y é limitado superiormente e não possui supremo. Para mostrar que X não possui ínfimo é necessário mostrar antes que Y não possui elemento máximo.

De fato, dado $s \in Y$ novamente pelo teorema 21 se pode tomar um racional $y < 1$ tal que $0 < y < \frac{2-s^2}{2s+1}$. Da desigualdade $y < 1$ seque que $y^2 < y$ e da desigualdade $y < \frac{2-s^2}{2s+1}$ segue que $y\,(2s+1) < 2-s^2$. Mas $(s+y)^2 = s^2+2sy+y^2 < s^2+2sy+y = s^2+y\,(2s+1) < s^2+2-s^2 = 2$. Assim dado s arbitrário pertencente a Y sempre é possível encontrar $s+y$ maior do que s que ainda é um elemento de S, mostrando que Y não possui elemento máximo.

Além disso, se $s \in Y$ e $r \in X$ segue que $s^2 < 2 < r^2$ e, portanto, $s^2 < r^2$. Como r e s são ambos positivos segue que $s < r$.

Supondo agora que exista $a \in \mathbb{Q}$ tal que $a = \inf(X)$. Deve necessariamente ocorrer que $a > 0$, pois 1 é uma cota inferior para X e sendo $a = \inf(X)$ deve ocorrer $a \geq 1$. Não pode ocorrer $2 < a^2$, porque isso obrigaria $a \in X$ e a seria o elemento mínimo de X, mas, como demosntrado, X não possui elemento mínimo.

Da mesma forma, não pode ocorrer $a^2 < 2$, porque isso implicarira em $a \in Y$, então então existiria $b \in Y$ tal que $a < b$, porque como demosntrado Y não possui elemento máximo. Como $a, b \in Y$ com $a < b$, valeria $a^2 < b^2 < 2 < r^2$ e, consequentemente, $a < b < r$ para todo $r \in X$, o que contradiz o fato $a = \inf(X)$.

Desse modo, se existir $a \in \mathbb{Q}$ tal que $a = \inf(X)$, deve, necessariamente, ocorrer $a^2 = 2$. Mas como visto na seção 3.7 não existe número racional cujo quadrado é igual a 2.

Logo o conjunto X não possui ínfimo em $\mathbb{Q}$.

Analogamente se mostra que o conjunto Y não possui supremo em $\mathbb{Q}$. Supondo que existe $b \in \mathbb{Q}$ tal que $b = \sup(Y)$, então deve ser, forçosamente, $b > 0$, pois $0 < 1 \in Y$ e sendo $b = \sup(Y)$ deve ser $1 \leq b$. Além disso, não pode ser $b^2 < 2$, pois isso implicaria em $b \in Y$ e então b seria o maior elemento de Y, mas como demonstrado tal elemento não existe.Igualmente não pode ser $2 < b^2$, porque isso implicaria em $b \in X$, que não possui menor elemento. Então existitia $a \in X$ tal que $a < b$. Como $a, b \in Y$ com $a < b$ valeria $a^2 < b^2 < 2 < s^2$ e, consequentemente, $a < b < s$ para todo $s \in Y$, o que contradiz o fato $b = \sup(Y)$.

Desse modo, se existir $b \in \mathbb{Q}$ tal que $b = \sup(Y)$, deve, necessariamente, ocorrer $b^2 = 2$. Mas como visto na seção 3.7 não existe número racional cujo quadrado é igual a 2. Logo o conjunto Y não possui supremo em $\mathbb{Q}$.

4.2 Cortes de Dedekind

Como demonstrado na seção 4.1 existem subconjuntos do conjunto dos números racionais que não possuem ínfimo (e outros que não possuem supremo). Do ponto de vista da Análise Matemática este é um problema grave, porque impossibilita a demonstração de vários resultados importantes. Justamente por esse motivo vários matemáticos dedicaram-se ao trabalho de apresentar uma formalização para um conjunto numérico que não possui essa falha, ou seja, um conjunto no qual conjuntos limitados superiormente sempre possuam supremos (e conjuntos limitados inferiormente sempre possuam ínfimo).

Dentre esses matemáticos se destaca Richard Dedekind,[1] que criou o conceito de cortes de números racionais e a partir deles construiu um conjunto com a propriedade desejada.

Um *corte de Dedekind* ou simplesmente um *corte* é um subconjunto próprio e não vazio de números racionais que não possui elemento máximo e tal que, se um número racional r pertence ao corte, qualquer outro número racional s menor do que r também pertence ao corte. Note que todo corte é limitado superiormente. De fato, se X é um corte de Dedekind, todo racional $r \in \mathbb{Q} \setminus X$ é uma cota superior para X pois, caso contrário, como X não possui elemento máximo, existiria um $s \in X$ tal que $r < s$, obrigando assim $r \in X$, mas isso é uma contradição; portanto, r é mesmo uma cota superior para X, o que mostra que X é limitado superiormente.

Como um corte é um subconjunto de $\mathbb{Q}$ limitado superiormente, pelo que foi demonstrado em 4.1, existem cortes que não possuem supremo como, por exemplo, o conjunto $Y = \{s \in \mathbb{Q} \mid s^2 < 2 \text{ ou } s < 0\}$. Há, entretanto, tantos cortes quantos números

[1] Julius Wihelm Richard Dedekind foi um matemático alemão que contribuiu para várias áreas da Matemática, incluindo a formalização do conceito de número real.

racionais que possuem supremo, basta observar que cada racional r é o supremo do corte $X_r = \{s \in \mathbb{Q} \mid s < r\}$. Não se engane, porém, o professor de Matemática acreditando que existem em $\mathbb{Q}$ mais cortes que possuem supremo do que aqueles que não possuem.

Observação 8. *Neste trabalho estão sendo considerados como números primos apenas números positivos. Tal postura não acarreta nenhuma perda na teoria, apenas evita a necessidade de fazer observações enfadonhas ao longo do texto. Por isso todos os resultados aqui obtidos continuam válidos ao serem considerados primos positivos e negativos.*

Fato talvez não tão famoso assim é que o conjunto dos números primos é um conjunto *enumerável*[2]. Uma demonstração desse fato pode ser encontrada em (LIMA, 2017). Outro conjunto infinito e (surpreendentemente) enumerável é o conjunto $\mathbb{Q}$ dos números racionais (para uma demonstração da enumerabilidade de $\mathbb{Q}$ consulte (NERI,)). Como são ambos $\mathbb{P}$ e $\mathbb{Q}$ infinitos e enumeráveis existe um função bijetora que os relaciona, logo $\mathbb{P}$ e $\mathbb{Q}$ possuem a mesma cardinalidade, ou seja, a mesma quantidade de elementos, ou em outras palavras são equipotentes.

Sabendo disso, pode-se concluir que há tantos cortes que não possuem supremo em $\mathbb{Q}$ quanto aqueles que possuem, pois todo corte do tipo $Y_p = \mathbb{Q}_-^* \cup \{s \in \mathbb{Q}_+ \mid s^2 < p\}$ onde $p \in \mathbb{P}$ não possui supremo em $\mathbb{Q}$. O supremo do corte Y_p é o número que elevado ao quadrado resulta em p e esse número não é um número racional. Para uma demostração desse fato consulte o apêndice A. Há então tantos cortes que não possuem supremo em $\mathbb{Q}$ quanto aqueles que possuem, pois há tantos conjuntos X_r quantos números racionais e tantos conjuntos Y_p quanto os números primos. Como racionais e primos existem numa mesma quantidade, pois são ambos infinitos e enumeráveis, o mesmo acontece com os conjuntos X_r e Y_p.

Fato inesperado e contraintuitivo é que existem mais cortes que não possuem supremo em $\mathbb{Q}$ do que aqueles que possuem! O supremo do corte $Z = \{r \in \mathbb{Q} \mid r^3 < 2\}$ é o número que elevado ao cubo tem como resultado o número 2. Tal número não é racional, uma demonstração desse fato pode ser encontrada em (NIVEN, 2012). Portanto, a quantidade de cortes que não possuem supremo em $\mathbb{Q}$ é maior do que a quantidade de cortes que possuem, em pelo menos uma unidade.

Na verdade os cortes que não possuem um supremo no conjunto dos números racionais superam em muito aqueles que possuem; este fato inclusive é o que mostra que existem tipos ou qualidades diferentes de infinitos. Para comprovar este fato na seção 4.3 é desenvolvido o trabalho feito por Dedekind.

[2] Um conjunto é dito ser enumerável quando é finito ou quando é infinito pode ser colocado em correspondência biunívoca com o conjunto dos números naturais.

4.3 A Construção de Dedekind

O objetivo desta seção é provar o Teorema de Dedekind, por isso esta é uma seção cheia de definições, teoremas e demonstrações. Sua leitura pode demandar um pouco mais de atenção e paciência, mas o trabalho vale a pena, pois ao final dela será constatada a existência de um conjunto numérico no qual qualquer corte possui supremo. E, além disso, este tal conjunto contém o conjunto dos números racionais e obviamente contém números que não são racionais, a saber, os supremos que não existiam em $\mathbb{Q}$.

Definição 14 (Corte de Dedekind)**.** *Um conjunto X de números racionais é um corte se satisfaz as seguintes condições:*

1. $\emptyset \neq X \neq \mathbb{Q}$.
2. *Se* $x \in X$ *e* $\mathbb{Q} \ni y < x$, *então* $y \in X$.
3. *Não existe elemento máximo em* X.

A título de exemplo, o conjunto $Z = \mathbb{Q}^*_- \cup \{s \in \mathbb{Q}_+ \mid s^2 < 2\}$ é um corte. Como mencionado em 4.2 os conjuntos $X_r = \{x \in \mathbb{Q} \mid x < r\}$ para algum r racional e $Y_p = \mathbb{Q}^*_- \cup \{y \in \mathbb{Q}_+ \mid y^2 < p\}$ para algum p primo são cortes. Estas afirmações serão demonstradas agora.

Proposição 29. *O conjunto $Z = \mathbb{Q}^*_- \cup \{z \in \mathbb{Q}_+ \mid z^2 < 2\}$ é um corte.*

Demonstração. $Z \neq \emptyset$, pois $0 \in Z$, por exemplo. $Z \neq \mathbb{Q}$, pois $2 \neq Z$. Logo Z cumpre a condição (1) da definição 14.

Todo número negativo está em Z, pois $\mathbb{Q}^*_- \subset Z$. Suponha que para um $z \in Z$ exista um $0 < y \in \mathbb{Q}$ tal que $y < z$ e $y \notin Z$. Como y é positivo e não está em Z segue que $2 \leq y^2$, logo $z^2 < 2 \leq y^2 \Rightarrow z^2 < y^2$. Mas com são ambos z e y positivos $z^2 < y^2 \Rightarrow z < y$, o que é uma contradição, pois por hipótese $y < z$. Portanto, $y < z \Rightarrow y \in Z$ e Z cumpre a condição (2) da definição 14.

Pelo que foi demonstrado em 4.1, Z cumpre a condição (3) da definição 14. E isso mostra que Z é um corte. QED

Proposição 30. *O conjunto $X_r = \{x \in \mathbb{Q} \mid x < r\}$ é um corte.*

Demonstração. Para qualquer que seja o racional r o número $r - 1$ é um racional menor do que r, logo $r - 1 \in X_r$ e $X_r \neq \emptyset$, também o racional $r + 1$ é maior do que r e, portanto, $r + 1 \notin X_r$ o que significa que $X_r \neq \mathbb{Q}$. O que mostra que X_r cumpre a condição (1) da definição 14.

Pela própria definição do conjunto X_r é óbvio que ele cumpre a condição (2) da definição 14.

Pelo teorema 21, não existe elemento máximo em X_r, logo ele cumpre a condição (3) da definição 14, mostrando que X_r é um corte. QED

Proposição 31. *O conjunto* $Y_p = \mathbb{Q}_-^* \cup \{y \in \mathbb{Q}_+ \mid y^2 < p\}$ *onde* p *é um número primo é um corte.*

Demonstração. Argumentos inteiramente análogos aos utilizados na demonstração da proposição 29 e usando o que foi demosntrado em 4.1 mostram que Y_p com p primo é um corte. QED

Serão listadas e demonstradas agora outras afirmações essenciais para alcançar o objetivo desejado, isto é, demonstrar o Teorema de Dedekind. Também serão apresentadas algumas definições importantes.

Proposição 32. *Todo corte é um subconjunto de* $\mathbb{Q}$ *limitado superiormente.*

Demonstração. $\mathbb{Q}$ é arquimediano, ou seja, é ilimitado superiormente. Se X for um corte ilimitado superiormente segue, da Propriedade Arquimediana e de (2) na definição de corte, que $X = \mathbb{Q}$. Mas isso é uma contradição, pois X é um corte. Logo X é limitado superiormente. QED

Proposição 33. *Se* X *um corte,* $r \in \mathbb{Q}$ *é uma cota superior de* X *se, e somente se,* $r \in \mathbb{Q} \setminus X$.

Demonstração. Se r é cota superior de X, então $r \notin X$, caso contrário r seria o elemento máximo de X, contradizendo (3) da definição de corte. Logo $r \in \mathbb{Q} \setminus X$.

Reciprocamente se $r \in \mathbb{Q} \setminus X$, então r é cota superior de X, pois, caso contrário, haveria $s \in X$ tal que $r < s$, o que, pelo item (2) da definição de corte obrigaria r a pertencer a X, novamente uma contradição. QED

Definição 15. *Os cortes do tipo* X_r *são denominados cortes racionais e são representados por* $r^\diamond$.

Proposição 34. *Todo corte que possui supremo é racional.*

Demonstração. Se o corte é racional, isto é, se o corte é do tipo X_r é claro que $\sup(X_r) = r$, pois $x \leq r \ \forall x \in X_r$ e qualquer outro número menor do r pertence a X_r.

Reciprocamente se X é um corte que possui supremo, $\exists r \in \mathbb{Q}$ tal que $x \leq r \ \forall x \in X$, ou seja, $X_r \subset X$. Note que r não pode pertencer a X, pois sendo X um corte não possui

elemento máximo, e se ocorresse $r \in X$ o número r seria o máximo do corte X. Dessa forma, $\forall x \in X$ se tem $x < r$, ou $X \subset X_R$. O que mostra que $X = X_r$. QED

Teorema 22. *O corte* $Z = \mathbb{Q}_-^* \cup \{s \in \mathbb{Q}_+ \mid s^2 < 2\}$ *não é um corte racional.*

Demonstração. O desenvolvimento feito em 4.1 mostra que o corte Z não é racional. QED

Definição 16. $\mathcal{C} = \{X \subset \mathbb{Q} \mid X \text{ é um corte}\}$.

