UNIVERSIDADE DE SÃO PAULO
Instituto de Ciências Matemáticas e de Computação

Construção dos números reais via cortes de Dedekind

Thiago Trindade Pimentel

Dissertação de Mestrado do Programa de Mestrado Profissional em Matemática em Rede Nacional (PROFMAT)

ICMC USP
SÃO CARLOS

SERVIÇO DE PÓS-GRADUAÇÃO DO ICMC-USP

Data de Depósito:

Assinatura: ______________________

Thiago Trindade Pimentel

Construção dos números reais via cortes de Dedekind

Dissertação apresentada ao Instituto de Ciências Matemáticas e de Computação – ICMC-USP, como parte dos requisitos para obtenção do título de Mestre em Ciências – Mestrado Profissional em Matemática em Rede Nacional. *VERSÃO REVISADA*

Área de Concentração: Mestrado Profissional em Matemática em Rede Nacional

Orientadora: Profa. Dra. Márcia Cristina Anderson Braz Federson

USP – São Carlos
Outubro de 2018

Ficha catalográfica elaborada pela Biblioteca Prof. Achille Bassi
e Seção Técnica de Informática, ICMC/USP,
com os dados inseridos pelo(a) autor(a)

P644c

Pimentel, Thiago Trindade
Construção dos números reais via cortes de Dedekind / Thiago Trindade Pimentel; orientadora Márcia Cristina Anderson Braz Federson. -- São Carlos, 2018.
49 p.

Dissertação (Mestrado - Programa de Pós-Graduação em Mestrado Profissional em Matemática em Rede Nacional) -- Instituto de Ciências Matemáticas e de Computação, Universidade de São Paulo, 2018.

1. Conjuntos numéricos. 2. Cortes de Dedekind. 3. Classes de Equivalência. 4. Relação de ordem. 5. Propriedades aritméticas. I. Anderson Braz Federson, Márcia Cristina , orient. II. Título.

Bibliotecários responsáveis pela estrutura de catalogação da publicação de acordo com a AACR2:
Gláucia Maria Saia Cristianini - CRB - 8/4938
Juliana de Souza Moraes - CRB - 8/6176

Thiago Trindade Pimentel

Construction of the real numbers via Dedekind cuts

Master dissertation submitted to the Institute of Mathematics and Computer Sciences – ICMC-USP, in partial fulfillment of the requirements for the degree of Mathematics Professional Master's Program. *FINAL VERSION*

Concentration Area: Professional Master Degree Program in Mathematics in National Network

Advisor: Profa. Dra. Márcia Cristina Anderson Braz Federson

USP – São Carlos
October 2018

Este trabalho é dedicado às crianças adultas que,
quando pequenas, sonharam em se tornar cientistas.
Em especial, ao pesquisadores do Instituto de Ciências Matemáticas e de Computação (ICMC).

AGRADECIMENTOS

Primeiramente, gostaria de agradecer a Deus por guiar meu caminho até a cidade de São Carlos, onde está localizado o ICMC-USP, e por ter encontrado pesquisadores/professores brilhantes que me orientaram ao longo desses últimos anos. *Se enxerguei mais longe, foi porque estava apoiado sobre ombros de gigantes* escreveu Issac Newton certa vez. Essa frase resume bem o que senti aos longo dos 3 anos de estudo no mestrado. Gostaria de agradecer, em especial, à minha orientadora Márcia Cristina Federson, à coordenadora Ires Dias, ao professor Hermano de Souza Ribeiro, à minha mãe, à minha namorada, Fernanda Puti, à amiga e doutoranda Fernanda de Andrade Silva, aos professores das disciplinas, aos amigos que fiz no curso de mestrado e ao Bruno Glasses, pelas vídeo-aulas no Youtube.

Todas essas pessoas contribuíram para minha formação de professor. Minhas aulas, tanto no Ensino Fundamental como no Ensino Médio, melhoram muito graças ao esforço coletivo e dedicação de cada um. Fiz amigos de sala de aula no Profmat que muito me ajudaram, pois trocamos experiências de conhecimento e estudo. Essa equipe de estudo formada, onde nos encontrávamos em São Carlos, possibilitou uma agregação de conhecimento e vivência fundamentais, as quais levei nas classes que trabalhei. O ICMC-USP tornou-se um lugar privilegiado para mim, pois foi um espaço de estudo intensivo e imersão nos saberes para construir uma Matemática séria.

“As invenções são, sobretudo,
o resultado de um trabalho de teimoso.”
(Santos Dumont)

RESUMO

PIMENTEL, T. T. **Construção dos números reais via cortes de Dedekind**. 2018. 49 p. Dissertação (Mestrado em Ciências – Mestrado Profissional em Matemática em Rede Nacional) – Instituto de Ciências Matemáticas e de Computação, Universidade de São Paulo, São Carlos – SP, 2018.

O objetivo desta dissertação é apresentar a construção dos números reais a partir de cortes de Dedekind. Para isso, vamos estudar os números naturais, os números inteiros, os números racionais e as propriedades envolvidas. Então, a partir dos números racionais, iremos construir o corpo dos números reais e estabelecer suas propriedades.

Um corte de Dedekind, assim nomeado em homenagem ao matemático alemão Richard Dedekind, é uma partição dos números racionais em dois conjuntos não vazios A e B em que cada elemento de A é menor do que todos os elementos de B e A não contém um elemento máximo. Se B contiver um elemento mínimo, então o corte representará este elemento mínimo, que é um número racional. Se B não contiver um elemento mínimo, então o corte definirá um único número irracional, que "preenche o espaço" entre A e B. Desta forma, pode-se construir o conjunto dos números reais a partir dos racionais e estabelecer suas propriedades.

Esta dissertação proporcionará aos estudantes do Ensino Médio, interessados em Matemática, uma formação sólida em um de seus pilares, que é o conjunto dos números reais e suas operações algébricas e propriedades. Isso será muito importante para a formação destes alunos e sua atuação educacional.

Palavras-chave: Cortes de Dedekind; Números Reais; Conjuntos; Partição; Números Inteiros; Números Racionais; Números Naturais; Relação de Ordem; Relação de Equivalência.

ABSTRACT

PIMENTEL, T. T. **Construction of the real numbers via Dedekind cuts**. 2018. 49 p. Dissertação (Mestrado em Ciências – Mestrado Profissional em Matemática em Rede Nacional) – Instituto de Ciências Matemáticas e de Computação, Universidade de São Paulo, São Carlos – SP, 2018.

The purpose of this dissertation is to present the construction of the real numbers from Dedekind cuts. For this, we study the natural numbers, the integers, the rational numbers and some properties involved. Then, based on the rational numbers, we construct the field of the real numbers and establish their properties.

A Dedekind cut, named after the German mathematician Richard Dedekind, is a partition of the rational numbers into two non-empty sets A and B, such that each element of A is smaller than all elements of B and A does not contain a maximum element. If B contains a minimum element, then the cut represents this minimum element, which is a rational number. If B does not contain a minimal element, then the cut defines a single irrational number, which "fills the gap" between A and B. In this way, one can construct the set of real numbers from the rationals and establish their properties.

This dissertation provides students who like Mathematics a solid basis in one of the pillars of Mathematics, which is the set of real numbers and their algebraic operations and properties. This text will be very important for your educational background and performance.

Keywords: Cuts of Dedekind; Real Numbers; Sets; Partition; Integers; Rational Numbers; Natural Numbers; Order; Equivalence Relation.

SUMÁRIO

1 O CONJUNTO DOS NÚMEROS NATURAIS: MODELO DE CONTAGEM . . . 1
1.1 O conjunto $\mathbb{N}$ e os axiomas de Peano . . . 2
1.2 O Axioma de Indução . . . 4
1.3 Adição, Multiplicação e Ordem em $\mathbb{N}$ . . . 4
1.4 Relação de Ordem em $\mathbb{N}$ . . . 5
1.5 Demonstrações de propriedades de $\mathbb{N}$ . . . 7

2 CONSTRUÇÃO DOS NÚMEROS INTEIROS . . . 13
2.1 Por que criar os inteiros negativos? . . . 14
2.2 O conjunto $\mathbb{Z}$ . . . 15
2.3 Adição em $\mathbb{Z}$ . . . 16
2.4 Multiplicação em $\mathbb{Z}$ . . . 18
2.5 Relação de Ordem em $\mathbb{Z}$ . . . 21
2.6 Imersão de $\mathbb{N}$ em $\mathbb{Z}$ . . . 22

3 CONSTRUÇÃO DOS NÚMEROS RACIONAIS . . . 25
3.1 Adição em $\mathbb{Q}$ . . . 26
3.2 Multiplicação em $\mathbb{Q}$ . . . 28
3.3 Relação de Ordem em $\mathbb{Q}$ . . . 29
3.4 Imersão de $\mathbb{Z}$ em $\mathbb{Q}$ . . . 31

4 CONSTRUÇÃO DOS NÚMEROS REAIS . . . 33
4.1 Cortes de Dedekind . . . 33
4.2 O corpo dos números reais . . . 40
4.3 $\mathbb{Q}$ não é completo e $\mathbb{R}$ é completo . . . 41

A APÊNDICE . . . 45
A.1 Relações . . . 45
A.2 Relações de Equivalência e Partições . . . 47
A.3 Classes de Equivalência . . . 48

REFERÊNCIAS . . . 49

INTRODUÇÃO

Quando assisti, em 1997, às primeiras aulas de Matemática no Ensino Fundamental II na Escola SESI em Monte Alto - SP, cidade onde nasci em 1986, algo interessante me despertou para o assunto: números naturais. Nos anos de 1998 e 1999, nas sexta e sétima séries, correspondentes aos sétimos e oitavos anos escolares de hoje em dia, fui apresentado aos conjuntos dos números inteiros e racionais. Na época, queria saber mais sobre números. Mas, inicialmente, tive apenas a noção de *evolução* dos conjuntos numéricos. A percepção de concatenamento e expansão dos conjuntos estava primitiva, mas percebida. Essa expansão ficou, por muitos anos, na minha memória e, em 2015, quando ingressei no Mestrado Profissional em Matemática, tive a real motivação para compreender e interpretar melhor a extensão dos conjuntos numéricos.

Essa motivação fez-me escolher o tema: construção dos números reais usando cortes de Dedekind. O tema é interessante e, neste trabalho, evidenciamos um tipo de relação muito importante na Matemática moderna, que são as relações de equivalência. Demonstramos como as propriedades da associatividade e comutatividade da adição e multiplicação, entre outras, são importantes para trabalharmos corretamente com as operações fundamentais da Aritmética: adição, subtração, multiplicação e divisão. Usamos, muitas vezes, o Princípio de Indução para provar propriedades. Também usamos técnicas de demonstração como: demonstração direta, contrapositiva e por redução ao absurdo. Apresentar e utilizar essas técnicas na dissertação foi um trabalho fino e motivador, uma vez que a Matemática necessita de sustenção (provas) para dar a base à teoria.

Em sua essência, a Matemática trabalha com dois objetos principais: números e espaços. O primeiro é um ente abstrato, produto da mente humana, que modela e permite fazermos contagem e medição, possibilitando, assim, comparar diferentes quantidades de uma grandeza. O segundo objeto é um ente geométrico em que perfazem as figuras geométricas e relações entre dimensões.

O espaço nasce de noções primitivas como ponto, reta e plano. Sua estrutura é desenvolvida relacionando-se conceitos primitivos com postulados ou axiomas para dar base à teoria. Em [7], há uma descrição profunda desses conceitos.

Nesta dissertação, estudaremos o objeto números. Assim sendo, começaremos dedicando alguns comentários sobre os conjuntos numéricos, pois o objetivo final será construir o conjunto dos números reais a partir dos Cortes de Dedekind. Serão estudados [3], [9] e [10] para a construção dos Cortes.

Esta dissertação inicia-se com a construção do conjunto dos números naturais ($\mathbb{N}$) e os axiomas de Peano. Em seguida, demonstramos as propriedades principais de $\mathbb{N}$ pelo Princípio de Indução. O Capítulo 1 é o ponto de partida para o entendimento e interpretação dos capítulos posteriores, já que nele estão definidas as operações fundamentais, as propriedades e a relação de ordem em $\mathbb{N}$. No Capítulo 2, construímos o conjunto dos números inteiros ($\mathbb{Z}$) através de classes de equivalência. Fatos provados no Capítulo 1 são usados para dar continuidade às demonstrações das propriedades dos números inteiros. Apresentamos a adição, multiplicação e a relação de ordem em $\mathbb{Z}$, além da imersão de $\mathbb{N}$ em $\mathbb{Z}$.

No Capítulo 3, construimos os números racionais ($\mathbb{Q}$) e percebemos que sua construção é semelhante à construção dos inteiros. Descrevemos a adição e multiplicação em $\mathbb{Q}$ e suas propriedades principais como associatividade e comutatividade, além dos elementos neutro, oposto e inverso. A relação de ordem em $\mathbb{Q}$ e a imersão de $\mathbb{Z}$ em $\mathbb{Q}$ também foram mostradas.

No Capítulo 4, construímos o conjunto dos números reais a partir dos racionais. Usamos a proposta dada por Julius Wilhelm Richard Dedekind (1831 - 1916), ou seja, definimos a noção de corte de Dedekind, a adição e multiplicação nos reais, em seguida, mostramos que os reais possuem as propriedades aritméticas de $\mathbb{Q}$ e mais uma propriedade que $\mathbb{Q}$ não possui: a completude. A este conjunto de cortes, chamamos de conjunto de números reais o qual é comumente denotado por $\mathbb{R}$.

CAPÍTULO 1

O CONJUNTO DOS NÚMEROS NATURAIS: MODELO DE CONTAGEM

Uma das estradas pelas quais a Matemática caminha chama-se conjuntos, que são modelos para disciplinar o raciocínio lógico. A linguagem dos conjuntos é uma referência utilizada pela Matemática atual para expressar-se, pois essa linguagem é a mais simples das ideias matemáticas e, a partir dela, todos os outros conceitos podem ser expressos.

A adoção da linguagem e da notação de conjuntos em Matemática só se tornou uma prática universal a partir da terceira ou quarta década do século vinte. Esse uso, responsável pelos elevados graus de precisão, generalidade e clareza nos enunciados, raciocínios e definições, provocou uma grande revolução nos métodos, no alcance e na profundidade dos resultados matemáticos (veja [8]).

Evidentemente, para a Aritmética, os conjuntos numéricos, ou seja, aqueles formados por números são de suma importância. Entre os conjuntos numéricos, alguns são especiais pela sua grande utilização e, por isso, recebem nomes convencionais. Em particular, é fundamental compreender a noção de conjuntos numéricos, $\mathbb{N}$, $\mathbb{Z}$ e $\mathbb{Q}$, por exemplo, que serão evidenciados mais à frente, pois a construção dos números reais advém da sequência: conjuntos dos naturais ($\mathbb{N}$), dos inteiros ($\mathbb{Z}$) e dos racionais ($\mathbb{Q}$).

A vantagem de se utilizar a linguagem e a notação de conjuntos numéricos é que, nestes, existe uma álgebra montada sobre as operações, ou seja, existem conceitos e operações que advém da Aritmética como adição, subtração, multiplicação e divisão, que serão comprovadas para todos os números pertencentes a determinados conjuntos numéricos. A operação adição, por exemplo, funciona para todos os números pertencentes ao conjunto dos números naturais. As propriedades e regras operatórias da adição são extremamente fáceis de se manipular e representam um enorme ganho em simplicidade e exatidão. Assim, também, com respeito à multiplicação.

Para o presente capítulo, a referência principal é [8].

1.1 O conjunto $\mathbb{N}$ e os axiomas de Peano

Historicamente, o modelo de contagem inicial serviu para contar animais, pedras, mercadorias e objetos em geral. É nesse contexto de contar objetos em geral que o símbolo "0" ganhou destaque. O símbolo "0" e o nome zero estão relacionados à ideia de nenhum, não existente, nulo. Seu conceito foi pouco estudado ao longo dos séculos. Hoje, mal desperta alguma curiosidade, apesar de ser absolutamente instigante. "O ponto principal é o fato de o zero ser e não ser. Ao mesmo tempo indicar o nada e trazer embutido em si algum conteúdo", diz o astrônomo Walter Maciel, professor da Universidade de São Paulo. [...]

A cultura indiana antiga já trazia uma noção de vazio bem antes do conceito matemático de zero. "Num dicionário de sânscrito, você encontra uma explicação bastante detalhada sobre o termo indiano para o zero, que é "shúnya", afirma o físico Roberto de Andrade Martins, do Grupo de História e Teoria da Ciência da Universidade Estadual de Campinas (Unicamp). Como adjetivo, shúnya significa vazio, deserto, estéril. Aplica-se a uma pessoa solitária, sem amigos; a um indivíduo indiferente ou insensível. O termo descreve um sentimento de ausência, a falta de algo, uma ação sem resultados. Como substantivo, shúnya refere-se ao nada, ao vácuo, à inexistência. A partir do século VIII d.C, os árabes levaram para a Europa, junto com os outros algarismos, tanto o símbolo que os indianos haviam criado para o zero quanto a própria ideia de vazio, nulo, não existente. E difundiram o termo shúnya - que, em árabe, se tornou *shifr* e foi latinizado para *zephirum*, depois *zéfiro*, *zefro* e, por fim, zero [1].

