UNIVERSIDADE DO ESTADO DE SANTA CATARINA - UDESC
CENTRO DE CIÊNCIAS TECNOLÓGICAS - CCT
CURSO DE LICENCIATURA EM MATEMÁTICA

MATEUS SCHROEDER DA SILVA

DOS AXIOMAS DE PEANO AOS CORTES DE DEDEKIND: UMA FORMALIZAÇÃO PARA OS CONJUNTOS NUMÉRICOS

JOINVILLE - SC

2023

MATEUS SCHROEDER DA SILVA

DOS AXIOMAS DE PEANO AOS CORTES DE DEDEKIND: UMA FORMALIZAÇÃO PARA OS CONJUNTOS NUMÉRICOS

Trabalho de conclusão de curso apresentado como requisito parcial para obtenção do título de licenciado em Matemática pelo curso de Licenciatura em Matemática do Centro de Ciências Tecnológicas - CCT, da Universidade do Estado de Santa Catarina - UDESC.
Orientador: Prof. Me. Marnei Luis Mandler

JOINVILLE - SC

2023

MATEUS SCHROEDER DA SILVA

DOS AXIOMAS DE PEANO AOS CORTES DE DEDEKIND: UMA FORMALIZAÇÃO PARA OS CONJUNTOS NUMÉRICOS

Trabalho de conclusão de curso apresentado como requisito parcial para obtenção do título de licenciado em Matemática pelo curso de Licenciatura em Matemática do Centro de Ciências Tecnológicas - CCT, da Universidade do Estado de Santa Catarina - UDESC.
Orientador: Prof. Me. Marnei Luis Mandler

BANCA EXAMINADORA

Prof. Me. Marnei Luis Mandler
DMAT/CCT/UDESC

Membros:

Prof. Dr. Luis Gustavo Longen
DMAT/CCT/UDESC

Prof. Dr. Sidnei Furtado Costa
DMAT/CCT/UDESC

Joinville, 20 de junho de 2023.

À minha mãe

AGRADECIMENTOS

Agradeço à minha mãe, sem ela não teria sido possível concluir este curso. Agradeço também a todos que ajudaram direta ou indiretamente na elaboração do trabalho. Em especial aos meus padrinhos, aos desenvolvedores das ferramentas utilizadas na elaboração do trabalho, aos contribuintes do LaTeX, ao Overleaf, e da comunidade Debian.

Consolo para os principiantes

Vejam a criança, os porcos grunhem em torno dela,
Abandonada a si mesma, os artelhos encolhidos!
Só sabe chorar e chorar mais ainda -
Será que um dia vai aprender a ficar de pé e a caminhar?
Não tenham medo! Muito breve, penso,
Poderão ver a criança dançar!
Logo que conseguir manter-se de pé,
Haverão de vê-la caminhando de cabeça para baixo.

Nietzsche

RESUMO

Este trabalho tem como objetivo principal estender o conceito de número natural até os números reais, e dar significado às inclusões $\mathbb{N} \subset \mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R}$, em que cada inclusão será compreendida por meio da existência de uma função que é aditiva, multiplicativa e que preserva a relação de ordem. A metodologia utilizada é a pesquisa bibliográfica. O estudo inicia com algumas definições e proposições de álgebra. Em seguida é formalizado o conjunto dos números naturais, através dos axiomas de Peano. O conjunto dos números inteiros é obtido por meio de classes de equivalência de uma relação com números naturais. A construção dos números racionais é feita também por classes de equivalência, desta vez com uma relação de números inteiros. Para estender o conjunto $\mathbb{Q}$ e obter $\mathbb{R}$, fazemos o desenvolvimento via Cortes de Dedekind. É provado que $\mathbb{R}$ é um corpo ordenado completo, não enumerável e é único, a menos de isomorfismo.

Palavras-chave: Números. Conjuntos Numéricos. Cortes de Dedekind.

ABSTRACT

The main objective of this work is to extend the concept of natural number up to the concept of real number, and then to give meaning to the following inclusions $\mathbb{N} \subset \mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R}$, where each inclusion will be understood by means of the existence of a function that is additive, multiplicative and order preserving. The methodology is bibliographic research. The study begins with some algebra definitions and propositions. Then the set of natural numbers is formalized using Peano axioms. The set of integers is obtained through equivalence classes of a relation of natural numbers. The construction of rationals is done again by equivalence classes, this time with a relation of integers. We extend from $\mathbb{Q}$ to $\mathbb{R}$ through Dedekind Cuts. It is proven that $\mathbb{R}$ is a complete ordered field, and it is unique, except by isomorphisms.

Keywords: Numbers. Number sets. Dedekind Cuts.

LISTA DE ILUSTRAÇÕES

LISTA DE SÍMBOLOS

$\mathbb{N}$	Conjunto dos números naturais (sem o zero)
$\mathbb{Z}$	Conjunto dos números inteiros
$\mathbb{Q}$	Conjunto dos números racionais
$\mathbb{R}$	Conjunto dos números reais
$\mathbb{A}^*$	Conjunto $A \setminus \{0\}$ (retira o zero), sendo A um conjunto qualquer
$\mathbb{Z}_+^*$	Conjunto dos números inteiros positivos
$\mathbb{Z}_+$	Conjunto dos números inteiros não negativos
$\mathbb{Z}_-^*$	Conjunto dos números inteiros negativos
$\mathbb{Z}_-$	Conjunto dos números inteiros não positivos
$\mathbb{Q}_+^*$	Conjunto dos números racionais positivos
$\mathbb{Q}_+$	Conjunto dos números racionais não negativos
$\mathbb{Q}_-^*$	Conjunto dos números racionais negativos
$\mathbb{Q}_-$	Conjunto dos números racionais não positivos
$:=$	O que está à esquerda do símbolo é, por definição, igual ao que está à direita
$\wedge$	Conjunção (E) das proposições, uma à esquerda e outra à direita.
$\vee$	Disjunção (OU) das proposições, uma à esquerda e outra à direita.
$\subset$	O conjunto à esquerda é subconjunto do conjunto da direita.
$\exists! x$	Existe um único x

SUMÁRIO

1. INTRODUÇÃO

Os números fazem parte do dia-a-dia das pessoas no mundo contemporâneo. Não apenas pela sua utilização nas ciências naturais, onde são usados para explicar fenômenos naturais. Também são utilizados para o estudo de fenômenos das chamadas ciências humanas. Além disso, os números aparecem como uma ferramenta para o manuseio do dinheiro e do controle do tempo, coisas que na sociedade contemporânea são essenciais.

Na prática, normalmente não nos perguntamos o que é um número, e por que as operações com números funcionam da maneira como funcionam. Por outro lado, é essencial para um professor de matemática saber porquê podemos usar números de determinadas maneiras e não de outras, as limitações que cada tipo de número tem, face a cada tipo de problema. Um caso essencial é que os números racionais não são suficientes ou adequados para medir a diagonal de um quadrado de lado 1. Por outro lado, a natureza intrínseca do número não é tão importante para nós, porque a pergunta "o que é um número" é mais filosófica do que matemática.

A partir das limitações dos conjuntos numéricos utilizados, surge a necessidade humana de estender o conceito de número. Entender como essas extensões funcionam, em especial as extensões do conceito de número natural para os números inteiros e para os números racionais é importante para um professor de matemática. Nesse contexto, o objetivo principal deste trabalho é apresentar as extensões do conceito de número, para poder justificar a maneira como operamos com eles cotidianamente. Um dos objetivos específicos é apresentar a justificativa para as inclusões $\mathbb{N} \subset \mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R}$. Num sentido análogo, pretende-se mostrar que o conjunto $\mathbb{R}$ é único.

O trabalho iniciará com os axiomas de Peano, e terminará com o estudo dos números reais. Escolhemos iniciar com os axiomas de Peano por dois motivos: o primeiro é por causa da simplicidade de trabalhar com os axiomas de Peano, o segundo é devido à necessidade de escolher um ponto de partida para iniciar o trabalho. Poderíamos ter iniciado desenvolvendo uma teoria de conjuntos suficiente para poder provar os axiomas de Peano, mas seria necessário para isso, ainda assim, assumir a lógica e os axiomas da teoria de conjuntos. Mas se fosse optado por iniciar com a própria lógica ou pela teoria de conjuntos, o trabalho perderia seu foco principal, que é e justificar propriedades relacionadas aos diferentes conjuntos numéricos. Uma abordagem para a dedução dos

axiomas de Peano a partir da teoria de conjuntos pode ser encontrada em Suppes (1972).

A metodologia usada no desenvolvimento deste trabalho é a pesquisa bibliográfica, que incluirá em especial os temas de aritmética, álgebra e análise real. Para o tema de aritmética, as referências principais são Ferreira (2013) e Domingues (2009). A referência principal para álgebra é Domingues e Iezzi (2018). As referências principais para análise real são Guidorizzi (2018) e Lima (2016).

O trabalho está dividido em sete capítulos, começando com esta introdução. O segundo capítulo contém definições e teoremas básicos de álgebra, que têm o objetivo de centralizar definições que são usadas ao longo do restante do texto. O terceiro capítulo aborda o conjunto dos números naturais, iniciando pelos axiomas de Peano, depois definimos uma adição, uma multiplicação e uma relação de ordem nesse conjunto, e provamos algumas propriedades aritméticas básicas. Vale destacar que neste trabalho, o 0 (zero) não será considerado número natural, pois pretende-se mostrar que as extensões para os conjuntos dos números inteiros, racionais e reais pode ser feita também com essa escolha. As bibliografias da área normalmente preferem incluir o 0, pois isso simplifica a obtenção de alguns resultados. O quarto capítulo trabalha com os números inteiros, que são obtidos por meio de classes de equivalência de uma relação adequadamente estabelecida com números naturais. São definidas uma adição, uma multiplicação e uma relação de ordem, e provadas algumas propriedades básicas. No quinto capítulo estudamos os números racionais, que são construídos por meio de classes de equivalência de uma relação envolvendo números inteiros. Novamente, são definidas uma adição, uma multiplicação e uma relação de ordem, e provada propriedades aritméticas básicas. O sexto capítulo desenvolve os números reais. A literatura clássica de análise aborda dois métodos principais para a construção dos números reais, que são via Cortes de Dedekind e via Sequências de Cauchy. Optamos por seguir a abordagem de cortes de Dedekind, pois temos uma familiaridade maior com o manuseio de conjuntos, do que com sequências. O sétimo capítulo apresenta dois resultados importantes sobre os números reais, o primeiro deles é a sua não enumerabilidade. O segundo estabelece a unicidade do conjunto dos números reais, num contexto de isomorfismos de corpos ordenados completos.

2. ÁLGEBRA BÁSICA

Neste capítulo apresentaremos as definições usadas ao longo do texto e também apresentaremos alguns resultados importantes que, embora simples, podem ser generalizados para os conjuntos (numéricos) que trabalharemos. A referência principal para este capítulo é Domingues e Iezzi (2018).

Assumimos familiaridade com a Teoria dos Conjuntos e com os símbolos e ideias básicas da lógica tais como implicação, conjunção e disjunção. O objetivo aqui é colocar uma fundamentação inicial mais sólida para os capítulos subsequentes, para que o conteúdo principal (a construção dos conjuntos numéricos) fique melhor consolidada.

2.1. Conjuntos e relações

Neste primeiro momento vamos abordar conjuntos, pares ordenados e relações, e veremos algumas definições básicas. É claro que no estudo mais profundo de conjuntos precisaríamos de mais axiomas e outras definições, mas foge do escopo do nosso trabalho.

Definição 2.1. *Dados um conjunto não vazio A e $a, b \in A$, definimos o par ordenado (a, b) como o conjunto $\{\{a\}, \{a, b\}\}$.*

O elemento a dizemos que está na primeira entrada do par ordenado, e o b está na segunda entrada do par ordenado.

Essa definição de par ordenado visa "corrigir" o problema que os conjuntos $\{a, b\}$ e $\{b, a\}$, com b diferente de a, são o mesmo conjunto. A Definição 2.1 é satisfatória para esse objetivo, mas para nós o que irá importar é o lema a seguir:

Lema 2.1. *Dois pares ordenados (a, b) e (c, d) são iguais se, e somente se, $a = c$ e $b = d$.*

A demonstração do Lema 2.1 pode ser encontrada em Suppes (1972, p. 42).

Exemplo 2.1. Consideremos os pares ordenados $(1, 2)$ e $(2, 1)$. Eles não são iguais porque $1 \neq 2$ e $2 \neq 1$. Podemos observar também que os pares ordenados $(1, 2)$ e $(1, 1)$ não são iguais pois embora $1 = 1$, $2 \neq 1$, e basta que uma coordenada seja diferente para que o par como um todo, seja diferente.