4.3.1 Adição de Cortes

Nesta seção são catalogadas definições, proposições e teoremas, e suas respectivas demonstrações, que estabelecem a maneira de operar a adição entre os elementos de $\mathcal{C}$.

Definição 17. *Para* $X, Y \in \mathcal{C}$ *se define* $X + Y$ *como sendo o conjunto* $X + Y = \{x + y \mid x \in X \text{ e } y \in Y\}$.

Teorema 23. *O conjunto* $Z = \{x + y \mid x \in X \text{ e } y \in Y\}$ *da definição 17 é um corte.*

Demonstração. Como X e Y são cortes, $X \neq \emptyset \neq Y$, logo $\exists x \in X$ e $\exists y \in Y$ e $x+y \in X+Y$, mostrando que $\emptyset \neq Z$. Da mesma forma, como X e Y são cortes, $X \neq \mathbb{Q} \neq Y$, logo $\exists x' \in \mathbb{Q} \setminus X$ e $\exists y' \in \mathbb{Q} \setminus Y$ e $x' + y' > x + y \ \forall x \in X$ e $\forall y \in Y$, pois $x' > x \ \forall x \in X$ e $y' > y \ \forall y \in Y$. Portanto, $x' + y' \in \mathbb{Q} \setminus Z$, mostrando que $Z \neq \mathbb{Q}$ o que comprova a condição (1).

Sejam $r \in Z$ e $\mathbb{Q} \ni s < r$. Mostraremos que $s \in Z$. Como $r \in Z$, r é do tipo $x + y$ com $x \in X$ e $y \in Y$. Então, de $s < x + y$, podemos escrever $s = x + y'$ com $y' < y$ e, portanto, $y' \in Y$. Logo, $s = x + y'$ com $x \in X$ e $y' \in Y$, isto é, $s \in Z$. Isso mostra a condição (2).

Seja $r \in Z$, então $r = x + y$ com $x \in X$ e $y \in Y$. Como existe $x' \in X$ com $x' > x$, o racional $s = x' + y \in Z$ e é maior do que r, o que mostra a condição (3). Portanto, Z é um corte. QED

O teorema 23 mostra que a adição entre cortes dada em 17 está bem definida, isto é, a soma ainda é um corte.

Proposição 35. *Se* $r, s \in \mathbb{Q}$, *então* $r^\diamond + s^\diamond = (r + s)^\diamond$.

Demonstração. Seja $t \in r^\diamond + s^\diamond$, então $t = x + y$ com $x < r$ e $y < s$, logo $t = x + y < r + s$. Isso mostra que $r^\diamond + s^\diamond \subset (r + s)^\diamond$.

Seja agora $t \in (r + s)^\diamond$, então $t = r' + s'$ com $r' < r$ e $s' < s$. Isso mostra que $(r + s)^\diamond \subset r^\diamond + s^\diamond$ e, portanto, $r^\diamond + s^\diamond = (r + s)^\diamond$. QED

A proposição 35 diz que a operação de adição em $\mathcal{C}$ generaliza a operação de adição em $\mathbb{Q}$. Dito de outra forma, a operação de adição no conjunto dos cortes preserva a operação de adição do conjunto dos números racionais. Já o teorema 24 mostra que, assim como nos conjuntos numéricos, a adição em $\mathcal{C}$ respeita as regras convencionais.

Teorema 24. *A adição em $\mathcal{C}$ é comutativa, associativa e tem o corte $X_0 = 0^\diamond$ como elemento neutro.*

Demonstração. Sejam $X, Y, Z \in \mathcal{C}$. Da definição 17 vem que $X+Y = \{x+y \mid x \in X \text{ e } y \in Y\}$, mas como a adição em $\mathbb{Q}$ é comutativa $\{x+y \mid x \in X \text{ e } y \in Y\} = \{y+x \mid x \in X \text{ e } y \in Y\}$, que, novamente pela definição 17, é igual a $Y+X$, logo $X+Y = Y+X$, ou seja, a adição de cortes é comutativa.

Da definição 17 vem que $X + (Y+Z) = \{x + (y+z) \mid x \in X \text{ e } y+z \in Y+Z\}$, mas como a adição em $\mathbb{Q}$ é associativa $\{x + (y+z) \mid x \in X \text{ e } y+z \in Y+Z\} = \{(x+y)+z \mid x+y \in X+Y \text{ e } z \in Z\}$, que, novamente pela definição 17, é igual a $(X+Y)+Z$, logo $X + (Y+Z) = (X+Y)+Z$, ou seja, a adição de cortes é associativa.

Sejam agora o corte $X + 0^\diamond$ e $z \in X + 0^\diamond$. Então $z = x + y$ com $x \in X$ e $y < 0$. Assim, $z < x$ e, portanto, $z \in X$. Logo $X + 0^\diamond \subset X$. Agora seja $x \in X$. Tomando $y \in X$ com $y > x$, podemos expressar x como $x = y + (x - y)$, onde $x - y < 0$ e, portanto pertence a $0^\diamond$. Assim, $x \in X + 0^\diamond$ e $X \subset X + 0^\diamond$. QED

Deseja-se mostrar que todo corte em $\mathcal{C}$ possui simétrico (inverso aditivo), para isso são necessários dois lemas.

Lema 2. *Se $s \in \mathbb{Q}$ e $r \in \mathbb{Q}_+^*$, então o conjunto $A = \{s + mr \mid m \in \mathbb{N}\}$ não é limitado superiormente em $\mathbb{Q}$.*

Demonstração. Como o conjunto dos números naturais não é limitado superiormente em $\mathbb{Q}$ e $r > 0$, para qualquer natural m dado, existe $n \in \mathbb{N}$ tal que $m < n$ e, portanto, $mr < nr$, o que implica em $s + mr < s + nr$. O número $s + nr \in A$, logo A não é limitado superiormente em $\mathbb{Q}$. QED

Lema 3. *Sejam $X \in \mathcal{C}$ e $r \in \mathbb{Q}_+^*$. Então existem números racionais p e q tais que $p \in X$, $q \notin X$, q não é o supremo de X e $q - p = r$.*

Demonstração. Tomemos $s \in X$ arbitrário e consideremos a sequência $s, s+r, s+2r + \cdots + s + nr + \cdots$. Pelo lema 2 esta sequência é ilimitada, como X é um corte é limitado superiormente. Então pelo Princípio da Boa Ordenação existe um único natural m tal que $s + mr \in X$ e $s + (m+1)\,r \notin X$. Se $s + (m+1)\,r$ não for cota superior mínima de X, tome $p = s + mr$ e $q = s + (m+1)\,r$. Se $s + (m+1)\,r$ for a cota superior mínima de X, tome $p = s + mr + \frac{r}{2}$ e $q = s + (m+1)\,r + \frac{r}{2}$. QED

O teorema 25 mostra a existência e a unicidade do simétrico em $\mathcal{C}$.

Teorema 25. *Seja $X \in \mathcal{C}$. Existe um único $Y \in \mathcal{C}$ tal que $X + Y = X_0 = 0^\diamond$. Como nos casos dos inteiros e racionais, tal Y se denota por $-X$ e se chama simétrico (ou inverso aditivo) de X.*

Demonstração. Dado $X \in \mathcal{C}$ seja o conjunto $Y = \Big\{p \in \mathbb{Q} \mid -p \text{ é cota superior NÃO mínima de } X\Big\}$.

Como X é um corte pelo lema 3 existe $q \in \mathbb{Q}$ cota superior não mínima de X. Basta fazer $-p = q$ que se tem $p \in Y$ mostrando que $\emptyset \neq Y$. Como X é um corte, pela proposição 32 X é limitado superiormente, ou seja, existe $k \in \mathbb{Q}$ tal que $x < k\ \forall x \in X$. Se toda cota superior k de X for positiva, basta tomar um racional p tal que $0 < p < k$ e $p \in X$ que se tem $-p \in X$, pois $-p < p$. Isto é $-p$ não é cota superior não mínima de X e, portanto, $-p \in \mathbb{Q} \setminus Y$, o que mostra que $Y \neq \mathbb{Q}$. Agora se X admite cota superior negativa, digamos $-k$. Existe $-p < -k$ tal que $-p \in X$, assim $p \notin Y$, pois $-p$ não é cota superior não mínima de X. Novamente mostrando que $\mathbb{Q} \setminus Y \neq \emptyset$, o seja $Y \neq \mathbb{Q}$.

Seja $y \in Y$. Como $-y$ é cota superior de X, mas não mínima, então existe $z \in \mathbb{Q}$, $-z < -y$, tal que $-z$ é cota superior de X e, portanto, $-z \in X$. Seja $t = \frac{y+z}{2}$. Temos que $-z < -t < -r$, de modo que $-t$ é cota superior de X, mas não é mínima, logo $t \in Y$ e $t > y$, como queríamos.

Seja $z \in X + Y$, então $z = x + y$ com $x \in X$ e $y \in Y$. Como $-y \notin X$ segue que $-y > x$, de modo que $0 > x + y = z$, ou seja, $z \in 0^\diamond$. Reciprocamente, suponhamos $z \in 0^\diamond$, isto é $z < 0$. Sejam $x \in X$ e $x' \notin X$ com x' não sendo cota superior mínima, tais que $x' - x = -z$, o que é garantido pelo lema 3. Segue que $z = x + (-x')$ com $x \in X$ e $x' \in Y$, ou seja, $z \in X + Y$. Logo $Y = -X$.

A unicidade do simétrico decorre da associatividade e da existência do elemento neutro da adição: suponha que existam Y_1 e $Y_2 \in \mathcal{C}$ tais que $X + Y_1 = 0^\diamond = X + Y_2$. Então $Y_2 = Y_2 + 0^\diamond = Y_2 + (X + Y_1) = (Y_2 + X) + Y_1 = 0^\diamond + Y_1 = Y_1$. QED

Definição 18. *Assim como nos casos de $\mathbb{Z}$ e $\mathbb{Q}$, define-se a subtração em $\mathcal{C}$ por $X - Y = X + (-Y)$, $\forall\ X, Y \in \mathcal{C}$.*

Por fim a proposição 36 reúne mais algumas propriedades preservadas pela adição de cortes.

Proposição 36. *Para $X, Y, Z \in \mathcal{C}$, vale:*

1. $-(-X) = X$
2. $-X + Y = Y - X$
3. $X - (-Y) = X + Y$

4. $-X - Y = -(X + Y)$

5. $X - (Y + Z) = X - Y - Z$

Demonstração.

1. $-(-X) = -(-X)+0^\diamond = -(-X)+(-X+X) = (-(-X)+(-X))+X = 0^\diamond+X = X$

2. $-X + Y = (-X) + Y = Y + (-X) = X - Y$

3. $X - (-Y) = X + (-(-Y)) = X + Y$

4. $-(X+Y) = -(X+Y) + 0^\diamond + 0^\diamond = -(X+Y) + X - X + Y - Y = -(X+Y) + X + Y - X - Y = -(X+Y) + (X+Y) - X - Y = 0^\diamond - X - Y = -X - Y$

5. segue direto do item (4)

QED

4.3.2 Relação de Ordem entre Cortes

A lista de proposições, definições e teoremas dada agora tem como objetivo estabelecer uma relação de ordem em $\mathcal{C}$.

Definição 19. *Seja $X, Y \in \mathcal{C}$. Diz-se que X é menor do que Y e se escreve $X < Y$ quando $Y \setminus X \neq \emptyset$.*

Definição 20. *Se $X \in \mathcal{C}$ e $X > 0^\diamond$, X se chama corte positivo. Se $X < 0^\diamond$, X se chama corte negativo. Se $X \geq 0^\diamond$, X se chama corte não-negativo e se $X \leq 0^\diamond$, X se chama corte não-positivo.*

A proposição 37 diz que a relação de ordem de $\mathcal{C}$ generaliza a relação de ordem de $\mathbb{Q}$. Dito de outra forma, a relação de ordem no conjunto dos cortes preserva a relação de ordem do conjunto dos números racionais.

Proposição 37. *Se $r, s \in \mathbb{Q}$, então $r^\diamond \leq s^\diamond$ se, e somente se, $r \leq s$.*

Demonstração. Se $r^\diamond \leq s^\diamond$ segue que $s^\diamond \setminus r^\diamond \neq \emptyset$ ou $s^\diamond = r^\diamond$. No primeiro caso $\exists p \in s^\diamond \setminus r^\diamond$, mas isso é o mesmo que $r \leq p < s$, logo $r < s \Rightarrow r \leq s$. No segundo caso, isto é, se $s^\diamond = r^\diamond$, então $r = s$ e, portanto, $r \leq s$.

Reciprocamente se $r = s$ segue que $s^\diamond = r^\diamond$ e, portanto, $s^\diamond = r^\diamond$ ou $s^\diamond \setminus r^\diamond \neq \emptyset$. Agora se $r < s$ existe p tal que $r < p < s$ e, portanto, $p \in s^\diamond \setminus r^\diamond$, ou seja, $s^\diamond \setminus r^\diamond \neq \emptyset$, logo $s^\diamond \setminus r^\diamond \neq \emptyset$ ou $s^\diamond = r^\diamond$. E isso mostra que $r^\diamond \leq s^\diamond$. QED

Proposição 38. *Para $X, Y \in \mathcal{C}$, valem as equivalências:*

1. $X < Y \Leftrightarrow X \subset Y$ *e* $X \neq Y$.
2. $X \leq Y \Leftrightarrow X \subset Y$.

Demonstração.

1. $X < Y \Rightarrow Y \setminus X \neq \emptyset \Leftrightarrow \exists y$ tal que $y \in Y$ e $y \notin X \Rightarrow X \neq Y$. Suponha, por absurdo, que X não esteja contido em Y, isto é, que exista $x \in X$ tal que $x \notin Y$. Como X é um corte $\forall z < x$ vale $z \in X$. Mas todo elemento de $y \in Y$ e tal que $y < x$, pois como $x \notin Y$ segue que $x \in \mathbb{Q} \setminus Y$ e pela proposição 33, x é uma cota superior de Y. Mas isso significa que $Y \setminus X = \emptyset$, o que é uma contradição. Logo $X \subset Y$.
   Reciprocamente, $X \subset Y$ e $X \neq Y \Rightarrow Y \setminus X \neq \emptyset$, o que, por definição significa $X < Y$.

2. $X \leq Y \Rightarrow X = Y$ ou $Y \setminus X \neq \emptyset$. Se $X = Y$ segue que $X = Y \subset Y$ e a implicação é verdadeira. Se $Y \setminus X \neq \emptyset$, pelo item (1) $X \subset Y$ e a implicação é ver verdadeira.
   A recíproca é imediata, pois $X \subset Y \Rightarrow X = Y$ ou $Y \setminus X \neq \emptyset$, o que, por definição significa $X \leq Y$.