Os babilônios, que viveram na mesopotâmia (onde hoje é o Iraque) por volta do ano 2500 a.C., foram os primeiros a chegar a uma noção de zero. Pioneiros na arte de calcular, criaram o que hoje se chama de "sistema de numeração posicional". Apesar do nome comprido, a ideia é simples. Nesse sistema, os algarismos têm valor pela posição (lugar) que ocupam. Trata-se do sistema que utilizamos atualmente. Veja o número 222 - o valor do 2 depende da posição em que ele se encontra: o primeiro vale 200, o segundo 20 e o terceiro 2. Outros povos antigos, como os egípcios, romanos e os gregos, não usavam esse sistema - continuavam a atribuir a cada número um sinal diferente ou um desenho qualquer para indicar os algarismos, fechando os olhos para a possibilidade matemática do zero [1].

Apesar de ser atraente, o zero não foi recebido de braços abertos na Europa, quando apareceu por lá, levado pelos árabes. "É surpreendente ver quanta resistência a noção de zero encontrou: o medo do novo e do desconhecido, superstições sobre o nada relacionadas ao diabo, uma relutância em pensar" diz o matemático americano Robert Kaplan, autor do livro *The nothing that is* (O nada que existe [...]) e orientador de um grupo de estudos sobre matemática na Universidade Harvard. O receio diante do zero vem desde a Idade Média. Os povos medievais o ignoravam solenemente. Os matemáticos da época achavam que popularizar o cálculo era o mesmo que jogar pérolas aos porcos. Seria uma revolução.

Com a divulgação do zero pelos árabes e do sistema de numeração posicional na Idade Média, as mudanças sociais e econômicas no século XV começaram a provocar, cada vez mais, a necessidade de organização numérica. Aperfeiçoar o instrumento de contagem era motivação necessária e suficiente para a continuação da evolução dos povos. Descrever, de forma concisa e precisa, o conjunto dos números naturais era fator essencial, que se tornou possível pela notável síntese feita pelo matemático italiano Giuseppe Peano (1858-1932) no início do século 20.

Ao longo desta dissertação, consideraremos $\mathbb{N}$ o conjunto cujos elementos são chamados números naturais, ou seja, $\mathbb{N} = \{0, 1, 2, 3, \ldots\}$. O fundamento da caracterização desse conjunto reside na palavra **sucessor**. Se 1 for o sucessor de 0, então não haverá nenhum número natural entre 0 e 1, ou seja, 1 virá logo depois de 0. Se 2 for o sucessor de 1, então não haverá nenhum número natural entre 1 e 2, ou seja, 2 virá logo depois de 1 e, assim, sucessivamente.

É preciso compreender que os números naturais são sequências de objetos abstratos, os quais, em princípio, são vazios de significado. Entretanto, uma vez ordenados, cada um dos quais ocupando uma posição definida nessa sequência, tais objetos passam a ter significado. Vale a pena observar que os números naturais são números ordinais, ou seja, indicam uma ordem, uma posição ou lugar ocupado na sequência: 0 é o primeiro, 1 é o segundo, 2 é o terceiro, etc.

Como dito inicialmente, conjunto é um conceito primitivo. Vale ressaltar que, neste capítulo, os conceitos primitivos principais são "número natural" e "sucessor".

Para podermos empregar um conceito primitivo adequadamente, necessitamos dispor de princípios ou regras que disciplinem sua utilização e estabeleçam suas propriedades. Tais princípios são chamados *axiomas* ou *postulados*.

Uma necessidade crucial para o que apresentaremos a seguir é ter o entendimento correto de axioma ou postulado, pois a construção dos números naturais inicia-se com os axiomas de Peano, que podem ser encontrados em [8], por exemplo. Os axiomas ou postulados de Peano são proposições não demonstradas e tudo que se sabe sobre números naturais pode ser demonstrado como consequência desses axiomas.

De acordo com [8], os axiomas de Peano podem ser enunciados como a seguir.

1. Existe uma função injetiva $h\colon \mathbb{N} \to \mathbb{N}$ e a imagem h(n) de um número natural $n \in \mathbb{N}$ dado chama-se sucessor de n.

   Noutras palavras, todo número natural tem um único sucessor. Logo, números naturais diferentes têm sucessores diferentes.

2. Existe um único número natural $0 \in \mathbb{N}$ tal que $0 \neq h(n)$ para todo $n \in \mathbb{N}$.

   Noutras palavras, existe um único número natural, chamado zero e representado pelo símbolo 0, que não é sucessor de nenhum outro número natural.

3. Seja X um conjunto de números naturais, isto é, $X \subset \mathbb{N}$. Se 0 pertencer a X e se, além disso, o sucessor de todo elemento de X ainda pertencer a X, então $X = \mathbb{N}$.

   O axioma 3 é conhecido como Princípio de Indução (ou recorrência).

1.2 O Axioma de Indução

O último dos axiomas de Peano é conhecido como *Axioma de Indução* ou *Princípio de Indução*. Ele é a base de um eficiente método de demonstração de proposições referentes a números naturais. Utilizaremos tal método diversas vezes nesse e nos capítulos subsequentes.

A seguir, apresentamos o Princípio de Indução na forma como vamos utilizá-lo.

Princípio de Indução. Seja $P(n)$ uma propriedade relativa a um número natural n dado arbitrário. Suponhamos que

(i) $P(0)$ seja válida;

(ii) (*Hipótese de Indução*). Para todo $n \in \mathbb{N}$, a validez de $P(n)$ implica na validez de $P(n+0)$, sendo que $h(n)$ é o sucessor de n. Então $P(n)$ será válida qualquer que seja o número natural n.

Observação 1.1. *Note que, se chamarmos de X o subconjunto dos números naturais n para os quais a propriedade $P(n)$ é válida, e se $0 \in X$ (em virtude de (i)) e se $n \in X$ implicar que $h(n) \in X$ (em virtude de (ii)), então, pelo Princípio de Indução, concluiremos que $X = \mathbb{N}$.*

1.3 Adição, Multiplicação e Ordem em $\mathbb{N}$

No conjunto $\mathbb{N}$ dos números naturais são definidas duas operações fundamentais: adição $(+)$ e multiplicação $(\cdot)$, a saber, a adição que, aos números n, $p \in \mathbb{N}$, faz corresponder a soma $(n+p)$, e a multiplicação que, aos números n e $p \in \mathbb{N}$, associa o produto $(n \cdot p)$ (veja [4]).

Nos próximos parágrafos, iremos definir adição, elemento neutro da adição, multiplicação e elemento neutro da multiplicação.

Definição 1.2. ***Adição:***

$$\begin{cases} n+0 = 0, \forall\, n \in \mathbb{N} \\ n+h(p) = h(n+p), \forall\, n,\ p \in \mathbb{N} \end{cases}$$

Note que desta definição segue o fato de $n+1$ ser o sucessor de n.

***Elemento Neutro da Adição**: Um elemento $x \in \mathbb{N}$ será dito elemento neutro da adição se para todo $n \in \mathbb{N}$ temos $n+x = n$. O elemento $0 \in \mathbb{N}$ é um elemento neutro da adição (por definição) e sua unicidade é verificada através da Lei do cancelamento da adição.*

Multiplicação:

$$\begin{cases} n \cdot 0 = 0, \forall\, n \in \mathbb{N} \\ n \cdot h(p) = (n \cdot p) + n, \forall\, n,\, p \in \mathbb{N} \end{cases}$$

Elemento Neutro da Multiplicação: *Um elemento $x \in \mathbb{N}$ será dito elemento neutro da multiplicação se para todo $n \in \mathbb{N}$ temos $1 \cdot n = n$. O elemento $1 \in \mathbb{N}$ é um elemento neutro da multiplicação (por definição), ou seja, $1 = h(n)$ e sua unicidade será verificada através da Lei do cancelamento da multiplicação.*

A seguir, iremos apresentar propriedades fundamentais para podermos fazer as operações de adição e multiplicação com clareza e exatidão. Essas propriedades são as bases para a compreensão da Aritmética dos Ensinos Fundamental e Médio nas escolas.

Sejam m, n e $p \in \mathbb{N}$ arbitrários. Valem as seguintes propriedades:

(H1) (***Associatividade da adição***): $(m+n)+p = m+(n+p)$;

(H2) (***Associatividade da multiplicação***): $m \cdot (n \cdot p) = (m \cdot n) \cdot p$;

(H3) (***Comutatividade da adição***): $m+n = n+m$;

(H4) (***Comutatividade da multiplicação***): $m \cdot n = n \cdot m$;

(H5) (***Distributividade***): $m \cdot (n+p) = m \cdot n + m \cdot p$;

(H6) (***Lei do cancelamento da adição***): $m+n = m+p \Longrightarrow n = p$;

(H7) (***Lei do cancelamento da multiplicação***): $m \cdot n = m \cdot p \Longrightarrow n = p$, *desde que* $m \neq 0$.

(H8) (***Lei do anulamento***): $m \cdot n = 0 \iff m = 0$ *ou* $n = 0$.

Mais à frente, provaremos cada uma destas propriedades. Agora, prosseguiremos apresentando uma relação de ordem em $\mathbb{N}$ e suas propriedades principais.

1.4 Relação de Ordem em $\mathbb{N}$

Iremos assumir conhecido o conceito de relação. O leitor pode consultar o Apêndice para obter mais detalhes.

Definição 1.3. *Uma relação $\mathscr{R}$ sobre um conjunto não vazio X será dita uma relação de ordem sobre X, se $\mathscr{R}$ for reflexiva, antissimétrica e transitiva (veja Apêndice). Se existir uma relação de ordem sobre o conjunto X, diremos que X é um conjunto parcialmente ordenado ou, simplesmente, um conjunto ordenado.*

Definição 1.4. *Dada uma relação de ordem $\mathscr{R}$ sobre um conjunto X, diremos que os elementos $x, y \in X$ são comparáveis mediante $\mathscr{R}$, se $x\mathscr{R}y$ ou $y\mathscr{R}x$. Se quaisquer dois elementos de X forem comparáveis mediante $\mathscr{R}$, então diremos que $\mathscr{R}$ é uma ordem total sobre X e, neste caso, diremos que X é um conjunto totalmente ordenado.*

Em uma relação de ordem $\mathscr{R}$, se $x\mathscr{R}y$, também usaremos a notação $x < y$ que leremos "x precede y na relação $\mathscr{R}$". Definiremos a relação de ordem $(<)$ mais adiante.

A seguir, apresentamos alguns exemplos de relações de ordem.

Exemplo 1.5.

(a) A relação $\mathscr{R}$ = {(a, a), (b, b), (c, c), (a, b), (a, c), (b, c)} é uma relação de ordem total sobre $X = \{a, b, c\}$.

(b) A relação de inclusão sobre uma família de subconjuntos de um dado conjunto é uma relação de ordem que, em geral, não é total.

Agora, iremos definir as noções de maior, menor, maior ou igual e menor ou igual e apresentaremos a compatibilidade da ordem com a adição e a multiplicação.

Definição 1.6. *Sejam $x, y \in \mathbb{N}$. Diremos que "x é menor do que y" e escreveremos $x < y$, se existir $t \neq 0$ tal que*

$$y = x + t.$$

Neste mesmo caso, poderemos dizer que "y é maior do que x" e escreveremos $y > x$.

A seguir, apresentaremos algumas propriedades da relação $(<)$ em $\mathbb{N}$. Sejam $m, n, p \in \mathbb{N}$. Então temos:

*(P1) (**Transitiva**): Se $m < n$ e $n < p$, então $m < p$;*

*(P2) (**Tricotomia**): Vale uma, e somente uma, das opções: $m = n$, $m < n$ ou $n < m$;*

*(P3) (**Monotonicidade**): Se $m < n$, então para qualquer $p \in \mathbb{N}$, $m + p < n + p$ e $m \cdot p < n \cdot p$;*

*(P4) (**Boa Ordenação**): Todo subconjunto não vazio $X \subset \mathbb{N}$ tem um menor elemento, ou seja, existe um elemento $k \in \mathbb{N}$ que é menor do que todos os demais elementos de X.*

Observação 1.7. *A propriedade $(P4)$ acima chama-se Princípio da Boa Ordenação. O Princípio da Boa Ordenação pode, muitas vezes, substituir, com vantagens, o Princípio de Indução como método de prova de resultados referentes a números naturais, pois a soma $(n + p)$ nada mais é do que n aplicado p vezes seguidas à operação de tomar seu sucessor, ou seja, n é o sucessor de $(n-1)$, $(n+1)$ é o sucessor de n, etc. Note que $(n \cdot p)$ é a soma de p parcelas iguais a n. Por exemplo, o número 6 é o mesmo que tomar o número 2 três vezes, sendo $6 = 2+2+2 = 3 \cdot 2 = 6$. Demonstraremos o Princípio da Boa Ordenação na próxima seção.*

Definição 1.8. *Sejam $x, y \in \mathbb{N}$. Se $x < y$ ou $x = y$, então escreveremos $x \leq y$ e leremos "x é menor ou igual a y". Analogamente, se $y > x$ ou $y = x$, então escreveremos $y \geq x$ e, neste caso, leremos "y é maior ou igual a x".*

Sejam $x, y, z \in \mathbb{N}$ arbitrários. Então valem as seguintes propriedades:

(O1) ***(Reflexiva)*** *$x \leq x$;*

(O2) ***(Antissimétrica)*** *$x \leq y \;\; e \;\; y \leq x \implies x = y$;*

(O3) ***(Transitiva)*** *$x \leq y \;\; e \;\; y \leq z \implies x \leq z$;*

(O4) ***($\leq$ é uma relação de ordem total)*** *$x \leq y$ ou $y \leq x$;*

(OA) ***(Compatibilidade da ordem com a adição)*** *$x \leq y \implies x + z \leq y + z$, ou seja, somando-se um mesmo número a ambos os membros de uma desigualdade, o sentido da desigualdade se mantém.*

(OM) ***(Compatibilidade da ordem com a multiplicação)*** *$x \leq y$ e $z \geq 0 \implies xz \leq yz$, ou seja, multiplicando-se ambos os membros de uma desigualdade por um mesmo número positivo, o sentido da desigualdade se mantém.*

Note que as propriedades válidas para $(<)$ são analogamente válidas para $(>)$, colocando-se o símbolo $>$ no lugar de $<$. Similarmente, as propriedades válidas para $(\leq)$ também valem para $(\geq)$, colocando-se o símbolo $\geq$ no lugar de $\leq$.

1.5 Demonstrações de propriedades de $\mathbb{N}$

Nesta seção, vamos demonstrar alguns fatos básicos sobre os números naturais, que aparecem com frequência em problemas, mas que, normalmente, não nos perguntamos como prová-los. A ideia é verificar como esses fatos resultam dos axiomas de Peano. Utilizaremos, principalmente, o Princípio de Indução nas demonstrações.

Teorema 1.9. *[**Associatividade da Adição**] Para quaisquer números naturais m, n, p, temos*

$$m + (n + p) = (m + n) + p.$$

Demonstração. Sejam $m, n \in \mathbb{N}$. Por indução, provaremos que, para todo $p \in \mathbb{N}$, vale

$$m + (n + p) = (m + n) + p.$$

Para $p = 1$, a igualdade $m + (n + 1) = (m + n) + 1$ é verdadeira pela definição de adição.

Suponhamos, agora, que a propriedade seja verdadeira para um certo $p \in \mathbb{N}$. Então temos

$$\begin{aligned} m+[n+(p+1)] &= m+[(n+p)+1] && (1.1)\\ &= [m+(n+p)]+1 && (1.2)\\ &= [(m+n)+p]+1 && (1.3)\\ &= (m+n)+(p+1), && (1.4) \end{aligned}$$

sendo que as igualdades (1.1) , (1.3) e (1.4) seguem da definição de adição e a igualdade (1.2) deve-se à hipótese de indução. Portanto, concluímos que

$$m+[n+(p+1)] = (m+n)+(p+1)$$

e a prova está completa. □

Teorema 1.10. *[**Comutatividade da Adição**] Para quaisquer números naturais m, $n \in \mathbb{N}$, temos*

$$m+n = n+m.$$

Demonstração. Seja $m \in \mathbb{N}$. Por indução, provaremos que $m+n = n+m$ para qualquer $n \in \mathbb{N}$.

Para $n = 1$, a igualdade $m+1 = 1+m$ será provada por indução em m. Quando $m = 1$, tem-se $1+1 = 1+1$, ou seja, $2 = 2$.

Suponhamos que a propriedade seja verdadeira para um certo $m \in \mathbb{N}$. Então $m+1 = 1+m$. Logo

$$(m+1)+1 = (1+m)+1 = 1+(m+1),$$

sendo que a primeira igualdade é verdadeira pela hipótese de indução e a segunda igualdade segue da associatividade provada no Teorema 1.10. Portanto $(m+1)+1 = 1+(m+1)$. Daí, segue do Princípio de Indução o fato de que $m+1 = 1+m$, para qualquer $m \in \mathbb{N}$.

Suponhamos, agora, que $m+n = n+m$ para algum $n \in \mathbb{N}$. Temos

$$\begin{aligned} m+(n+1) &= (m+n)+1 && (1.5)\\ &= (n+m)+1 && (1.6)\\ &= 1+(n+m) && (1.7)\\ &= (1+n)+m && (1.8)\\ &= (n+1)+m, && (1.9) \end{aligned}$$

sendo que a igualdade (1.5) segue da definição de adição, a igualdade (1.6) segue da hipótese de indução, as igualdades (1.7) e (1.9) seguem do parágrafo acima e (1.8) segue da associatividade da adição. □

Teorema 1.11. *[**Distributividade**] Para quaisquer m, n e $p \in \mathbb{N}$, temos*

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

Demonstração. Sejam m, $n \in \mathbb{N}$. Por indução, provaremos que a igualdade é verdadeira para todo $p \in \mathbb{N}$. Para $p = 1$, pela definição de multiplicação, a igualdade do enunciado é verdadeira.