Definição 2.2. *Dados dois conjuntos não vazios, A, B, o produto cartesiano de A por B, denotado por $A \times B$, é o conjunto de todos os pares ordenados (a, b) onde $a \in A$ e $b \in B$, isto é, $A \times B = \{(a, b) : a \in A \wedge b \in B\}$.*

Exemplo 2.2. Consideremos os conjuntos $A = \{1, 5, 6\}$ e o conjunto $B = \{1, 3, 4, 9\}$. Temos que

$$A \times B = \{(1,1), (1,3), (1,4), (1,9), (5,1), (5,3), (5,4), (5,9), (6,1), (6,3), (6,4), (6,9)\}.$$

Já se

$$A = \{-1, 3, 4\} \text{ e } B = \{0, 5\},$$

então

$$A \times B = \{(-1,0), (-1,5), (3,0), (3,5), (4,0), (4,5)\}.$$

Definição 2.3. *Uma relação binária R num conjunto A é qualquer subconjunto do produto cartesiano $A \times A$, isto é, $R \subset A \times A$.*

Frequentemente utiliza-se a notação aRb para indicar que o par ordenado $(a, b) \in R$.

Exemplo 2.3. No conjunto $\mathbb{R}$ a relação binária definida por uma função quadrática, onde a parábola $P \subset \mathbb{R} \times \mathbb{R}$ é $P = \{(a, a^2) : a \in \mathbb{R}\}$. Embora nesses casos de funções não seja comum utilizar a notação $(a, a^2) \in P$ ou aPa^2.

Exemplo 2.4. Ainda mais importante é a desigualdade, que em geral, ao invés de trabalhar com pares ordenados (a, b), normalmente se opta pela utilização do símbolo da relação entre os elementos $a < b$.

Definição 2.4. *Seja A um conjunto não vazio e seja R uma relação sobre A. Dizemos que a relação R tem a propriedade:*

(i) Reflexiva, quando para qualquer $a \in A$ valer aRa;

(ii) Simétrica, quando para quaisquer $a, b \in A$, valer $aRb \implies bRa$.

(iii) Antissimétrica, quando para quaisquer $a, b \in A$, valer $(aRb \wedge bRa) \implies a = b$;

(iv) Transitiva, quando para quaisquer $a, b, c \in A$, valer $(aRb \wedge bRc) \implies aRc$;

(v) Totalidade, quando para quaisquer $a, b \in A$, valer $aRb \vee bRa$.

Trabalharemos com dois tipos especiais de relações: as relações de equivalência e as relações de ordem. As relações de equivalência são necessárias para a criação dos conjuntos $\mathbb{Z}$ e $\mathbb{Q}$. A relação de ordem aparece em todos os conjuntos mas é nos números reais que sua apresentação será necessária, considerando o desenvolvimento deste trabalho.

Definição 2.5. *Uma relação R é chamada de relação de equivalência, quando possuir as seguintes propriedades:*

(i) reflexiva;

(ii) simétrica;

(iii) transitiva.

Exemplo 2.5. Seja $A = \{0, 1, 2, 3, 4, 5, 6, 7, 8\}$. A relação

$$\begin{aligned} R = \{&(0,0),(0,3),(0,6),(3,0),(3,3),(3,6),(6,0),(6,3),(6,6),\\ &(1,1),(1,4),(1,7),(4,1),(4,4),(4,7),(7,1),(7,4),(7,7),\\ &(2,2),(2,5),(2,8),(5,2),(5,5),(5,8),(8,2),(8,5),(8,8)\} \end{aligned}$$

é uma relação de equivalência, pois cumpre os critérios da Definição 2.5.

Definição 2.6. *Seja R uma relação de equivalência num conjunto A não vazio e seja $a \in A$ um elemento fixado arbitrariamente. O conjunto*

$$\bar{a} = \{x \in A : xRa\}$$

chama-se classe de equivalência de a pela relação R.

Exemplo 2.6. Podemos citar o resto da divisão em $\mathbb{N}$. A divisão euclidiana de um número a por um número b tinha resto r quando $n \cdot b + r = a$ para algum natural n. Consideramos para este exemplo que $0 \in \mathbb{N}$. Se fixarmos $b = 4$, e atribuindo valores para a obtemos:

$$\begin{aligned} a &= 0 = 0 \cdot 4 + 0,\\ a &= 1 = 0 \cdot 4 + 1,\\ a &= 2 = 0 \cdot 4 + 2,\\ a &= 3 = 0 \cdot 4 + 3,\\ a &= 4 = 1 \cdot 4 + 0,\\ a &= 5 = 1 \cdot 4 + 1,\\ a &= 6 = 1 \cdot 4 + 2,\\ a &= 7 = 1 \cdot 4 + 3,\\ a &= 8 = 2 \cdot 4 + 0,\\ a &= 9 = 2 \cdot 4 + 1,\\ a &= 10 = 2 \cdot 4 + 2,\\ a &= 11 = 2 \cdot 4 + 3. \end{aligned}$$

Observando essas divisões podemos perceber que são 4 números possíveis para r, com $r \in \{\, 0, 1, 2, 3 \,\}$. Assim temos 4 classes de equivalência, que são os valores possíveis para o resto r, que são as classes $\bar{0}, \bar{1}, \bar{2}$ e $\bar{3}$. A classe de resto do 4, que é $\bar{4}$, é a mesma classe do $\bar{0}$. Vamos considerar $r = 3$, e vamos expressar essa classe como um conjunto, temos $\bar{3} = \{\, a \in \mathbb{N} : aR3 \,\}$, onde R é a relação de equivalência sobre $\mathbb{N}$ cujos elementos são (m, n) com $(m, n) \in \mathbb{N} \times \mathbb{N}$ e m, n tem o mesmo resto na divisão por 4.

Teorema 2.1. *Seja R uma relação de equivalência em um conjunto não vazio A e sejam a, b elementos quaisquer de A, então:*

(i) $a \in \bar{a}$;

(ii) $\bar{a} = \bar{b} \iff aRb$;

(iii) $\bar{a} \neq \bar{b} \implies \bar{a} \cap \bar{b} = \emptyset$.

Demonstração: Seja R uma relação de equivalência. Tem-se que

(i) $a \in A$ e como R é reflexiva, vale aRa, assim $a \in \bar{a}$.

(ii) Para a ida, pelo item anterior temos $a \in \overline{a}$ logo $a \in \overline{b} = \overline{a}$, assim aRb. Para provar a volta, temos que aRb, e por contradição suponhamos sem perda de generalidade, que exista $c \in \bar{a} \setminus \bar{b}$. Daí temos cRa e aRb. Como R é transitiva temos cRb, desse modo $c \in \bar{b}$ o que é uma contradição.

(iii) Por contradição suponhamos que $\bar{a} \cap \bar{b} \neq \emptyset$. Assim existe $c \in \bar{a} \cap \bar{b}$, então $cRa \wedge cRb$. Como R é simétrica, vale $aRc \wedge cRb$, e como também é transitiva tem-se que aRb, pelo item anterior $\bar{a} = \bar{b}$, o que conclui a demonstração.

■

Definição 2.7. *Seja R uma relação de equivalência num conjunto A. O conjunto constituído das classes de equivalência em A pela relação R é denotado por A/R e denominado conjunto quociente de A por R. Assim*

$$A/R = \{\bar{a} : a \in A\}.$$

O conjunto quociente serve para particionar o conjunto em subconjuntos distintos. No Exemplo 2.6 consideramos a divisão por 4 no conjunto dos números naturais. Notamos que formamos 4 classes de equivalência distintas, e qualquer número natural pertence à uma, e apenas uma classe de equivalência.

Exemplo 2.7. No Exemplo 2.6, se formos utilizar essa notação, usamos:

$$\mathbb{N}/R = \{\, \bar{a} : a \in \mathbb{N} \,\} = \{\, \bar{0}, \bar{1}, \bar{2}, \bar{3} \,\}.$$

Definição 2.8. *Seja R uma relação sobre A. Ela é chamada de relação de ordem parcial se valer as propriedades:*

(i) Reflexiva;

(ii) Antissimétrica;

(iii) Transitiva.

Além da relação de ordem habitual, dada por $aRb \iff a \leq b$, podemos citar em $\mathbb{N}$ a relação de ordem parcial que é obtida pela divisão, isto é, $aRb \iff a|b$ (a divide b). Note que a divide a, se $a|b$ e $b|c$, então $a|c$, e que $a|b \wedge b|a \implies a = b$. A prova dessas afirmações será omitida neste texto, mas pode ser encontrada em Domingues (2009, p. 52).

Notação: Utilizaremos a notação $a < b$ quando $a \leq b$ mas $a \neq b$. Também utilizaremos a notação $b \geq a$ e $b > a$ quando $a \leq b$ e $a < b$, respectivamente.

Definição 2.9. *Sejam $a, b \in A$, os elementos a e b são ditos comparáveis através da relação de ordem parcial $\leq$, caso $a \leq b$ ou caso $b \leq a$.*

Definição 2.10. *Uma relação de ordem parcial $\leq$ sobre um conjunto A é chamada de relação de ordem total caso quaisquer elementos de A sejam comparáveis através da relação $\leq$.*

Considerando a estrutura do nosso trabalho, com a Definição 2.10 esclarecemos que utilizaremos apenas relações de ordem que são totais, em especial as relações de ordem usuais em $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$ e $\mathbb{R}$ são todas relações de ordem totais.

Outra coisa que pode ser dito à respeito das relações, é que usaremos os significados usuais para $=, <, \leq$. Também trabalharemos com a notação usual $a \leq b$ ao invés de colocar $(a, b) \in \leq$, que embora correto, fica estranho.

Definição 2.11. *Seja A um conjunto numérico, e sejam $a, b \in A$. Considere uma relação de ordem parcial $\leq$ sobre A, ela é dita tricotômica, quando para quaisquer $a, b \in A$, valer um e apenas um caso dos a seguir: ou $a < b$ ou $b < a$ ou $a = b$.*

Definição 2.12. *Sejam A e E conjuntos, com $\emptyset \neq A \subset E$, e $\leq$ uma relação de ordem parcial sobre E. Um elemento L de E é chamado de cota superior de A se para qualquer elemento $a \in A$ vale $a \leq L$.*

Analogamente definimos cota inferior, como na definição a seguir:

Definição 2.13. *Sejam A e E conjuntos, com $\emptyset \neq A \subset E$, e $\leq$ uma relação de ordem parcial sobre E. Um elemento l de E é chamado de cota inferior de A se para qualquer elemento $a \in A$ vale $l \leq a$.*

Exemplo 2.8. Considere o conjunto $A = \{ 1, 2, 3, 4, 5 \} \subset \mathbb{N}$. Esse conjunto é limitado superiormente pelo 5, e inferiormente pelo 1. Notemos que os números naturais $6, 7, 8$ também são cotas superiores desse conjunto. Por outro lado, o número $-1 \in \mathbb{Z}$ é uma cota inferior que não é um número natural.

Definição 2.14. *Sejam A e E conjuntos, com $\emptyset \neq A \subset E$, e $\leq$ uma relação de ordem parcial sobre E. Um elemento M de A é chamado de máximo de A se para qualquer elemento $a \in A$ vale $a \leq M$, assim, um máximo é uma cota superior que pertence ao conjunto A.*

Definição 2.15. *Sejam A e E conjuntos, com $\emptyset \neq A \subset E$, e $\leq$ uma relação de ordem parcial sobre E. Um elemento m de A é chamado de mínimo de A se para qualquer elemento $a \in A$ vale $m \leq a$, assim, um mínimo é uma cota inferior que pertence ao conjunto A.*

Exemplo 2.9. No Exemplo 2.8 o 1 é mínimo e o 5 é máximo. O 6 é uma cota superior mas não é máximo de A pois $6 \notin A$.

Teorema 2.2. *Seja $A \neq \emptyset$ um subconjunto de um conjunto parcialmente ordenado E. Se existir um máximo para A então esse elemento é único.*

Demonstração: Sejam $\leq$ uma relação de ordem sobre A, e M_1 e M_2 dois máximos de A. Temos $M_1, M_2 \in A$, e também $M_1 \leq M_2$ e $M_2 \leq M_1$. Como uma relação de ordem é antissimétrica, na Definição 2.8, concluí-se que $M_1 = M_2$. ∎

2.2. Operações

Nesta seção apresentaremos algumas definições que tem como objetivo fundamentar o conceito de operação. Intuitivamente o conceito de operação é pegar algum elemento qualquer e fazer alguma coisa sobre ele. Poderíamos citar a operação de negação da lógica, ou a operação de troca de sinal para um número inteiro. Nesses dois casos trata-se de uma operação que utiliza um elemento para chegar em outro elemento (como resultado, resposta).

Nós focaremos nas operações binárias, isto é, que utilizam dois elementos como entradas. Na verdade a nossa definição vai considerar uma operação como sendo exatamente duas entradas, e como será uma função, o resultado será fixo, exato e único. Isso será explicado na Observação 2.1.