QED

Teorema 26 (Lei da Tricotomia em $\mathcal{C}$)**.** *Para quaisquer $X, Y \in \mathcal{C}$, tem-se que uma, e apenas uma, das relações seguintes ocorre:*

1. $X < Y$.
2. $X = Y$.
3. $X > Y$.

Demonstração. Da igualdade de conjuntos vem que $X = Y$ implica que não podem ocorrer $X < Y$ tampouco $X > Y$. Da proposição 38 vem que $X < Y$, assim como $X > Y$ excluem a ocorrência de $X = Y$. Supondo que ocorram simultaneamente $X < Y$ e $X > Y$, existem $x \in X \setminus Y$ e $y \in Y \setminus X$. De $x \in X$ e $y \notin X$ resulta $x < y$ e de $y \in Y$ e $y \notin Y$ resulta $y < x$ tricotomia de $\mathbb{Q}$, portanto, no máximo uma das alternativas ocorre.

Agora temos que $X = Y$ ou $X \neq Y$. Caso seja $X = Y$ não há o que provar. Supondo $X \neq Y$, então $X \setminus Y \neq \emptyset$ ou $Y \setminus X \neq \emptyset$. No primeiro caso, $X < Y$, no segundo $Y < X$. QED

Teorema 27. *A relação $\leq$ é uma relação de ordem em $\mathcal{C}$.*

Demonstração. Sejam $X, Y, Z \in \mathcal{C}$. Para todo e qualquer corte X vale $X \subset X$, então pela proposição 38, $X \leq X$, ou seja, a relação $\leq$ é reflexiva.

Também pela proposição 38, $X \leq Y \Rightarrow X \subset Y$ e $Y \leq X \Rightarrow Y \subset X$, mas $X \subset Y$ e $Y \subset X \Leftrightarrow X = Y$. Logo $X \leq Y$ e $Y \leq X \Rightarrow X = Y$ e, portanto a relação $\leq$ é antissimétrica.

Finalmente, também pela proposição 38 $X \leq Y \Rightarrow X \subset Y$, $Y \leq Z \Rightarrow Y \subset Z$. Mas $X \subset Y$ e $Y \subset Z \Rightarrow X \subset Z$ e isso é o mesmo que $X \leq Z$, mostrando que a relação $\leq$ e transitiva e, portanto, uma relação de ordem em $\mathcal{C}$. QED

Teorema 28 (Compatibilidade da relação de ordem com a adição em $\mathcal{C}$)**.** *Sejam $X, Y, Z \in \mathcal{C}$ tais que $X \leq Y$. Então $X + Z \leq Y + Z$.*

Demonstração. Como $X \subset Y$, para todo $x \in X$ se tem que $x = y$ para algum $y \in Y$. Desse modo, para todo $z \in Z$ segue-se que $x + z = y + z$. O que mostra que $X + Z \subset Y + Z$ e, portanto, $X + Z \leq Y + Z$. QED

De posse de uma relação de ordem em $\mathcal{C}$ pode-se definir a noção de *valor absoluto* de um corte, e provar algumas proposições e teoremas que serão importantes para definição da operação de multiplicação.

Definição 21. *Dado $X \in \mathcal{C}$, define-se o valor absuluto de X (ou módulo de X), representado por $|X|$, do seguinte modo:*

$$|X| = \begin{cases} X, & \text{se } X \geq 0^\diamond \\ -X, & \text{se } X < 0^\diamond \end{cases}$$

Teorema 29. *Se $\mathcal{C} \ni X > 0^\diamond \Rightarrow -X < 0$.*

Demonstração. Se $X > 0^\diamond$ segue, por definição, que $X \setminus 0^\diamond \neq \emptyset$. Então existe um racional p tal que $p \in X$ e $p \notin 0^\diamond$, e portanto, p é positivo, pois se ele fosse negativo valeria $p \in 0^\diamond$ e a diferença $X \setminus 0^\diamond$ seria vazia. Isso implica que $-p \in 0^\diamond$, pois $-p < 0$ e que $-p \notin -X$, porque $-(-p) = p$ não é cota superior não mínima de X, ou seja, $0^\diamond \setminus -X \neq \emptyset$ ou $-X < 0^\diamond$. QED

Corolário 29.1. *Se $\mathcal{C} \ni -X > 0^\diamond \Rightarrow X < 0$.*

Demonstração. Decorre do teorema 29, trocando X por $-X$ e vice-versa na demonstração. QED

Corolário 29.2. *Se $\mathcal{C} \ni X \geq 0^\diamond \Rightarrow -X \leq 0^\diamond$.*

Demonstração. Se $X \geq 0^\diamond$, então $X = 0^\diamond$ ou $X > 0^\diamond$. Se $-X = 0^\diamond$ vale que $-X = -0^\diamond$, pois $0 = -0$ em $\mathbb{Q}$. Mas é claro que se $-X = 0^\diamond$ vale que $-X \leq 0^\diamond$.

Agora se basta observar que $-X < 0^\diamond \Rightarrow -X \leq 0^\diamond$ e o resultado decorre imediatamente do teorema 29. QED

Proposição 39. *Para qualquer $X \in \mathcal{C}$, tem-se:*

1. $|X| \geq 0^\diamond$
2. $|X| = 0^\diamond$ *se, e somente se,* $X = 0^\diamond$
3. $|X| = |-X|$

Demonstração.

1. Se $X \geq 0^\diamond$, $|X| = X \geq 0^\diamond$ e segue o resultado. Agora se $X < 0^\diamond$ é claro que $X \leq 0^\diamond$ e pela contatibilidade da relação de ordem com a adição, $-X + X \leq -X + 0^\diamond \Rightarrow 0^\diamond \leq -X$ e como $|X| = -X$ segue que $|X| \geq 0^\diamond$.

2. Se $|X| = 0^\diamond$, então $X \geq 0^\diamond$. Isto é, $X > 0^\diamond$ ou $X = 0^\diamond$. Na primeira hipótese, ou seja, se $X > 0^\diamond$ segue que $0^\diamond \subset X$ e $0^\diamond \neq X$, mas se $0^\diamond \neq X$ se tem $|X| = X \neq 0^\diamond$, pois $X > 0^\diamond$. Mas isso é uma contradição, porque $|X| = 0^\diamond$. Logo, não pode ser $X > 0^\diamond$ e, necessariamente, $X = 0^\diamond$.
   A recíproca é imediata, pois $0^\diamond \geq 0^\diamond$.

3. Se $X = 0^\diamond$ segue da ordem de $\mathbb{Q}$ que $-X = 0^\diamond$, da mesma forma que, se $-X = 0^\diamond$ segue da ordem de $\mathbb{Q}$ que $X = 0^\diamond$ e, portanto, neste caso $|X| = |0^\diamond| = 0^\diamond = -0^\diamond = |0^\diamond| = |-X|$.
   Se $X > 0^\diamond$ segue que do corolário 29.2 que $-X < 0^\diamond$, então $|X| = X = -(-X) = |-X|$.
   Se $X < 0^\diamond$ segue que do corolário 29.2 que $-X > 0^\diamond$, então $|X| = -X = |-X|$.

QED

4.3.3 Multiplicação de Cortes

Por fim, para munir o conjunto $\mathcal{C}$ de uma operação de multiplicação são necessárias mais algumas definições, proposições e teoremas.

Definição 22. *Para $X, Y \in \mathcal{C}$ com $0^\diamond \leq X$ e $0^\diamond \leq Y$ se define o produto XY como sendo o conjunto $XY = \mathbb{Q}^*_- \cup \{z \in \mathbb{Q} \mid z = xy, \text{com } x \in X, y \in Y, 0 \leq x \text{ e } 0 \leq y\}$.*

Teorema 30. *O conjunto $Z = \mathbb{Q}^*_- \cup \{z \in \mathbb{Q} \mid z = xy, \text{com } x \in X, y \in Y, 0 \leq x \text{ e } 0 \leq y\}$ da definição 22 é um corte e $0^\diamond \leq Z$.*

Demonstração. O conjunto Z é não vazio, pois qualquer racional negativo pertence a Z. Tome p cota superior de X e q cota superior de Y, como $0^\diamond \leq X$ e $0^\diamond \leq Y$ segue que $0 < p$ e $0 < q$, logo $0 < pq$ e $r < pq$ para todo $r \in \mathbb{Q}^*_-$. Para quaisquer outros elementos $z = xy \in Z$ segue que $z < pq$, pois $0 \leq x$, $0 \leq y$ e p e q são cotas superiores de X e Y, respectivamente. Logo $pq \notin Z$, mostrando que $Z \neq \mathbb{Q}$.

Seja $z \in Z$, se $z \leq 0$ é imediato que $\forall r \in \mathbb{Q}^*_-$ tal que $r < z$ se tem $r \in Z$, pois $\mathbb{Q}^*_- \subset Z$. Sejam agora $0 < z \in Z$ e $r \in \mathbb{Q}$ tais que $0 < r < z$, então $z = xy$ com $0 < x$ e $0 < y$. Então $r < xy$, podemos escrever $r = xy'$ com $0 < y' < y$. Logo $r = xy'$ com $0 < x$ e $0 < y'$, o que é o mesmo que, $x \in X$ e $y' \in Y$. Ou seja, $r \in Z$.

Se Z possuir uma cota superior mínima ela será, necessariamente não negativa, pois há em Z elementos do tipo xy com $0 \leq x$ e $0 \leq y$. Tomemos então $z = xy$ com $0 \leq x$ e $0 \leq y$ como existe $x' \in X$ com $x' > x \geq 0$ o racional $r = x'y$ é maior do que z e $r \in Z$. Logo Z não possui elemento máximo. E isso mostra que Z é um corte. QED

O teorema 30 mostra que a multiplicação entre cortes dada em 22 está bem definida, isto é, o produto ainda é um corte. Além disso, a definição 22 ensina apenas como multiplicar cortes não-negativos.

Teorema 31. *Para qualquer corte não-negativo $X \in \mathcal{C}$ vale $X \cdot 0^\diamond = 0^\diamond = 0^\diamond \cdot X$.*

Demonstração. Da definição 22 vem que
$X \cdot 0^\diamond = \mathbb{Q}^*_- \cup \{z \in \mathbb{Q} \mid z = xy, \text{com } x \in X, y \in 0^\diamond, 0 \leq x \text{ e } 0 \leq y\}$, pois $0^\diamond \leq 0^\diamond$. Mas não existe em $0^\diamond$ nenhum $y \geq 0$. Logo não é possível encontrar elemento $z = xy$ com x e y satisfazendo as condições requeridas, logo o conjunto $\{z \in \mathbb{Q} \mid z = xy, \text{com } x \in X, y \in 0^\diamond, 0 \leq x \text{ e } 0 \leq y\} = \emptyset$. Então, $X \cdot 0^\diamond = \mathbb{Q}^*_- \cup \emptyset = \mathbb{Q}^*_-$. Agora observando que $\mathbb{Q}^*_- = 0^\diamond$ é possível concluir que $0^\diamond \subset X \cdot 0^\diamond$ e que $X \cdot 0^\diamond \subset 0^\diamond$. Isso mostra que os conjuntos são iguais, ou seja, $X \cdot 0^\diamond = 0^\diamond$.
Da definição 22 vem que
$0^\diamond \cdot X = \mathbb{Q}^*_- \cup \{z \in \mathbb{Q} \mid z = xy, \text{com } y \in 0^\diamond, x \in X, 0 \leq y \text{ e } 0 \leq x\}$, pois $0^\diamond \leq 0^\diamond$. Mas não existe em $0^\diamond$ nenhum $x \geq 0$. Logo não é possível encontrar elemento $z = xy$ com x e y satisfazendo as condições requeridas, logo o conjunto $\{z \in \mathbb{Q} \mid z = xy, \text{com } y \in 0^\diamond, x \in X, 0 \leq y \text{ e } 0 \leq x\} = \emptyset$. Então, $0^\diamond \cdot X = \mathbb{Q}^*_- \cup \emptyset = \mathbb{Q}^*_-$. Agora observando que $0^\diamond = \mathbb{Q}^*_-$ é possível concluir que $0^\diamond \subset 0^\diamond \cdot X$ e que $0^\diamond \cdot X \subset 0^\diamond$. Isso mostra que os conjuntos são iguais, ou seja, $0^\diamond = 0^\diamond \cdot X$. QED

Definição 23. *Para todo negativo $X \in \mathcal{C}$ se define o porduto $X \cdot 0^\diamond = -X \cdot 0^\diamond$.*

Note que, pelo teorema 29, se $X < 0$, necessariamente, $-X > 0$. Assim, com a definição 23, fica estabelecido que para qualquer que seja o corte $X \in \mathcal{C}$ vale $X \cdot 0^\diamond = 0^\diamond = 0^\diamond \cdot X$.