Suponhamos, agora, que a igualdade seja verdadeira para um certo $p \in \mathbb{N}$, isto é,

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

Temos

$$\begin{aligned} m \cdot [n + (p+1)] &= m \cdot [(n+p)+1] && (1.10) \\ &= m \cdot (n+p) + m && (1.11) \\ &= (m \cdot n + m \cdot p) + m && (1.12) \\ &= m \cdot n + (m \cdot p + m) && (1.13) \\ &= m \cdot n + m \cdot (p+1), && (1.14) \end{aligned}$$

sendo que a igualdade (1.10) segue da definição de adição, (1.11) e (1.14) seguem da definição de multiplicação, (1.12) segue da hipótese de indução e (1.13) segue da associatividade da adição. □

Teorema 1.12. ***[Comutatividade da Multiplicação]*** *Para quaisquer m, $n \in \mathbb{N}$, temos*

$$m \cdot n = n \cdot m.$$

Demonstração. Seja $m \in \mathbb{N}$. Provaremos, por indução, que $m \cdot n = n \cdot m$ para qualquer $n \in \mathbb{N}$.

Para $n = 1$, usa-se o Princípio da Indução para provar que vale $m \cdot 1 = 1 \cdot m$ para qualquer $m \in \mathbb{N}$. Como $m \cdot 1 = m$, devemos mostrar que $1 \cdot m = m$.

Para $m = 1$, temos $1 \cdot 1 = 1$, pois 1 é elemento neutro da multiplicação. Seja $m \in \mathbb{N}$ dado arbitrário. Então $1 \cdot (m+1) = 1 \cdot m + 1 \cdot 1 = m + 1$, pois 1 é elemento neutro da multiplicação.

Suponhamos, agora, que a igualdade $m \cdot n = n \cdot m$ seja verdadeira e provaremos que isso implica em $m \cdot (n+1) = (n+1) \cdot m$. De fato. Basta notarmos que

$$\begin{aligned} m \cdot (n+1) &= m \cdot n + m && (1.15) \\ &= (n \cdot m) + m && (1.16) \\ &= (n+1) \cdot m, && (1.17) \end{aligned}$$

sendo que (1.15) segue da definição de multiplicação, (1.16) segue da hipótese de indução e (1.17) segue da distributividade e do parágrafo anterior. □

Teorema 1.13. ***[Lei do Cancelamento da Adição]*** *Se m, n, $p \in \mathbb{N}$, então*

$$m + p = n + p \quad \textit{implica que} \quad m = n.$$

Demonstração. Sabemos que

$$m+1=n+1 \implies m=n,$$

pois, pela definição de sucessor, números com o mesmo sucessor são iguais.

Consideremos a seguinte hipótese de indução:

$$m+p=n+p \quad \text{implica que} \quad m=n.$$

Pela propriedade associativa, sabemos que

$$m+(p+1)=n+(p+1) \text{ se, e somente se, } (m+p)+1=(n+p)+1.$$

Logo $m+p=n+p$, pois pela definição de sucessor, números com o mesmo sucessor são iguais. Finalmente, $m=n$ pela hipótese indutiva e segue a tese. □

Teorema 1.14. *[**Transitividade da Relação de Ordem**] Dados m, n, $p \in \mathbb{N}$, temos*

$$m<n \text{ e } n<p \quad \textit{implica que} \quad m<p.$$

Demonstração. A demonstração aqui é direta, pois as hipóteses $m<n$ e $n<p$ implicam que existem k, $l \in \mathbb{N}$ tais que $n=m+k$ e $p=n+l$. Logo $p=(m+k)+l=m+(k+l)>m$ e, então, $m<p$ e a prova está completa. □

Teorema 1.15. *[**Tricotomia**] Dados m, n e $p \in \mathbb{N}$, vale uma, e somente uma, das condições seguintes:*

(i) $m=n$

(ii) $m<n$

(iii) $n<m$

Demonstração. Precisamos provar que dois números naturais m e n são sempre comparáveis, isto é, ou $m=n$ ou $m<n$ ou $n<m$.

Primeiramente, note que 0 é comparável com todo número natural, pois todo número natural $n \neq 0$ é sucessor de outro natural e, portanto, é da forma $n=k+1$ para algum $k \in \mathbb{N}$. Assim, $n>1>0$. Logo $n>0$, pois para a relação $(>)$ vale a transitividade.

Seja $A \subset \mathbb{N}$ o conjunto dos números naturais comparáveis com m. Provaremos que $A=\mathbb{N}$.

Pelo segundo parágrafo, $0 \in A$. Mostraremos que se $k \in A$, então $k+1 \in A$. De fato, sendo $k \in A$, então ou $m=k$ ou $m<k$ ou $k<m$. Suponhamos que $m=k$. Então $m<k+1$. Logo $k+1 \in A$.

Suponhamos, agora, que $k < m$. Então $m = k + t$, para algum $t \in \mathbb{N}$. Consideremos dois casos.

Caso 1. Se $t = 1$, então $m = k + 1$. Logo $k + 1$ é comparável com m, isto é, $k + 1 \in A$.

Caso 2. Se $t \neq 1$ e $t > 0$, pois $k < m$, então $t > 1$ e, portanto, $m = k + t > k + 1$. Logo $k + 1$ é comparável com m, isto é, $k + 1 \in A$, e a prova está completa. □

Teorema 1.16. *[**Monotonicidade**] Sejam m, n $\in \mathbb{N}$. Se m $<$ n, então valem*

$$\mathrm{m} + \mathrm{p} < \mathrm{n} + \mathrm{p} \quad e \quad \mathrm{m} \cdot \mathrm{p} < \mathrm{n} \cdot \mathrm{p},$$

para todo p $\neq 0$.

Demonstração. Por hipótese, $m < n$. Então $n = m + k$ para algum $k \in \mathbb{N}$. Logo,

$$n + p = (m + p) + k, \text{ ou seja, } m + p < n + p.$$

Em relação à multiplicação, se $m < n$, então $n = m + k$ para algum $k \in \mathbb{N}$. Assim,

$$n \cdot p = (m + k) \cdot p = m \cdot p + k \cdot p,$$

ou seja, $m \cdot p < n \cdot p$ e a prova está completa. □

Teorema 1.17. *[**Lei do Cancelamento para Desigualdades**] Se m, n e p $\neq 0$ forem tais que*

$$\mathrm{m} + \mathrm{p} < \mathrm{n} + \mathrm{p} \quad ou \quad \mathrm{m} \cdot \mathrm{p} < \mathrm{n} \cdot \mathrm{p},$$

então m $<$ n.

Demonstração. Se $m + p < n + p$, então existe $k \in \mathbb{N}$ tal que

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

Daí, pela Lei do Cancelamento da Adição (Teorema 1.13), $n = k + m$. Mas isso significa que

$$m < n.$$

Agora, se $m \cdot p < n \cdot p$, então existirá $k \cdot p \in \mathbb{N}$ tal que

$$n \cdot p = k \cdot p + m \cdot p = (k + m) \cdot p.$$

Daí, pela Lei do Cancelamento da Multiplicação (H7), $n = k + m$. Mas isso significa que

$$m < n$$

e a prova está completa. □

O leitor pode consultar o Apêndice para achar a definição de conjunto ordenado. Agora, iremos apresentar uma proposição que diz que um certo conjunto ordenado $A \subset \mathbb{N}$ admite um menor elemento que será denotado por $\min A$.

Definição 1.18. *Dado um conjunto ordenado $A \subset \mathbb{N}$, com a relação de ordem total $(\leq)$, diremos que $a \in A$ é um menor elemento de A, se tivermos $a \leq x$ para todo $x \in A$.*

A demonstração do próximo resultado é análoga à demonstração da Proposição 1.18.

Proposição 1.19. *Se $A \subset \mathbb{N}$ for um conjunto ordenado que admite um menor elemento, então este menor elemento será único e será chamado de elemento mínimo de A e denotado por* $\min A$.

Demonstração. Sejam a_1 e a_2 menores elementos de A. Como a_1 é um menor elemento de A, $a_1 \in A$ e $a_1 \leq x$, para todo $x \in A$. Logo $a_1 \leq a_2$, já que $a_2 \in A$, pois é menor elemento de A. Analogamente, $a_2 \leq a_1$. Pela antissimetria (propriedade (O2)), $a_1 = a_2$, como queríamos. □

De modo análogo ao que foi feito na proposição anterior, $\max A$ *denota o maior elemento ou elemento máximo de um conjunto ordenado.*

Definição 1.20. *Dado um conjunto ordenado $A \subset \mathbb{N}$, com a relação de ordem total $(\leq)$, diremos que $a \in A$ é um maior elemento de A, se tivermos $x \leq a$ para todo $x \in A$.*

Proposição 1.21. *Se $A \subset \mathbb{N}$ for um conjunto ordenado que admite um maior elemento, então este maior elemento será único e será chamado de elemento máximo de A e denotado por* $\max A$, *ou seja,* $\max A$ *é o maior elemento que A pode ter.*

O próximo teorema aborda um conceito intuitivamente claro desde o Ensino Fundamental: todo subconjunto não vazio de números naturais possui um menor elemento.

Teorema 1.22. ***[Princípio da Boa Ordenação]*** *Todo subconjunto não vazio de $\mathbb{N}$ tem um menor elemento.*

Demonstração. Seja $S \subset \mathbb{N}$, $S \neq \emptyset$, e consideremos o conjunto

$$M = \{n \in \mathbb{N} : n \leq x, \text{para todo } x \in S\}.$$

Como S é não vazio, tomemos $s \in S$. Então $s+1 \notin M$, pois $s+1$ não é menor ou igual a s. Assim, $M \subsetneq \mathbb{N}$. Como $0 \in M$ e $M \subsetneq \mathbb{N}$, deve existir $k \in M$ tal que $k+1 \notin M$, pois, caso contrário, pelo Princípio de Indução, teríamos $M = \mathbb{N}$.

Afirmamos que este k é o menor elemento de S, isto é, $k = \min S$. De fato. Como $k \in M$, então $k \leq x$, para todo $x \in S$.

Falta mostrarmos que $k \in S$. Suponhamos, por absurdo, que $k \notin S$. Então $k < x$, para todo $x \in S$. Pelo Teorema 1.17, $k+1 \leq x$, para todo $x \in S$, o que significa que $k+1 \in M$, contradizendo a escolha de k. Logo $k \in S$, como queríamos. □

CAPÍTULO

2

CONSTRUÇÃO DOS NÚMEROS INTEIROS

Alguns historiadores utilizam o símbolo $\mathbb{Z}$ para representar o conjunto dos números inteiros, associando-o à primeira letra da palavra zahlen que, em português, significa números. Outros associam o símbolo $\mathbb{Z}$ à primeira letra do sobrenome do matemático alemão Ernst Zermelo (1871-1953), que se dedicou ao estudo dos conjuntos numéricos. Curiosidades deixadas à parte, iremos definir um número inteiro como uma classe de equivalência e o conjunto dos números inteiros como o conjunto dessas classes de equivalência.

O matemático alemão Richard Dedekind (1831-1916) também estabeleceu uma relação de equivalência para definir os número inteiros, mas entre pares ordenados de números naturais. Para Dedekind, os pares (a,b) e (c,d) de números naturais seriam equivalentes, se $a-b=c-d$ implicasse $a + d = b + c$. Ele também observou que a subtração é a operação inversa da adição. Assim, foi possível escrever todos os números sem mencionar qualquer subtração (veja [2]). A contribuição exemplar de Dedekind foi que ele demonstrou que esta relação é, de fato, uma relação de equivalência (veja o Apêndice). Ele também formalizou o fato de que o conjunto destas classes de equivalência é o conjunto dos números inteiros.

A dificuldade, solucionada por outro matemático alemão, chamado Georg Ferdinand Ludwing Phillip Cantor (1845-1918), e que, por muitos séculos, ficou obscura na Matemática, era conseguir estender o conjuntos dos números naturais, $\mathbb{N}$. Precisou-se identificar e nomear, através de classes de equivalências, os números inteiros negativos, por pares ordenados, a partir dos naturais.

R. Freiward, em [2], mencionou que os inteiros negativos e o zero foram desenvolvidos depois dos números naturais, apesar de muitas civilizações terem a noção intuitiva de valor negativo, como, por exemplo, temperaturas muito frias e profundidade marítima. A dificuldade em aceitá-los era enorme e a prerrogativa era que não fazia sentido haver algo menor do que nada (zero). Com esse pensamento dogmático, não era familiar lidar com tais números. Na Europa, somente no século XVII, os números inteiros negativos foram aceitos. Uma vez feito *isso, o terreno dos números inteiros estava sedimentado.*

2.1 Por que criar os inteiros negativos?

Conforme dissemos no capítulo anterior, uma das formas de expressão na Matemática é através de conjuntos. Denotaremos por $\mathbb{Z}$ o conjunto em que cada elemento chama-se inteiro. Uma pergunta interessante que podemos fazer é "qual a motivação para estender um conjunto dos números naturais, ou melhor, por que criar um novo conjunto de números?

No desenvolvimento da Aritmética, uma simples equação, como a seguinte, demanda solução:

$$x+3=2.$$

Em $\mathbb{N}$, conseguimos resolver $x+2=3$, ou seja, há solução para este tipo de equação, mas não há para a equação $x+3=2$. Assim, surgiu um problema que, embora parecesse simples, não tinha uma solução satisfatória.

Curiosamente, as pessoas achavam mais satisfatório esteticamente inventar novos números para que a equação

$$x+m=n \quad (m,n\in\mathbb{N}), \tag{2.1}$$

fosse solucionada, ou seja, pensou-se primeiramente na disposição visual do conjunto $\mathbb{Z}$, para depois caracterizá-lo. Em $\mathbb{N}$, por exemplo, a equação (2.1) terá solução se, e somente se, tivermos $m\leqslant n$. Era, então, necessário ampliar o conjunto dos naturais, construindo um conjunto para que a equação (2.1) sempre tivesse solução única, mesmo quando não ocorresse $m\leqslant n$ (veja [6]). Assim, essa percepção estética teve força valiosa e ajudou a motivar o desenvolvimento algébrico dos inteiros negativos.

Definir o conjunto $\mathbb{Z}$ com algo que já se tinha em mãos era a semente da ideia que se precisava, pois não havia a fundamentação sólida do conjunto $\mathbb{Z}$. Logo não se poderia denotar, de imediato, -1, -2, -3, etc (veja [2]). Os estudiosos queriam construir um conjunto maior que tivesse a resposta do que seria $2-3$ e, mais geralmente, que houvesse uma solução para todos os problemas de "subtração", quando alguém trabalhasse com números inteiros, independentemente de que equações do tipo (2.1) fossem resolvidas. Quanto à isso, houve algo interessante quando se iniciou a elaboração matemática rigorosa dos inteiros negativos no século XIX. Para simplificar os passos, os estudiosos de Matemática poderiam ter declarado que os novos números seriam -1, -2, -3, etc. Este era o comportamento que os estudiosos queriam quando estudavam. Mas, ao invés de apenas anunciar "nós declaramos que os tais números são ...", o objetivo era mostrar como definir esses números usando o que já se tinha.

A genialidade para estender o conjunto dos naturais, $\mathbb{N}$, veio do fato de se considerar sentenças do tipo $2-3$, $4-5$ e $10-11$, por exemplo, como pares ordenados $(2,3)$, $(4,5)$ e $(10,11)$ respectivamente. Em outras palavras, esses pares ordenados diferentes devem ser *considerados como sendo o mesmo número inteiro. Representar o conjunto $\mathbb{Z}$ através de uma propriedade característica (pares ordenados) de seus elementos foi a contribuição que faltava. Portanto, seguindo essa ideia intuitiva, a construção formal dos números inteiros surgiu da necessidade de se ampliar o conjunto dos naturais para definir a diferença entre dois números naturais m e n, mesmo para o caso em que $m > n$ (veja [6]).*

2.2 O conjunto $\mathbb{Z}$

Podemos observar, por exemplo, que expressões do tipo $5-2$, $7-4$, $3-0$, $15-12$, representam, todas, o número 3. Assim, é interessante ter uma unicidade de representação, pois a igualdade $5-2=7-4$ em $\mathbb{N}$ é equivalente a $5+4=7+2$. Isso nos ajuda entender a construção que faremos a seguir.