Definição 2.16. *Seja A um conjunto arbitrário. Uma operação $*$ sobre A é uma função que a cada $a, b \in A$ associa um único elemento $a * b \in A$, ou seja, associa a cada dois elementos em A a sua imagem $a * b$, que também é um elemento de A.*

Observação 2.1. Anteriormente falamos em fixo, exato e único. Com fixo queremos dizer que se $a * b = c$, o elemento c será fixo se a e b também forem fixos. O elemento c é também único, pois a operação é uma função, e com exato queremos dizer que ele existe, é fixo e é único.

Pela Definição 2.16, a adição em $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$ e $\mathbb{R}$ são operações, sobre cada um desses conjuntos, cada um com sua adição. Por outro lado, a subtração em $\mathbb{N}$ não é uma operação em $\mathbb{N}$ pois $1 - 2 \notin \mathbb{N}$. Também a divisão não é uma operação em $\mathbb{N}$ e em $\mathbb{Z}$, pelo mesmo motivo.

Definição 2.17. *Seja A um conjunto e seja $*$ uma operação em A. Se existir um $\mathfrak{e} \in A$ tal que, para qualquer $a \in A$, valer $\mathfrak{e} * a = a$ dizemos que $\mathfrak{e}$ é elemento neutro à esquerda da operação $*$.*

Por analogia definimos neutro à direita da operação $*$ como $\mathfrak{e}' \in A$ tal que $a * \mathfrak{e}' = a$ para qualquer a em A.

Definição 2.18. *Seja A um conjunto e seja $*$ uma operação sobre A. Dizemos que a operação $*$ tem a propriedade:*

- *associativa, quando para quaisquer $a, b, c \in A$ é válido que $a * (b * c) = (a * b) * c$.*
- *comutativa, quando para quaisquer $a, b \in A$ é válido que $a * b = b * a$.*
- *da existência do elemento neutro, quando existe $\mathfrak{e} \in A$, em que $\mathfrak{e}$ é neutro à esquerda e à direita. Ou seja, $\mathfrak{e} * a = a * \mathfrak{e} = a$, para qualquer $a \in A$.*
- *da existência do elemento simétrico, quando para qualquer $a \in A$ existe algum $d \in A$, em que é válido que $a * d = d * a = \mathfrak{e}$, em que $\mathfrak{e}$ é o elemento neutro de $*$.*
- *do fechamento, quando para quaisquer $a, b \in A$ ocorre que $a * b \in A$.*

Tradicionalmente o neutro da soma é denotado por 0 e o neutro do produto é denotado por 1 (nós faremos da mesma maneira). Além disso, denotaremos o neutro de uma operação $*$ por $\mathfrak{e}$, onde o contexto deixará claro que estaremos nos referindo ao neutro por apenas um lado, caso ainda não esteja provado que se trata de um neutro de ambos os lados. Quando omitido o lado, considera-se que é neutro de ambos os lados.

A propriedade do fechamento na verdade é imediata da definição de operação, colocamos para realçar o fato de que a operação tem imagem em A e não qualquer elemento que não esteja em A.

Observação 2.2. Neste trabalho em geral trabalharemos com duas operações principais para cada um dos conjuntos $\mathbb{N}, \mathbb{Z}, \mathbb{Q}$ e $\mathbb{R}$. Para cada um desses conjuntos haverá uma adição (soma) e uma multiplicação (produto). O elemento simétrico da Definição 2.18 continuará sendo chamado de simétrico caso seja uma adição, e passará a ser chamado de inverso, quando se tratar de multiplicação.

Poderemos omitir os parênteses numa operação associativa, uma vez que poderemos realizar as operações em qualquer ordem.

A Definição 2.18 é uma definição inicial, que utiliza a quantidade mínima de elementos para indicar a propriedade da operação.

Exemplo 2.10. A "comutatividade entre três elementos" pode ser feita assim:

$$a*b*c = a*(b*c) = a*(c*b) = (c*b)*a = (b*c)*a = \\ b*(c*a) = b*(a*c) = b*(c*a) = (c*a)*b = c*a*b.$$

A associatividade pode ser feita de maneira análoga.

Teorema 2.3. *Seja A um conjunto e $*$ uma operação em A. Se existir elemento neutro para $*$, então ele é único.*

Demonstração: Sejam $\mathfrak{e}_1$ e $\mathfrak{e}_2$ dois elementos neutros para $*$. Temos que

$$\mathfrak{e}_1 = \mathfrak{e}_1 * \mathfrak{e}_2 = \mathfrak{e}_2,$$

portanto $\mathfrak{e}_1 = \mathfrak{e}_2$. A primeira igualdade é porque $\mathfrak{e}_2$ é neutro à direita, a segunda igualdade é porque $\mathfrak{e}_1$ é neutro à esquerda. ∎

Em particular, deve ser observada a comutatividade do elemento neutro com qualquer elemento, para uma dada operação.

Teorema 2.4. *Sejam A um conjunto e $*$ uma operação em A. Se $*$ é associativa e tem a propriedade da existência do elemento simétrico, então o simétrico de cada elemento é único.*

Demonstração: Seja $a \in A$, e sejam b, c dois elementos simétricos de a, assim temos que $b * a = \mathfrak{e} = a * c$. Com isso,

$$b = b*\mathfrak{e} = b*(a*c) = (b*a)*c = (a*b)*c = \mathfrak{e}*c = c.$$

∎

Proposição 2.1. *Seja A um conjunto e $*$ uma operação sobre A que seja associativa e admita simétrico. Seja a um elemento de A. O simétrico do simétrico de a é o próprio a.*

Demonstração: Seja $a \in A$. Considere a' o simétrico de a e a'' o simétrico de a'. Assim temos que $a * a' = \mathfrak{e}$, além disso $a' * a'' = \mathfrak{e}$. Com isso

$$a = a * \mathfrak{e} = a * (a' * a'') = (a * a') * a'' = \mathfrak{e} * a'' = a''.$$

■

Definição 2.19. *Sejam A um conjunto, $*$ uma operação em A e b, c elementos de A. Dizemos que um elemento $a \in A$ cumpre a lei do cancelamento à esquerda se vale que*

$$a * b = a * c \implies b = c.$$

Analogamente define-se que um elemento cumpre a lei do cancelamento à direita. E caso o elemento cumpra ambos os tipos de cancelamento à direita e à esquerda para uma mesma operação, dizemos apenas que ele cumpre a lei do cancelamento para aquela operação.

Teorema 2.5. *Seja A um conjunto e $*$ uma operação em A. Se $*$ for associativa e admitir simétrico, então vale a lei do cancelamento para a operação $*$.*

Demonstração: Sejam a, b, c, a' elementos de A, e seja a' simétrico de a para a operação $*$. Temos que

$$a*b = a*c \implies a'*(a*b) = a'*(a*c) = (a'*a)b = (a'*a)*c \implies \mathfrak{e}*b = \mathfrak{e}*c \implies b = c.$$

Assim, a é cancelável à esquerda, analogamente prova-se que é cancelável à direita. ■

Até agora utilizamos uma única operação $*$ com o intuito de generalizar resultados que são válidos tanto para as adições quanto para as multiplicações que trabalharemos. Agora passaremos a distinguir duas operações, que chamaremos de adição (ou soma) e multiplicação (ou produto), denotadas respectivamente por $+$ e $\cdot$.

Deixemos claro que o nome de soma e de multiplicação não agregam em nada como serão definidas essas operações, isso falando de uma maneira genérica. É claro que as somas e produtos que trabalharemos serão os usuais (vistos apenas de uma maneira mais formal).

Observação 2.3. Na Teorema 2.5 quando estamos nos referindo a lei do cancelamento para uma soma, não há excessões, todas as somas (neste trabalho) tem a propriedade da lei

do cancelamento válidas para qualquer elemento de A. Por outro lado, quando a operação é um produto, diremos que esse produto tem a propriedade da lei do cancelamento quando todo elemento diferente do neutro da soma é cancelável no produto.

Observação 2.4. Às vezes, quando conveniente, omitiremos o símbolo da multiplicação por simplicidade. E para omitir parênteses estabeleceremos a seguinte convenção:

$$a + b \cdot c := a + (b \cdot c);$$
$$a \cdot b + c := (a \cdot b) + c;$$
$$a \cdot b := ab.$$

Definição 2.20. *Sejam A um conjunto e sejam $+$ e $\cdot$ as operações de adição e multiplicação sobre A. Dizemos que a multiplicação é distributiva em relação a soma quando para quaisquer $a, b, c \in A$ é válido que*

$$a \cdot (b + c) = a \cdot b + a \cdot c.$$

Definição 2.21. *Uma relação de ordem parcial $\leq$ é dita compatível com a adição, quando para quaisquer $a, b, c \in A$, valer*

$$a \leq b \implies a + c \leq b + c.$$

Definição 2.22. *Dizemos que um número[1] a é positivo quando ocorre ao menos uma situação dos itens abaixo:*

- *$a \in \mathbb{N}$;*
- *a é um elemento de algum conjunto de $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ e é maior do que o elemento neutro aditivo desse conjunto.*

Definição 2.23. *Dizemos que um número a é negativo, quando a é um elemento de algum conjunto de $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ e é menor do que o elemento neutro aditivo desse conjunto.*

A Definição 2.22 acima nos permite a definição a seguir.

Definição 2.24. *Seja A um conjunto parcialmente ordenado pela relação $\leq$. Sejam $a, b, c \in A$, em que c é um número positivo. Seja também $\cdot$ uma multiplicação sobre A. Dizemos que $\leq$ é compatível com a multiplicação quando*

$$a \leq b \implies ac \leq bc.$$

Definição 2.25. *Seja A um conjunto, e sejam $+, \cdot$ duas operações sobre A, chamadas de adição e multiplicação. Dizemos que $(A, +, \cdot)$ é um anel se são válidas as propriedades:*

[1] Para nós, números são elementos de $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$ ou $\mathbb{R}$, exceto se explicitamente mencionados de outra maneira.

(i) Associativa da adição;

(ii) Comutativa da adição;

(iii) Da existência do elemento neutro para adição;

(iv) Da existência do elemento simétrico para a adição;

(v) Associativa da multiplicação;

(vi) Comutativa da multiplicação;

(vii) Da existência do elemento neutro da multiplicação;

(viii) Da distributividade da multiplicação em relação à adição;

Quando não houver ambiguidade chama-se $(A, +, \cdot)$ *apenas de anel* A*.*

Teorema 2.6. *Seja* A *um anel. Então para qualquer* $a \in A$ *vale que* $a \cdot 0 = 0 = 0 \cdot a$*.*

Demonstração: Temos que as seguintes igualdades são válidas:

$$a \cdot 0 + 0 = a \cdot 0 = a \cdot (0 + 0) = a \cdot 0 + a \cdot 0.$$

Assim $a \cdot 0 + 0 = a \cdot 0 + a \cdot 0$ e pela lei do cancelamento, $0 = a \cdot 0$. Ainda, como o produto é comutativo, vale $a \cdot 0 = 0 \cdot a$. ■

Teorema 2.7. *Seja* A *um anel. Então se* $a, b \in A$*, vale que* $ab = 0$ *se, e somente se,* $a = 0$ *ou* $b = 0$*.*

Demonstração: Se $a = 0$ ou se $b = 0$ então $ab = 0$ pela Teorema 2.6. Agora, se $ab = 0$, e suponhamos $b \neq 0$, então temos $ab = 0 = 0b$, como $b \neq 0$ podemos aplicar o cancelamento para o produto e ficamos com $a = 0$. Analogamente caso $a \neq 0$. ■

Definição 2.26. *Um corpo é um anel* A *em que cada elemento diferente do neutro aditivo admite um simétrico multiplicativo.*

3. O CONJUNTO DOS NÚMEROS NATURAIS E OS AXIOMAS DE PEANO

Neste capítulo apresentaremos a formalização aritmética do conjunto dos números naturais. Primeiro será apresentada uma breve parte histórica e, após isso, enunciaremos os axiomas de Peano. Depois definiremos uma adição, uma multiplicação e uma relação de ordem, bem como listaremos algumas propriedades básicas e faremos suas demonstrações. As referências básicas desse capítulo são Domingues (2009) e Ferreira (2013).

3.1. Um pouco de história

Uma possível narrativa para o início do trabalho com números seria a necessidade de pastores efetuarem a contagem de animais em seus rebanhos, embora essa narrativa não seja definitiva (ROQUE, 2012). Essa iniciação com números e o conhecimento obtido pode ter encontrado dois caminhos (ou fins) possíveis, foram mantidos ao longo do tempo ou não. Nesse sentido não é possível estabelecer uma matemática definitiva e uma única evolução (ROQUE, 2012, p. 35).