Agora é possível definir a multiplicação para quaisquer que sejam os cortes. A definição 24 não envolve cortes nulos, isto é, cortes iguais ao corte $0^\diamond$. pois

Definição 24. *Se $X, Y \in \mathcal{C}$, define-se:*

$$XY = \begin{cases} -\left(|X|\,|Y|\right), & \text{se } X < 0^\diamond, Y > 0^\diamond \\ -\left(|X|\,|Y|\right), & \text{se } X > 0^\diamond, Y < 0^\diamond \\ \quad |X|\,|Y|\,, & \text{se } X < 0^\diamond, Y < 0^\diamond \end{cases}$$

Teorema 32. *A multiplicação em $\mathcal{C}$ é comutativa, associativa e tem o corte $X_1 = 1^\diamond$ como elemento neutro.*

Demonstração. Iniciemos observando que o teorema 31 garante que a multiplicação é comutativa se um dos fatores envolvidos for o corte $0^\diamond$.
Agora verifiquemos que para cortes positivos a operação é comutativa. Sejam então $X, Y \in \mathcal{C}$ dois cortes positivos. Fazendo $P = \{z \in \mathbb{Q} \mid z = xy, \text{com } x \in X, y \in Y, 0 \leq x \text{ e } 0 \leq y\}$ temos, por definição, que $XY = \mathbb{Q}^*_- \cup P$. Como a operação de multiplicação é comutativa em $\mathbb{Q}$ temos que para quaisquer $x, y \in \mathbb{Q}$ ocorre $xy = yx$ em particular isso ocorre para todos $x, y \in \mathbb{Q}^*_-$ e todos $x, y \in P$, portanto $XY = YX$.
Fazendo $P' = \{z \in \mathbb{Q} \mid t = (xy)\,z, \text{com } xy \in XY, z \in Y, 0 \leq xy \text{ e } 0 \leq z\}$ vem da definição de produto que $(XY)\,Z = \mathbb{Q}^*_- \cup P'$, associatividade de $\mathbb{Q}$ segue que $(xy)\,z = x\,(yz)$ de onde decorre que $(XY)\,Z = X\,(YZ)$.
Agora vamos verificar as propriedades para produto envolvendo cortes negativos. Sejam então $X, Y \in \mathcal{C}$.
Se $X < 0^\diamond$ e $Y < 0^\diamond$ temos, por definição, que $XY = (-X)\,(-Y) = (-Y)\,(-X) = YX$.
Se $X < 0^\diamond$ e $Y > 0^\diamond$ temos, por definição, que $XY = -\left((-X)\,Y\right) = -\left(Y\,(-X)\right) = YX$.
Se $X > 0^\diamond$ e $Y < 0^\diamond$ temos, por definição, que $XY = -\left(X\,(-Y)\right) = -\left((-Y)\,X\right) = YX$.
E isso mostra que a multiplicação é comutativa para quaisquer que sejam $X, Y \in \mathcal{C}$.
Para estender a associatividade para cortes negativos sejam agora $X, Y, Z \in \mathcal{C}$.
Se $X < 0^\diamond$, $Y < 0^\diamond$ e $Z < 0^\diamond$ temos, por definição, que $(XY)\,Z = (|X|\,|Y|)\,Z = -\left(||X|\,|Y||\,|Z|\right) = -\left((|X|\,|Y|)\,|Z|\right) = -\left(|X|\,(|Y|\,|Z|)\right) = -\left(|X|\,||Y|\,|Z||\right) = X\,(YZ)$.
Se $X < 0^\diamond$, $Y < 0^\diamond$ e $Z > 0^\diamond$ temos, por definição, que $(XY)\,Z = (|X|\,|Y|)\,Z = -\left(||X|\,|Y||\,|Z|\right) = -\left((|X|\,|Y|)\,|Z|\right) = -\left(|X|\,(|Y|\,|Z|)\right) = -\left(|X|\,||Y|\,|Z||\right) = X\,(YZ)$.
Se $X < 0^\diamond$, $Y > 0^\diamond$ e $Z > 0^\diamond$ temos, por definição, que $(XY)\,Z = (-(|X|\,|Y|))\,Z = -\left(||X|\,|Y||\,|Z|\right) = -\left((|X|\,|Y|)\,|Z|\right) = -\left(|X|\,(|Y|\,|Z|)\right) = -\left(|X|\,||Y|\,|Z||\right) = X\,(YZ)$.
Se $X < 0^\diamond$, $Y > 0^\diamond$ e $Z < 0^\diamond$ temos, por definição, que $(XY)\,Z = (-(|X|\,|Y|))\,Z = -\left(||X|\,|Y||\,|Z|\right) = -\left((|X|\,|Y|)\,|Z|\right) = -\left(|X|\,(|Y|\,|Z|)\right) = -\left(|X|\,||Y|\,|Z||\right) = X\,(YZ)$.
Se $X > 0^\diamond$, $Y < 0^\diamond$ e $Z < 0^\diamond$ temos, por definição, que $(XY)\,Z = (-(|X|\,|Y|))\,Z = -\left(||X|\,|Y||\,|Z|\right) = -\left((|X|\,|Y|)\,|Z|\right) = -\left(|X|\,(|Y|\,|Z|)\right) = -\left(|X|\,||Y|\,|Z||\right) = X\,(YZ)$.
Se $X > 0^\diamond$, $Y < 0^\diamond$ e $Z > 0^\diamond$ temos, por definição, que $(XY)\,Z = (-(|X|\,|Y|))\,Z = -\left(||X|\,|Y||\,|Z|\right) = -\left((|X|\,|Y|)\,|Z|\right) = -\left(|X|\,(|Y|\,|Z|)\right) = -\left(|X|\,||Y|\,|Z||\right) = X\,(YZ)$.

Se $X > 0^\diamond$, $Y > 0^\diamond$ e $Z < 0^\diamond$ temos, por definição, que $(XY)\,Z = (XY)\,Z = -\left(||X|\,|Y||\,|Z|\right) = -\left((|X|\,|Y|)\,|Z|\right) = -\left(|X|\,(|Y|\,|Z|)\right) = -\left(|X|\,||Y|\,|Z||\right) = X\,(YZ)$.
Isso mostra que a multiplicação é associativa para quaisquer que sejam os cortes $X, Y, Z \in \mathcal{C}$.
Por fim, considere o corte $X_1 = 1^\diamond = \{x \in \mathbb{Q} \mid x < 1\}$, para algum $0^\diamond < X \in \mathcal{C}$ se tem: $X \cdot 1^\diamond = \mathbb{Q}^*_- \cup P_1$, onde $P_1 = \{z \in \mathbb{Q} \mid z = xy, \text{com } x \in X, y \in 1^\diamond, 0 \leq x \text{ e } 0 \leq y < 1\}$. Vamos mostrar que $X \subset X \cdot 1^\diamond$ e $X \cdot 1^\diamond \subset X$.
Tome $r \in X \cdot 1^\diamond$ tal que $r < 0$, como $0^\diamond < X$ existe $p \in X$ tal que $p \notin 0^\diamond$ e, portanto, $p \geq 0$. Assim, $r < 0 \leq p$, logo $r \in X$. Tome agora $r \in X \cdot 1^\diamond$ tal que $0 \leq r$. Assim $r = pq$ com $p \in X$, $q \in 1^\diamond$, $0 \leq p$ e $0 \leq q$. Como $q \in 1^\diamond$, temos que $q < 1$, daí $pq < p \cdot 1$, isto é, $r = pq < p$. Como $p \in X$ e X é um corte, segue que $r \in X$. E isso mostra que $X \cdot 1^\diamond \subset X$.
Por outro lado, tome $r \in X$. Se $r < 0$, pela definição de produto, $r \in X \cdot 1^\diamond \subset X$. Suponha então que $r \geq 0$. Tome $p \in X$ tal que $0 < r \leq p$, isso é possível, pois X é um corte e por isso não possui máximo. Se $q = \frac{r}{q}$ então $0 \leq q < 1$ e, portanto, $q \in 1^\diamond$. concluímos então que $r \in X \cdot 1^\diamond$, porque $r = pq$ como $p \in X$, $q \in^\diamond$, $0 < p$ e $0 \leq q$, mostrando que $X \subset X \cdot 1^\diamond$.
Logo $X = X \cdot 1^\diamond$.
Se $0^\diamond > X \in \mathcal{C}$ segue que $X \cdot 1^\diamond = -\left(|X| \cdot |1^\diamond|\right) = -\left(-X \cdot 1^\diamond\right) = -\left(-X\right) = X$.
Logo $1^\diamond$ é, de fato, o elemento neutro da multiplicação. QED

Teorema 33. *Seja $\mathcal{C} \ni X \neq 0^\diamond$. Existe um único $Y \in \mathcal{C}$ tal que $XY = X_1 = 1^\diamond = YX$. Como nos casos dos racionais, tal Y se denota por X^{-1} e se chama inverso X.*

Demonstração. Dado $X \in \mathcal{C}$ tal que $0^\diamond < X$ seja o conjunto $Y = \left\{r \in \mathbb{Q} \mid r < \frac{1}{p},\ \text{com } p \notin X\right\}$.
O conjunto Y é um corte. De fato, seja $y > 0$ tal que $y \notin Y$. Assim, $-1 < \frac{1}{y}$, isto é, $-1 \in Y$, ou seja, $Y \neq \emptyset$. Como $0^\diamond < X$ existe $p \in X$ tal que $p > 0$. Segue que $\frac{1}{p} \notin Y$, de fato, se $\frac{1}{p} \in Y$ teríamos que $\frac{1}{\frac{1}{p}} = p \notin X$, o que é um absurdo. Logo $Y \neq \mathbb{Q}$.
Sejam $p \in X$ e $q \in \mathbb{Q}$ tais que $q < p$. Assim, dado $y > 0$ tal que $y \notin X$ temos $p < \frac{1}{y}$. Como $q < p$, temos $q < \frac{1}{y}$, o que implica em $q \in Y$.
Sejam $p \in Y$ e $y > 0$ tais que $x \notin X$ e $p < \frac{1}{y}$. Como entre dois racionais existe outro racional, temos que existe $q \in \mathbb{Q}$ tal que $p < q < \frac{1}{y}$. Logo $p < q$ e $q \in X$, mostrando que Y não tem máximo. Concluindo então que Y é um corte.
Agora vamos mostrar que $XY = 1^\diamond$
Sejam $p \in X$ e $q \in Y$. Como $X > 0^\diamond$ temos que $Y > 0^\diamond$, logo, assumimos $p, q > 0$. Sabemos que existe $x \notin X$, $x > 0$ tal que $q < \frac{1}{x}$. Também $p < x$. Concluímos então que $pq < p\frac{1}{x} < x\frac{1}{x} = 1$. Isto é, $pq \in 1^\diamond$. Assim, $XY \subset 1^\diamond$. A unicidade do simétrico decorre da associatividade e da existência do elemento neutro da adição: suponha que existam Y_1 e $Y_2 \in \mathcal{C}$ tais que $X + Y_1 = 0^\diamond = X + Y_2$. Então $Y_2 = Y_2 + 0^\diamond = Y_2 + (X + Y_1) = (Y_2 + X) + Y_1 = 0^\diamond + Y_1 = Y_1$.
Como $X > 0^\diamond$ resulta que existe $n_0 \in \mathbb{N}$ tal que para todo $n > n_0$ existe $k_n \in \mathbb{N}$ com a propriedade $\frac{k_n}{n} \in X$ e $\frac{k_{n+1}}{n} \notin X$. Observe que $K_n < k_{n+1}$. Seja $p \in 1^\diamond$ Claro que existem $n \in \mathbb{N}$ e seu correspóndente k_n tal que $p < \frac{k_n}{k_{n+1}}$. Como $\frac{pn}{k_n} < \left(\frac{k_{n+1}}{n}\right)^{-1}$ e entre dois racionais

sempre existe outro racional, existe S_n tal que $\frac{pn}{k_n} < S_n < \left(\frac{k_{n+1}}{n}\right)^{-1}$. Claro que $S_n \in Y$ e $p < \frac{k_n}{n}$. Isto é, $p \in XY$. Logo $1^\diamond \subset XY$ e, portanto, $XY = 1^\diamond$.
A unicidade do inverso decorre da associatividade e da existência do elemento neutro da multiplicação: seja $X \in \mathcal{C}$ suponha que existam Y_1 e $Y_2 \in \mathcal{C}$ tais que $XY_1 = 1^\diamond = XY_2$. Então $Y_2 = Y_2 \cdot 1^\diamond = Y_2\,(XY_1) = (Y_2X)\,Y_1 = 1^\diamond \cdot Y_1 = Y_1$. QED

Proposição 40 (Propriedade do Anulamento da Multiplicação)**.** *Dados $X, Y \in \mathcal{C}$ se tem $XY = 0^\diamond \Leftrightarrow X = 0^\diamond$ ou $Y = 0^\diamond$.*

Demonstração. Se $X = 0^\diamond$ não há o que provar e a proposição é verdadeira. Supondo $X \neq 0$, então $XY = 0^\diamond \Leftrightarrow X^{-1}XY = X^{-1} \cdot 0^\diamond \Leftrightarrow Y = 1^\diamond \cdot Y = X^{-1} \cdot 0^\diamond = 0^\diamond$. QED

Teorema 34 (Propriedade Distributiva)**.** *Sejam $X, Y, Z \in \mathcal{C}$, vale: $XY + XZ = X\,(Y + Z)$*

Demonstração. Consideremos o caso $X > 0^\diamond$, $Y < 0^\diamond$ e $Y + Z > 0^\diamond$. Então $Z = (Y + Z) + (-Y)$. Como a distributividade vale para os racionais, temos que $XZ = X\,(Y + Z) + X\,(-Y) = X\,(Y + Z) - (XY)$. Portanto, $XY + XZ = X\,(Y + Z)$. O demais casos são tratados de maneira análoga. QED

A proposição 41 diz que a operação de multiplicação em $\mathcal{C}$ generaliza a operação de multiplicação em $\mathbb{Q}$. Dito de outra forma, a operação de multiplicação no conjunto dos cortes preserva a operação de multiplicação do conjunto dos números racionais.

Proposição 41. *Se $r, s \in \mathbb{Q}$, então $r^\diamond \cdot s^\diamond = (rs)^\diamond$.*

Demonstração. Tomando $p \in r^\diamond \cdot s^\diamond$, temos que $p \leq uv$ para alguma escolha de $u \in r^\diamond$ e $v \in s^\diamond$ o que implica em $u < r$ e $v < s$. Assim, podemos escrever $p \leq uv < rs$. Logo, $p < rs$ e daí $p \in (rs)^\diamond$. Por outro lado, se $p \in (rs)^\diamond$, então $p < rs$, o que significa que $p \leq rs$ e, portanto, $p \in r^\diamond \cdot s^\diamond$. Mostrando que $r^\diamond \cdot s^\diamond = (rs)^\diamond$. QED

Proposição 42. *Se $X \in \mathcal{C}$, $r \in X \Leftrightarrow r^\diamond < X$.*

Demonstração. Se $r \in X$ decorre que $r^\diamond \subset X$, pois para todo x racional menor do que r se tem $x \in X$, mas $r^\diamond = \{x \in \mathbb{Q} \mid x < r\}$. Além disso, como X é um corte, ele não possui elemento máximo, logo existe $s \in X$ tal que $r < s$. Isso mostra que $X \setminus r^\diamond \neq \emptyset$, portanto, $r^\diamond < X$.
Reciprocamente, se $r^\diamond < X$ da proposição 38 vem que $r^\diamond \subset X$ e $r^\diamond \neq X$. Como $X \neq r^\diamond$ existe s racional tal que $s \in X$ e $s \in r^\diamond$, então $r < s$, pois se fosse $s < r$ aconteceria $s \in r^\diamond$. De onde decorre que $r \in X$. QED

Teorema 35. *Se $X, Y \in \mathcal{C}$ e $X < Y$, então existe um corte racional $r^\diamond$ tal que $X < r^\diamond < Y$.*

Demonstração. Caso 1: X é um corte racional, digamos $X = s^\diamond$. Como $X < Y$ existe r racional tal que $r \in X \setminus Y$, com $r > s$. Pois caso contrário $Y \setminus X = \{s\}$, isto é, $Y = X \cup \{s\}$, contrariando a condição (3) da definição de corte. De $r \in Y$ e $r \notin r^\diamond$ obtemos $r^\diamond < Y$. Como $s < r$, então $X = s^\diamond < r^\diamond$.
Caso 2: X não é um corte racional. Como $X < Y$ existe r racional tal que $r \in Y \setminus X$. De $r \in Y$ e $r \notin r^\diamond$, obtemos $r^\diamond < Y$. Como r é cota superior de X e X não é racional, então r não é cota superior mínima de X e, daí existe $s \in r^\diamond \setminus X$, ou seja, $X < r^\diamond$. QED

4.4 O Conjunto dos Números Reais

Como demonstrado na seção 4.3 as operações de adição e multiplicação e a relação de ordem em $\mathcal{C}$ preservam as operações de adição e multiplicação e a relação de ordem em $\mathbb{Q}$. Identificando cada número racional r com o corte $r^\diamond$. Ficou demonstrado também que há em $\mathcal{C}$ cortes que não são racionais, isto é, existem cortes que não estão relacionados com nenhum $r \in \mathbb{Q}$. Com isso é possível definir o *conjunto dos números reais.*

Definição 25. *O conjunto $\mathcal{C}$ dos cortes será, a partir de agora, denominado conjunto dos números reais e será denotado por $\mathbb{R}$. Os cortes racionais serão identificados com os números racionais. E todo corte que não for racional será denominado número irracional.*

Com essa definição pode-se escrever $\mathbb{Q} \subset \mathbb{R}$ e que o conjunto $\mathbb{R} \setminus \mathbb{Q}$ é o conjunto dos números irracionais. Pode-se dizer então que um número real é um corte de Dedekind, ou seja, é um conjunto de números racionais e fazendo a identificação $r \to r^\diamond$ (que é uma bijeção) se pode dizer que todo número racional é um número real. Com isso é possível escrever $\mathbb{N} \subset \mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R}$.