Definição 2.1. *Sejam $(a,b),(c,d) \in \mathbb{N}\times\mathbb{N}$. Escreveremos*

$$(a,b) \simeq (c,d) \quad \textit{sempre que} \quad a+d=b+c.$$

Proposição 2.2. *A relação $(\simeq)$ é uma relação de equivalência sobre $\mathbb{N}\times\mathbb{N}$.*

Demonstração. O leitor pode querer consultar o Apêndice para relembrar a noção de relação. De fato, abaixo mostraremos que realmente $(\simeq)$ é uma relação de equivalêcia, pois as seguintes propriedades estão satisfeitas:

- $(\simeq)$ é reflexiva, pois para cada $(a,b) \in \mathbb{N}\times\mathbb{N}$, temos $a+b=b+a$, ou seja, $(a,b)\simeq(a,b)$.
- $(\simeq)$ é simétrica, pois para cada (a,b) e $(c,d) \in \mathbb{N}\times\mathbb{N}$, com $(a,b)\simeq(c,d)$, temos $a+d=b+c$, o que implica que $c+b=d+a$, ou seja, $(c,d)\simeq(a,b)$.
- $(\simeq)$ é transitiva, pois para $(a,b),(c,d)$ e $(e,f) \in \mathbb{N}\times\mathbb{N}$, com $(a,b)\simeq(c,d)$ e $(c,d)\simeq(e,f)$, temos $a+d=b+c$ e $c+f=d+e$. Somando f em ambos os lados da primeira igualdade e b em ambos os lados da segunda igualdade, por transitividade, obtemos $a+d+f=e+d+b$ e, portanto, $a+f=b+e$, ou seja, $(a,b)\simeq(e,f)$.

  Isso termina a prova. □

É fácil ver que a relação de equivalência $(\simeq)$, definida acima, determina uma partição (veja o Apêndice) de $\mathbb{N}\times\mathbb{N}$ em classes de equivalências. Para cada $(a,b)\in\mathbb{N}\times\mathbb{N}$, seja $[(a,b)]$ a classe de equivalência determinada por $(a,b)\in\mathbb{N}\times\mathbb{N}$, segundo a relação de equivalência $(\simeq)$, ou seja,

$$[(a,b)] = \{(x,y)\in\mathbb{N}\times\mathbb{N};\ (x,y)\simeq(a,b)\} = \{(x,y)\in\mathbb{N}\times\mathbb{N};\ x+b=y+a\}.$$

Definição 2.3. *O conjunto quociente de $\mathbb{N}\times\mathbb{N}$ pela relação ($\simeq$), ou seja, o conjunto de todas as classes de equivalência $[(a,b)]$, com $(a,b)\in\mathbb{N}\times\mathbb{N}$, será indicado por $\mathbb{Z}$. Assim*

$$\mathbb{Z} = (\mathbb{N}\times\mathbb{N})/\simeq = \{[(a,b)];\ (a,b)\in\mathbb{N}\times\mathbb{N}\}.$$

Exemplo 2.4. *Abaixo estão ilustradas algumas classes de equivalências segundo ($\simeq$).*

(a) $4 = [(6,2)] = \{(6,2),(4,0),(7,3),...\}$,

(b) $-6 = [(3,9)] = \{(3,9),(0,6),(4,10),...\}$,

(c) $1 = [(1,0)] = \{(1,0),(2,1),(3,2),(4,3),...,(n+1,n),...\}$,

(d) $-1 = [(0,1)] = \{(0,1),(1,2),(2,3),(3,4),...,(n,n+1),...\}$,

(f) $n = [(n,0)] = \{(n,0),(n+1,1),(n+2,2),(n+3,3),...,(n+m,m),...\}$,

(g) $-n = [(0,n)] = \{(0,n),(1,n+1),(2,n+2),(3,n+3),...,(m,n+m),...\}$.

2.3 Adição em $\mathbb{Z}$

Começamos esta seção definindo a adição de dois números inteiros m e n através do uso de classes de equivalências.

Definição 2.5. *Sejam $m,n\in\mathbb{Z}$ tais que $m = [(a,b)]$ e $n = [(c,d)]$. Definimos a **adição** de m com n, e indicamos por m + n, como sendo o elemento de $\mathbb{Z}$ tal que*

$$m+n = [(a+c,b+d)].$$

Vale observar que a definição da adição em $\mathbb{Z}$ não depende da escolha dos representantes de cada classe de equivalência. Mostraremos esse fato mais à frente.

A seguir, vamos provar algumas propriedades da adição em $\mathbb{Z}$. Mas, antes, daremos um exemplo de adição de dois números.

Exemplo 2.6. *Para os números naturais $7 = [(8,1)]$ e $3 = [(4,1)]$, temos*

$$7+3 = [(8+4,1+1)] = [(12,2)].$$

Teorema 2.7. ***[Associatividade da Adição]*** *Para quaisquer números inteiros m, n, p, tem-se*

$$(m+n)+p = m+(n+p).$$

Demonstração. Sejam $m = [(a,b)]$, $n = [(c,d)]$ e $p = [(e,f)]$ elementos de $\mathbb{Z}$. Pela associatividade da adição de números naturais (Teorema 1.9), obtemos

$$\begin{aligned}
(m+n)+p &= ([(a,b)]+[(c,d)])+[(e,f)] = [(a+c,b+d)]+[(e,f)] \\
&= [((a+c)+e,(b+d)+f)] = [(a+(c+e),b+(d+f))] \\
&= [(a,b)]+[(c+e,d+f)] = [(a,b)]+([(c,d)]+[(e,f)]) \\
&= m+(n+p),
\end{aligned}$$

o que mostra o teorema. □

Teorema 2.8. ***[Comutatividade da Adição]*** *Para quaisquer números inteiros m, n, p, tem-se*

$$m+n = n+m.$$

Demonstração. Sejam $m = [(a,b)]$ e $n = [(c,d)]$ elementos de $\mathbb{Z}$. Então, usando a comutatividade da adição de números naturais (Teorema 1.10), obtemos

$$\begin{aligned}
m+n &= ([(a,b)]+[(c,d)]) = [(a+c,b+d)] \\
&= [(c+a,d+b)] = ([(c,d)]+[(a,b)]) \\
&= n+m,
\end{aligned}$$

o que mostra o teorema. □

Teorema 2.9. ***[Elemento Neutro]*** *Existe* $0 = [(0,0)] = \{(m,m) \in \mathbb{N}\times\mathbb{N}\}$ *tal que, para todo* $m \in \mathbb{Z}$*, tem-se*

$$m+0 = m.$$

Demonstração. Para todo $m = [(a,b)] \in \mathbb{Z}$, queremos mostrar que existe $0 \in \mathbb{Z}$ tal que $m+0 = m$.

Seja $0 = [(a',b')] \in \mathbb{Z}$ satisfazendo esta igualdade. Então,

$$\begin{aligned}
m+0 &= [(a,b)]+[(a',b')] \\
&= [(a+a',b+b')] \\
&= [(a,b)] \\
&= m,
\end{aligned}$$

se, e somente se, $(a+a',b+b') \simeq (a,b)$, ou seja, $(a+a')+b = (b+b')+a$ em $\mathbb{N}$. Usando a Lei do Cancelamento da adição de números naturais (Teorema 1.13), obtemos $a' = b'$. Assim, existe

$$0 = [(a',a')] = [(0,0)] \in \mathbb{Z},$$

e a demonstração está completa. □

Teorema 2.10. ***[Elemento Oposto]*** *Para cada* $m \in \mathbb{Z}$*, existe um único elemento* $m' \in \mathbb{Z}$ *tal que*

$$m+m' = 0.$$

Demonstração. Dado $m = [(a,b)] \in \mathbb{Z}$, seja $m' = [(a',b')] \in \mathbb{Z}$ tal que $m + m' = 0$. Então,

$$\begin{aligned} m + m' &= [(a+a', b+b')] \\ &= [(0,0)], \end{aligned}$$

o que implica que $a + a' = b + b'$ em $\mathbb{N}$. Porém a igualdade $a + a' = b + b'$ é equivalente a $m' = (b,a)$, o que prova o teorema. □

Teorema 2.11. *[**Lei do Cancelamento**] Sejam m, $p \in \mathbb{N}$. Se $m + p = n + p$, então*

$$m = n.$$

Demonstração. Se $m + p = n + p$, seja $p' \in \mathbb{Z}$ o elemento oposto de p. Assim, usando as propriedades dos números naturais dos Teoremas 1.17 e 1.11, obtemos

$$\begin{aligned} m &= m + 0 = m + p + p' \\ &= (m+p) + p' = (n+p) + p' \\ &= n + (p + p') = n + 0 \\ &= n, \end{aligned}$$

o que mostra o teorema. □

Observação 2.12. *Escreveremos $m - n$ para denotar o elemento $m + (-n)$ em $\mathbb{Z}$ e, com isso, teremos a operação de subtração em $\mathbb{Z}$, dada por*

$$\begin{array}{ccc} \mathbb{Z} \times \mathbb{Z} & \to & \mathbb{Z} \\ (m,n) & \mapsto & m - n. \end{array}$$

2.4 Multiplicação em $\mathbb{Z}$

A seguir, definiremos a multiplicação de dois numeros inteiros m e n através de classes de equivalências.

Definição 2.13. *Para $m = [(a,b)]$ e $n = [(c,d)]$ em $\mathbb{Z}$, definimos a **multiplicação** de m por n, e indicamos por $m \cdot n$ ou, simplesmente, mn, o elemento de $\mathbb{Z}$ dado por*

$$mn = [(ac + bd, ad + bc)].$$

Agora, vamos provar algumas propriedades da multiplicação em $\mathbb{Z}$. Porém, antes, daremos um exemplo de multiplicação de dois números inteiros.

Exemplo 2.14. *Para os números naturais $7 = [(8,1)]$ e $3 = [(4,1)]$, temos*

$$7 \cdot 3 = [(32 + 1, 8 + 4)] = [(33, 12)] = 21.$$

Portanto $7 \cdot 3 = 21$.

Teorema 2.15. *[**Associatividade da Multiplicação**] Para quaisquer números inteiros m, n, p, tem-se*

$$(mn)p = m(np).$$

Demonstração. Sejam $m = [(a,b)]$, $n = [(c,d)]$ e $p = [(e,f)]$ elementos de $\mathbb{Z}$. Então, usando a associatividade da multiplicação de números naturais (propriedade (H2), página 4), obtemos

$$\begin{aligned}(mn)p &= ([(a,b)]\cdot[(c,d)])\cdot[(e,f)] = [(ac,bd)]\cdot[(e,f)]\\ &= [((ac)\cdot e,(bd)\cdot f)] = [(a\cdot(ce),b\cdot(df))]\\ &= [(a,b)]\cdot[(ce,df)] = [(a,b)]\cdot([(c,d)]\cdot[(e,f)])\\ &= m(np),\end{aligned}$$

o que mostra o teorema. □

Teorema 2.16. *[**Comutatividade da Multiplicação**] Para quaisquer números inteiros m, n, p, tem-se*

$$mn = nm.$$

Demonstração. Sejam $m = [(a,b)]$ e $n = [(c,d)]$ elementos de $\mathbb{Z}$. Então, usando a comutatividade da multiplicação de números naturais (Teorema 1.12), obtemos

$$\begin{aligned}mn &= ([(a,b)]\cdot[(c,d)]) = [(ac,bd)]\\ &= [(ca,db)] = ([(c,d)]\cdot[(a,b)])\\ &= nm,\end{aligned}$$

o que mostra o teorema. □

Teorema 2.17. *[**Elemento Neutro**] Existe $1 = [(1,0)] \in \mathbb{Z}$ tal que, para todo $m \in \mathbb{Z}$, tem-se*

$$1m = m.$$

Demonstração. Para todo $m = [(a,b)] \in \mathbb{Z}$, queremos encontrar $m' = [(a',b')] \in \mathbb{Z}$, tal que $m'm = m$. Se existir tal elemento m', então teremos

$$\begin{aligned}m &= [(a,b)] = mm'\\ &= [(a,b)]\cdot[(a',b')] = [(aa'+bb',ab'+ba')]\\ &= [(a,b)] = m,\end{aligned}$$

ou seja, $(a,b) \simeq (aa'+bb',ab'+ba')$, o que é equivalente a $a+(ab'+ba') = b+(aa'+bb')$ em $\mathbb{N}$, para quaisquer a e $b \in \mathbb{N}$. Em particular, tomando $a = 0$ e $b \neq 0$, temos $ba' = b(1+b')$, ou seja, $a' = 1+b'$ em $\mathbb{N}$, para todo $b \in \mathbb{N}$. E, mais ainda, substituindo $a' = 1+b'$ na equação $mm' = m$, obtemos $a+ab'+b(1+b') = b+a(1+b')+bb'$ em $\mathbb{N}$, isto é, $[(a,b)] = [(a,b)]$. Assim,

$$m' = [(a',b')] = [(1+b',b')] = [(1,0)]+[(b',b')] = [(1,0)].$$

Para $b = 0$ e $a \neq 0$ o resultado segue análogo como acima. Portanto m' é o único elemento de $\mathbb{Z}$ satisfazendo esta igualdade, o qual denotaremos por $1 = [(1,0)]$. □

Teorema 2.18. *[**Distributividade**] Para quaisquer m, n e $p \in \mathbb{N}$, tem-se*

$$m(n+p) = mn + mp.$$

Demonstração. Sejam $m = [(a,b)]$, $n = [(c,d)]$ e $p = [(e,f)]$ elementos de $\mathbb{Z}$. Então, usando a distributividade da multiplicação de números naturais (Teorema 1.11), obtemos

$$\begin{aligned} m(n+p) &= [(a,b)] \cdot ([(c,d)] + [(e,f)]) \\ &= [(a,b)] \cdot [(c,d)] + [(a,b)] \cdot [(e,f)] \\ &= mn + mp, \end{aligned}$$

o que mostra o teorema. □

Teorema 2.19. *[**Lei do Anulamento**] Se m e $n \in \mathbb{Z}$ forem tais que $m \cdot n = 0$, então teremos*

$$m = 0 \quad ou \quad n = 0.$$

Demonstração. Cada número $m \in \mathbb{Z}$ pode ser tomado da forma $m = [(a,0)]$ ou $m = [(0,a)]$, com a $\in \mathbb{N}$. Então, para mostrarmos a Lei do Anulamento em $\mathbb{Z}$, consideremos m e $n \in \mathbb{Z}$ tais que $m \cdot n = 0$, e separemos em quatro casos:

1) $m = [(a,0)]$ e $n = [(b,0)]$, com m e $n \in \mathbb{N}$.

2) $m = [(a,0)]$ e $n = [(0,b)]$, com m e $n \in \mathbb{N}$.

3) $m = [(0,a)]$ e $n = [(b,0)]$, com m e $n \in \mathbb{N}$.

4) $m = [(0,a)]$ e $n = [(0,b)]$, com m e $n \in \mathbb{N}$.

O que pode-se perceber é que, nos quatro casos acima, recaímos na igualdade $a \cdot b$ em $\mathbb{N}$ e, pela propriedade $(H8)$, obtemos $a = 0$ ou $b = 0$, o que implica que $m = 0$ ou $n = 0$ em $\mathbb{Z}$. □

A seguir, iremos separar o conjunto dos números inteiros em dois subconjuntos chamados inteiros não positivos e inteiros não negativos.

Definição 2.20. *O conjunto $\mathbb{Z}$, com as operações de adição e multiplicação introduzidas anteriormente, é dito ser o **conjunto dos números inteiros** e seus elementos são chamados **números inteiros**. Podemos, ainda, separar este conjunto em dois subconjuntos, a saber*

$$\mathbb{Z}_+ = \{[(a,0)] \in \mathbb{Z} : a \in \mathbb{N}\} \qquad e \qquad \mathbb{Z}_- = \{[(0,a)] \in \mathbb{Z} : a \in \mathbb{N}\}.$$

*Os elementos de $\mathbb{Z}_+$ são chamados **inteiros não negativos** e os elementos de $\mathbb{Z}_-$ são chamados **inteiros não positivos**. Note que, para todo $m \in \mathbb{Z}$, teremos $m \in \mathbb{Z}_+$ se, e somente se, $-m \in \mathbb{Z}_-$.*

2.5 Relação de Ordem em $\mathbb{Z}$

Uma relação de ordem em $\mathbb{Z}$ é definida de maneira análoga à dos números naturais. Vejamos.

Definição 2.21. *Sejam m e $n \in \mathbb{Z}$. Diremos que m é **menor ou igual** a n, e escrevemos $m \leqslant n$, se $n = m + p$ para algum $p \in \mathbb{Z}_+$. Neste caso, também podemos escrever $n \geqslant m$ e dizer que n é **maior ou igual** a m. Se $p \in \mathbb{Z}_+$, com $p \neq 0$, escreveremos $m < n$ e diremos m é **menor** do que n. Neste último caso, também escreveremos $n > m$.*

Teorema 2.22. *A relação $(\leqslant)$ definida acima é uma relação de ordem total sobre $\mathbb{Z}$, ou seja, quaisquer dois elementos de $\mathbb{Z}$ são comparáveis com respeito a esta relação.*

Demonstração. Sejam m e $n \in \mathbb{Z}$. Vamos analisar quatro casos.

1) $m = [(a,0)]$ e $n = [(b,0)]$, com a e $b \in \mathbb{N}$.

   Neste caso, como $a \leqslant b$ ou $b \leqslant a$ em $\mathbb{N}$, então existe $k \in \mathbb{N}$ tal que $b = a + k$ ou $a = b + k$. Assim, $n = [(b,0)] = [(a+k,0)] = m + [(k,0)]$ ou $m = [(a,0)] = [(b+k,0)] = n + [(k,0)]$, com $[(k,0)] \in \mathbb{Z}_+$, o que mostra que $m \leqslant n$ ou $n \leqslant m$.

2) $m = [(a,0)]$ e $n = [(0,b)]$, com a e $b \in \mathbb{N}$.