Ao longo da históra, foram desenvolvidos muitos conjuntos numéricos, para resolver problemas em que os conjuntos anteriores não eram adequados ou suficientes. Com o avanço da matemática, acabou-se esbarrando em problemas que as crenças e técnicas da época não conseguiam resolver, assim uma formalização era necessária, mesmo que esse não fosse o objetivo principal, mas sim resolver esses problemas (ROQUE, 2012, p. 407).

Quem fundamentou a aritmética como conhecemos hoje foi o italiano Giuseppe Peano (1858 - 1932), mas houve tentativas anteriores, em que podemos citar Frege (1848-1925). Peano conseguiu, entre outros fatores, usar boas escolhas para símbolos, muitos dos quais usamos atualmente, e também por causa da explicitação das regras por meio de símbolos e a ausência de hipóteses ocultas (BOYER, 1996, p. 415)

O trabalho de Peano ficou conhecido como Axiomas de Peano. Ele fundamentou a sua aritmética com 9 axiomas e 3 conceitos primitivos, como está apresentado na Figura 1.

Antes de continuarmos, podemos recolocar uma analogia da matemática com um jogo:

> Ao criar um jogo, é importante que suas regras sejam suficientes e consistentes. Por *suficiente* queremos dizer que as regras devem estabelecer o que é permitido

Figura 1 – A versão original dos axiomas de Peano

ARITHMETICES PRINCIPIA.

§ 1. De numeris et de additione.

Explicationes.

Signo N significatur *numerus (integer positivus).*
» 1 » *unitas.*
» $a+1$ » *sequens a,* sive *a plus* 1.
» $=$ » *est aequalis.* Hoc ut novum signum considerandum est, etsi logicae signi figuram habeat.

Axiomata.

1. $1 \in \mathrm{N}$.
2. $a \in \mathrm{N} . \supset . a = a$.
3. $a, b, c \in \mathrm{N} . \supset : a = b . = . b = a$.
4. $a, b \in \mathrm{N} . \supset \therefore a = b . b = c : \supset . a = c$.
5. $a = b . b \in \mathrm{N} : \supset . a \in \mathrm{N}$.
6. $a \in \mathrm{N} . \supset . a + 1 \in \mathrm{N}$.
7. $a, b \in \mathrm{N} . \supset : a = b . = . a + 1 = b + 1$.
8. $a \in \mathrm{N} . \supset . a + 1 - = 1$.
9. $k \in \mathrm{K} \therefore 1 \in k \therefore x \in \mathrm{N} . x \in k : \supset_x . x + 1 \in k : : \supset . \mathrm{N} \supset k$.

Definitiones.

10. $2 = 1 + 1$; $3 = 2 + 1$; $4 = 3 + 1$; etc.

Fonte: Archive.org; Giuseppe Peano (1889)

> fazer em qualquer situação que possa vir a ocorrer no desenrolar de uma partida do jogo. Por *consistente* queremos dizer que as regras não devem contradizer-se, ou sua aplicação levar a situações contraditórias (BARBOSA, 2012, p. 13-14).

Para nós, as peças do jogo serão o conceito de um, o conceito de número natural, e o conceito da relação sucessor. As regras do jogo serão os axiomas que relacionarão esses três conceitos primitivos. Nessa analogia, as peças não são muito importantes, mas as regras o serão.

3.2. Axiomas de Peano

O nosso estudo dos números naturais será iniciado pela apresentação dos axiomas de Peano, que relacionam os conceitos primitivos adotados. Serão apresentados 5 axiomas ao invés de 9 porque assumimos a teoria de conjuntos e a lógica elementar como fundamental, assim dispomos de uma relação de igualdade '=' que é reflexiva, simétrica e transitiva. Peano colocou essas propriedades da igualdade como axiomas, o que não precisamos fazer aqui. Na verdade, pode-se até optar por versões mais reduzidas desse conjunto de axiomas, podemos citar Ferreira (2013) e Lima (2016), em que ambos utilizam 3 axiomas.

Axioma 1. *Existe um conjunto de exatamente todos os números naturais, que será denotado por* $\mathbb{N}$*, e existe uma função* $s : \mathbb{N} \to \mathbb{N}$*, que é a relação "sucessor".*

Axioma 2. *Um é um número natural, isto é,* $1 \in \mathbb{N}$*.*

Axioma 3. *Um não é sucessor de nenhum número, isto é,* $1 \notin Im(s)$ *ou ainda,* $\nexists a \in \mathbb{N} : s(a) = 1$*.*

Axioma 4. *s é injetora, isto é,* $s(a) = s(b) \implies a = b$ [(1)]*.*

Axioma 5. *Seja* $\mathbb{S}$ *um subconjunto de* $\mathbb{N}$*. Caso* $1 \in \mathbb{S}$ *e se, para todo k em* $\mathbb{S}$*, ocorrer que* $s(k)$ *também esteja em* $\mathbb{S}$*, então* $\mathbb{S} = \mathbb{N}$*. Isso é o mesmo que colocar:*

$$\mathbb{S} \subseteq \mathbb{N} \wedge 1 \in \mathbb{S} \wedge (k \in \mathbb{S} \Rightarrow s(k) \in \mathbb{S}) \implies \mathbb{S} = \mathbb{N}.$$

Este último axioma é chamado de axioma da indução finita.

Conforme os axiomas apresentados, deve ser notado que o conjunto $\mathbb{N}$ (na nossa axiomatização) não tem o 0 (zero) que é, usualmente, o neutro da soma em $\mathbb{N}$. O intuito de construir $\mathbb{N}$ a partir do 1 é pela questão que às vezes surge em diversas situações: "0 é um número natural?". Em especial, o próprio Lima (2023) diz que o zero pode ser ou pode não ser um número natural. É dito que fica a critério de conveniência, embora para nós, seja 'inconveniente' perder o neutro da soma (que aparecerá sua primeira vez em $\mathbb{Z}$).

(1) Vale notar a contra-positiva que estabelece, nesse caso: $a \neq b \implies s(a) \neq s(b)$.

Justificamos essa escolha pois a ausência do zero terá algumas consequências e exigirá alguns ajustes, que poderão ser observados na nossa construção. Além disso, a bibliografia principal trata o zero como um número natural, então a construção será necessariamente com essas adaptações, o que, em nossa visão, é algo positivo para o desenvolvimento do trabalho, apesar do resultado final, em certo ponto de vista, ficar prejudicado pela ausência do 0.

Observemos também que o próprio Peano começou sua teoria originalmente pelo 1 e, somente em trabalho posterior, colocou o 0 como o primeiro número natural.

Para comerçarmos nosso desenvolvimento, podemos notar que o Axioma 2 garante que $\mathbb{N} \neq \emptyset$. Além disso, o Axioma 1 garante que $s(1) \in \mathbb{N}$, também $s(s(1)) \in \mathbb{N}$, $s(s(1)) \in \mathbb{N}$ e assim por diante.

Em seguida, apresentamos um lema que será necessário para a ampliação de nosso ferramental inicial.

Lema 3.1. *Nenhum número natural é seu próprio sucessor, ou seja,* $a \in \mathbb{N} \implies a \neq s(a)$.

Demonstração: Faremos por indução.
Seja $\mathbb{S} = \{a \in \mathbb{N} : a \neq s(a)\}$. Os axiomas 2 e 3 garantem que $1 \in \mathbb{S}$.
Supondo que $k \in \mathbb{S}$, onde $k \neq s(k)$, vamos provar que o sucessor de k é diferente do sucessor do sucessor de k, isto é, $s(k) \neq s(s(k))$. Como $k \neq s(k)$ e s é injetora pela contrapositiva do Axioma 4, concluímos que $s(k) \neq s(s(k))$. Pelo Axioma 5, conclui-se que $\mathbb{S} = \mathbb{N}$ e, portanto, para qualquer natural a tem-se que $a \neq s(a)$. ■

Teorema 3.1. *Todo número natural, exceto o* 1*, é sucessor de algum outro número natural, que é único.*

Demonstração: A prova é feita por indução.
Seja $\mathbb{S} = \{x \in \mathbb{N} : x \neq 1 \implies (\exists y \in \mathbb{N} \wedge s(y) = x)\}$.
Sabemos que $1 \in \mathbb{S}$ porque $x = 1$ torna o antecedente falso, assim a implicação é logicamente verdadeira. Suponhamos $k \in \mathbb{S}$. Assim, k é o sucessor de algum $y \in \mathbb{N}$, ou seja, $k = s(y)$. É imediato que $s(k)$ é sucessor de $k \in \mathbb{N}$, e portanto $s(k) \in \mathbb{S}$. Pelo Axioma 5 concluímos que $\mathbb{S} = \mathbb{N}$, ou seja, todo número natural diferente de 1 é sucessor de algum número natural.

Além disso, fixado um $k \in \mathbb{N}$ com $k \neq 1$, o elemento $y \in \mathbb{N}$ tal que $s(y) = k$ é único. De fato, se x, y são naturais tais que $s(x) = s(y) = k$, pelo Axioma 4 obtemos que $x = y$. ■

Observação 3.1. Diremos que o número y do teorema anterior é o antecessor de $x = s(y)$. Além disso vale notar que s (conforme definida no Axioma 1) não é sobrejetora somente

pelo fato de seu contradomínio ser $\mathbb{N}$. Mas se considerarmos o caso restrito para $\mathbb{N} \setminus \{1\}$, teremos que s é uma bijeção.

Utilizaremos a notação usual para os números naturais, isto é, $\mathbb{N} = \{1, 2, 3, 4, ...\}$, onde $2 := s(1), 3 := s(2), 4 := s(3)$ e assim por diante.

3.3. A adição em $\mathbb{N}$

A adição em $\mathbb{N}$ é a operação que mais intuitivamente está relacionada com a contagem e união de coisas discretas.

Definição 3.1. *Sejam $a, b \in \mathbb{N}$. A adição entre a e b, denotada por $a + b$ é definida com as seguintes condições:*

(i) $a + 1 = s(a)$;

(ii) $a + s(b) = s(a + b)$.

A ideia por trás desta definição de adição é a de recursão. Nesse caso o item (i) nos diz como somar qualquer número natural com o 1. O item (ii) nos diz como somar um elemento qualquer com o sucessor de outro, só que pelo Teorema 3.1 todo natural diferente de 1 é sucessor de alguém.

Exemplo 3.1. Podemos somar $2 + 3$ do seguinte modo:

$$2+3 = 2+s(2) = s(2+2) = s(2+s(1)) = s(s(2+1))) = s(s(s(2))) = s(s(3)) = s(4) = 5.$$

Teorema 3.2. *A adição dada pela Definição 3.1 é uma função, que associa uma dupla de números naturais em um único número natural.*

Demonstração: A prova de que a soma está bem definida para quaisquer $a, b \in \mathbb{N}$ é dada a seguir: Dado $a \in \mathbb{N}$ fixo, seja $\mathbb{S} = \{x \in \mathbb{N} : a + x \text{ está definido}\}$. Temos que $a + 1 = s(a)$ está definido, portanto 1 está em $\mathbb{S}$. Agora consideremos um dado $k \in \mathbb{N}$, em que $a + k$ esteja bem definida. Temos então que $a + s(k) = s(a + k)$, como $a + k$ está definido, o sucessor também está definido, pelo Axioma 5, temos que $\mathbb{S} = \mathbb{N}$. ∎

Lema 3.2. *O 1 comuta com qualquer número na soma, isto é, $\forall x \in \mathbb{N}, x + 1 = 1 + x$.*

Demonstração: Seja $\mathbb{S} = \{x \in \mathbb{N} : x+1 = 1+x\}$. O 1 está em $\mathbb{S}$ pois $1+1 = 1+1$. Supondo $k \in \mathbb{S}$, temos que $k + 1 = 1 + k$. Queremos provar que $s(k)$ também está em $\mathbb{S}$. Como $s(k) + 1 = s(s(k)) = s(k + 1) = s(1 + k) = 1 + s(k)$. Portanto $s(k)$ também está em

$\mathbb{S}$ sempre que k também está, o que pelo Axioma 5, $\mathbb{S} = \mathbb{N}$. ■

Proposição 3.1. *A adição no conjunto dos números naturais tem as seguintes propriedades:*

(i) Fechamento;

(ii) Associativa;

(iii) Comutativa;

(iv) Lei do cancelamento;

(v) Se $a, b \in \mathbb{N}$, então $a + b \neq a$;

(vi) Inexistência de neutro: $\nexists \mathfrak{e} \in \mathbb{N} : \forall a, a + \mathfrak{e} = \mathfrak{e} + a = a$.

Demonstração: Antes de demonstrarmos propriamente, façamos a suposição que $a, b, c \in \mathbb{N}$ são números fixados.