A título de exemplo, o número real $z = \{r \in \mathbb{Q} \mid r^3 < 2\}$, como visto em 4.2, não é racional e, portanto, é irracional. Também como exemplo pertence ao conjunto $\mathbb{R} \setminus \mathbb{Q}$ o número que representa a medida da diagonal do quadrado de lado 1, que como demosntrado em 3.7 não é um número racional. Tal número é representado pelo símbolo $\sqrt{2}$ e é o corte $Y = \mathbb{Q}^*_- \cup \{y \in \mathbb{Q}_+ \mid y^2 < 2\}$.

Os próximos resultados apresentados nesta seção visam explicitar a grade diferença entre $\mathbb{Q}$ e $\mathbb{R}$. Como demonstrado as operações aritméticas e a relação de ordem nesses conjuntos respeitam as mesmas regras, entretanto, em $\mathbb{R}$ todo conjunto limitado superiormente possui supremo, diferente do que ocorre em $\mathbb{Q}$.

Teorema 36 (Teorema de Dedekind)**.** *Sejam A e B subconjuntos de $\mathbb{R}$ tais que:*

1. $\mathbb{R} = A \cup B$
2. $A \cap B = \emptyset$

3. $A \neq \emptyset$ *e* $B \neq \emptyset$

4. *Se* $x \in A$ *e* $y \in B$ *com* $x < y$.

Então, existe um, e apenas um, número real z *tal que* $x \leq z \leq y$, *para todo* $x \in A$ *e para todo* $y \in B$.

Demonstração. Cada ponto $x \in A$ define um corte de Dedekind, portanto, um subconjunto de $\mathbb{Q}$. Podemos, então tomar a união destes conjuntos.

Seja $z = \bigcup_{x \in X} x = \{r \in \mathbb{Q} \mid \exists\ x_0 \in A \text{ tal que } r \in x_0\}$. Mostremos que z é um corte nas condições requeridas.

(1) $\emptyset \neq z \neq \mathbb{Q}$: a desigualdade $\emptyset \neq z$ resulta imediatamente de $A \neq \emptyset$. Como $A \neq \emptyset$, existe $x \in A$, então $x \in z \neq \emptyset$. Para mostrar que $z \neq \mathbb{Q}$, tomemos $y \in B$ e seja $p \notin y$ um racional. Como, por hipótese, $x \subset y$, $\forall x \in A$, então $p \notin x$, $\forall x \in A$, de onde resulta $p \notin z$.

(2) Seja $p \in z$ e seja $q \in \mathbb{Q}$ tal que $q < p$. Como z é uma união, $p \in x$ para algum $x \in A$. Como x é um corte, $q \in x$, portanto, $q \in z$.

(3) Seja $p \in z$. Como z é uma união, $p \in x$ para algum $x \in A$. Como x é um corte de Dedekind, existe $q \in x$ tal que $p < q$. Por definição, é claro que $q \in z$, o que mostra que z não possui elemetno máximo.

Assim, z é um corte, e portanto, número real e temos que $x \leq z$, $\forall x \in A$, pois pela definição de z, sabemos que $x \subset z$, $\forall x \in A$.

Mostremos agora que $z \leq y$, $\forall y \in B$. Suponhamos que exista $y \in B$ com $y < z$. neste caso, existe um racional $r \in z \setminus y$. Por pertencer a z, r é um elemento de algum $x \in A$ e, não sendo elemento de y, obtemos $y < x$, uma contradição com (4).

Para verificar a unicidade, suponhamos que existam dois números z_1 e z_2, com $z_1 < z_2$ nas condições do enunciado. Consideremos z_3 tal que $z_1 < z_3 < z_2$, o que é possível pelo teorema 35. De $z_3 < z_2$ resulta que $z_3 \in A$, pois $y \geq z_2 > z_3$, para todo $y \in B$ e $A \cup B = \mathbb{R}$. Analogamente, de $z_1 < z_3$ resulta $z_3 \in B$. Obtemos então que $z_3 \in A \cap B$, uma contradição. Isso prova a unicidde de z. QED

Corolário 36.1. *Nas condições do teorema 36, ou existe em* X *um número máximo, ou em* Y, *um número mínimo.*

Demonstração. Seja z como no teorema 36. Então z está em X ou em Y, pela hipótese (1) e, por (2) em apenas um desses conjuntos. Se $z \in X$, então z é elemento máximo de X e, se $z \in Y$, z é elemento mínimo de Y. QED

4.5 Um Corpo Ordenado Completo

Como ficou demonstrado em 4.3 as operações de adição e multiplicação em $\mathbb{R}$ são ambas associativas, comutativas, possuem elemento neutro, possuem elemento oposto (que

para a adição é chamado de simétrico e para a multiplicação é chamado do inverso) e vale a distributividade da multiplicação em relação à adição, e que a ordem estabelecida em $\mathbb{R}$ é compatível com estas operações. Portanto, assim como $\mathbb{Q}$ o cojunto dos números reais é um corpo ordenado.

Para mostrar que $\mathbb{R}$ possui uma propriedade muito importante que $\mathbb{Q}$ não possui, considere os conjuntos $X = \mathbb{Q}_-^* \cup \{r \in \mathbb{Q}_+ \mid r^2 < 2\}$ e $Y = \{t \in \mathbb{Q}_+ \mid 2 < t^2\}$. Como demonstrado em 4.1 o conjunto X não possui supremo e o conjunto Y não possui ínfimo em $\mathbb{Q}$. Ou seja, não existe em $\mathbb{Q}$ um número racional s satisfazendo $r \leq s \leq t\ \forall r \in X$ e $\forall t \in Y$. Também ocorre que $\mathbb{Q} = X \cup Y$, $X \cap Y = \emptyset$, $X \neq \emptyset \neq Y$, pois por exemplo, $0 \in X$ e $2 \in Y$, e para todo $\forall r \in X$ e $\forall t \in Y$ vale $r < t$. Isso mostra que os conjuntos X e Y satisfazem a todas as hipóteses do Teorema de Dedekind, mas não cumprem a tese. Isso acontece porque no lugar de $\mathbb{R}$ está sendo usado $\mathbb{Q}$. Informalmente isso significa que em $\mathbb{Q}$ existem "lacunas" o que não acontece em $\mathbb{R}$. Por esse motivo diz-se que $\mathbb{R}$ tem a propriedade de ser *completo*. Se diz então que $\mathbb{R}$ é um corpo ordenado completo.

Observa-se que se o conjunto A do teorema 36 não contiver z, então ele é um corte em $\mathbb{R}$, no mesmo sentido da definição 14 de corte em $\mathbb{Q}$. A diferença é que em $\mathbb{Q}$ não se tem necessariamente, como em $\mathbb{R}$, o elemento z. Essas lacunas é que dão origem aos números irracionais. Como em $\mathbb{R}$ não ocorrem lacunas, cortes em $\mathbb{R}$ não geram novos números.

O teorema 37 é muito importante, porque dele deviram dois outros teoremas, a saber, o Teorema do Valor Médio e o Teorema de Weierstrass dos quais decorrem todos os demais resutados da Análise, incluindo o famoso Teorema Fundamental do Cálculo.

Teorema 37. *Se X é um subconjunto não vazio de $\mathbb{R}$ limitado superiormente, existe um único $\alpha \in \mathbb{R}$ tal que $\alpha = \sup(X)$.*

Demonstração. Definamos $A = \{\alpha \in \mathbb{R} \mid \alpha < x, \text{ para algum } x \in X\}$, isto é, A é o conjunto constituído precisamente pelos números reais que não são cotas superiores de X. Seja $B = \mathbb{R} \setminus A$, isto é, B é o conjunto constituído pelas cotas superiores de X. Vamos verificar que A e B satisfazem as condições do teorema 36. As condições (1) e (2) são claramente válidas. Quanto a (3), temos que, sendo $X \neq \emptyset$, existe $x \in X$ e, portanto, qualquer $\alpha < x$ é elemento de A, logo $A \neq \emptyset$. Ainda, como X é limitado superiormente, $B \neq \emptyset$. Para verificar (4), sejam $\alpha \in A$ e $\beta \in B$. Assim, existe $x \in X$ tal que $\alpha < x$. Como $\beta \geq X$, obtemos $\beta > \alpha$. Pelo corolário 36.1, ou A possui máximo, ou B possui mínimo. Vamos mostrar que a primeira alternativa não pode ocorrer, de onde decorrerá que B possui mínimo, que é a tese do teorema. Tomemos, então, α arbitrário em A. Existe $x \in X$ tal que $\alpha < x$. Consideremos α' tal que $\alpha < \alpha' < x$. Como $\alpha' < x$, então $\alpha' \in A$ e é maior do que α, ou seja, nenhum elemento de A é maior do que os demais, como queríamos verificar. QED

Finalmente é possível porvar o teorema 38.

Teorema 38 (Propriedade Arquimediana)**.** *O conjunto* $\mathbb{N}$ *dos naturais é ilimitado em* $\mathbb{R}$*.*

Demonstração. Suponhamos $\mathbb{N}$ limitado superiormente em $\mathbb{R}$ e seja $\alpha = \sup(\mathbb{N})$. Assim, $\alpha \geq n$, para todo $n \in \mathbb{N}$. Como $n+1 \in \mathbb{N}$, para todo $n \in \mathbb{N}$, então $n+1 \leq \alpha$, para todo $n \in \mathbb{N}$, de onde $\alpha - 1 \geq n$, para todo $n \in \mathbb{N}$, isto é, $\alpha - 1$ é cota superior para $\mathbb{N}$ menor do que o supremo de $\mathbb{N}$, uma contradição. QED

4.6 Axioma do Supremo

Durante todo o texto a motivação para a construção de um conjunto numérico mais amplo foi sempre dada pela exibição de uma falta ou deficiência do conjunto numérico já conhecido. Sendo assim cabe a pergunta: será o conjunto dos números reais autosuficiente? Isto é, não existe a necessidade de seguir ampliando a ideia de número e com isso ganhar novos resultados com tal procedimento?

Neste ponto há dois caminhos a serem tomados: se o conjunto $\mathbb{R}$ for considerado sem a estrutura de corpo, é bem sabido pelo professor da educação básica que existe um conjunto chamado de Conjunto dos Números Complexos denotado pela letra $\mathbb{C}$, do qual $\mathbb{R}$ é um subconjunto próprio, e traz consigo muitas possibilidades não existentes no conjunto dos números reais. Por exemplo, a resolução da equação como $x^2 + 1 = 0$ e de infinitas outras similares a esta. O estudo dos números complexos, embora muito interessante, foge da proposta deste trabalho. Uma observação interessante a respeito de $\mathbb{C}$ é que este conjunto é um corpo, entretanto não é ordenado.

Agora olhando $\mathbb{R}$ como um corpo ordenado, isto é, considerando a estrutura $[\mathbb{R}, +, \cdot, <]$ o própio Dedekind mostrou em seu trabalho, como feito em 4.5, que $\mathbb{R}$ é completo. Isso significa que não surgem novos elementos ao se tentar expandir $\mathbb{R}$ para um corpo ordenado maior. Juntando esse fato ao teorema 37 pode-se dizer que um corpo ordenado completo é aquele no qual todo conjunto limitado superiormente possui um supremo. Além disso, se pode mostrar que a menos de isomorfismo[3] $\mathbb{R}$ é o único corpo ordenado completo que existe.

Por esses motivos muitas vezes o conjunto dos números reais é estabelecido axiomaticamente como sendo um corpo ordenado no qual *todo conjunto limitado superiormente possui supremo*. Ou resumidamente, $\mathbb{R}$ é um corpo ordenado completo. Em geral quando $\mathbb{R}$ é apresentado axiomaticamente junto com a afimação de ser o conjunto dos números reais um corpo ordenado completo, vem um resumo das propriedades operativas de $\mathbb{R}$ como a seguir:

[3] Um isomorfismo é um homomorfismo bijetivo. E um homomorfismo é uma aplicação que preserva a estrutura algébrica.

Propriedades da Adição e da Multiplicação em $\mathbb{R}$. *Dados os números reais x, y e z a adição e a multiplicação satisfazem as seguintes propriedades:*

1. *Propriedade associativa da adição:* $x + (y + z) = (x + y) + z$.
2. *Propriedade comutativa da adição:* $x + y = y + x$.
3. *Existência do elemento neutro da adição:* $x + 0 = x = 0 + x$.
4. *Existência do elemento oposto da adição:* $x + (-x) = x - x = 0 = -x + x = (-x) + x$.
5. *Lei do cancelamento da adição:* $x + y = x + z \Rightarrow y = z$.
6. *Propriedade associativa da multiplicação:* $x \cdot (y \cdot z) = (x \cdot y) \cdot z$.
7. *Propriedade comutativa da multiplicação:* $x \cdot y = y \cdot x$.
8. *Existência do elemento neutro da multiplicação:* $x \cdot 1 = x = 1 \cdot x$.
9. *Existência do elemento inverso da multiplicação: Se* $x \neq 0$ *existe* $x^{-1} \in \mathbb{R}$ *único, tal que* $x \cdot x^{-1} = 1 = x^{-1} \cdot x$.
10. *Propriedade Distributiva:* $x \cdot (y + z) = x \cdot y + x \cdot z$.