   Neste caso, $m = [(a,0)] = [(a+b,b)] = [(a+b,0)] + n$, com $[(a + b,0)] \in \mathbb{Z}_+$, ou seja, $n \leqslant m$.

3) $m = [(0,a)]$ e $n = [(b,0)]$, com a e $b \in \mathbb{N}$.

   Neste caso, $m = [(0,a)] = [(a,a+b)] = [(0,a+b)] + n$, com $[(0,a + b)] \in \mathbb{Z}_+$, ou seja, $n \leqslant m$.

4) $m = [(0,a)]$ e $n = [(0,b)]$, com a e $b \in \mathbb{N}$. De maneira análoga ao caso 1, obtemos $m \leqslant n$ ou $n \leqslant m$. □

Os resultados abaixo mostram que a relação de ordem $(\leqslant)$ é compatível com as operações de adição e multiplicação em $\mathbb{Z}$.

Teorema 2.23. ***[Compatibilidade da Adição]*** *Para quaisquer números inteiros m, n, p, se $m \leqslant n$, então*

$$m + p \leqslant n + p.$$

Demonstração. Se $m \leqslant n$, então existirá $k \in \mathbb{Z}_+$ tal que $n = m + k$. Logo,

$$n + p = (m+k) + p = (m+p) + k,$$

com $k \in \mathbb{Z}_+$, ou seja, $m + p \leqslant n + p$. □

Teorema 2.24. *[**Compatibilidade da Multiplicação**] Para quaisquer números inteiros m, n, p, se $m \leqslant n$ e $0 \leqslant p$, então*

$$mp \leqslant np.$$

Demonstração. Se $m \leqslant n$, então existirá $k = [(a,0)] \in \mathbb{Z}_+$ tal que $n = m+k$. Se $p = [(b,0)]$, pela Lei do Cancelamento da multiplicação (propriedade (H7), página 4), temos

$$np = (m+k)p = mp+kp,$$

com $kp = [(ab,0)] \in \mathbb{Z}_+$, ou seja, $mp \leqslant np$. □

2.6 Imersão de $\mathbb{N}$ em $\mathbb{Z}$

Nesta seção, vamos mostrar que $\mathbb{Z}_+$ é equivalente a $\mathbb{N}$, ou seja, uma cópia de $\mathbb{N}$. Estamos buscando identificar o conjunto dos números naturais como um subconjunto de $\mathbb{Z}$ em que há uma função injetiva $f : \mathbb{N} \to \mathbb{Z}$, que preserva as operações de adição e multiplicação e a relação de ordem ($\leqslant$).

Seja $f : \mathbb{N} \to \mathbb{Z}$ uma função definida por $f(k) = [(k,0)]$, para todo $k \in \mathbb{N}$. Esta função f satisfaz as propriedades que enumeramos a seguir.

1) A imagem de f é $\mathbb{Z}_+$, isto é, $Im(f) = \{f(k);\ k \in \mathbb{N}\} = \mathbb{Z}_+$.

2) f é injetora, ou seja, elementos distintos do domínio têm imagens distintas. De fato, pois

$$f(x_1) = f(x_2) \Longrightarrow [(x_1,0)] = [(x_2,0)]$$

em $\mathbb{Z}$, o que implica que $x_1 = x_2$ em $\mathbb{N}$, para quaisquer x_1 e $x_2 \in \mathbb{N}$.

3) f preserva a operação de adição. De fato, pois

$$f(x_1+x_2) = [(x_1+x_2,0)] = [(x_1,0)]+[(x_2,0)] = f(x_1)+f(x_2),$$

para quaisquer x_1 e $x_2 \in \mathbb{N}$.

4) f preserva a operação de multiplicação. De fato, pois

$$f(x_1x_2) = [(x_1x_2,0)] = [(x_1,0)]\cdot[(x_2,0)] = f(x_1)f(x_2),$$

para quaisquer x_1 e $x_2 \in \mathbb{N}$.

5) f preserva a relação de ordem ($\leqslant$). De fato, pois se $x_1 \leqslant x_2$ em $\mathbb{N}$, então existirá $k \in \mathbb{N}$ tal que $x_2 = x_1+k$. Logo,

$$f(x_2) = [(x_2,0)] = [(x_1+k,0)] = [(x_1,0)]+[(k,0)] = f(x_1)+[(k,0)],$$

com [(k,0)] $\in \mathbb{Z}_+$, o que implica que $f(x_1) \leqslant f(x_2)$.

Como dissemos inicialmente, o conjunto dos números inteiros surgiu para dar sentido às sentenças do tipo $2-3, 4-5, 10-11$*, como pares ordenados* $(2,3),(4,5),(10,11)$*. Esses pares ordenados diferentes devem ser considerados como sendo o mesmo número inteiro. Assim, representar o conjunto* $\mathbb{Z}$ *através de uma propriedade característica (pares ordenados) de seus elementos foi a contribuição que faltava para fundamentar o* $\mathbb{Z}$*. Em suma, identificamos o número natural* 0 *com o número inteiro* $[(0,0)]$*, o número natural* 1 *com o número inteiro* $[(1,0)]$ *e, generalizando, identificamos o conjunto dos números inteiros* $\mathbb{N}$ *com o conjunto* $\mathbb{Z}_+ = [(\mathbb{N},0)] = \{[(n,0)];\ n \in \mathbb{N}\}$*. Logo* $\mathbb{N} = \mathbb{Z}_+$ *e, para cada elemento* $[(0,y)] \in Z_-$*, temos* $[(0,y)] = -[(y,0)]$ *que está identificado com* $-y$*, ou seja,* $Z_- = \{-y;\ y \in \mathbb{N}\}$*, (veja [6]).*

Assumindo estas identificações, temos

$$\mathbb{Z} = \{\ldots,-2,-1,0,1,2,3,\ldots\}$$

e cada número inteiro k *pode ser visto como uma diferença de dois números naturais, isto é,*

$$k = [(x,y)] = [(x,0)] + [(0,y)] = x - y,$$

com x *e* $y \in \mathbb{N}$*, mesmo quando* $x \leqslant y$*, que era o que tínhamos em vista com a construção do conjunto dos números inteiros (veja [6]).*

Nos próximos capítulos escreveremos, simplesmente, $n \in \mathbb{Z}$*, se* $n = [(a,b)] \in \mathbb{Z}$*.*

CAPÍTULO

3

CONSTRUÇÃO DOS NÚMEROS RACIONAIS

Neste capítulo, vamos nos ater a definir o conjunto de números racionais a partir dos inteiros, usando classes de equivalência de pares de números inteiros. Vamos usar as propriedades dos números inteiros, já provadas no capítulo anterior. Não vamos repetir tais provas para os números racionais.

Iniciamos nossa discussão observando que a razão entre as grandezas de mesma espécie é a razão dos números que expressam suas medidas em uma mesma unidade. Portanto, a ideia é construir um conjunto que contenha $\mathbb{Z}$, de maneira que faça sentido o quociente (divisor) e tal conjunto contenha todos os divisores desse tipo.

De maneira geral, em $\mathbb{Z}$, a equação $c \cdot X = d$, com c e d pertencentes aos números inteiros, terá solução se, e somente se, d for divisível por c, ou seja, se d for um múltiplo de c. O objetivo, agora, é ampliar o conjunto dos números inteiros, construindo um conjunto em que esta equação sempre tenha solução única, mesmo que c não seja divisor de d. Repare que a solução única da equação $c \cdot X = d$ será $X = d/c$, com c diferente de zero e d e c pertencentes ao conjunto dos números inteiros. Chamamos de razão entre c e d ou razão de c para d o quociente $c : d$ ou c/d.

Observe, por exemplo, que expressões do tipo $4/2$, $6/3$, $12/6$, representam, todas elas, o mesmo número inteiro 2. Mas seria muito bom se tivéssemos uma certa ***"unicidade"*** *de representação (veja [6]). Note que a igualdade $4/2 = 6/3$ em $\mathbb{Z}$ é equivalente a $4 \cdot 3 = 2 \cdot 6$, pois são frações diretamente proporcionais. Essa noção vai nos ajudar a entender a construção que faremos a seguir.*

Seja $\mathbb{Z}^* = \{p \in \mathbb{Z};\ p \neq 0\}$ e consideremos o conjunto $\mathbb{Z} \times \mathbb{Z}^* = \{(p,q);\ p \in \mathbb{Z} \text{ e } q \in \mathbb{Z}^*\}$.

Definição 3.1. *Em $\mathbb{Z} \times \mathbb{Z}^*$, definimos uma relação, que denotaremos por ($\simeq$), como segue*

$$(m,n) \simeq (p,q) \quad \Longleftrightarrow \quad m \cdot q = n \cdot p,$$

para quaisquer pares (m,n) e (p,q) pertencentes a $\mathbb{Z} \times \mathbb{Z}^*$.

Para cada par $(m,n) \in \mathbb{Z} \times \mathbb{Z}^*$, consideremos a classe de equivalência $[(m,n)]$ representada pelo elemento (m,n). Vamos escrever $[(m,n)] = m/n$, ou seja,

$$m/n = \{(x,y) \in \mathbb{Z} \times \mathbb{Z}^* : (x,y) \simeq (m,n)\} = \{(x,y) \in \mathbb{Z} \times \mathbb{Z}^* : x \cdot n = y \cdot m\}.$$

A seguir, iremos mostrar alguns exemplos de classe de equivalências em $\mathbb{Z} \times \mathbb{Z}^*$, do tipo apresentado na Definição 3.1.

Exemplo 3.2.

- $7/11 = \{(x,y) \in \mathbb{Z} \times \mathbb{Z}^* : (x,y) \simeq (7,11)\} = \{(x,y) \in \mathbb{Z} \times \mathbb{Z}^* : 11 \cdot x = 7 \cdot y\} =$
  $= \{(7,11), (-7,-11), (14,22), (-14,-22), ...\}$.
- $13/14 = \{(x,y) \in \mathbb{Z} \times \mathbb{Z}^* : (x,y) \simeq (13,14)\} = \{(x,y) \in \mathbb{Z} \times \mathbb{Z}^* : 14 \cdot x = 13 \cdot y\} =$
  $= \{(13,14), (-13,-14), (26,28), (-26,-28), ...\}$.
- $1/2 = \{(x,y) \in \mathbb{Z} \times \mathbb{Z}^* : (x,y) \simeq (1,2)\} = \{(x,y) \in \mathbb{Z} \times \mathbb{Z}^* : 2 \cdot x = 1 \cdot y\} =$
  $= \{(1,2), (-1,-2), (2,4), (-2,-4), ...\}$.

Observação 3.3. *Sejam $m, x \in \mathbb{Z}$ e $n, y \in \mathbb{Z}^*$. Note que $m/n = x/y$ se, e somente se, $(m,n) \simeq (x,y)$. Ou seja, $m/n = x/y$ se, e somente se, $m \cdot y = n \cdot x$.*

Definição 3.4. *O conjunto quociente $\mathbb{Z} \times \mathbb{Z}^* / \simeq$, de todas as classes de equivalência determinadas pela relação $\simeq$ sobre $\mathbb{Z} \times \mathbb{Z}^*$, será denotado por $\mathbb{Q}$, ou seja,*

$$\mathbb{Q} = \{m/n : (m,n) \in \mathbb{Z} \times \mathbb{Z}^*\}.$$

Após definirmos operações de adição e multiplicação e uma relação de ordem em $\mathbb{Q}$ satisfazendo certas propriedades, chamaremos $\mathbb{Q}$ de conjuntos dos números racionais. Cada $x \in \mathbb{Q}$ admitirá infinitas representações m/n, com $m \in \mathbb{Z}$ e $n \in \mathbb{Z}^*$.

3.1 Adição em $\mathbb{Q}$

Definição 3.5. *Sejam $x = \dfrac{a}{b}$ e $y = \dfrac{c}{d}$ elementos de $\mathbb{Q}$. Definimos a adição de x com y, indicando-a por $x+y$, como sendo o elemento de $\mathbb{Q}$ tal que*

$$x + y = \frac{a}{b} + \frac{c}{d} = \frac{ad}{bd} + \frac{bc}{bd} = \frac{(ad+bc)}{bd}.$$

Proposição 3.6. *A operação de adição em $\mathbb{Q}$ está bem definida.*

Como a definição 3.5 *envolve a escolha de representantes das classes de equivalência, devemos mostrar que tal definição não depende da escolha dos representantes, ou seja, que a adição está bem definida em $\mathbb{Q}$. Assim sendo, se $x = a/b = a'/b'$ e $y = c/d = c'/d'$, então valem as igualdades a seguir.*

Demonstração.

$$ab' = ba' \quad \text{e} \quad cd' = dc'.$$

Se multiplicarmos $ab' = ba'$ por dd' e $cd' = dc'$ por bb' e somarmos membro a membro, obteremos

$$add'b' + cbb'd' = bda'd' + bdc'd'$$

ou seja,

$$b'd'(ad + cb) = bd(a'd' + c'd')$$

e, portanto,

$$(ad + cb)/bd = (a'd' + c'd')/b'd',$$

o que mostra que a adição está bem definida. □

A seguir, iremos apenas enunciar resultados relativos aos números racionais, a saber, os teoremas (propriedades) da associatividade da adição, comutatividade da adição, elemento neutro, elemento oposto e lei do cancelamento. Deixaremos a cargo do leitor tais provas.

Para a adição em $\mathbb{Q}$, dada pela Definição 3.5 , valem propriedades elementares como as que seguem.

Sejam m, n e $p \in \mathbb{Q}$. Então temos:

(A1) ***(Associatividade da Adição)**: $(m+n)+p = m+(n+p)$.*

(A2) ***(Comutatividade da Adição)**: $m+n = n+m$.*

(A3) ***(Elemento Neutro)**: Existe $0 = 0/1 = 0/2 = \ldots$ em $\mathbb{Q}$ tal que $0+m = m$, para todo $m \in \mathbb{Q}$.*

(A4) ***(Elemento Oposto)**: Dado $m \in \mathbb{Q}$, existe $n \in \mathbb{Q}$ tal que $m+n = 0$.*

(A5) ***(Lei do Cancelamento da Adição)**: $m+n = m+p \Longrightarrow n = p$.*

Usando a Lei do Cancelamento da Adição (propriedade (A5)), pode-se mostrar que o elemento neutro da adição em $\mathbb{Q}$ é único e que, para cada $m \in \mathbb{Q}$, o elemento y satisfazendo a propriedade (A5) do elemento neutro também é único, o qual será denotado por $-m$ e será chamado oposto ou simétrico aditivo de m.

Para m e $n \in \mathbb{Q}$, chamamos diferença entre m e n, e indicamos por $m-n$, o número racional $m+(-n)$.

Assim como em $\mathbb{Z}$, com demonstrações análogas, temos algumas propriedades em $\mathbb{Q}$ envolvendo adição e opostos. Portanto não faremos tais provas. O leitor interessado pode consultar [6], por exemplo.

Proposição 3.7. *Sejam m, n e $p \in \mathbb{Q}$. Então valem as seguintes propriedades:*

(i) $-(m+n) = -m-n$;

(ii) $(m-n)+n = m$;

(iii) $m+p = n \iff p = n-m$.

3.2 Multiplicação em $\mathbb{Q}$

Definição 3.8. *Sejam $m = a/b$ e $n = c/d$ elementos de $\mathbb{Q}$. O elemento de $\mathbb{Q}$ dado por $m \cdot n$ $= ac/bd$ é dito ser o produto de m por n.*

Para a multiplicação em $\mathbb{Q}$, dada pela Definição 3.8 *, valem propriedades elementares como as que seguem.*

Sejam m, n e $p \in \mathbb{Q}$. Então:

(M1) ***(Associatividade da Multiplicação)**: $m \cdot (n \cdot p) = (m \cdot n) \cdot p$.*

(M2) ***(Comutatividade da Multiplicação)**: $m \cdot n = n \cdot m$.*

(M3) ***(Elemento Neutro)**: Existe $1 = 1/1 = 2/2 = 3/3$ ... em $\mathbb{Q}$ tal que $1 \cdot m = m$, para todo $m \in \mathbb{Q}$.*

(M4) ***(Elemento Inverso)**: Para cada $m \in \mathbb{Q}$, com $m \neq 0$, existe $n \in \mathbb{Q}$ tal que $m \cdot n = 1$.*

(M5) ***(Distributividade)**: $m \cdot (n+p) = m \cdot n + m \cdot p$.*

(M6) ***(Lei do Cancelamento da Multiplicação)**: Se $m \cdot n = m \cdot p$ e $m \neq 0$, então $n = p$.*

Vamos demonstrar as propriedades (M3), (M4) e (M6). Os itens (M1), (M2) e (M5) a cargo do leitor.