(i) Fechamento:
Seja $\mathbb{S} = \{x \in \mathbb{N} : a + x \in \mathbb{N}\}$. Obviamente o 1 está em $\mathbb{S}$. Suponhamos então que $k \in \mathbb{S}$, queremos garantir que $s(k) \in \mathbb{S}$. Temos então que $a + k \in \mathbb{N}$ o que implica que $a + s(k) = s(a + k) \in \mathbb{N}$, pois pelo Axioma 1, a função s tem contradomínio $\mathbb{N}$. Como $s(k) \in \mathbb{S}$, pelo Axioma 5 concluímos que $\mathbb{S} = \mathbb{N}$.

(ii) Associativa:
Seja $\mathbb{S} = \{x \in \mathbb{N} : (a + b) + x = a + (b + x)\}$. Temos que
$(a + b) + 1 = s(a + b) = a + s(b) = a + (b + 1)$, o que mostra que o 1 está em $\mathbb{S}$. Mostraremos que $k \in \mathbb{S} \implies s(k) \in \mathbb{S}$. De fato, supondo que $(a+b)+k = a+(b+k)$, temos:

$$(a + b) + s(k) = s((a + b) + k) = s(a + (b + k)) = a + s(b + k) = a + (b + s(k)).$$

Pelo Axioma 5 concluímos que $\mathbb{S} = \mathbb{N}$.

(iii) Comutativa:
Consideremos o conjunto $\mathbb{S} = \{x \in \mathbb{N} : a + x = x + a\}$. O $1 \in \mathbb{S}$ pois $a + 1 = 1 + a$ conforme o Lema 3.2. Provemos então que, se $k \in \mathbb{S}$, então $s(k) \in \mathbb{S}$. De fato, supondo $a + k = k + a$ temos que

$$a + s(k) = s(a + k) = s(k + a) = k + s(a) = k + (a + 1) = (k + 1) + a = s(k) + a.$$

Pelo Axioma 5 concluímos que $\mathbb{S} = \mathbb{N}$.

(iv) Lei do cancelamento:
Seja $\mathbb{S} = \{x \in \mathbb{N} : x + b = x + c \implies b = c\}$, vamos provar que $\mathbb{S} = \mathbb{N}$. Obviamente o 1 está em $\mathbb{S}$ pois $1 + b = 1 + c \iff s(b) = s(c)$ e pelo Axioma 4, se dois elementos tem sucessores iguais, eles próprios são iguais. Suponha $k + b = k + c \implies b = c$, temos que

$$\begin{aligned} s(k) + b = s(k) + c &\implies (k + 1) + b = (k + 1) + c \\ &\implies (k + b) + 1 = (k + c) + 1 \\ &\implies s(k + b) = s(k + c) (\text{pelo Axioma 4}) \\ &\implies k + b = k + c. \end{aligned}$$

A hipótese de indução garante que $b = c$. Desse modo, $s(k) \in \mathbb{S}$ e, pelo Axioma 5 concluímos que $\mathbb{S} = \mathbb{N}$.

(v) $a + b \neq a$;
A demonstração consiste em usar o Teorema 3.1, pois sabemos que um número natural ou é igual a 1, ou é sucessor de algum outro número natural e no final obter que 1 é sucessor de algum número natural, contrariando o Axioma 3. Assim, consideremos quatro casos para a e b, sendo iguais a 1 ou diferente de 1 (que são todas as combinações possíveis), supondo que $a + b = a$, e mostraremos que todos são absurdos:

(1) $a = 1 \wedge b = 1$:
Temos $a + b = a \iff 1 + 1 = 1$, o que é absurdo.

(2) $a = s(x) \wedge b = 1$, para algum $x \in \mathbb{N}$:
Temos $a + b = a \iff s(x) + 1 = s(x) \iff s(s(x)) = s(x)$, o que é absurdo.

(3) $a = 1 \wedge b = s(y)$, para algum $y \in \mathbb{N}$:
Temos $a + b = a \iff 1 + s(y) = 1 \iff s(1 + y) = 1$, o que é absurdo.

(4) $a = s(x) \wedge b = s(y)$, para algum $x \in \mathbb{N}$ e algum $y \in \mathbb{N}$:
Temos

$$a+b = a \iff s(x)+s(y) = s(x) \iff x+1+y+1 = x+1 \iff s(1+y) = 1,$$

o que é absurdo.

(vi) Inexistência de neutro:
Como consequência da demonstração anterior, não existe neutro na adição no nosso conjunto de números naturais, isto é, não existe $\mathfrak{e} \in \mathbb{N}$ tal que para qualquer $a \in \mathbb{N}$, vale $a + \mathfrak{e} = \mathfrak{e} + a = a$.

■

3.4. A multiplicação em $\mathbb{N}$

Definição 3.2. *Sejam $a, b \in \mathbb{N}$. A multiplicação entre a e b, denotada por $a \cdot b$ é definida com a as seguintes condições:*

(i) $a \cdot 1 = a$;

(ii) $a \cdot s(b) = a \cdot b + a$.

Teorema 3.3. *Para a multiplicação de números naturais são válidas as seguintes propriedades:*

(i) Fechamento;

(ii) Da existência do elemento neutro;

(iii) Distributiva;

(iv) Comutativa;

(v) Associativa;

(vi) Para $a, b \in \mathbb{N}$ ocorre que, $a \cdot b = 1 \implies a = b = 1$.

Demonstração: Antes de demonstrarmos propriamente, façamos a suposição que $a, b, c \in \mathbb{N}$ são números fixos. Provaremos por indução, exceto no último item.

(i) Fechamento:
Seja $\mathbb{S} = \{x \in \mathbb{N} : a \cdot x \in \mathbb{N}\}$. O 1 está em $\mathbb{S}$ pois $1 \cdot 1 = 1$. Supondo que é válido $ak \in \mathbb{N}$ para algum $k \in \mathbb{N}$, temos $a \cdot s(k) = ak + a$. Como tanto ak quanto a são números naturais, e como a soma é fechada em $\mathbb{N}$, temos que $ak + a \in \mathbb{N}$. Pelo Axioma 5, $\mathbb{S} = \mathbb{N}$.

(ii) Da Existência do elemento neutro:
Seja $\mathbb{S} = \{x \in \mathbb{N} : 1 \cdot x = x \cdot 1 = x\}$. O 1 está em $\mathbb{S}$ pois $1 \cdot 1 = 1 \cdot 1 = 1$. Supondo que $k \in \mathbb{S}$ vamos concluir que $s(k) \in \mathbb{S}$. De fato, supondo $1 \cdot k = k \cdot 1$ temos que

$$1 \cdot s(k) = 1 \cdot k + 1 = k \cdot 1 + 1 = k + 1 = s(k) = s(k) \cdot 1.$$

Pelo Axioma 5, $\mathbb{S} = \mathbb{N}$.

(iii) Distributiva à direita: Seja $\mathbb{S} = \{x \in \mathbb{N} : (a + b)x = ax + bx\}$. Temos que o $1 \in \mathbb{S}$ pois $(a + b)1 = a + b = a \cdot 1 + b \cdot 1$. Provemos que se $k \in \mathbb{S}$ então $s(k) \in \mathbb{S}$. De fato, supondo que $(a + b)k = ak + bk$ temos que:
$(a+b) \cdot s(k) = (a+b)k + (a+b) = ak + bk + a + b = ak + a + bk + b = a \cdot s(k) + b \cdot s(k)$.

Pelo Axioma 5 tem-se que $\mathbb{S} = \mathbb{N}$.

Distributiva à esquerda:
A prova da distributiva à esquerda é facilmente obtida quando já dispusermos da propriedade comutativa. Por sua vez a prova da comutatividade que faremos precisará apenas da distributiva à direita.

(iv) Comutativa:
Seja $\mathbb{S} = \{x \in \mathbb{N} : ax = xa\}$. Com certeza o 1 está em $\mathbb{S}$, porque 1 é o neutro da multiplicação. Agora suponhamos que $k \in \mathbb{S}$, vejamos se $s(k) \in \mathbb{S}$. Temos que $ak = ka$ implica que $a \cdot s(k) = ak + a = 1 \cdot a + ka = (1 + k)a = s(k) \cdot a$. Pelo Axioma 5 tem-se que $\mathbb{S} = \mathbb{N}$.

(v) Associativa:
Seja $\mathbb{S} = \{x \in \mathbb{N} : a(bx) = (ab)x\}$. Sabemos que o 1 está em $\mathbb{S}$ pois
$a(b \cdot 1) = a(b) = ab = (ab) \cdot 1$. Agora suponhamos $k \in \mathbb{S}$, assim, podemos omitir parênteses em abk. Consideremos $s(k)$, para ver se ele está em $\mathbb{S}$. Temos que
$a(bk) = (ab)k$ implica

$$a(b \cdot s(k)) = a(bk + b) = abk + ab = s(k) \cdot (ab),$$

o que pelo Axioma 5 concluímos que $\mathbb{S} = \mathbb{N}$.

(vi) $a \cdot b = 1 \implies a = b = 1$.
Vamos separar em dois casos. O primeiro caso é se $a = 1$ ou $b = 1$. Sem perda de generalidade, suponhamos $a = 1$. Temos que $1 \cdot b = 1 \implies b = 1$ pois 1 é o elemento neutro. Portanto se a ou se b forem 1, obrigatoriamente o outro também deverá ser. O segundo caso, se $a \neq 1$ e $b \neq 1$. Então existem c e d naturais tais que $a = s(c)$ e $b = s(d)$. Assim,

$$ab = 1 \iff (c + 1)(d + 1) = 1 \implies cd + c + d + 1 = 1 \implies s(cd + c + d) = 1,$$

o que obviamente não pode ocorrer, de acordo com o Axioma 3.

■

Nesse desenvolvimento, as propriedades da multiplicação são semelhantes às que teríamos se tivéssemos tomado o 0 como número natural. Uma propriedade que essa multiplicação não tem agora é o anulamento, que ainda carece de significado. As propriedades associativa e comutativa já eram presentes na soma. Agora no produto, temos um elemento neutro que não há para a soma, além da distributiva que pode ser aplicada com soma e produto.

Até agora dispomos de uma soma e um produto em $\mathbb{N}$, mas isso ainda não nos possibilita comparar dois elementos de $\mathbb{N}$. Agora, com intuito de responder à pergunta, qual número vem "antes" ou qual número é "menor", devemos estabelecer uma relação de ordem em $\mathbb{N}$.

Reforçamos que existem diferentes relações de ordem num mesmo conjunto, conforme o exemplo que segue à Definição 2.8.

3.5. A relação de ordem em $\mathbb{N}$

Definição 3.3. *Sejam $a, b \in \mathbb{N}$. Definiremos a relação $\leq$ entre a e b, denotado por $a \leq b$, e diremos que a se relaciona com b através de $\leq$ quando uma das seguintes situações ocorre:*

- $a = b$;
- $a + n = b$, *para algum* $n \in \mathbb{N}$.

Observação 3.2. Deve ser notado que quando $a \leq b$ uma e apenas uma das seguintes situações pode ocorrer $a = b$ ou $a + n = b$, com $n \in \mathbb{N}$. Isso é devido à Proposição 3.1 item (v), que mostra que ambas não podem ocorrer simultaneamente. Já considerando que pelo menos uma situação deve ocorrer, teremos a totalidade, que será provada no final deste capítulo.

A necessidade de colocar a relação de ordem em dois itens vem do fato de não considerarmos zero como um número natural. Ainda assim, queremos ter uma relação de ordem total, e a desigualdade $<$ não é total pois $a \not< a$, qualquer que seja o natural a.

Teorema 3.4. *A relação de ordem em $\mathbb{N}$ tem as seguintes propriedades:*

(i) Reflexiva;

(ii) Antissimétrica;

(iii) Transitiva;

(iv) Tricotomia;

(v) Compatibilidade com a adição;

(vi) Compatibilidade com a multiplicação.

Demonstração: Primeiro, suponhamos que a, b, c, m, n são números naturais.

(i) Reflexiva:
É imediato que $a = a$. Logo $a \leq a$.

(ii) Antissimétrica, $a \leq b \wedge b \leq a \implies a = b$:
Se $a = b$ não há nada a provar. Consideremos que sejam diferentes.
Então $a \leq b \iff b = a + n$ e também, como $b \leq a \iff a = b + m$, substituindo, temos $b = (b + m) + n \implies b = b + r$ para algum r natural, o que não pode ocorrer, conforme Proposição 3.1.

(iii) Transitiva $a \leq b \wedge b \leq c \implies a \leq c$:
Vamos considerar quatro casos em vista da nossa relação de ordem ter sido definida em dois itens:

(1) $a = b = c$.
Temos $a = c \implies a \leq c$.

(2) $a = b < c$.
Temos $b + n = c$, para algum $n \in \mathbb{N}$. Como $a = b < b + n = c$, temos $a \leq c$.

(3) $a < b = c$.
Temos $a + n = b$ para algum $n \in \mathbb{N}$. Como $a + n = b = c$, temos $a \leq c$.