Em um corpo a afirmação "todo conjunto limitado superiormente possui supremo" é conhecida como axioma do supremo.

4.7 Outra Abordagem Além de Dedekind

Outros matemáticos além de Dedekind dedicaram-se à formalização dos números reais, dentre eles pode-se citar George Cantor[4]. Cantor desenvolveu um trabalho similar ao de Dedekind. Enquanto Richard Dedekind mostrou que no conjunto dos cortes todo e qualquer subconjunto limitado superiormente possui supremo, o caminho tomado por George Cantor foi utilizar a ideia das sequências de Cauchy[5], mostrar que no universo dos números racionais infinitas sequências desse tipo não convergem, criar um conjunto $\mathcal{S}$ chamado Conjunto de Cauchy cujos elementos são classes de equivalência e mostrar que neste conjunto todas as sequências de Cauchy convergem. Ou de forma equivalente mostrar que em $\mathcal{S}$ todos os conjunto limitados superioremente possuem supremo.

Em última análise, o trabalho de Cantor e o trabalho de Dedekind foi o mesmo. Ambos motivados por uma inquietação persistente a respeito dos números, utilizaram

[4] Georg Ferdinand Ludwig Philipp Cantor foi um proeminente matemático alemão famoso pelos seus trabalhos relacionados à Teoria dos Conjuntos.

[5] Augustin Louis Cauchy foi um matemático francês e foi um dos responsáveis pela introdução do rigor na análise matemática.

ideias matemáticas existentes para criar novos conceitos. A partir destas novas ideias foram capazes de comprovar a existência de um conjunto numérico que colocou fim no desassossego dos matemáticos em relação à incompletude dos racionais.

5 Sugestões para abordar o Conjunto dos Números Reais no Ensino Médio

5.1 Considerações Iniciais

Este trabalho tem como pricinpal objetivo apoiar o porfessor de Matemática da escola básica em sua formação contínua, contribuindo para a construção de um corpo docente de excelência atuante na Educação Básica.

O tópico escolhido para ser abordado neste texto foi Conjuntos Numéricos, com o objetivo de se percorrer um caminho que culminasse na construção do Conjunto dos Números Reais. Tal escolha se deveu ao fato de ser este um assunto de extrema importância na formação dos discentes da Educação Básica. Conjuntos Numéricos constituem uma boa parte da base necessária para o desenvolvimento da Matemática e, portanto, é essencial que os discentes concluam o Ensino Médio com conhecimentos sólidos sobre o tema.

Outro fator relevante na escolha do foco do texto foi a experiência do autor no magistério. Atuando por mais de uma década na Educação Básica, prioritariamente no Ensino Médio, este autor pôde notar que o assunto **Números Reais** na maioria das vezes aparenta ser "espinhoso"e não dominado completamente por professores de Matemática Educação Básica. Este é um fato inquietante, pois se aqueles que vão ensinar não dominam o tema, decerto seus alunos serão afetados por essa lacuna.

O autor se considera parte dos professores da Educação Básica que, por deficiência na formação, já tiveram dificuldades em ministrar com propriedade aos seus alunos o conteúdo Números Reais. Por isso, tendo a oportunidade de aprofundar e aprimorar seus conhecimentos no curso de mestrado, este autor desejou modestamente compartilhar com seus pares algumas novidades aprendidas ao longo do curso a respeito desse tema tão interessante.

Acontece que boa parte do que foi desenvolvido nos capítulos precedentes tem foco em expandir o conhecimetno teórico do professor de Matemática a respeito dos conjuntos numéricos. Por esse motivo, muito do que foi desenvolvido não pode ser apresentado diretamente aos estudantes da Educação Básica, pois traz em sua apresentação definições, conceitos e métodos que são próprios de cursos superiores e, portanto, não são aprendidos na escola básica.

Como este programa de mestrado se destina à formação de docentes para a Educação Básica, este trabalho não poderia se encerrar sem sugerir algumas ideias para a apresentação do tema no nível básico de ensino. E é sobre este ponto que este capítulo vai se dedicar,

isto é, uma abordagem pedagógica de sobre como abordar o Conjunto dos Números Reais no Ensino Médio. Vale destacar que este capítulo não pretende ser um roteiro de atividades a serem desenvolvidas com os alunos da Educação Básica, mas sim servir como fonte de inspiração para os professores a respeito de formas de se abordar o Conjunto dos Números Reais na Educação Básica.

5.2 Recontar a História

Talvez uma boa estratégia para falar do Conjunto dos Números Reais seja repetir os passos da história. Os matemáticos só passaram a se preocupar em formalizar um conjunto numérico que viria a ser chamado de conjunto dos números reais, depois da descoberta da existência de números que não eram racionais. Até então a crença de que o Conjunto dos Números Racionais era capaz de suprir todas as necessidades humanas era muito bem aceita. Os problemas começaram a aparecer quando da descoberta da incomensurabilidade, podendo citar inclusive a Crise dos Incomensuráveis[1].

Algo parecido acontece no ensino de Matemática na Educação Básica. Até o conjunto dos números racionais, a construção dos conjuntos numéricos parece ser mais facilmente aceita ou compreendida pelos estudantes. Eles aparentam estar confortáveis com todas as definições e operações que lhes são apresentadas. Salvo raras exceções não há questionamentos sobre a possível existência de outros números. Isso se dá é claro, dentre outros motivos, pela perspicácia dos professores em não apresentar problemas que recaiam em números ainda desconhecidos pelos alunos.

Os conjuntos numéricos aparecem algumas vezes ao longo do Ensino Fundamental, mas é no Ensino Médio que eles são tratados com um pouco mais de formalismo. Nesta etapa da Educação Básica, os estudantes já estão familiarizados com os conceitos de fatoração, fração e raíz quadrada. Por isso, é aceitável supor que, após algumas discussões, atividades práticas, apresentação dos conceitos de argumentação e provas matemáticas, um discente neste nível seja capaz de compreender a demonstração da existência de segmentos incomensuráveis dada em 3.7. Ou seja, a demonstração de que a raiz quadrada do número 2 não é um número racional e, portanto, não é nenhum número, até então, conhecido pelos estudantes.

A partir daí, se abre um mundo novo cheio de possibilidades. Muitas coisas a serem descobertas e exploradas. O professor baseado na demosntração 3.7 pode construir uma ponte para a demonstração dada em A e levar os estudantes a conhecerem, literalmente, uma infinidade desses novos números. Isto é, de números que não são racionais.

[1] Muitos historiadores defendem que a descoberta de segmentos incomensuráveis gerou uma crise na Escola Pitagórica, pois esta se baseava na creça de que a essência de todas as coisas, na geometria bem como nos negócios práticos e teóricos do homem, é explicável em termos da aritmética, ou propriedades intrínsecas de números inteiros ou suas razões. Isto é, por meio de números racionais.

Nesta altura dos fatos, o professor pode definir o Conjunto dos Números Reais, denotado por $\mathbb{R}$, como sendo o conjunto que contém os números resultantes de medidas, seus inversos aditivos (ou simétricos) e o número zero. Logo, estão neste conjunto todos os números racionais, e além disso, pertencem também a este conjunto, infinitos números que não são racionais.

Em outras palavras, neste ponto é apresentado ao aluno um conjunto numérico chamado Conjunto dos Números Reias ($\mathbb{R}$) que contém o Conjunto dos Números Racionais ($\mathbb{Q}$), isto é, $\mathbb{Q} \subset \mathbb{R}$ e, para mais, contém uma infinidade de outros números que não são racionais.

Estes números reais que não são racionais passam então a serem chamados de Números Irracionais. Na literatura de Educação Básica o Conjunto dos Números Irracionais costuma ser denotado pela letra $\mathbb{I}$, já na literatura de Ensino Superior o mesmo conjunto é mais comumente representado por $\mathbb{R} \setminus \mathbb{Q}$.

Com essa construção chega-se ao primeiro fato importante sobre o conjuntos dos reais, a saber, $\mathbb{R} = \mathbb{Q} \cup \mathbb{I}$. Ou seja, o Conjunto dos Números Reais é a união disjunta do Conjuntos dos Números Racionais com o Conjunto dos Números Irracionais. Além disso, para uma boa caracterização de $\mathbb{R}$ falta mostrar que há no conjunto dos números reais muito mais números irracionais do que números racionais. Esta é uma etapa importante, porém crítica de ser cumprida, pois para cumpri-la não há como escapar do conceito de enumerabilidade, normalmente não trabalhado no Ensino Médio.

5.3 Enumerabilidade

Para chegar à afirmação feita no final da seção 5.2, isto é, que há em $\mathbb{R}$ mais números irracionais do que números racionais, será preciso passar pela enumerabilidade de todos os conjuntos numéricos aqui estudados. E para isto se faz necessária seguinte definição:

Definição 26. *Um conjunto é dito ser enumerável quando é finito ou quando é infinito e existe uma função bijetora entre tal conjunto e o conjunto dos números naturais.*

Infelizmente o conceito de enumerabilidade não é muito abordado na Educação Básica. Certamente não se trata de um conceito trivial ou simples de ser entender, porém ele é de extrema importância para possibilitar ao discente do Ensino Médio concluir este ciclo com uma noção correta e consistente da estrutura do Conjunto dos Números Reais. Este autor acredita firmemente que poupar os alunos da Educação Básica deste e de outros conceitos comumente abandonados nesta etapa do ensino é uma postura que mais prejudica do que ajuda. Dito isto, a sugestão dada nesas páginas para trabalhar com números reais no Ensino Médio passa, necessariamente, pela enumerabilidade e alguns

outros conceitos muitas vezes considerados avaçados demais. Entretanto, acreditando no potencial de cada estudante e no trabalho do professor de Matemática, este autor insiste que este é um bom caminho.

Passando a analisar a enumerabilidade dos conjunto estudados, diante da definição 26 é imediato concluir que o Conjunto dos Números Naturais é ele próprio enumerável, basta tomar a função identidade de $\mathbb{N}$ em $\mathbb{N}$.

Um conceito bastante conhecido para conjuntos finitos é a cardinalidade. Diz-se que dois conjuntos X, Y possuem a mesma cardinalidade, e se denota este fato por $\text{card}(X) = \text{card}(Y)$, quando existe uma função bijetora que os relaciona. Em se tratando de conjuntos finitos a cardinalidade diz respeito à quantidade de elementos do conjunto. Isto é, escrever $\text{card}(A) = 3$ significa que o conjunto A é constituído de três elementos. É útil estender a ideia de cardinalidade para conjuntos infinitos. Pode-se dizer que $\text{card}(\mathbb{N}) = \infty$, esta igualdade deve ser entendida como uma notação para expressar o fato que há em $\mathbb{N}$ infinitos elementos, uma vez que o símbolo ∞ não é um número. Além disso, se X for um conjunto infinito e enumerável, então $\text{card}(X) = \text{card}(\mathbb{N})$.

Considere um conjunto infinto X. Existem então tantos subconjnutos não-vazios $A_n \subset X$ quanto desejáveis. Como os subconjuntos A_n são não vazios pode-se escolher em cada um deles um elemento x_n. Sejam $A_1 \subset X$ tal que $x_1 \in A_1$, $X \supset A_2 = X \setminus \{x_1\}$ tal que $x_2 \in A_2$, $X \supset A_3 = X \setminus \{x_1, x_2\}$ tal que $x_3 \in A_3$, $X \supset A_4 = X \setminus \{x_1, x_2, x_3\}$ tal que $x_4 \in A_4$, $\cdots$, $X \supset A_n = X \setminus \{x_1, x_2, x_3, x_4, \cdots, x_{n-1}\}$ tal que $x_n \in A_n$. Definindo-se indutivamente a função $f : \mathbb{N} \to X$ da seguinte forma: $f(1) = x_1, f(2) = x_2, f(3) = x_3, f(4) = x_4, \cdots, f(n) = x_n$ e assim sucessivamente, é claro que a função f é uma injeção de $\mathbb{N}$ no conjunto $f(\mathbb{N}) \subset X$. Portanto, está contido no conjunto infinito X um subconjunto equipotente[2] ao conjunto dos números naturais, ou seja, um subconjunto infinito e enumerável. Como o conjunto X é arbitrário é razoável afirmar que qualquer conjunto infinto X possui um subconjunto infinito e enumerável.

Assim para todo conjunto X infinito tem-se $\text{card}(\mathbb{N}) \leq \text{card}(X)$, ou seja, dentre os conjuntos infinitos a cardinalidade de $\mathbb{N}$ (ou de um conjunto enumerável) é a menor de todas.

5.3.1 $\mathbb{Z}$ é enumerável

Analisando de forma superficial a cardinalidade do Conjunto dos Números Inteiros poderíamos ser levados a pensar que há o dobro menos um, ou o dobro mais um (a depender se o zero é ou não considerado natural) números inteiros do que números naturais. Esta constatação é um exemplo claro de como, em Matemática, a intuição pode levar a conclusões equivocadas.

[2] Dois ou mais conjuntos são ditos equipotentes quando possuem a mesma cardinalidade.

Fazendo uma análise mais cuidadosa, com o auxílio da figura 2 pode-se inferir a seguinte função de $\mathbb{Z}$ em $\mathbb{N}$:

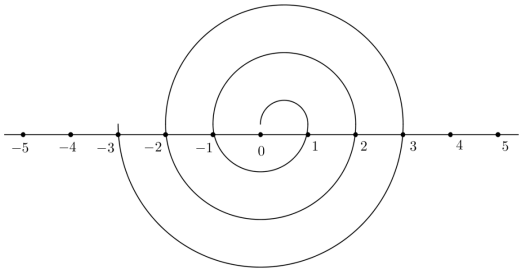

Figura 2 – Função Alternada.

$0 \to 1$	$1 \to 2$
$-1 \to 3$	$2 \to 4$
$-2 \to 5$	$3 \to 6$
$-3 \to 7$	$4 \to 8$
$-4 \to 9$	$5 \to 10$
$\vdots$	$\vdots$

Tabela 1 – Função Alternada

Isto é, a função $f : \mathbb{Z} \to \mathbb{N}$ leva o número zero e os números inteiros negativos nos naturais ímpares e leva os inteiros positivos nos naturias pares. Escrevendo isso de forma algébrica: $f : \mathbb{Z} \to \mathbb{N}$, tal que $f(n) = \begin{cases} 2n, & \text{se } n \in \mathbb{N} \\ -2n+1, & \text{se } n \in \mathbb{Z} \setminus \mathbb{N} \end{cases}$.

Agora, diante da figura 2, da tabela 1 e da função f é mais fácil aceitar que os conjuntos $\mathbb{N}$ e $\mathbb{Z}$ possuem a mesma quantidade de elementos. Entretanto, só aceitar não é suficiente, é necessário mostrar tal fato. Para isso se deve constatar que a função f é bijetora.