Teorema 3.9. ***[Elemento Neutro]** Dado $a \in \mathbb{Q}$, tem-se*

$$a \cdot 1 = a.$$

Demonstração. Seja $a = m/n$, com $m \in \mathbb{Z}$ e $n \in \mathbb{Z}^*$. Então

$$a \cdot 1 = \frac{m}{n} \cdot \frac{1}{1} = (m \cdot 1)/(n \cdot 1) = m/n = a,$$

o que mostra o que queríamos. □

Teorema 3.10. *[**Elemento Inverso**] Se $a = m/n$ em $\mathbb{Q}$, $a \neq 0$, então $m \neq 0$ e, consequentemente, $b = n/m \in \mathbb{Q}$. Assim,*

$$a \cdot b = 1.$$

Demonstração. Temos

$$a \cdot b = \frac{m}{n} \cdot \frac{n}{m} = (m \cdot n)/(m \cdot n) = 1/1 = 1,$$

o que mostra o que queríamos. □

Teorema 3.11. *[**Lei do Cancelamento**] Se $a \cdot b = a \cdot c$ e $a \neq 0$, então*

$$b = c.$$

Demonstração. Se $ab = ac$ e $a \neq 0$, então, da propriedade (M2), temos $ba = ca$. Como $a \neq 0$ da propriedade (M4), existe $a' \in \mathbb{Q}$ tal que $aa' = 1$. Portanto, multiplicando a equação $ba = ca$ por a' e usando a associatividade da multiplicação (propriedade (M1)), obtemos $b(aa') = c(aa')$, ou seja, $b \cdot 1 = c \cdot 1$, o que implica que $b = c$. □

Observação 3.12. *Assim como na adição (veja [6]), usando a Lei do Cancelamento para a multiplicação (propriedade (M6)), pode-se mostrar que o elemento neutro é único e que o elemento b satisfazendo a propriedade (M4) também é único. Este último elemento será chamado **inverso** ou **simétrico multiplicativo** de a e será denotado por $1/a$.*

Para a e $b \in \mathbb{Q}$, com relação aos inversos temos a proposição seguinte.

Proposição 3.13. *Se $a \neq 0$, então $1/(1/a) = a$ e $1/(a \cdot b) = (1/a) \cdot (1/b)$, ou seja,*

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

Ainda, usando a noção de inverso, podemos definir a operação de divisão sobre $\mathbb{Q}$ como segue.

Definição 3.14. *Sejam $a \in \mathbb{Q}$ e $b \in \mathbb{Q}^* = \{a \in \mathbb{Q},\ a \neq 0\}$. A operação de $\mathbb{Q} \times \mathbb{Q}^*$ em $\mathbb{Q}$ que a cada par (a, b) associa o número racional $a \cdot (1/b)$ é chamado de **divisão** em $\mathbb{Q}$. O elemento $a \cdot (1/b)$ é dito ser o **quociente** de a por b e também poderá ser indicado por a/b ou $\dfrac{a}{b}$.*

3.3 Relação de Ordem em $\mathbb{Q}$

Considere $a \in \mathbb{Q}$, com $a = m/n = -m/(-n)$. Vale observar que podemos considerar uma representação para a em que o denominador seja um número inteiro maior que zero. Com isso em mente, vamos definir racionais positivos e negativos, entre outras noções.

A relação que definiremos abaixo, é análoga à relação de ordem definida sobre $\mathbb{Z}$.

Definição 3.15. *Sejam a e b* $\in \mathbb{Q}$ *frações em que os denominadores sejam inteiros positivos, ou seja,* $a = m/n$ *e* $b = k/p$*, com* $n > 0$ *e* $p > 0$ *em* $\mathbb{Z}$*. Assim, a será* ***menor ou igual*** *a b, e escreveremos* $a \leq b$*, se* $mp \leq nk$ *em* $\mathbb{Z}$*. Nestas mesmas condições, b será dito* ***maior ou igual*** *a a, e escreveremos* $b \geq a$*. Caso* $mp < nk$ *em* $\mathbb{Z}$*, diremos que a é* ***menor que*** *b* $(a < b)$ *ou que b é* ***maior que*** *a* $(b > a)$*.*

Exemplo 3.16. *Observe que* $\frac{-2}{3} < \frac{4}{5}$ *e* $\frac{7}{4} > \frac{2}{7}$*, pois* $(-2) \cdot 5 < 3 \cdot 4$ *e* $7 \cdot 7 > 4 \cdot 2$*.*

Definição 3.17. *Diremos que um elemento* $a = m/n \in \mathbb{Q}$ *é* ***não negativo****, se* $mn \in \mathbb{N}$ *e é* ***positivo*** *se* $mn \in \mathbb{N}$ *e* $m \neq 0$*. Agora, dizemos que um elemento* $a = m/n \in \mathbb{Q}$ *é* ***não positivo****, se m/n não for positivo, e diremos que é* ***negativo****, se m/n não for não negativo.*

Proposição 3.18. *Sejam a e b em* $\mathbb{Q}$ *tais que* $a \leq b$*. Então existe c não negativo em* $\mathbb{Q}$ *tal que* $b = a + c$*.*

Demonstração. Dados a e b em $\mathbb{Q}$, sem perda de generalidade, podemos escrever $a = m/n$ e $b = k/n$, com $n > 0$.

Se $a \geq b$ em $\mathbb{Q}$, então $mn \geq nk$ em $\mathbb{Z}$ e, como $n > 0$, obtemos $m \geq k$. Pela definição da relação de ordem sobre $\mathbb{Z}$ (Definição 2.21), existe p que pertence aos inteiros não negativos tal que $k = m + p$. Portanto,

$$b = k/n = (m + p)/n = m/n + p/n = a + c,$$

em que $c = p/n \in \mathbb{Q}$ é não negativo, pois $p \geq 0$ e $n > 0$, o que mostra o resultado. $\square$

No próximo resultado, mostraremos que a relação $(\leq)$*, é uma relação de* ***ordem total*** *sobre* $\mathbb{Q}$*.*

Iremos considerar que todos os denominadores dos elementos em $\mathbb{Q}$*, serão positivos.*

Teorema 3.19 (Ordem Total sobre $\mathbb{Q}$**).** *A relação* $(\leq)$ *é uma relação de ordem total sobre* $\mathbb{Q}$*.*

Demonstração. Sejam $a = x/y$, $b = z/w$ e $c = k/p$ elementos de $\mathbb{Q}$. Precisamos provar as propriedades que seguem.

1. $(\leq)$ é reflexiva.

   Neste caso, de fato, para todo $a \in \mathbb{Q}$, tem-se

   $$a \leq a \iff \frac{x}{y} \leq \frac{x}{y} \iff xy = yx,$$

   pois o produto de números inteiros é comutativo.

2. $(\leq)$ é antissimétrica.

   Neste caso, sejam a e b elementos de $\mathbb{Q}$ tais que $a \leq b$ e $b \leq a$, ou seja, $\frac{x}{y} \leq \frac{z}{w}$ e $\frac{z}{w} \leq \frac{x}{y}$. Então $xw \leq yz$ e $zy \leq wx$ em $\mathbb{Z}$. Portanto, $xw = yz$, o que implica que $\frac{x}{y} = \frac{z}{w}$, isto é, $a = b$.

3. $(\leq)$ é transitiva.

   Neste caso, sejam a, b e c elementos de $\mathbb{Q}$ tais que $a \leq b$ e $b \leq c$, isto é, $\frac{x}{y} \leq \frac{z}{w}$ e $\frac{z}{w} \leq \frac{k}{p}$. Então, $xw \leq yz$ e $zp \leq wk$ em $\mathbb{Z}$. Logo, $xwp \leq yzp$ e $zpy \leq wky$. Usando a transitividade da relação de ordem em $\mathbb{Z}$, $xwp \leq wky$ e como $w > 0$, segue que $xp \leq ky$. Assim, $\frac{x}{y} \leq \frac{k}{p}$, ou seja, $a \leq b$.

4. $(\leq)$ é comparável.

   Sejam a e b elementos de $\mathbb{Q}$. Queremos mostrar que $a \leq b$ ou $b \leq a$, ou seja, $\frac{x}{y} \leq \frac{z}{w}$ ou $\frac{z}{w} \leq \frac{x}{y}$. Isso ocorre pois, em $\mathbb{Z}$, tem-se $xw \leq yz$ ou $zy \leq wx$, como queríamos demonstrar.

Pelas propriedades 1 até 4 demonstradas acima, $(\leq)$ é uma relação de ordem total. □

O resultado que enunciaremos a seguir mostra que a relação de ordem em $\mathbb{Q}$ é compatível com as operações de adição e multiplicação em $\mathbb{Q}$.

Proposição 3.20. *Sejam a, b e c $\in$ em $\mathbb{Q}$. Valem as seguintes propriedades:*

(01) ***(Compatibilidade da adição)****: Se $a \leq b$, então $a + c \leq b + c$.*

(02) ***(Compatibilidade da multiplicação)****: Se $a \leq b$ e $0 \leq c$, então $ac \leq bc$.*

3.4 Imersão de $\mathbb{Z}$ em $\mathbb{Q}$

A ideia aqui é análoga à usada no capítulo anterior, com a imersão de $\mathbb{N}$ em $\mathbb{Z}$, ou seja, a nossa motivação é identificar $\mathbb{Z}$ como uma partição (subconjunto) de $\mathbb{Q}$. Vamos considerar uma imersão de $\mathbb{Z}$ em $\mathbb{Q}$, isto é, uma função injetiva $h : \mathbb{Z} \longrightarrow \mathbb{Q}$ que preserve as operações de adição e multiplicação e a relação de ordem $(\leq)$ (veja [6]).

Definição 3.21. *Seja $h : \mathbb{Z} \longrightarrow \mathbb{Q}$ dada por $h(k) = a/1$, para todo $k \in \mathbb{Z}$. Assim,*

1) $Im(k)$ = {k/1; $k \in \mathbb{Z}$}.

2) h é injetora, isto é, se $h(k) = h(p)$, então $k/1 = p/1$ em $\mathbb{Q}$, o que implica que $k \cdot 1 = p \cdot 1$ em $\mathbb{Z}$, ou seja, $k = p$, para todo k e $p \in \mathbb{Z}$.

3) h preserva as operações de adição, ou seja, $h(k+p) = (k+p)/1 = k/1 + p/1 = h(k) + h(p)$, para todo k e $p \in \mathbb{Z}$.

4) h preserva as operações de multiplicação, ou seja, $h(k\cdot p)$ *= (k · p)/1* $= k/1\cdot p/1 = h(k)\cdot h(p)$*, para todo k e* $p\in\mathbb{Z}$*.*

5) h preserva as relações de ordem, isto é, se $k\leq p$ *em* $\mathbb{Z}$*, então existe w pertencente aos inteiros positivos tal que* $p=k+w$*. Logo,* $h(p)=p/1=(k+w)/1=\dfrac{k}{1}+\dfrac{w}{1}=h(k)+\dfrac{w}{1}$*, com* $\dfrac{w}{1}$ *não negativo em* $\mathbb{Q}$*, o que implica que* $h(k)\leq h(p)$ *em* $\mathbb{Q}$*.*

Portanto, no que se refere aos aspectos algébricos e quanto à ordenação, Im(h) *= {k/1; k* $\in\mathbb{Z}$*} é uma cópia de* $\mathbb{Z}$ *dentro de* $\mathbb{Q}$ *(veja [6]). Identificamos* $\mathbb{Z}$ *com Im*(h) *através de h e consideramos que o conjunto dos números inteiros está* ***propriamente contido*** *no conjunto dos números racionais e como* $\mathbb{N}$ *pode ser visto como um subconjunto de* $\mathbb{Z}$*, temos as inclusões* $\mathbb{N}\subset\mathbb{Z}\subset\mathbb{Q}$*.*

Assim sendo, após as demonstrações acima mencionadas, além das propriedades colocadas, temos como responder à pergunta inicialmente feita no capítulo, ou seja, em $\mathbb{Q}$ *a equação* $c\cdot X=d$ *admite uma única solução, com c e d pertencentes aos inteiros,* $c\neq 0$*, a saber,* $X=(1/c)\cdot d=\dfrac{d}{c}$*, mesmo quando c não é múltiplo de d.*

CAPÍTULO

4

CONSTRUÇÃO DOS NÚMEROS REAIS

Os números reais podem ser construídos de duas formas diferentes a partir dos racionais. Uma delas é por classes de equivalência de sequências de Cauchy. A outra forma foi através dos cortes de Dedekind. Apresentaremos esta segunda forma proposta por Julius Wilhelm Richard Dedekind (1831-1916).

Quando se fala do conjunto dos números reais no contexto escolar, diz-se que nem todos os pontos da reta correspondem a números racionais, sendo que a esses pontos correspondem números chamados irracionais. Geralmente isto é introduzido exemplificando a medida da diagonal de um quadrado de lado 1. *Faremos esse exemplo mais à frente neste capítulo. Vamos, inicialmente, definir a noção de corte de Dedekind, considerar o conjunto de todos os cortes. Este conjunto de cortes chamaremos de conjunto de números reais o qual será denotado por* $\mathbb{R}$. *Em seguida, vamos definir a adição e multiplicação nos reais e mostrar que os reais possuem as propriedades aritméticas de* $\mathbb{Q}$ *e mais uma propriedade que* $\mathbb{Q}$ *não possui (a completude).*

Para entender a construção dos números reais, vamos seguir os passos dados no livro de W. Rudin [3].

4.1 Cortes de Dedekind

O objetivo desta seção é estabelecer um resultado que garanta a existência de um corpo ordenado (veja a Definição 4.28) (que será indicado por $\mathbb{R}$*) completo que contenha o conjunto dos racionais e que resolva o problema dos "buracos" encontrados na reta real. Os elementos de* $\mathbb{R}$ *serão certos subconjuntos de* $\mathbb{Q}$*, denominados cortes. Mais precisamente, temos a definição seguinte.*

Definição 4.1. *Diremos que um conjunto* α *de números racionais é um corte, se estiverem satisfeitas as seguintes condições:*

(i) $\alpha \neq \varnothing$ *e* $\alpha \neq \mathbb{Q}$.

(ii) *Seja* $q \in \mathbb{Q}$. *Se* $p \in \alpha$ *e* $q < p$, *então* $q \in \alpha$.

(iii) *Se* $p \in \alpha$, *então* $p < r$, *para algum* $r \in \alpha$.

A primeira condição na Definição 4.1 *implica que* α *contém pelo menos um racional, mas não todos. A segunda condição afirma que todo número racional do conjunto* α *é menor do que todo número racional que não pertence ao conjunto* α. *A última condição implica que, em* α, *não existe racional máximo, isto é, não existe um elemento em* α *que seja maior ou igual a todos os outros elementos de* α.

Exemplo 4.2. *Qualquer número racional r determina um corte, digamos* α, *que é o conjunto de todos os números racionais menores do que r. É fácil ver que* α *satisfaz os itens* (i) *e* (ii) *da Definição* 4.1. *Para provar o item* (iii), *basta observar que qualquer que seja* $p \in \alpha$, *tem-se*

$$p < (p+r)/2 < r,$$

e, portanto, $(p+r)/2 \in \alpha$. *Note que* $r \notin \alpha$.

Observação 4.3. *Os cortes foram inventados em 1872 pelo matemático alemão chamado Julius Wilhelm Richard Dedekind que viveu de (06-10-1831 a 12-02-1916). As seguintes palavras foram extraídas do livro, de Dedekind, "Essays on the Theory of Numbers":*

> *"Minha atenção voltou-se primeiramente para as considerações que constituem o assunto deste folheto no outono de 1858. Como professor na Escola Politécnica em Zurique, vi-me pela primeira vez obrigado a dar aulas sobre os elementos do cálculo diferencial e senti mais agudamente do que nunca a falta de um fundamento realmente científico para a aritmética. Ao discutir a noção de limite e especialmente ao provar o teorema segundo o qual toda magnitude que cresce continuamente, mas não além de todas os limites, deve certamente se aproximar de um valor finito, tive que recorrer a evidências geométricas. Mesmo agora, esse recurso à intuição geométrica numa primeira apresentação do cálculo diferencial, eu o vejo como extremamente útil, do ponto de vista didático, e até mesmo indispensável se não se quer perder muito tempo. Mas ninguém pode negar que essa forma de introdução ao cálculo diferencial não pode se pretender científica. Para mim, esse sentimento de insatisfação foi tão esmagador que mantive a firme intenção de continuar refletindo sobre a questão até encontrar um fundamento puramente aritmético e perfeitamente rigoroso para os princípios da análise infinitesimal."*

Definição 4.4 (Cortes racionais e não racionais)**.**

- *Seja $q \in \mathbb{Q}$. Definimos $q^* = \{r \in \mathbb{Q} : r < q\}$. Então q^* será um corte que chamaremos racional. Os cortes que não são racionais serão chamados irracionais.*

- $\sqrt{2} = \{q \in \mathbb{Q} : q^2 < 2\} \cup \{q \in \mathbb{Q} : q < 0\}$ *é irracional.*

O corte dado pelo Exemplo 4.2 *é chamado de corte racional. Para indicar que um corte α é o corte racional relacionado a r escreveremos $\alpha = r^*$.*

A propriedade (ii) da Definição 4.1 *implica na propriedade seguinte.*

Teorema 4.5. *Sejam α um corte e $p, q \in \mathbb{Q}$ tais que $p \in \alpha$ e $q \notin \alpha$. Então $p < q$.*

Demonstração. Suponhamos, por absurdo, que $q \leq p$. Conclui-se de (ii) que $q \in \alpha$. Contradição. Logo, $p < q$. □

Observação 4.6. *Note que:*

- *Se α for um corte, $p \in \alpha$ e $q \notin \alpha$, então $p < q$.*

- *Se α for um corte, $r \notin \alpha$ e $r < s$, então $s \notin \alpha$.*

A seguir, iremos definir o que significa um corte ser menor do que outro. Também vamos definir adição e multiplicação de cortes e vamos demonstrar algumas propriedades dessas operações, com base nas propriedades já provadas para os racionais.