(4) $a < b < c$.
Temos $a + m = b$ para algum $m \in \mathbb{N}$ e $b + n = c$ para algum $n \in \mathbb{N}$. Assim temos que

$$c = b + n = (a + m) + n = a + (m + n)$$

e assim $a \leq c$.

(iv) Tricotomia:
Vamos provar por indução.
Seja $\mathbb{S} = \{x \in \mathbb{N} : x = a \vee x < a \vee x > a\}$. Sabemos que o $1 \in \mathbb{S}$ porque, ou ocorre que $a = 1$, ou $a = s(m) = m + 1$, para algum m natural, assim, $1 < a$.
Supondo que $k \in \mathbb{S}$ seja tal que $k = a \vee k < a \vee k > a$. Consideremos quatro casos.

No primeiro caso, $k = a$, assim $s(k) > a$, portanto $k \in \mathbb{S}$.
No segundo caso, $k < a$, assim $k + m = a$, para algum m natural. Se $m = 1$, $k + 1 = s(k) = a$. Se por outro lado, $m \neq 1$, então $m = s(n)$ para algum n natural, assim, $a = k + m = k + n + 1 = s(k) + n$, dessa forma $a > s(k)$. Em ambos as situações temos $s(k) \in \mathbb{S}$.
No terceiro caso, $k > a$, assim $k = a+m$ para algum m natural, e $s(k) = a+m+1 > a$, e novamente $s(k) \in \mathbb{S}$.

A unicidade, embora não esteja explícita na criação do conjunto, pode ser vista no desenvolvimento de cada caso. Portanto, em todos os casos, $s(k) \in \mathbb{S}$, e pelo Axioma 5, $\mathbb{S} = \mathbb{N}$.

(v) Compatível com adição:
Seja $a \leq b$. Se $a = b$ teremos que $a + c = b + c$ porque a adição é uma função. Consideremos agora $a < b$. Então $b = a + m$ para algum $m \in \mathbb{N}$. Temos que

$$b + c = (a + m) + c \implies b + c = (a + c) + m \implies a + c < b + c.$$

e portanto $a + c \leq b + c$.

(vi) Compatível com multiplicação:
Seja $a \leq b$. Se $a = b$ é imediato que $ac = bc$. Consideremos $a < b$.
Temos $a < b \iff b = a + m$ para algum $m \in \mathbb{N}$. Temos que

$$ac + mc = (a + m)c = bc$$

e portanto $ac \leq bc$.

■

Corolário 3.1. *A relação de ordem $\leq$ definida anteriormente é total.*

Demonstração: Como a relação de ordem é tricotômica, se $a, b \in \mathbb{N}$, temos que uma das três situações sempre ocorre: $a < b \vee a = b \vee a > b$. Se for $a < b$ temos $a \leq b$. Se for $a = b$ temos $a \leq b$. E se for $a > b$ temos $b \leq a$. O que mostra que em todos os casos ocorre que $a \leq b$ ou $b \leq a$. ■

Corolário 3.2. *Vale a lei do cancelamento para a multiplicação de números naturais.*

Demonstração: Vamos provar que, dados $a, b, c \in \mathbb{N}$, $ac = bc \implies a = b$. Por contradição, suponha que possa ocorrer $a \neq b$, com $ac = bc$. Sem perda de generalidade, suponha que $a < b$. Temos que o Teorema 3.4 garante que a relação de ordem é compatível com a multiplicação, para quaisquer elementos de $\mathbb{N}$. Logo, segue que $ac < bc$. Mas isso é uma contradição pois tínhamos como hipótese que $ac = bc$. ■

Proposição 3.2. *Se $a, b, c \in \mathbb{N}$ e $a + c \leq b + c$ então $a \leq b$.*

Demonstração: Se $a + c = b + c$, pela lei do cancelamento para a adição temos $a = b$, e assim $a \leq b$. Se $a + c + m = b + c$, para algum m natural, novamente pelo cancelamento da adição temos $a + m = b$, assim $a < b$, e assim $a \leq b$. Portanto em qualquer caso temos $a \leq b$, como queríamos mostrar. ■

Proposição 3.3. *Se $a, b, c \in \mathbb{N}$ e $a \cdot c \leq b \cdot c$ então $a \leq b$.*

Demonstração: Se $ac = bc$, pela lei do cancelamento do produto, $a = b$, e assim $a \leq b$. Se por outro lado, $ac < bc$, então $bc = ac + m$, para algum m natural. Mostraremos por contradição, que não pode ocorrer $a > b$. Suponhamos que ocorra $a > b$, então $ac > bc$ e assim $ac = bc + n$ para algum n natural. Então temos que

$$bc = ac + m \iff bc = (bc + n) + m \iff bc = bc + (n + m),$$

o que não pode ocorrer pela Proposição 3.1, $a + b \neq a$. Uma outra demonstração dessa segunda parte seria pela tricotomia, que não permite que ocorra $ac < bc$ e $ac > bc$. ■

Teorema 3.5. *O conjunto $\mathbb{N}$ não é limitado superiormente.*

Demonstração: Por contradição, suponha que $n \in \mathbb{N}$ seja uma cota superior de $\mathbb{N}$. Como $n + 1 > n$, e como $n + 1 \in \mathbb{N}$, temos uma contradição. Logo, não existe cota superior para $\mathbb{N}$. ■

Teorema 3.6. *Todo subconjunto não vazio $A \subset \mathbb{N}$ possui elemento mínimo, ou seja, um número que é menor do que qualquer outro número naquele conjunto.*

Demonstração: Seja $A \subset \mathbb{N}$. Vamos usar a notação $C_n = \{\, p \in \mathbb{N} : 1 \leq p \leq n \,\}$ para algum número natural n dado. Seja $X \subset \mathbb{N}$ o conjunto de todos os n onde $C_n \subset \mathbb{N} \setminus A$. Assim $X \cap A = \emptyset$.

Caso $1 \in A$, já temos o mínimo. Caso contrário, então tanto X quanto A são não vazios. Para cada $n \in X$ temos que $C_n \subset X$, e também que $C_n \cap A = \emptyset$. Ao observarmos o Axioma 5 temos que $X \subset \mathbb{N}$ mas $X \neq \mathbb{N}$, assim deve existir algum $n_1 \in X$ onde $s(n_1) \notin X$. O elemento $s(n_1)$ deve estar em A, isso porque se não estivesse, então $s(n_1)$ seria elemento de X, o que é uma contradição. Dessa forma, identificamos o elemento mínimo de A, o que conclui a demonstração. ■

4. O CONJUNTO DOS NÚMEROS INTEIROS

Neste capítulos faremos a construção dos números inteiros. A bibliografia principal continua sendo Ferreira (2013) e Domingues (2009). Será apresentada uma relação de equivalência que servirá para criar $\mathbb{Z}$. Depois definiremos uma adição e um produto que tenham algumas propriedades que já eram válidas em $\mathbb{N}$, isto é, queremos "estender" $\mathbb{N}$.

Devemos observar que em $\mathbb{N}$ temos que a subtração, tal como conhecemos no ensino básico, não é uma operação (no sentido da álgebra), pois a subtração não está definida para quaisquer dois elementos de $\mathbb{N}$ tal que o resultado esteja em $\mathbb{N}$.

Com o objetivo de contornar esse problema (e portanto poder recriar a subtração como no ensino básico, em que ela seja uma operação sobre um conjunto), iremos criar um novo conjunto a partir de $\mathbb{N}$. Veremos que isso é possível, tal conjunto será denotado por $\mathbb{Z}$ e o chamaremos ele de conjunto dos *números inteiros*.

Nos números naturais, poderíamos ter definido uma função que tivesse o intuito de fazer o papel de inverso da soma, que seria a subtração, denotada por "$-$". Seguindo esse raciocínio poderíamos mostrar que $9-3=8-2=7-1$. Concluiríamos com base nessas igualdades, que $9+2=8+3$ e $8+1=7+2$, o que em ambos os casos, os resultados são números naturais.

Além disso, queremos expressar um número inteiro sem ter que assumir novos conceitos além de $\mathbb{N}$, da lógica e a teoria de conjuntos que já foram assumidas no capítulo anterior. Além disso, daremos significado à expressões do tipo $3-5, 4-8, 2-3$, que nesses exemplos não são números naturais.

A maneira como expressaremos será por meio de uma relação binária $\sim$ sobre $\mathbb{N}\times\mathbb{N}$ definida desse modo: $(a,b)\sim(c,d) \iff a+d=b+c$, sendo a,b,c,d números naturais quaisquer.

Exemplo 4.1. Os pares ordenados $(1,2)$ e $(5,6)$ se relacionam através da relação $\sim$, pois $1+6=2+5$.

Exemplo 4.2. Os pares ordenados $(1,2)$ e $(5,5)$ não se relacionam através da relação $\sim$, pois $1+5\neq 2+5$.

Exemplo 4.3. Os pares ordenados $(6,6)$ e $(8,8)$ se relacionam por meio da relação $\sim$, pois $6+8=6+8$. Fica claro que para quaisquer naturais m, n temos que $(m,m) \sim (n,n)$, uma vez que sempre ocorrerá $m+n=m+n$.

Teorema 4.1. *A relação $\sim$ é de equivalência.*

Demonstração: Sejam $a, b, c, d \in \mathbb{N}$. A relação $(a,b) \sim (c,d) \iff a+d=b+c$ possui as seguintes propriedades:

(i) Reflexiva: $(a,b) \sim (a,b)$, pois $a+b=b+a$.

(ii) Simétrica: $(a,b) \sim (c,d) \implies (c,d) \sim (a,b)$
Temos $a+d=b+c \implies c+b=d+a \iff (c,d) \sim (a,b)$.

(iii) Transitiva: $(a,b) \sim (c,d) \wedge (c,d) \sim (e,f) \implies (a,b) \sim (e,f)$.
Supondo $(a,b) \sim (c,d)$ e $(c,d) \sim (e,f)$ obtemos $a+d=b+c$ e $c+f=d+e$.
Somando termo a termo temos:
$(a+d)+(c+f)=(b+c)+(d+e) \iff a+f=b+e \iff (a,b) \sim (e,f)$.

■

Exemplo 4.4. Sabemos que $(1,1) \sim (2,2)$, e conforme a notação utilizada no capítulo anterior, temos que $\overline{(1,1)} = \overline{(2,2)}$.

Exemplo 4.5. As representações $\overline{(1,5)}, \overline{(2,6)}, \overline{(3,7)}$ representam a mesma classe de equivalência, pois $1+6=5+2$ e $2+7=6+3$.

Exemplo 4.6. Os elementos $\overline{(10,1)}$ e $\overline{(12,3)}$ representam a mesma classe de equivalência pois $(10,1) \sim (12,3)$ uma vez que $10+3=1+12$, e conforme o Teorema 2.1 se os elementos estão relacionados via relação de equivalência, então eles estão na mesma classe de equivalência.

Exemplo 4.7. Os elementos $\overline{(1,5)} = \overline{(2,6)} = \overline{(3,7)}$, em que cada representante da classe, a saber, $(1,5), (2,6)$ e $(3,7)$ representam a mesma classe de equivalência. A ideia de criar essas classes é que um número inteiro é uma classe de equivalência. Embora essa não seja uma ideia normal de ser encontrada fora do contexto de criação dos conjuntos numéricos (porque o objetivo de usar pares ordenados e classes de equivalência não é facilitar o manuseio de $\mathbb{Z}$, mas sim formalizar esse conjunto, com suas operações e relações como conhecemos).

Definição 4.1. *O conjunto quociente* $\mathbb{N} \times \mathbb{N}/\sim = \{\overline{(a,b)} : (a,b) \in \mathbb{N} \times \mathbb{N}\}$ *será chamado de* conjunto dos números inteiros *e será denotado por* $\mathbb{Z}$.

Observação 4.1. Utilizaremos a mesma notação para adição e multiplicação de números inteiros, que utilizamos nos números naturais. Inicialmente para o desenvolvimento do texto, sempre que $a, b \in \mathbb{N}$ entenderemos a soma $a + b$ como sendo executada em $\mathbb{N}$. Caso $a, b \in \mathbb{Z}$ entenderemos a soma $a + b$ sendo executada em $\mathbb{Z}$. Posteriormente justificaremos a escolha de utilizar os mesmos símbolos sendo que os conjuntos são diferentes. Isso se repetirá com a multiplicação e com a relação de ordem.

Com essa definição de número inteiro poderemos interpretar, a nível de ensino básico, que o número $\overline{(a, b)}$ é $a - b$. Caso fôssemos definir a subtração em $\mathbb{N}$, ela não seria uma operação, pois estaria definida apenas quando $a > b$.