Para verificar a sobrejetividade da função f tome um natural n qualquer. Se n é ímpar, $n-1$ é par e, portanto, $\frac{n-1}{2}$ é natural. Logo $-\frac{n-1}{2}$ é um inteiro negativo tal que $f\left(\frac{n-1}{2}\right) = n$. Agora se n é par, $\frac{n}{2}$ é um inteiro posito tal que $f\left(\frac{n}{2}\right) = n$. O que mostra que f é uma função sobrejetiva.

Para a injetividade, suponha que existam dois inteiros n_1 e n_2 tais que $f(n_1) = f(n_2)$. Note que, necessariamente, $n_1 \times n_2 \geq 0$, isto é, n_1 e n_2 devem ter o mesmo sinal. Pois caso contrário suas imagens seriam uma par e outra ímpar e, portanto, diferentes. Se $n_1 > 0$ e $n_2 > 0$, então $2n_1 = 2n_2 \Leftrightarrow n_1 = n_2$. Agora se $n_1 \leq 0$ e $n_2 \leq 0$, então $-2n_1 + 1 = -2n_2 + 1 \Leftrightarrow -2n_1 = -2n_2 \Leftrightarrow n_1 = n_2$. Mostrando que a função f é injetiva e, consequentemente, é uma bijeção. Dessa forma ficou demonstrado que há em $\mathbb{Z}$ a mesma quantidade de elementos que há em $\mathbb{N}$, ou seja, $\text{card}(\mathbb{N}) = \text{card}(\mathbb{Z})$.

Como comentado, o estudo da enumerabilidade de conjuntos não é trivial. Entretanto, dentre os conjuntos abordados neste texto, aquele que pode mais facilmente ser aceito como um conjunto enumerável é o conjunto dos números inteiros. Apesar deste não ser um fato intuitivo, a demosntração busca inspiração numa ilustração, isto é, na figura 2 o que auxilia muito a aceitação do resultado. E a função bijetora exibida é composta por funções amplamente estudadas no Ensino Médio. É uma função definida por partes (apenas duas partes), composta por duas funções polimoniais do primeiro grau. Ademais, os conceitos de função injetora, sobrejetora e bijetora também são bastante estudados na Educação Básica. Tudo isso facilita o entendimento da enumerabilidade deste primeiro conjunto.

5.3.2 $\mathbb{Q}$ é enumerável

Tão contraintuitivo quanto ou até mais contraintuitivo do que a enumerabilidade de $\mathbb{Z}$, é a enumerabilidade de $\mathbb{Q}$. Para olhos desatentos a cardinalidade do conjunto $\mathbb{Z}$ era alguma coisa perto do dobro da cardinalidade do conjunto $\mathbb{N}$. Imagina então a quantidade de elementos de um conjunto que além de possuir todos os númeos inteiros, possui todas as quantidades representadas por frações com numerador e denominador inteiros. É fácil concordar que, guiado pela intuição, qualquer um afirmaria categoricamente que há em $\mathbb{Q}$ mais elementos do que em $\mathbb{N}$. Acontece que a verdade não é esta! Surpreendentemente o Conjunto dos Números Racionais é enumerável. Isto é, existem tantos números racionais quanto números naturias.

Demonstrar esta afirmação é um tanto mais complicado do que foi demonstrar a enumerabilidade de $\mathbb{Z}$. Contudo, seguindo o espírito adotado neste capítulo, isto é, acreditando que mesmo no nível da Educação Básica é possível lidar com alguns teoremas e suas demonstações. Vamos listar e demonstrar algumas proposições que permitirão chegar à enumerabilidade de $\mathbb{Q}$.

Teorema 39. *A união de dois conjuntos enumeráveis é enumerável.*

Demonstração. Sejam $X = \{x_1, x_2, x_3, \cdots\}$ e $Y = \{y_1, y_2, y_3, \cdots\}$ dois conjuntos enumeráveis. Se X e Y são disjuntos, isto é, se não há interseção entre eles, ou ainda, se $X \cap Y = \emptyset$. A função $f : X \cup Y \to \mathbb{N}$, tal que $f(x_n) = 2n - 1$ e $f(y_n) = 2n$, pelo que foi demonstrado em 5.3.1, é uma bijeção. Agora, se $X \cap Y \neq \emptyset$ basta escrever $X \cup Y = X \cup (Y \setminus X)$. Assim a demonstração recai no caso anterior e temos demosntrado que a união de dois conjuntos enumeráveis é enumerável. QED

Teorema 40. *Sejam $X_1, X_2, \cdots, X_n$ conjuntos enumeráveis. Então $\bigcup_{i=1}^{n} X_i$ é enumerável.*

Demonstração. Esta demostração será feita por indução sobre o índice dos conjuntos. O passo base da indução está demonstrado no teorema 39. Por hipótese de indução

suponhamos que $\bigcup_{i=1}^{n} X_i$ seja enumerável. Então $\bigcup_{i=1}^{n+1} X_i$ é enumerável, pois $\bigcup_{i=1}^{n+1} X_i = (\bigcup_{i=1}^{n} X_i) \cup X_{n+1}$, é a união de dois conjuntos enumeráveis, a saber, $\bigcup_{i=1}^{n} X_i$ que é enumerável, por hipótese de indução e X_{n+1} que é enumerável, por definição. Portanto, a união de uma quantidade finita de conjuntos enumeráveis é enumerável. QED

Dizer que um conjunto é enumerável é o mesmo que dizer que é possível enumerar, ou listar, todos os seus elementos. O que será feito para mostrar a enumerabilidade de $\mathbb{Q}$ é mostrar um algoritmo que permite listar todos os racionais positivos e todos os racionais negativos, e depois utilizar o teorema 40.

Observe a tabela 2. Nela todas as frações com numeradores e denominadores inteiros positivos estão organizados numa matriz infinita. A fim de criar uma lista, ou uma enumeração, destas frações a matriz infinita será percorrida pelas diagonais, como indicam as setas. A primeira diagonal é composta apenas pela fração $1/1 = 1$, a segunda diagonal é composta pelas frações $1/2$ e $2/1$ que devem ser consideradas nesta ordem, como indica a seta. Considerando a direção indicada pela próxima seta, o grupo subsequente de frações a ser listado é $3/1$, $2/2$ e $1/3$.

$1/1$	$1/2$	$1/3$	$1/4$	$1/5$	$1/6$	$1/7$	$1/8$	$1/9$	$1/10$	$1/11$	$\cdots$
$2/1$	$2/2$	$2/3$	$2/4$	$2/5$	$2/6$	$2/7$	$2/8$	$2/9$	$2/10$	$2/11$	$\cdots$
$3/1$	$3/2$	$3/3$	$3/4$	$3/5$	$3/6$	$3/7$	$3/8$	$3/9$	$3/10$	$3/11$	$\cdots$
$4/1$	$4/2$	$4/3$	$4/4$	$4/5$	$4/6$	$4/7$	$4/8$	$4/9$	$4/10$	$4/11$	$\cdots$
$5/1$	$5/2$	$5/3$	$5/4$	$5/5$	$5/6$	$5/7$	$5/8$	$5/9$	$5/10$	$5/11$	$\cdots$
$6/1$	$6/2$	$6/3$	$6/4$	$6/5$	$6/6$	$6/7$	$6/8$	$6/9$	$6/10$	$6/11$	$\cdots$
$7/1$	$7/2$	$7/3$	$7/4$	$7/5$	$7/6$	$7/7$	$7/8$	$7/9$	$7/10$	$7/11$	$\cdots$
$8/1$	$8/2$	$8/3$	$8/4$	$8/5$	$8/6$	$8/7$	$8/8$	$8/9$	$8/10$	$8/11$	$\cdots$
$9/1$	$9/2$	$9/3$	$9/4$	$9/5$	$9/6$	$9/7$	$9/8$	$9/9$	$9/10$	$9/11$	$\cdots$
$10/1$	$10/2$	$10/3$	$10/4$	$10/5$	$10/6$	$10/7$	$10/8$	$10/9$	$10/10$	$10/11$	$\cdots$
$11/1$	$11/2$	$11/3$	$11/4$	$11/5$	$11/6$	$11/7$	$11/8$	$11/9$	$11/10$	$11/11$	$\cdots$
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\ddots$

Tabela 2 – Organização das frações positivas numa matriz infinita.

Para criar uma lista de todas as frações positivas coloca-se os elementos ordenados da primeira diagonal, seguidos dos elementos ordenados da segunda diagonal, depois os elemetnos ordenados da terceira diagonal e assim por diante. Com esse processo chega-se a seguinte lista:

$$\frac{1}{1}, \frac{1}{2}, \frac{2}{1}, \frac{3}{1}, \frac{2}{2}, \frac{1}{3}, \frac{1}{4}, \frac{2}{3}, \frac{3}{2}, \frac{4}{1}, \frac{5}{1}, \frac{4}{2}, \frac{3}{3}, \frac{2}{4}, \frac{1}{5}, \frac{1}{6}, \frac{2}{5}, \frac{3}{4}, \frac{4}{3}, \frac{5}{2}, \frac{6}{1}, \cdots$$

Observe que cada diagonal possui um número finito de elementos. Então para listar todas a frações positivas basta escrever todos os elementos de cada diagonal um após o outro, na ordem indicada pela seta. Note ainda que na lista apresentada há repetição de números racionais. Por exemplo, o racional 1 aparece infinitas vezes com as suas infinitas representações fracionárias, a saber, $1/1, 2/2, 3/3, \cdots$. O mesmo acontece com todos os demais números racionais positivos, citando um caso análogo, pode-se observar o número racional $0,25$ que é representado por meio das fações $1/4, 2/8, 3/12, \cdots$.

Isso acontece, porque cada racional possui infinitas representações fracionárias. Como o intresse é construir uma enumeração do conjunto dos números racionais positivos, para resolver esse problema basta seguir o algoritmo das diagonais e retirar de cada grupo as frações que não são irredutíveis. Gerando a lista:

$$\frac{1}{1}, \frac{1}{2}, \frac{2}{1}, \frac{3}{1}, \frac{1}{3}, \frac{1}{4}, \frac{2}{3}, \frac{3}{2}, \frac{4}{1}, \frac{5}{1}, \frac{1}{5}, \frac{1}{6}, \frac{2}{5}, \frac{3}{4}, \frac{4}{3}, \frac{5}{2}, \frac{6}{1}, \cdots$$

Dessa forma cada grupo, ou cada diagonal, continuará possuindo um número finito de elementos. E é claro que, seguindo o algoritmo, todos os números racionais aparecerão na lista. Dessa maneira, basta, por exemplo, criar a enumeração $1 \to \frac{1}{1}, 2 \to \frac{1}{2}, 3 \to \frac{2}{1}, 4 \to \frac{3}{1}, 5 \to \frac{1}{3}, 6 \to \frac{1}{4}, 7 \to \frac{2}{3}, 8 \to \frac{3}{2}, 9 \to \frac{4}{1}, \cdots$. Com isso fica comprovado que o conjunto $\mathbb{Q}_+^*$ é enumerável.

De forma totalmente análoga mostra-se que o conjunto $\mathbb{Q}_-^*$ também é enumerável e por definição o conjunto $\{0\}$ é enumerável, pois é finito. Então se conclui, do teorema 40, que o conjunto $\mathbb{Q}_-^* \cup \{0\} \cup \mathbb{Q}_+^*$ é enumerável. Mas $\mathbb{Q}_-^* \cup \{0\} \cup \mathbb{Q}_+^* = \mathbb{Q}$, logo o Conjuntos dos Números Racionais é enumerável.

Isto significa que o Conjunto dos Números Racionais e o Conjunto dos Números Naturais e consequnetemente o Conjunto dos Números Inteiros possuem a mesma quantidade de elementos ou são equipotentes. Portanto, $\text{card}\,(\mathbb{N}) = \text{card}\,(\mathbb{Z}) = \text{card}\,(\mathbb{Q})$.

5.4 Outros Conjuntos Enumeráveis

O objetivo desta seção é apresentar outros conjuntos enumeráveis que não estão contidos em $\mathbb{Q}$, mas estão contidos em $\mathbb{R}$ e assim concluir que há em $\mathbb{R}$ muito mais números irracionais do que números racionais. Para tanto faz-se necessário mostar que a soma de um número irracional com um número racional é um número irracional, assim como o produto de um número irracional por um número racional é um número irracional. Ambas as demostrações são feitas por redução ao absurdo.

Teorema 41. *Sejam $a \neq 0$ um número racional e α um número irracional. Então $a+\alpha$ e $a \cdot \alpha$ são números irracionais.*

Demonstração. Suponha por absurdo que $a+\alpha$ e $a \cdot \alpha$ sejam números racionais. Então podemos escrever $a+\alpha = \frac{p}{q}$ e $a \cdot \alpha = \frac{m}{n}$ com $p, q, m, n \in \mathbb{Z}$ e, q e $n \neq 0$. Além disso como $a \in \mathbb{Q}$ podemos escrever $a = \frac{x}{y}$ com $x, y \in \mathbb{Z}$ e, $y \neq 0$. Então $a+\alpha = \frac{x}{y}+\alpha = \frac{p}{q}$ e $a \cdot \alpha = \frac{x}{y} \cdot \alpha = \frac{m}{n}$. A partir daí, usando as propriedades de operação entre frações, podemos concluir: $\frac{x}{y}+\alpha = \frac{p}{q} \Rightarrow -\frac{x}{y}+\frac{x}{y}+\alpha = \frac{p}{q}-\frac{x}{y} \Rightarrow 0+\alpha = p \cdot q^{-1} - x \cdot y^{-1} \Rightarrow \alpha = p \cdot q^{-1} - x \cdot y^{-1} = \alpha = p \cdot q^{-1} \cdot (q \cdot y)^{-1} \cdot q \cdot y - x \cdot y^{-1} \cdot (q \cdot y)^{-1} \cdot q \cdot y \Rightarrow \alpha = p \cdot y \cdot (q \cdot y)^{-1} \cdot q \cdot q^{-1} - x \cdot q \, (q \cdot y)^{-1} \cdot y \cdot y^{-1} \Rightarrow \alpha = p \cdot y \cdot (q \cdot y)^{-1} - x \cdot q \, (q \cdot y)^{-1} \Rightarrow \alpha = (p \cdot y - x \cdot q) \cdot (q \cdot y)^{-1} \Rightarrow \alpha = \frac{p \cdot y - x \cdot q}{q \cdot y}$. Como $p, q, x, y \in \mathbb{Z}$, q e $y \neq 0$ e $\mathbb{Z}$ não possui divisores de zero temos que $p \cdot y - x \cdot q \in \mathbb{Z}$ e $0 \neq q \cdot y \in \mathbb{Z}$ e disso segue que $\frac{p \cdot y - x \cdot q}{q \cdot y} \in \mathbb{Q}$. Concluímos então que $\alpha \in \mathbb{Q}$ o que é um absurdo, pois por hipótese $\alpha \in \mathbb{R} - \mathbb{Q}$. Logo $a+\alpha \in \mathbb{R} - \mathbb{Q}$.