Definição 4.7. *Sejam α, β cortes. Escreveremos $\alpha = \beta$ se toda vez que $p \in \alpha$ tivermos $p \in \beta$ e toda vez que $q \in \beta$, tivermos $q \in \alpha$, isto é, se os dois conjuntos α e β forem idênticos. Caso contrário, escreveremos $\alpha \neq \beta$.*

A seguir, definiremos uma relação de ordem no conjunto dos cortes.

Definição 4.8. *Sejam α e β cortes. Escreveremos $\alpha < \beta$ (ou $\beta > \alpha$), se α for um subconjunto próprio de β, isto é, se existir um racional p tal que $p \in \beta$ e $p \notin \alpha$.*

Observação 4.9. *A seguir, faremos três observações fundamentais para a compreensão da definição de ordem. São elas:*

1. *$\alpha \leq \beta$ significa que $\alpha = \beta$ ou $\alpha < \beta$.*
2. *$\alpha \geq \beta$ significa que $\beta \leq \alpha$.*
3. *Se $\alpha > 0^*$, diremos que α é positivo; se $\alpha \geq 0^*$, diremos que α é não negativo. Analogamente, se $\alpha < 0^*$, diremos que α é negativo, e se $\alpha \leq 0^*$, diremos que α é não positivo.*

Agora, vamos demonstrar o teorema da tricotomia para dois cortes quaisquer.

Teorema 4.10. *Sejam α e β cortes. Vale uma e somente uma das condições seguintes:*

(i) $\alpha = \beta$

(ii) $\alpha < \beta$

(iii) $\beta < \alpha$

Demonstração. Pelas Definições 4.7 e 4.8, se $\alpha = \beta$, então não valem (ii) e (iii). Vamos mostrar que $\alpha < \beta$ e $\beta < \alpha$ são mutuamente excludentes. Suponha, por absurdo, que ambas as relações sejam válidas. Como $\alpha < \beta$, existe um racional p tal que $p \in \beta$ e $p \notin \alpha$. Como $\beta < \alpha$, existe um racional q tal que $q \in \alpha$ e $q \notin \beta$. Mas, pelo Teorema 4.5, de $p \in \beta$ e $q \notin \beta$ resulta $q < p$, enquanto que $q \in \alpha$ e $p \notin \alpha$ implicam $q < p$, o que é uma contradição, pois não podemos ter $p < q$ e $q < p$ pela propriedade de tricotomia dos números racionais. Assim, provamos que, no máximo, uma das três relações é válida. Suponhamos que $\alpha \neq \beta$. Então, ou existe um número racional p em α mas não em β e, neste caso, $\beta < \alpha$ ou existe um racional q em β, mas não em α, e, neste caso, $\alpha < \beta$. □

No próximo teorema, iremos demonstrar a propriedade de transitividade para $(<)$.

Teorema 4.11. *Sejam α, β e γ cortes. Se $\alpha < \beta$ e $\beta < \gamma$, então $\alpha < \gamma$.*

Demonstração. Como $\alpha < \beta$, existe um racional p tal que $p \in \beta$ e $p \notin \alpha$. Como $\beta < \gamma$, existe um racional q tal que $q \in \gamma$ e $q \notin \beta$. Mas, se $p \in \beta$ e $q \notin \beta$, então $p < q$. Como $p \notin \alpha$, então $q \notin \alpha$. Logo, $q \in \gamma$ e $q \notin \alpha$, o que significa que $\alpha < \gamma$. □

Note que, de fato, $(<)$ da Definição 4.7 é uma relação de ordem e, por conseguinte, o conjuntos dos cortes é ordenado. No próximo teorema, iremos definir a adição em tal conjunto.

Teorema 4.12. *Sejam α e β cortes. Seja γ o conjunto de todos os racionais r tais que $r = p + q$, com $p \in \alpha$ e $q \in \beta$. Então γ é um corte.*

Demonstração. Precisamos provar que γ cumpre as três condições da Definição 4.1.

(i) Nota-se que γ é não vazio. Consideremos $s \notin \alpha$, $t \notin \beta$, com $s, t \in \mathbb{Q}$. Então $s > p$, para todo $p \in \alpha$, e $t > q$, para todo $q \in \beta$. Assim, $s + t > p + q$ e $s + t \notin \gamma$. Logo γ não contém todos os racionais, ou seja, $\gamma \neq \mathbb{Q}$.

(ii) Suponhamos que $r \in \gamma$, $s < r$, com $s \in \mathbb{Q}$. Logo $r = p + q$, com $p \in \alpha$ e $q \in \beta$. Como $s < r$, então $s - q < p$, assim, $s - q \in \alpha$ e $s = (s - q) + q \in \gamma$.

(iii) Suponhamos que $r \in \gamma$. Logo, $r = p + q$, com $p \in \alpha$ e $q \in \beta$. Então existe um racional $s > p$ tal que $s \in \alpha$. Portanto, $s + q > r$ e r não é o maior racional em γ. □

Definição 4.13. *Se α, β forem cortes, então*

$$\gamma = \alpha + \beta = \{r + s; r \in \alpha \text{ e } s \in \beta\}$$

será um corte chamado soma de α e β.

A seguir, veremos algumas propriedades da operação de adição no conjunto dos cortes. Iremos apresentar e demonstrar as propriedades comutativa, associativa e elemento neutro dos cortes.

Teorema 4.14. *Sejam α, β e γ cortes. Então valem as seguintes propriedades:*

(i) $\alpha + \beta = \beta + \alpha$;

(ii) $(\alpha + \beta) + \gamma = \alpha + (\beta + \gamma)$;

(iii) $\alpha + 0^* = \alpha$.

Demonstração. Consideremos $\alpha + \beta$ o conjunto de todos os racionais da forma $p + q$, em que $p \in \alpha$ e $q \in \beta$.

(i) Na definição de $\beta + \alpha$, consideramos $q + p$, em vez de $p + q$. Pela comutatividade da adição de racionais, $p + q = q + p$. Portanto, $\alpha + \beta = \beta + \alpha$.

(ii) Resulta da propriedade associativa da adição de números racionais.

(iii) Seja $r \in \alpha + 0^*$. Logo $r = p + q$, com $p \in \alpha$ e $q \in 0^*$ (isto é, $q < 0$). Assim, $p + q < p$, de modo que, $p + q \in \alpha$ e $r \in \alpha$. Portanto, $\alpha + 0^* \subset \alpha$. Reciprocamente, suponhamos que $r \in \alpha$ e tomemos $s \in \alpha$ com $s > r$. Então $r - s \in 0^*$ e $r = s + (r - s) \in \alpha + 0^*$. Portanto $\alpha \subset \alpha + 0^*$. Assim, $\alpha + 0^* = \alpha$. □

No próximo teorema, apenas enunciaremos a unicidade do elemento oposto da adição de um corte arbitrário. Deixaremos a cargo do leitor a demonstração.

Teorema 4.15. *Seja α um corte. Existe um único corte β tal que $\alpha + \beta = 0^*$.*

Observação 4.16. *Designamos por $-\alpha$ o corte β do Teorema* 4.12.

A seguir, demonstraremos a lei do cancelamento da adição e a compatibilidade da ordem com a adição para os cortes α, β e γ.

Teorema 4.17. *Sejam α, β e γ cortes.*

(i) *Se $\alpha + \beta = \alpha + \gamma$, então $\beta = \gamma$.*

(ii) Se $\beta < \gamma$, então $\alpha+\beta < \alpha+\gamma$. Em particular, (para $\beta = 0^*$) temos $\alpha+\gamma > 0^*$, se $\alpha > 0^*$ e $\gamma > 0^*$.

Demonstração.

(i) Pelo Teorema 4.12,

$$\begin{aligned} \beta &= 0^* + \beta = (-\alpha+\alpha)+\beta = (-\alpha)+(\alpha+\beta) = \\ &= (-\alpha)+(\alpha+\gamma) = (-\alpha+\alpha)+\gamma = 0^*+\gamma = \gamma. \end{aligned}$$

(ii) É fácil ver que $\alpha+\beta \leq \alpha+\gamma$. Se $\alpha+\beta = \alpha+\gamma$, pelo item anterior, $\beta = \gamma$. □

Teorema 4.18. *Sejam α e β cortes. Existe um único corte γ tal que $\alpha+\gamma = \beta$.*

Demonstração. Se $\gamma_1 \neq \gamma_2$, então $\alpha+\gamma_1 \neq \alpha+\gamma_2$. Assim, existe no máximo um corte γ nas condições enunciadas.

Seja $\gamma = \beta+(-\alpha)$. Então

$$\begin{aligned} \alpha+\gamma &= \alpha+[\beta+(-\alpha)] = \alpha+[(-\alpha)+\beta] \\ &= [\alpha+(-\alpha)]+\beta = 0^*+\beta = \beta \end{aligned}$$

e a prova está completa. □

Observação 4.19. *Em vez de $\beta+(-\alpha)$, escrevemos $\beta-\alpha$.*

A seguir, definiremos a multiplicação no conjunto dos cortes e mostraremos que, na verdade, obtemos um corpo.

Teorema 4.20. *Sejam α e β cortes tais que $\alpha \geq 0^*$ e $\beta \geq 0^*$. Seja γ o conjunto de todos os racionais r tais que $r = pq$, em que $p \in \alpha$, $q \in \beta$, $p \geq 0$ e $q \geq 0$. Então γ será um corte.*

Definição 4.21. *Chamamos o corte γ do Teorema* 4.17 *de produto de α e β e representamos tal produto por $\alpha \cdot \beta$*

Definição 4.22. *Sejam α e β cortes. Definimos*

$$\alpha\cdot\beta = \begin{cases} (-\alpha)(-\beta), \text{ se } \alpha,\beta < 0^* \\ -[(-\alpha)\beta], \text{ se } \alpha < 0^* \text{ e } \beta > 0^* \\ -[\alpha(-\beta)], \text{ se } \alpha \geq 0^* \text{ e } \beta < 0^* \end{cases}$$

Teorema 4.23. *Quaisquer que sejam os cortes α, β e γ, valem as seguintes propriedades:*

(i) $\alpha\cdot\beta = \beta\cdot\alpha$;

(ii) $(\alpha\cdot\beta)\cdot\gamma = \alpha\cdot(\beta\cdot\gamma)$;

(iii) $\alpha \cdot (\beta + \gamma) = \alpha \cdot \beta + \alpha \cdot \gamma$;

(iv) $\alpha \cdot 0^* = 0^*$;

(v) $\alpha \cdot \beta = 0^*$ *se, e somente se,* $\alpha = 0^*$ *ou* $\beta = 0^*$;

(vi) $\alpha \cdot 1^* = \alpha$;

(vii) *Se* $0^* < \alpha < \beta$ *e* $\gamma > 0^*$, *então* $\alpha \cdot \gamma < \beta \cdot \gamma$.

Demonstração. Vamos provar o item (iii). Os demais itens ficam a cargo do leitor.

Suponhamos que $\alpha > 0^*$, $\beta < 0^*$, $\beta + \gamma > 0^*$. Então $\gamma = (\beta + \gamma) + (-\beta)$. Como a distributividade vale para os racionais, temos

$$\alpha \cdot \gamma = \alpha \cdot (\beta + \gamma) + \alpha \cdot (-\beta).$$

Mas $\alpha \cdot (-\beta) = -(\alpha \cdot \beta)$. Portanto, $\alpha \cdot \beta + \alpha \cdot \gamma = \alpha \cdot (\beta + \gamma)$. Os outros casos são análogos. □

Teorema 4.24. *Se* $\alpha \neq 0^*$, *para cada corte* β, *existirá um único corte* γ *(que designaremos por* β/α*) tal que* $\alpha \cdot \gamma = \beta$.

Teorema 4.25. *Quaisquer que sejam os racionais p e q, temos:*

(i) $p^* + q^* = (p+q)^*$;

(ii) $p^* \cdot q^* = (p \cdot q)^*$;

(iii) $p^* < q^*$ *se, e somente se,* $p < q$.

Demonstração.

(i) Se $r \in p^* + q^*$, então $r = s + t$, com $s < p$, $t < q$, de modo que $r < p + q$. Assim $r \in (p+q)^*$. Se $r \in (p+q)^*$, então $r < p + q$. Sejam $h = p + q - r$, $s = p - h/2$ e $t = q - h/2$. Logo $s \in p^*$, $t \in q^*$ e $r = p + q - h = (p - h/2) + (q - h/2) = s + t$, de modo que $r \in p^* + q^*$, o que prova (i).

(ii) Análogo ao item (i).

(iii) Se $p < q$, então $p \in q^*$. Mas $p \notin p^*$, de modo que $p^* < q^*$. Se $p^* < q^*$, existirá um racional r tal que $r \in q^*$, com $r \notin p^*$. Portanto, $p \leq r < q$, de modo que $p < q$. □

Teorema 4.26. *Se* α, β *forem cortes e* $\alpha < \beta$, *então existirá um corte racional* r^* *tal que* $\alpha < r^* < \beta$.

Demonstração. Se $\alpha < \beta$, então existirá um número racional p tal que $p \in \beta$ e $p \notin \alpha$. Escolhamos $r > p$ de modo que $r \in \beta$. Como $r \in \beta$ e $r \notin r^*$, temos $r^* < \beta$. Como $p \in r^*$ e $p \notin \alpha$, temos $\alpha < r^*$. □

Teorema 4.27. *Qualquer que seja o corte α, teremos $p \in \alpha$ se, e somente se, $p^* < \alpha$.*

Demonstração. Seja α um corte. Suponhamos que $p \in \alpha$. Como $pp*$, vale $p* < \alpha$. Reciprocamente, seja $p \in \mathbb{Q}$ tal que $p* < \alpha$. Então existe um racional q tal que $q \in \alpha$ e $q \notin p^*$. Assim, $q \geq p$, donde concluímos que $p \in \alpha$, pois $q \in \alpha$. □

4.2 O corpo dos números reais

Iniciaremos esta seção apresentando a definição de corpo.

Definição 4.28. *Um corpo é um conjunto não vazio $\mathbb{T}$ em que estão denotadas duas operações binárias, chamadas adição e multiplicação e definidas, respectivamente, por*

$$\begin{array}{rcl} +: \mathbb{T} \times \mathbb{T} \to \mathbb{T} & \quad e \quad & \cdot: \mathbb{T} \times \mathbb{T} \to \mathbb{T} \\ (x,y) \mapsto x+y & & (x,y) \mapsto x \cdot y \end{array}$$

satisfazendo:

(A1) ***(Associativa da adição)*** *$(x+y)+z = x+(y+z)$, para quaisquer $x,y,z \in \mathbb{T}$;*

(A2) ***(Comutativa da adição)*** *$x+y = y+x$, para quaisquer $x,y \in \mathbb{T}$;*

(A3) ***(Elemento neutro da adição)*** *Existe $0 \in \mathbb{T}$ tal que $x+0 = x$, para todo $x \in \mathbb{T}$;*

(A4) ***(Elemento oposto da adição)*** *Dado $x \in \mathbb{T}$, existe $y \in \mathbb{T}$ $(y = -x)$ tal que $x+y = 0$;*

(M1) ***(Associativa da multiplicação)*** *$(x \cdot y) \cdot z = x \cdot (y \cdot z)$, para quaisquer $x,y,z \in \mathbb{T}$;*

(M2) ***(Comutativa da multiplicação)*** *$x \cdot y = y \cdot x$, para quaisquer $x,y \in \mathbb{T}$;*

(M3) ***(Elemento neutro da multiplicação)*** *Existe $1 \in \mathbb{T}$, tal que $x \cdot 1 = x$, para todo $x \in \mathbb{T}$;*

(M4) ***(Elemento inverso da multiplicação)*** *Dado $x \in \mathbb{T}$, $x \neq 0$, existe $y \in \mathbb{T}$, $\left(y = \frac{1}{x}\right)$, tal que $x \cdot y = 1$;*

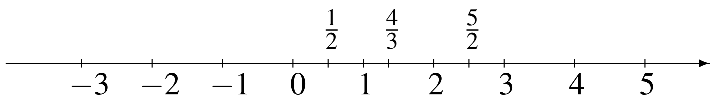
(D) ***(Distributiva da multiplicação)*** *$x \cdot (y+z) = x \cdot y + x \cdot z$, para quaisquer $x,y,z \in \mathbb{T}$.*

Com as propriedades de $\mathbb{Q}$ provadas no Capítulo 3, $\mathbb{Q}$, munido das operações de adição e multiplicação daquele capítulo, é um corpo. De modo análogo, o conjunto dos cortes, com as operações de adição e multiplicação apresentadas na seção anterior do presente capítulo, também é um corpo. Este último denotaremos por $\mathbb{R}$, pois será chamado de corpo dos números reais ou, simplesmente, reais.

4.3 $\mathbb{Q}$ não é completo e $\mathbb{R}$ é completo

Conforme vimos na seção anterior, se $\mathbb{T}$ for um conjunto qualquer não vazio com operações de adição e multiplicação, indicadas por $+$ e $\cdot$ respectivamente, que satisfazem as propriedades $(A1)$ a $(A4)$, $(M1)$ a $(M4)$ e (D), então diremos que a terna ($\mathbb{T}$, $+$, $\cdot$) é um corpo. Se, além disso, em $\mathbb{T}$ estiver definida uma relação de ordem total ($\leq$), de modo que a quádrupla ($\mathbb{T}$, $+$, $\cdot$,$\leq$) também satisfaça propriedades de compatibilidade com relação à adição e à multiplicação, então diremos que ($\mathbb{T}$, $+$, $\cdot$,$\leq$) é um corpo ordenado. Em particular, ($\mathbb{Q}$, $+$, $\cdot$,$\leq$) é um corpo ordenado por tudo que vimos no Capítulo 3. Por outro lado, ($\mathbb{Z}$, $+$, $\cdot$,$\leq$) com as operações de adição e multiplicação do Capítulo 2 não é um corpo ordenado, pois $(M4)$ não se verifica.