Proposição 4.1. *Se $a, b, c \in \mathbb{N}$ vale que: $\overline{(a + c, b + c)} = \overline{(a, b)}$.*

Demonstração: A demonstração é imediata, visto que $(a + c) + b = (b + c) + a$, ou seja, $(a + c, b + c) \sim (a, b)$ e pelo Teorema 2.1 temos $\overline{(a + c, b + c)} = \overline{(a, b)}$. ■

4.1. A adição em $\mathbb{Z}$

Vamos definir uma adição em $\mathbb{Z}$, mantendo algumas propriedades da adição em $\mathbb{N}$.

Definição 4.2. *Dados $\overline{(a, b)}$ e $\overline{(c, d)}$ em $\mathbb{Z}$, definimos a adição $\overline{(a, b)} + \overline{(c, d)}$ como $\overline{(a + c, b + d)}$.*

Proposição 4.2. *A operação de adição está bem definida em $\mathbb{Z}$. Isto é, a adição em $\mathbb{Z}$ não depende do representante das classes de equivalência envolvidas na adição.*

Demonstração: Sejam $a, a', b, b', c, c', d, d' \in \mathbb{N}$. Vamos provar que

$$\overline{(a, b)} = \overline{(a', b')} \wedge \overline{(c, d)} = \overline{(c', d')} \implies \overline{(a, b)} + \overline{(c, d)} = \overline{(a', b')} + \overline{(c', d')}.$$

Vamos desenvolver as duas somas e mostrar que são iguais. Consideremos

$$\overline{(a, b)} + \overline{(c, d)} = \overline{(a + c, b + d)}.$$

Considerando agora a segunda soma temos:

$$\overline{(a', b')} + \overline{(c', d')} = \overline{(a' + c', b' + d')}.$$

Precisamos agora apenas mostrar que

$$(a + c, b + d) \sim (a' + c', b' + d'),$$

isso mostrará que

$$\overline{(a+c, b+d)} = \overline{(a'+c', b'+d')}.$$

Como $\overline{(a,b)} = \overline{(a',b')} \iff a+b' = b+a'$ e ainda $\overline{(c,d)} = \overline{(c',d')} \iff c+d' = d+c'$ teremos então que

$$(a+b')+(c+d') = (b+a')+(d+c')$$

ou seja

$$(a+c)+(b'+d') = (b+d)+(a'+c')$$

isto é

$$(a+c, b+d) \sim (a'+c', b'+d').$$

■

Teorema 4.2. *Sejam $\overline{(a,b)}, \overline{(c,d)}, \overline{(e,f)}$ números inteiros quaisquer. Para a adição em $\mathbb{Z}$, valem as seguintes propriedades:*

(i) Fechamento;

(ii) Associativa;

(iii) Comutativa;

(iv) Da existência do elemento neutro;

(v) Da existência do elemento simétrico;

(vi) Lei do cancelamento.

Demonstração: Sejam $a, b, c, d, e, f \in \mathbb{N}$.

(i) Fechamento: $\overline{(a,b)} + \overline{(c,d)} \in \mathbb{Z}$: É imediata, pois

$$a+c \in \mathbb{N} \wedge b+d \in \mathbb{N} \implies \overline{(a+c, b+d)} \in \mathbb{Z}.$$

(ii) Associativa:

$$\begin{aligned}
\left(\overline{(a,b)} + \overline{(c,d)}\right) + \overline{(e,f)} &= \overline{(a+c, b+d)} + \overline{(e,f)} \\
&= \overline{(a+c+e, b+d+f)} \\
&= \overline{(a+(c+e), b+(d+f))} \\
&= \overline{(a,b)} + \overline{(c+e, d+f)} \\
&= \overline{(a,b)} + \left(\overline{(c,d)} + \overline{(e,f)}\right).
\end{aligned}$$

(iii) Comutativa: $\overline{(a,b)} + \overline{(c,d)} = \overline{(a+c, b+d)} = \overline{(c+a, d+b)} = \overline{(c,d)} + \overline{(a,b)}$.

(iv) Da existência do elemento neutro: $\exists! x \in \mathbb{Z} : x + \overline{(a,b)} = \overline{(a,b)} + x = \overline{(a,b)}$;
Consideremos $\overline{(1,1)}$, vamos mostrar que ele é o x acima. Provaremos que é neutro pela esquerda. Temos que $\overline{(1,1)} + \overline{(a,b)} = \overline{(1+a, 1+b)}$. Provemos que $\overline{(1+a, 1+b)} \sim \overline{(a,b)}$. Para isso basta notar que $(1+a)+b = (1+b)+a$. Portanto $\overline{(1,1)}$ é neutro pela esquerda. Analogamente prova-se que é neutro pela direita. Além disso, todo elemento neutro para uma operação é único, conforme o Teorema 2.3, o que conclui nossa prova. Denotaremos o elemento neutro da adição por 0 e chamaremos de zero. Conforme os Exemplos 4.3 e 4.4 podemos representar de maneiras diferentes esse elemento neutro, mas sempre entendendo, em última instância, como $\overline{(m,m)}$ para qualquer $m \in \mathbb{N}$.

(v) Da existência do simétrico:
Vamos mostrar que para qualquer inteiro $\overline{(a,b)}$, o elemento $\overline{(b,a)}$ é seu simétrico. Temos que $\overline{(a,b)}+\overline{(b,a)} = \overline{(a+b, b+a)} = \overline{(1,1)}$, onde esse último elemento é o neutro da soma. Uma vez que a adição também é comutativa, temos $\overline{(b,a)} + \overline{(a,b)} = \overline{(1,1)}$, o que mostra que $\overline{(b,a)}$ é simétrico de $\overline{(a,b)}$. Que ele é único é consequência do Teorema 2.4.

(vi) Lei do cancelamento: $\overline{(a,b)} + \overline{(c,d)} = \overline{(a,b)} + \overline{(e,f)} \implies \overline{(c,d)} = \overline{(e,f)}$.
Temos

$$\begin{aligned} \overline{(a,b)} + \overline{(c,d)} = \overline{(a,b)} + \overline{(e,f)} &\implies \overline{(a+c, b+d)} = \overline{(a+e, b+f)} \\ &\implies (a+c)+(b+f) = (b+d)+(a+e) \\ &\implies c+f = d+e \\ &\implies \overline{(c,d)} = \overline{(e,f)}. \end{aligned}$$

Desse modo a adição admite a lei do cancelamento à esquerda. Para ver que o cancelamento à direita também é válido, basta notar que a adição é comutativa.

■

Com o Teorema 4.2, podemos ver que a comutatividade, a associatividade e o fechamento são mantidos, com a diferença que agora trabalhamos com números inteiros e não naturais. Indo além, é possível ver que o elemento neutro da soma e o simétrico em $\mathbb{Z}$, surgem naturalmente, embora não possamos dizer que o neutro, de acordo com o Capítulo 3 é $\overline{(0,0)}$, pois nenhuma das coordenadas desse par ordenado são números naturais. Não obstante, para qualquer $a \in \mathbb{N}$ temos que $(a,a) \sim (1,1)$ o que garante que $\overline{(a,a)} = \overline{(1,1)} = 0 \in \mathbb{Z}$. Também temos agora um simétrico para a soma, o que em $\mathbb{N}$ não

ocorre. Por último, observando a Definição 2.16 concluímos que a adição em $\mathbb{Z}$ é uma operação.

Observação 4.2. Com relação ao elemento simétrico da soma, como ele sempre existe e é único, denotaremos o simétrico de $x = \overline{(a,b)} \in \mathbb{Z}$ por $-x = -\overline{(a,b)} = \overline{(b,a)}$. Com isso, podemos definir a subtração em $\mathbb{Z}$ de uma maneira relativamente simples.

Definição 4.3. *Sejam $x, y \in \mathbb{Z}$. A subtração de x por y, denotada $x - y$ é definida como $x + (-y)$, onde $-y$ é o simétrico de y.*

Proposição 4.3. *Sejam $x, y \in \mathbb{Z}$, são válidas as seguintes propriedades:*

(i) $-x + y = y - x$;

(ii) $x - (-y) = x + y$;

(iii) $-x - y = -(x + y)$.

Demonstração: Sejam $x, y \in \mathbb{Z}$, temos:

(i) Pela comutatividade da soma, $(-x) + y = y + (-x) = y - x$;

(ii) Como $-(-y) = y$, pela Proposição 2.1, segue que $x - (-y) = x + y$;

(iii) Vamos mostrar que $-(x+y)$ é simétrico de $x+y$, e também que $-x-y$ é simétrico de $x+y$. De $-(x+y)+(x+y)$ temos $(x+y)-(x+y) = 0$, o que mostra que $-(x+y)$ é simétrico de $(x+y)$. Para mostrar que $(-x-y)$ é simétrico de $(x+y)$ temos que $(-x-y)+(x+y) = (-x)+(-y)+(x)+(y) = x-x+y-y = 0$. Conforme o Teorema 2.4, o simétrico é único, e portanto $-(x+y) = -x-y$.

■

4.2. A multiplicação em $\mathbb{Z}$

Agora vamos definir uma multiplicação em $\mathbb{Z}$. Podemos entender a multiplicação em $\mathbb{Z}$ como uma tentativa de extensão da operação de multiplicação válida em $\mathbb{N}$. Com isso, várias propriedades que queremos serão mantidas em $\mathbb{Z}$.

Definição 4.4. *Dados $\overline{(a,b)}$ e $\overline{(c,d)}$ em $\mathbb{Z}$, definimos a multiplicação como*

$$\overline{(a,b)} \cdot \overline{(c,d)} = \overline{(a \cdot c + b \cdot d, a \cdot d + b \cdot c)}.$$

Teorema 4.3. *A operação de multiplicação está bem definida em $\mathbb{Z}$. Isto é, a multiplicação em $\mathbb{Z}$ não depende do representante das classes de equivalência.*

Demonstração: Sejam $a, a', b, b', c, c', d, d' \in \mathbb{N}$ tais que

$$\overline{(a,b)} = \overline{(a',b')} \wedge \overline{(c,d)} = \overline{(c',d')}$$

Vamos mostrar que

$$\overline{(a,b)} \cdot \overline{(c,d)} = \overline{(a',b')} \cdot \overline{(c',d')}.$$

Pela definição de multiplicação, temos que

$$\overline{(a,b)} \cdot \overline{(c,d)} = \overline{(ac+bd, ad+bc)} \text{ e } \overline{(a',b')} \cdot \overline{(c',d')} = \overline{(a'c'+b'd', a'd'+b'c')}.$$

Vamos considerar agora as igualdades das classes. Como

$$\overline{(a,b)} = \overline{(a',b')} \iff a + b' = b + a',$$

disso concluímos que

$$(a+b')c' = (b+a')c' \tag{4.1}$$

e que

$$(a+b')d' = (b+a')d'. \tag{4.2}$$

Considerando

$$\overline{(c,d)} = \overline{(c',d')} \iff c + d' = d + c',$$

temos que

$$a(c+d') = a(d+c') \tag{4.3}$$

e também que

$$b(c+d') = b(d+c'). \tag{4.4}$$

Considerando as Equações (4.1) a (4.4) que obtemos acima, aplicando a distributiva ficamos respectivamente, com:

$$\begin{aligned} ac' + b'c' &= bc' + a'c' \text{ (Equação (4.1))} , \\ bd' + a'd' &= ad' + b'd' \text{ (Equação (4.2))} , \\ ac + ad' &= ad + ac' \text{ (Equação (4.3))} , \\ bd + bc' &= bc + bd' \text{ (Equação (4.4))} . \end{aligned}$$

Vamos agora somar termo a termo essas equações e obter:

$$ac' + b'c' + bd' + a'd' + ac + ad' + bd + bc' = bc' + a'c' + ad' + b'd' + ad + ac' + bc + bd'.$$

Cancelando os termos ac', bd', ad', bc' ficamos com:

$$b'c' + a'd' + ac + bd = a'c' + b'd' + ad + bc,$$

ou seja,

$$ac + bd + a'd' + b'c' = ad + bc + a'c' + b'd'.$$

Com isso, provamos que $(ac+bd, ad+bc) \sim (a'c'+b'd', a'd'+b'c')$, o que nos mostra que $\overline{(a,b)} \cdot \overline{(c,d)} = \overline{(a',b')} \cdot \overline{(c',d')}$ e o produto não depende do representante da classe. ■

Teorema 4.4. *Sejam $\overline{(a,b)}, \overline{(c,d)}, \overline{(e,f)}$ números inteiros quaisquer. Para a multiplicação valem as seguintes propriedades:*

(i) Fechamento;

(ii) Associativa;

(iii) Comutativa;

(iv) Da existência do elemento neutro;

(v) Da existência do elemento simétrico;

(vi) Lei do cancelamento[1]*.*

Demonstração: Sejam $a, b, c, d, e, f \in \mathbb{N}$.

(i) Fechamento:
Temos $\overline{(a,b)} \cdot \overline{(c,d)} = \overline{(ac+bd, ad+bc)}$. Como $ac + bd \in \mathbb{N}$ e também $ad + bc \in \mathbb{N}$ temos $\overline{(ac+bd, ad+bc)} \in \mathbb{Z}$.