Também $\frac{x}{y} \cdot \alpha = \frac{m}{n} \Rightarrow \left(\frac{x}{y}\right)^{-1} \cdot \frac{x}{y} \cdot \alpha = \frac{m}{n} \cdot \left(\frac{x}{y}\right)^{-1} \Rightarrow 1 \cdot \alpha = m \cdot n^{-1} \cdot x^{-1} \cdot (y^{-1})^{-1} \Rightarrow \alpha = m \cdot y \cdot n^{-1} \cdot x^{-1} \Rightarrow \alpha = m \cdot y \cdot (n \cdot x)^{-1} \Rightarrow \alpha = \frac{m \cdot y}{n \cdot x}$ Como $m, n, x, y \in \mathbb{Z}$, n e $x \neq 0$ e $\mathbb{Z}$ não possui divisores de zero temos que $m \cdot y \in \mathbb{Z}$ e $0 \neq n \cdot x \in \mathbb{Z}$ e disso segue que $\frac{m \cdot y}{n \cdot x} \in \mathbb{Q}$. Concluímos então que $\alpha \in \mathbb{Q}$ o que é um absurdo, pois por hipótese $\alpha \in \mathbb{R} - \mathbb{Q}$. Logo $a \cdot \alpha \in \mathbb{R} - \mathbb{Q}$. QED

5.4.1 $X_{n+\sqrt{p}}$ é enumerável

Considere o conjunto $X_{n+\sqrt{p}} = \left\{n + \sqrt{p} \mid n \in \mathbb{Q} \text{ e } p \text{ é um número primo fixo}\right\}$. Ou seja, $X_{n+\sqrt{p}}$ é o conjunto formado por todas as somas $n+\sqrt{p}$ onde n percorre todo o conjunto dos números racionais e p é um número primo. Do apêndice A vem que $\sqrt{p}$ é irracional e do teorema 41 segue que $n+\sqrt{p}$ é um número irracional. Logo, o conjunto $X_{n+\sqrt{p}}$ possue apenas números irracionais. É fácil ver que $X_{n+\sqrt{p}}$ é enumerável, basta tomar a função $f : \mathbb{N} \to X_{n+\sqrt{p}}$ definida por $f(n) = n+\sqrt{p}$, é claro que esta função é uma bijeção. Logo, $\text{card}\left(X_{n+\sqrt{p}}\right) = \text{card}(\mathbb{N}) = \text{card}(\mathbb{Q})$. Ou seja, $X_{n+\sqrt{p}}$ e $\mathbb{Q}$ são equipotentes.

5.4.2 $X_{n\sqrt{p}}$ é enumerável

Considere o conjunto $X_{n\sqrt{p}} = \left\{n\sqrt{p} \mid n \in \mathbb{Q} \text{ e } p \text{ é um número primo fixo}\right\}$. Ou seja, $X_{n\sqrt{p}}$ é o conjunto formado por todas os produtos $n\sqrt{p}$ onde n percorre todo o conjunto dos números racionais e p é um número primo. Do apêndice A vem que $\sqrt{p}$ é irracional e do teorema 41 segue que $n\sqrt{p}$ é um número irracional. Logo, o conjunto $X_{n\sqrt{p}}$ possue apenas números irracionais. Também é fácil verificar que $X_{n\sqrt{p}}$ é enumerável. Qual é uma bijeção bastante intuitiva de $\mathbb{N}$ em $X_{n\sqrt{p}}$? Da mesma forma, $X_{n\sqrt{p}}$ e $\mathbb{Q}$ são equipotentes.

5.5 Tamanho de $\mathbb{R}$

Pelo demonstrado em 5.3.2 e 5.4 pode-se ter uma boa noção sobre a composição do conjunto dos números reais. Ficou demonstrado que existem infinitos conjnutos enumeráveis formados apenas por números irracionais. A saber, os conjuntos $X_{n+\sqrt{2}}, X_{n+\sqrt{3}}, X_{n+\sqrt{5}} \cdots$ e os conjuntos $X_{n\sqrt{2}}, X_{n\sqrt{3}}, X_{n\sqrt{5}}, \cdots$. Isso significa que $\mathbb{R}$ é constituído, além de $\mathbb{Q}$, por infintos conjuntos de números irracionais com a mesma cardinalidade de $\mathbb{Q}$, mostrando que há em $\mathbb{R}$ muito mais números irracionais do que números racionais. O entendimento desse fato completa uma boa caracterização do conjunto dos números reais. Ou seja, $\mathbb{R}$ é um conjunto numérico formado por números racionais e números irracionais e há em $\mathbb{R}$ mais irracionais do que racionais.

5.6 $\mathbb{R}$ é ou não é enumerável?

O principal conceito tratado neste capítulo foi o conceito de **enumerabilidade**. Esta noção foi usada para descrever o "tamanho", ou em linguagem matemática, a cardinalidade de conjuntos infinitos. E através dela se buscou mostrar a composição do conjunto dos números reais. A saber, que existem em $\mathbb{R}$ muito mais números irracionais do que números racionais.

Para encerrar a discussão a respeito dos reais é conveniente analisar a enumerabilidade do próprio conjunto $\mathbb{R}$. Para isso não há como escapar de um teorema clássico dos cursos de análise matemática. Tal teorema será apresentado, mas não demostrado. Entretato, após todo o desenvolvimento feito neste texto é uma afirmação razoável de ser aceita como verdadeira. Contudo sua demonstração pode ser encontrada em (LIMA, 2017).

Teorema 42. *Todo subconjunto de um conjunto enumerável é enumerável.*

É bastante plausível acreditar no enunciado do teorema 42. E apropriado lembrar que um conjunto é enumerável quando ele é finito ou quando ele é infinito e equipotente ao conjunto $\mathbb{N}$.

Para poder chegar a alguma conclusão a respeito da enumerabilidde de $\mathbb{R}$, ainda será necessário lançar mão da representação decimal dos números reais. Tanto alunos quanto professores do Ensino Médio já possuem em seu imaginário o conhecimento da representação decimal de números reais. Sobre tais representações há, na verdade, um importante detalhe técnico que pode ser visto em (FERREIRA, 2013). Porém nestas páginas a noção construída ao longo dos anos de Educação Básica é suficiente para alcançar o objetivo. Recordando que a cada número real não negativo e menor do que um corresponde uma única sequência de dígitos, a saber, $0, a_1a_2a_3 \ldots$. E a cada sequência do tipo $0, a_1a_2a_3 \ldots$ está relacionado um único número real não negativo menor do que um.

Finalmente considere o intervalo, subconjunto de $\mathbb{R}$, $I = (0, 1)$. Supondo que I é enumerável, pode-se escrever uma enumeração de seus elementos. Isto é, pode-se escrever $I = \{x_1, x_2, x_3, \cdots\}$. Para cada um dos elementos de I escreve-se sua representação decimal e as representam numa matriz infinita.

$$\begin{aligned} x_1 &= 0, x_{11}x_{12}x_{13}x_{14}x_{15}\cdots \\ x_2 &= 0, x_{21}x_{22}x_{23}x_{24}x_{25}\cdots \\ x_3 &= 0, x_{31}x_{32}x_{33}x_{34}x_{35}\cdots \\ &\vdots \\ x_n &= 0, x_{n1}x_{n2}x_{n3}x_{n4}x_{n5}\cdots \\ &\vdots \end{aligned}$$

Cada dígito x_{ij} dos números x_k são tais que $x_{ij} \in \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$. Como I foi suposto enumerável, todo elemento de I deve estar representado na matriz infinita construída acima.

Seja então o número real y tal que $y = 0, y_1y_2y_3\cdots$ produzido da seguinte forma: $y_1 \neq x_{11}$, $y_2 \neq x_{22}$, $y_3 \neq x_{33}$, $\cdots$, $y_n \neq x_{nn}$, $\cdots$. Note que $y \neq x_1$, pois $y_1 \neq x_{11}$ da mesma forma $y \neq x_2$, pois $y_2 \neq x_{22}$, de modo geral $y \neq x_n$, pois $y_n \neq x_{nn}$.

Ou seja, foi possível construir um número real não negativo menor do que um que não está represetado na matriz infinita acima definida. Portanto, este número não está na enumeração de I. Em outras palavras $y \notin \{x_1, x_2, x_3, \cdots\}$ o que mostra que I não é enumerável.

Agora, para analisar a enumerabilidade de $\mathbb{R}$ basta associar o teorema 42 com a não enumerabilidade do intervalo I. Claramente $I \subset \mathbb{R}$ e isso implica que o conjunto dos números reais não é enumerável, pois se assim o fosse o intervalo I também seria enumerável, e como foi demonstrado tal intervalo não é enumerável.

Por fim gostaria de destacar que estou ciente que existem diversos dedafios cognitivos no ensino/aprendizagem dos números reais, entretanto acredito que com paciência e algum esforço por parte do professor de Matemática seja possível implementar as sugestões aqui expostas no tratamento deste tópico tão delicado da Matemática.

6 Considerações Finais

A intenção deste trabalho é dotar o professor da educação básica de uma visão global a respeito dos principais conjuntos numéricos tratados nos ensinos fundamental e médio e uma percepção da existência, de fato, desses conjuntos. Por isso, na medida do possível, o tratamento dado para a apresentação dos conjuntos numéricos buscou ser construtivo, baseando-se na crença que conhecendo a natureza dos números o professor da educação básica seja capaz de criar estratégias didáticas que possibilitem o melhor aprendizado por parte dos alunos e que não sejam contraditórias com os fundamentos e com a essência dos números.

Vale destacar que o nível de profundidade dado neste trabalho está aquém daquele que se pode encontrar facilmente na literatura disponível sobre o assunto. Esse nível de aprofundamento é proposital, tentou-se ir tão profundo quanto o suficiente para dar justificativas claras e corretas e ficar tão raso quanto o suficiente para tornar o texto de fácil leitura e compreensão. Os leitores interessados em aprofundar os estudos aqui indicados, assim como as citações sobre teorias da matemática superior feitas ao longo do texto, podem consultar (MILIES, 2013), (NETO, 2013), (VIEIRA, 2020) e (ÁVILA, 2006) que certamente encontrarão material suficiente para satisfazer grande parte dos seus interesses e dar suporte para buscar outras fontes avançadas.

Referências

FERREIRA, J. *A Construção dos Números*. 3. ed. Rio de Janeiro: Sociedade Brasileira de Matemática, 2013. xiv+133 p. (Textos Universitários). ISBN 978-85-85818-91-3.

GARCIA, A. *Elementos de Álgebra*. Rio de Janeiro: IMPA, 2018. (Projeto Euclides). ISBN 975-85-244-0450-4.

HALMOS, P. R. *Teoria ingênua dos conjuntos*. Rio de Janeiro: Ciência Moderna, 2001. (Clássicos da Matemática). ISBN 85-7393-141-8.

LIMA, E. L. *Curso de Análise*. Rio de Janeiro: IMPA, 2017. v. 1. (Projeto Euclides, v. 1). ISBN 978-85-85818-81-4.

MILIES, F. C. P. *Números: Uma Introdução à Matemática*. 3. ed. São Paulo: Editora da Universidade de São Paulo, 2013. ISBN 978-85-314-0458-0.

NERI, C. *Curso de Análise Real*. 1. ed. Rio de Janeiro: [s.n.]. ISBN 978-85-906720-0-5.

NETO, A. C. M. *Números Reais*. 2. ed. Rio de Janeiro: Sociedade Brasileira de Matemática, 2013. (Tópicos de Matemática Elementar). ISBN 978-85-85818-80-7.

NIVEN, I. *Números: Racionais e Irracionais*. Rio de Janeiro: Sociedade Brasileira de Matemática, 2012. (Coleção Iniciação Científica). ISBN 978-85-85818-68-5.

VIEIRA, F. *Elementos de Aritmética e Álgebra*. Rio de Janeiro: Sociedade Brasileira de Matemática, 2020. (Coleção do Professro de Matemática). ISBN 978-65-990395-5-3.

ÁVILA, G. *Análise Matemática para Licenciatura*. 3. ed. São Paulo: Blucher, 2006. ISBN 978-85-212-0395-7.

Apêndices

APÊNDICE A – Não existe número racional cujo quadrado seja um número primo

Este apêndice ocupa-se do trabalho de mostrar a importante afirmação utilizada no texto: um número primo não é quadrado de nenhum número racional.

Suponha por absurdo que exista um número racional que elevado ao quadrado tenha como resultado o número primo p. Existem então a e $b \neq 0 \in \mathbb{Z}$ com $mdc\,(a,b) = 1$, isto é, com a e b primos entre si tais que $p = \frac{a^2}{b^2}$. Mas $p = \frac{a^2}{b^2} \Leftrightarrow p \cdot b^2 = a^2$, em outras palavras a^2 é divisível por p que é um número primo, logo a também é divisível por p e podemos escrever $a = p \cdot n$. Substituindo $a = p \cdot n$ em $p \cdot b^2 = a^2$ obtemos $p \cdot b^2 = (p \cdot n)^2 \Rightarrow p \cdot b^2 = p^2 \cdot n^2 \Rightarrow b^2 = p \cdot n^2$. Da última igualdade concluímos que b^2 também é divisível por p que é um número primo e, portanto, b é divisível por p. Mas isso é uma contradiação, pois sendo a e b ambos divisíveis por p não teríamos $mdc\,(a,b) = 1$ e a e b foram tomados inicialmente primos entre si. Logo não existem a e $b \neq 0 \in \mathbb{Z}$ tais que $\left(\frac{a}{b}\right)^2 = p$, o que mostra que $\sqrt{p}$ é um número irracional.

APÊNDICE B – O Conjunto dos Números Primos é Infinito

Também foi utilizada no texto a afirmação: o conjunto dos números primos é infinito. Aqui é dada uma demonstração para esse fato.

Suponha por absurdo que existe um número finito de números primos $p_1, p_2, \cdots, p_r$ e considere o número natural $n = p_1 p_2 \cdots p_r + 1$. Pelo Teorema Fundamental da Aritmética, n possui um fato primo p que de deve ser um dois primos $p_1, p_2, \cdots, p_r$ e, consequentemente, divide o produto $p_1 p_2 \cdots p_r$. Mas isso implica que p divide 1, o que é absurdo. Logo o conjunto dos números primos é infinito.