Sabemos que os números racionais podem ser representados geometricamente por pontos em uma reta horizontal ordenada, conhecida como reta real.

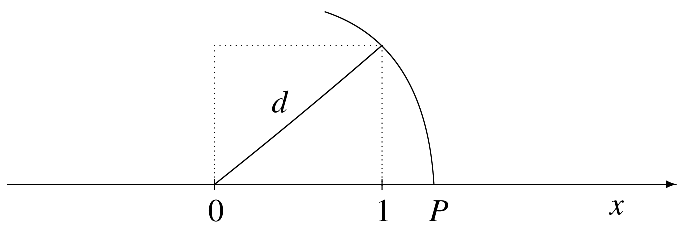


Se P for a representação de um número racional x, diremos que x é a abscissa de P. Mostraremos, a seguir, que nem todo ponto da reta real é racional.

Considere um quadrado de lado 1 e diagonal d . Pelo Teorema de Pitágoras,

$$d^2 = 1^2 + 1^2 = 2.$$

Seja P a interseção do eixo x com a circunferência de centro em 0 e raio d.



Mostraremos que P é um ponto da reta com abscissa $x \notin \mathbb{Q}$.

Consideremos a proposição seguinte, que apresentamos sem demonstração.

Proposição 4.29. *Seja $a \in \mathbb{Z}$. Então valem:*

(a) Se a for ímpar, então a^2 é ímpar;

(b) Se a^2 for par, então a é par.

Proposição 4.30. *A equação $x^2 = 2$ não admite solução em $\mathbb{Q}$.*

Demonstração. Suponhamos, por absurdo, que $x^2 = 2$ tenha solução em $\mathbb{Q}$. Então podemos tomar $x = \frac{a}{b}$ com $a, b \in \mathbb{Z}$ e $\frac{a}{b}$ irredutível. Logo

$$\left(\frac{a}{b}\right)^2 = 2,$$

ou seja, $a^2 = 2b^2$ e, portanto a^2 é par. Segue da proposição anterior, item (b), que a também é par. Portanto existe $k \in \mathbb{Z}$ tal que $a = 2k$. Mas

$$\left.\begin{array}{l} a^2 = 2b^2 \\ a = 2k \end{array}\right\} \implies 2b^2 = 4k^2 \implies b^2 = 2k^2.$$

Portanto b^2 é par e, pela proposição anterior, item (b), b também é par. Mas isto implica que $\frac{a}{b}$ é redutível (pois a e b são divisíveis por 2) o que é uma contradição. Logo não existe $\frac{a}{b} \in \mathbb{Q}$ tal que $\left(\frac{a}{b}\right)^2 = 2$. □

Agora, iremos definir o que é um Corpo Ordenado Completo e suas consequências.

Definição 4.31 (Corpo Ordenado Completo)**.**

- *Um subconjunto A de um corpo ordenado $(\mathbb{T}, +, \cdot, \leq)$ será limitado superiormente, se existir $L \in T$ tal que $a \leq L$, para todo $a \in A$. Neste caso, L será chamado limitante superior de A.*

- *Se A for um conjunto limitado superiormente, um número $sup(A) \in T$ será chamado o supremo de A se for o menor limitante superior de A. Isto quer dizer que $a \leq sup(A)$, para todo $a \in A$, e se $\mathbb{T} \ni f < sup(A)$, então existirá $a \in A$ tal que $f < a$.*

- *Um corpo para o qual todo subconjunto limitado superiormente possui supremo será chamado um corpo ordenado completo.*

Nem todo subconjunto limitado superiormente de $\mathbb{Q}$ tem supremo em $\mathbb{Q}$. Por exemplo, o conjunto $\{x \in \mathbb{Q} : x^2 < 2\}$ é limitado superiormente mas não possui supremo em $\mathbb{Q}$. Logo $\mathbb{Q}$ é um corpo ordenado que não é completo. Por outro lado, $\mathbb{R}$ é um corpo ordenado completo por construção e pelas propriedades provadas na seção anterior. Logo, podemos enunciar o seguinte teorema.

Teorema 4.32. *A quádrupla $(\mathbb{R}, +, \cdot, \leq)$ com as operações de adição, multiplicação e a relação de ordem total $(\leq)$ definidas na seção anterior, é um corpo ordenado completo.*

Finalmente, a cada corte $\alpha \in \mathbb{R}$, associamos seu supremo, o qual também denotaremos por α. Com esta identificação, em vez de considerarmos $\mathbb{R}$ como conjunto de cortes, os quais, por sua vez, são subconjuntos de $\mathbb{Q}$, consideramos $\mathbb{R}$ como o conjunto dos elementos que são supremos de cortes. Fazendo isso, temos $\mathbb{R} \supset \mathbb{Q}$ e todo número real que não é racional é dito irracional (por exemplo, $\sqrt{2}$ é irracional, já que é supremo de um corte que não é um corte racional). Com isso, temos o conjunto dos números reais, $\mathbb{R}$, como aprendemos do Ensino Médio, mas, agora, com suas operações de adição e multiplicação (e também subtração, dada por $\alpha - \beta = \alpha + (-\beta)$, e divisão, dada por $\frac{\alpha}{\beta} = \alpha \cdot \frac{1}{\beta}$) bem como suas propriedades, devidamente justificadas.

CAPÍTULO

A

APÊNDICE

Nesta seção, iremos apresentar tópicos que irão complementar nossa argumentação para não prejudicar/sobrecarregar os capítulos da dissertação. Iniciaremos o conceito de relação. Este conceito nos oferece a base para a compreensão do conceito de relação de ordem que está na Seção 1.4.

A.1 Relações

Inicialmente, vamos considerar o conjunto $X \times Y$, em que X é um conjunto das meninas e Y é um conjunto dos meninos. Suponhamos que Fernanda pertença a X e Thiago pertença a Y. Quando falamos "Fernanda é namorada de Thiago" estamos dizendo que Fernanda está relacionada com Thiago pela relação "ser namorada de", ou seja, o par ordenado (x,y), em que x = Fernanda e y = Thiago, pertence à relação. Note que o par (y,x) não pertence à relação, pois Thiago não é namorada de Fernanda. Se a relação fosse "ser casado com", então ambos os pares (x,y) e (y,x) estariam na relação. Formalmente temos a seguinte definição de relação.

Definição A.1. *Uma relação entre dois conjuntos não vazios X e Y, denotada por $\mathscr{R}(X,Y)$, ou simplesmente por $\mathscr{R}$, é um subconjunto do produto cartesiano de X por Y, $X \times Y$. Se um par $(x,y) \in \mathscr{R}$, diremos que x está relacionado com y, pela relação $\mathscr{R}$ e escreveremos $x\mathscr{R}y$. Se $\mathscr{R}(X,Y)$ for uma relação entre X e Y, diremos que $\mathscr{R}^{-1} = \{(y,x) \in Y \times X : x\mathscr{R}y\}$ é a relação inversa de $\mathscr{R}$. Se $X = Y$, então $\mathscr{R}(X,X)$ será dita uma relação sobre X.*

Exemplo A.2.

- *Sejam $X = \{1,2,3\}$ e $Y = \{a,b,c,d\}$. Definimos, a seguir, 3 relações:*

  $\mathscr{R}_1 = \{(1,a),(1,b),(3,c)\}$;

  $\mathscr{R}_2 = \{(2,a),(2,b),(1,a),(1,b),(3,a),(3,b)\}$;

  $\mathscr{R}_3 = \emptyset$.

- *Seja* $X = \{a,b,c\}$. *Definimos, sobre* X, *as relações:*

  $\mathscr{R}_1 = \{(a,a),(b,b),(c,c)\}$;

  $\mathscr{R}_2 = \{(a,a),(a,b),(b,a),(b,b),(c,b),(c,c)\}$;

  $\mathscr{R}_3 = X \times X$.

Mencionamos, a seguir, as propriedades mais importantes que uma relação $\mathscr{R}$ *sobre um conjunto* X *pode satisfazer.*

Definição A.3. *Seja* $\mathscr{R}$ *uma relação sobre um conjunto* X *não vazio. Diremos que:*

- $\mathscr{R}$ *é reflexiva, se a condição* ($x\mathscr{R}x$) *for verdadeira para todo* $x \in X$, *ou seja, se para todo* $x \in X$, *então teremos* $(x,x) \in \mathscr{R}$;
- $\mathscr{R}$ *é simétrica, se a condição* ($x\mathscr{R}y \Longrightarrow y\mathscr{R}x$) *for verdadeira para quaisquer* x, $y \in X$, *ou seja, para quaisquer* x, $y \in X$, *se* $(x,y) \in \mathscr{R}$, *então* $(y,x) \in \mathscr{R}$;
- $\mathscr{R}$ *é transitiva, se a condição* ($x\mathscr{R}y$ *e* $y\mathscr{R}z \Longrightarrow x\mathscr{R}z$) *for verdadeira para quaisquer* x, y, $z \in X$, *ou seja, se para quaisquer* x, y, $z \in X$, *se* $(x,y) \in \mathscr{R}$ *e* $(y,z) \in \mathscr{R}$, *então* $(x,z) \in \mathscr{R}$.
- $\mathscr{R}$ *é antissimétrica, se a condição* ($x\mathscr{R}y$ *e* $y\mathscr{R}x \Longrightarrow x = y$) *for verdadeira para quaisquer* x, $y \in X$, *ou seja, se para quaisquer* x, $y \in X$, *se* $(x,y) \in \mathscr{R}$ *e* $(y,x) \in \mathscr{R}$, *então* $x = y$.

Exemplo A.4.

- *Seja* X *um conjunto qualquer. A relação* $\phi = \{(x,x);\ x \in X\}$ *é uma relação sobre* X *que é reflexiva, simétrica, antissimétrica e transitiva. Esta é chamada a relação identidade ou a diagonal.*
- *Seja* X *um conjunto qualquer. O produto cartesiano de* X *por* X *é uma relação sobre* X *que é reflexiva, simétrica e transitiva. Tal relação não é antissimétrica.*
- *Seja* $X = \{a,b,c\}$ *e consideremos as seguintes relações:*

  $\mathscr{R}_1 = \{(a,a),(b,b),(c,c),(a,b)\}$ *é uma relação reflexiva, antissimétrica e transitiva. Não é simétrica.*

  $\mathscr{R}_2 = \{(a,a),(b,b),(a,b)\}$ *é uma relação simétrica e transitiva, que não é reflexiva e nem antissimétrica.*

  $\mathscr{R}_3 = \{(a,a),(b,b),(a,b),(b,a),(b,c)\}$ *é uma relação que não é simétrica, nem transitiva, nem reflexiva e nem antissimétrica.*
- *Seja* F *uma família de conjuntos não vazios. Para* X, $Y \in F$, *a relação "*X *está contido em* Y*" é uma relação reflexiva, antissimétrica e transitiva. Tal relação não é simétrica.*
- *Seja* F *o conjunto das proposições. Para* p, $q \in F$, *a relação "se* p *então* q*" é uma relação reflexiva e transitiva, que não é simétrica e nem antissimétrica.*

A.2 Relações de Equivalência e Partições

O conceito de relação de equivalência aparece cotidianamente. Por exemplo, em uma farmácia, podemos classificar como equivalentes os remédios que têm o mesmo princípio ativo; em uma escola, podemos classificar como equivalentes os alunos que estão em uma mesma turma, etc. Assim sendo, faremos uma formalização das ideias por trás do conceito de relação de equivalência.

Definição A.5. *Uma relação $\mathscr{R}$ sobre um conjunto X será dita uma relação de equivalência sobre X, se $\mathscr{R}$ for reflexiva, simétrica e transitiva.*

Alguns exemplos de relações de equivalências são apresentados abaixo.

Exemplo A.6. *A relação "igual a", denotada pelo símbolo "=", no conjunto dos naturais $\mathbb{N}$ satisfaz:*

(i) *Para todo x, vale $x = x$.*

(ii) *Para quaisquer x, $y \in \mathbb{N}$, se $x = y$, então $y = x$.*

(iii) *Para quaisquer x, y, $z \in \mathbb{N}$, se $x = y$ e $y = z$, então $x = z$.*

Exemplo A.7. *Seja X o conjunto de todas as retas no espaço euclidiano tridimensional. A relação de paralelismo entre duas retas é uma relação de equivalência, pois satisfaz:*

(i) *Para todo $x \in X$ $x \parallel x$.*

(ii) *Para quaisquer x, $y \in X$, se $x \parallel y$, então $y \parallel x$.*

(iii) *Para quaisquer x, y, $z \in X$, se $x \parallel y$ e $y \parallel z$, então $x \parallel z$.*

Relações de equivalências estão diretamente relacionadas com a noção de partição de um conjunto.

Definição A.8. *Seja X um conjunto não vazio. Dizemos que uma família F de subconjuntos não vazios de X é uma partição de X, se as seguintes afirmações forem verdadeiras:*

1. *dois elementos quaisquer de F ou são iguais ou são disjuntos;*

2. *a união dos elementos de F é igual a X.*

Exemplo A.9. *Exemplos de Partições:*

- *A família $F = \{\{1\},\{2\},\{3,4\}\}$ é uma partição do conjunto $X = \{1,2,3,4\}$;*

- *A família $F = \{1,\{\emptyset\}\}$ é uma partição do conjunto $X = \{1\}$.*

A.3 Classes de Equivalência

A seguir, vamos definir classe de equivalência e apresentar exemplos.

Definição A.10. *Sejam M um conjunto não vazio, $R \subset M \times M$ uma relação de equivalência em M e $m \in M$. Definimos a classe de equivalência do elemento $m \in M$, denotada por $\overline{m}$, como sendo o conjunto*

$$\overline{m} := \{x \in M : (x,m) \in R\}.$$

Exemplo A.11. *Seja M uma caixa que contém peças de um jogo de xadrez e peguemos sacolas plásticas e separamos as peças nas sacolas segundo a relação de equivalência: duas peças serão equivalentes, se forem da mesma cor. Cada sacola, neste caso, comportará apenas peças de mesma cor. Cada sacola representará uma classe de equivalência.*

A seguir, definiremos conjunto quociente.

Definição A.12. *Sejam M um conjunto não vazio e $R \subset M \times M$ uma relação de equivalência em M. Definimos o conjunto quociente de M por R, denotado M/R, por:*

$$M/R := \{\overline{m} \in M : x \in M\}.$$

Exemplo A.13. *Sejam $M = \{a,b,c\}$ e a relação de equivalência $R \subset M \times M$ dada por:*

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

Para este caso, temos:

- $\overline{a} = \{a,b\}$;
- $\overline{b} = \{a,b\}$;
- $\overline{c} = \{c\}$;
- $M/R = \{\{a,b\},\{c\}\}$.

Exemplo A.14. *Relembramos o exemplo do conjunto M, da caixa de xadrez. O conjunto de sacolas plásticas com as peças de xadrez separadas por cor e arrumadas dentro da sacola representa o conjunto quociente M/R.*

REFERÊNCIAS

[1] Fernanda, M. A importância do número zero. *Por: Redação Super. Edição 163, abr, 2001. Revista Superinteressante. Diposnível: goo.gl/sUdQCP. Acesso em 14/06/2018. Citado na página 2.*

[2] FREIWALD, R. http://www.math.wustl.edu/ freiwald/310integers. *Washington University - St. Louis - XXXX. Citado nas páginas 13 e 14.*

[3] RUDIN, W. Principles of Mathematical Analysis. *1^a Edition - University of Wisconsin - Madison - 1976. Citado nas páginas i e 33.*

[4] LIMA, E. L. Análise Real. *8^a Edição - Vol. I - Funções de Uma Variável - Rio de Janeiro - 2006. Citado na página 4.*

[5] DEDEKIND, Dover Publications, Inc., Nova York. Nenhuma citação no texto.

[6] DIAS, I E GODOY, S. Elementos de Matemática. *Notas de aula - Universidade de São Paulo (ICMC), São Carlos 2012. Citado nas páginas 14, 15, 23, 25, 27, 29, 31 e 32.*

[7] HEATH, T.L. Euclid: The Thirteen Books of The Elements. *School of Mathematics and Statistics, University of St. Andrews, Escócia. 2006. Disponível: goo.gl/ANaoDb. Acesso em 14/06/2018. Citado na página i.*

[8] LIMA, E. L. Números e Funções Reais. *1^a Ed. Sociedade Brasileira de Matemática, Rio de Janeiro, 2013. Citado nas páginas 1, 2 e 3.*

[9] MEDEIROS, L. A.; MALTA, S. M.; LIMACO, J.; CLARK, H.R. Lições de Análise Matemática. *Rio de Janeiro: UFRJ/IM, 2005. Citado na página i.*

[10] SCHWARTZ, R. Dedekind Cuts.*, Mathematics Department, Brown University, Estados Unidos. 2014. Disponível: goo.gl/8tBZsU. Acesso em 14/06/2018. Citado na página i.*