(ii) Associativa:

$$\begin{aligned}
\Big(\overline{(a,b)} \cdot \overline{(c,d)}\Big) \cdot \overline{(e,f)} &= \overline{(ac+bd, ad+bc)} \cdot \overline{(e,f)} \\
&= \overline{((ac+bd)e + (ad+bc)f, (ac+bd)f + (ad+bc)e} \\
&= \overline{(ace + bde + adf + bcf, acf + bdf + ade + bce)} \\
&= \overline{(ace + adf + bcf + bde, acf + ade + bce + bdf)} \\
&= \overline{(a(ce+df) + b(cf+de), a(cf+de) + b(ce+df))} \\
&= \overline{(a,b)} \cdot \overline{(ce+df, cf+de)} \\
&= \overline{(a,b)} \cdot \Big(\overline{(c,d)} \cdot \overline{(e,f)}\Big).
\end{aligned}$$

(iii) Comutativa:
$\overline{(a,b)} \cdot \overline{(c,d)} = \overline{(ac+bd, ad+bc)} = \overline{(ca+db, bc+da)} = \overline{(c,d)} \cdot \overline{(a,b)}$.

[1] A lei do cancelamento do produto é para todo elemento diferente do neutro da soma, ou seja, diferente de 0.

(iv) Da existência do elemento neutro:
Consideremos o número $\overline{(2,1)}$. Vamos mostrar que ele é neutro pela direita. Temos $\overline{(a,b)}\cdot\overline{(2,1)} = \overline{(2a+b, a+2b)} = \overline{(a,b)}$. A última igualdade ocorre porque $a+a+2b = b+2a+b$. Analogamente, se mostra que $\overline{(2,1)}$ é neutro pela esquerda. A unicidade é garantida pelo Teorema 2.3, a menos de escolha do representante da classe.

(v) Distributiva:
Primeiro vamos mostrar a distributiva à esquerda.

$$\begin{aligned}
\overline{(a,b)} \cdot \Big(\overline{(c,d)} + \overline{(e,f)}\Big) &= \overline{(a,b)} \cdot (\overline{(c+e, d+f)}) \\
&= \overline{(a(c+e)+b(d+f), a(d+f)+b(c+e)}} \\
&= \overline{(ac+ae+bd+bf, ad+af+bc+be)} \\
&= \overline{(ac+bd, ad+bc)} + \overline{(ae+bf, af+be)} \\
&= \Big(\overline{(a,b)} \cdot \overline{(c,d)}\Big) + \Big(\overline{(a,b)} \cdot \overline{(e,f)}\Big).
\end{aligned}$$

Pela comutatividade do produto em $\mathbb{Z}$ e pela distributividade à esquerda, a distributividade a direita está também provada.

(vi) Lei do cancelamento:
Suponha que $\overline{(a,b)} \neq 0$ seja tal que $\overline{(a,b)} \cdot \overline{(c,d)} = \overline{(a,b)} \cdot \overline{(e,f)}$. Ou seja,

$$\overline{(ac+bd, ad+bc)} = \overline{(ae+bf, af+be)},$$

o que equivale a

$$ac+bd+af+be = ad+bc+ae+bf,$$

isto é,

$$a(c+f)+b(d+e) = a(d+e)+b(c+f).$$

Como $\overline{(a,b)} \neq 0$, $a \neq b$. Suponhamos, sem perda de generalidade, que $a > b$. Temos que $a = b+m$ para algum m natural. Substituindo na igualdade anterior, ficamos com

$$(b+m)(c+f)+b(d+e) = (b+m)(d+e)+b(c+f)$$

e então,

$$bc+bf+mc+mf+bd+be = bd+be+md+me+bc+bf.$$

Cancelando os termos bc, bf, bd, be, obtemos

$$\begin{aligned}
mc+mf = md+me &\iff m(c+f) = m(d+e) \\
&\iff c+f = d+e \\
&\iff (c,d) \sim (e,f).
\end{aligned}$$

E portanto

$$\overline{(c,d)} = \overline{(e,f)}.$$

■

Podemos usar a notação como na Observação 4.2 e na Definição 4.3. Assim, se $x = \overline{(a,b)}$, poderemos quando conveniente trabalhar somente com a notação da variável x, ao invés de usar a classe. Por outro lado, em vista de necessidade, não abandonaremos a notação das classes de equivalência.

Teorema 4.5. *Sejam x, y números inteiros quaisquer. É válido que*

$$-(xy) = x(-y) = (-x)y.$$

Demonstração: A demonstração consiste em explorar a unicidade do simétrico, conforme o Teorema 2.4. Vamos mostrar que xy é o simétrico de todos no enunciado. Basta observar que $xy + (-xy) = 0$. Também vale que $xy + x(-y) = x(y + (-y)) = x0 = 0$. Por último, $xy + (-x)y = (x + (-x))y = 0y = 0$. ■

Corolário 4.1. *Se $x, y \in \mathbb{Z}$, então vale $(-x)(-y) = xy$.*

Demonstração: Observando o Teorema 4.5 concluímos que vale $(-x)(-y) = -(x(-y)$, como o produto é comutativo, temos $-((-y)x) = -(-(yx))$, o que, pela Proposição 2.1 implica que $-(-(yx)) = yx = xy$. ■

Com isso, podemos observar que $\mathbb{Z}$ com a soma dada na Definição 4.2 e com o produto dado na Definição 4.4, tem as propriedades enunciadas na Definição 2.25, e portanto é um anel.

4.3. A relação de ordem em $\mathbb{Z}$

Definição 4.5. *Dados $\overline{(a,b)}$ e $\overline{(c,d)}$ em $\mathbb{Z}$, definimos a relação de ordem $\leq$ e dizemos que $\overline{(a,b)}$ é menor do que ou igual a $\overline{(c,d)}$ quando $a+d \leq b+c$ e denotamos por $\overline{(a,b)} \leq \overline{(c,d)}$.*

Teorema 4.6. *A relação de ordem está bem definida, isto é, para $\overline{(a,b)} = \overline{(a',b')}$ e $\overline{(c,d)} = \overline{(c',d')}$, se $\overline{(a,b)} \leq \overline{(c,d)}$, então $\overline{(a',b')} \leq \overline{(c',d')}$.*

Demonstração:

Sejam $\overline{(a,b)} = \overline{(a',b')}$ e $\overline{(c,d)} = \overline{(c',d')}$. Logo $a + b' = b + a'$ e $c + d' = d + c'$.

Supondo $\overline{(a,b)} \leq \overline{(c,d)} \iff a + d \leq b + c$, temos $a + d \leq b + c$ e existe $m \in \mathbb{N}$ tal que $(a + d) + m = b + c$. Assim

$$b + a' + c + d' = a + b' + d + c'$$
$$a' + d' + a + d + m = b' + c' + a + d$$
$$a' + d' + m = b' + c'$$
$$a' + d' \leq b' + c',$$

o que mostra que $\overline{(a', b')} \leq \overline{(c', d')}$

■

Teorema 4.7. *Sejam $\overline{(a, b)}, \overline{(c, d)}, \overline{(e, f)}$ números inteiros quaisquer. Para a relação de ordem valem as seguintes propriedades:*

(i) Reflexiva;

(ii) Antissimétrica;

(iii) Transitiva;

(iv) Totalidade;

(v) Compatibilidade com a adição;

(vi) Compatibilidade com a multiplicação.

Demonstração:

(i) Reflexiva:
De fato, como $a + b \leq b + a$, segue que $\overline{(a, b)} \leq \overline{(a, b)}$.

(ii) Antissimétrica:
Supondo

$$\overline{(a, b)} \leq \overline{(c, d)} \ \wedge \ \overline{(c, d)} \leq \overline{(a, b)}$$

temos que

$$a + d \leq b + c \ \wedge \ c + b \leq d + a$$

Pela antissimetria em $\mathbb{N}$, temos que $a + d = c + b$, então $(a, b) \sim (c, d)$ e $\overline{(a, b)} = \overline{(c, d)}$.

(iii) Transitiva:
Supondo

$$\overline{(a, b)} \leq \overline{(c, d)} \ \wedge \ \overline{(c, d)} \leq \overline{(e, f)},$$

temos que

$$a + d \leq b + c \ \wedge \ c + f \leq d + e.$$

Logo

$$a + d + f \leq b + c + f \ \wedge \ c + f + b \leq d + e + b.$$

Assim

$$a + d + f \ \leq \ d + e + b,$$

ou seja

$$a + f \ \leq \ b + e.$$

Portanto

$$\overline{(a, b)} \ \leq \ \overline{(e, f)}.$$

(iv) Totalidade:
Pela totalidade em $\mathbb{N}$, dados $a, b, c, d \in \mathbb{N}$, temos que $a + d \leq b + c \vee c + b \leq d + a$. Logo $\overline{(a, b)} \leq \overline{(c, d)} \vee \overline{(c, d)} \leq \overline{(a, b)}$.

(v) Compatibilidade com a adição:
Supondo que $\overline{(a, b)} \ \leq \ \overline{(c, d)}$, temos que $a + d \ \leq \ b + c$.

Se e, f são também naturais, pela compatibilidade da adição em $\mathbb{N}$ temos:

$$a + d + e + f \leq b + c + e + f,$$

ou seja,

$$a + e + d + f \ \leq \ b + f + c + e.$$

Logo

$$\overline{(a + e, b + f)} \ \leq \ \overline{(c + e, d + f)}.$$

Portanto

$$\overline{(a, b)} + \overline{(e, f)} \ \leq \ \overline{(c, d)} + \overline{(e, f)}.$$

(vi) Compatibilidade com a multiplicação:
Suponhamos $\overline{(a, b)} \leq \overline{(c, d)}$ e também $0 = \overline{(1, 1)} < \overline{(e, f)}$. Desse modo, temos que $e > f$ pois $1 + f < 1 + e$. Seja então $e = f + m$ para algum m natural. As linhas abaixo são equivalentes:

$$\begin{aligned}
\overline{(a, b)} &\leq \overline{(c, d)} \\
a + d \ &\leq \ b + c \\
(a + d)m \ &\leq \ (b + c)m \\
(a + d)m + (a + d)f + (b + c)f \ &\leq \ (b + c)m + (a + d)f + (b + c)f \\
(a + d)(f + m) + (b + c)f \ &\leq \ (a + d)f + (b + c)(f + m)
\end{aligned}$$

$$\begin{aligned}(a+d)e+(b+c)f &\leq (a+d)f+(b+c)e\\ ae+bf+cf+de &\leq af+be+ce+df\\ \overline{(ae+bf, af+be)} &\leq \overline{(ce+df, cf+de)}\\ \overline{(a,b)}\cdot\overline{(e,f)} &\leq \overline{(c,d)}\cdot\overline{(e,f)}.\end{aligned}$$

■

Observação 4.3. A compatibilidade com a multiplicação, que acabamos de provar, também garante que se $\overline{(a,b)}\cdot\overline{(e,f)} \leq \overline{(c,d)}\cdot\overline{(e,f)}$, então $\overline{(a,b)} \leq \overline{(c,d)}$. Comentário análogo vale para a compatibilidade com a adição.

Proposição 4.4. *É válido que* $\overline{(a,b)} < \overline{(c,d)}$ *se, e somente se, existe um* $\overline{(e,f)} > 0$ *em que* $\overline{(a,b)} + \overline{(e,f)} = \overline{(c,d)}$.

Demonstração: Supondo $\overline{(a,b)} < \overline{(c,d)}$, temos $a+d < b+c$, ou seja, $a+d+m = b+c$, para algum m natural. Consideremos o número $\overline{(m+1,1)}$, vamos mostrar que ele é o número procurado. Sabemos que ele é positivo pois

$$\overline{(1,1)} < \overline{(m+1,1)} \iff 1+1 < 1+m+1.$$

Agora, $\overline{(a,b)} + \overline{(m+1,1)} = \overline{(a+m+1,b+1)} = \overline{(a+m,b)}$. Podemos observar que $\overline{(a+m,b)} = \overline{(c,d)}$, pois $a+m+d = b+c$.

Provemos a volta. Suponhamos que $\overline{(a,b)} + \overline{(e,f)} = \overline{(c,d)}$, para algum $\overline{(e,f)} > 0$. Temos $e = f+m$ para algum m natural. Assim, ficamos com

$$\overline{(a+f+m,b+f)} = \overline{(a+m,b)} = \overline{(c,d)}.$$

Assim, $a+m+d = b+c$, logo, $a+d < b+c$. Portanto $\overline{(a,b)} < \overline{(c,d)}$. ■

A próxima proposição complementa a proposição anterior.

Proposição 4.5. *É válido que* $\overline{(a,b)} \leq \overline{(c,d)}$ *se, e somente se, existe um* $\overline{(e,f)} \geq 0$ *em que* $\overline{(a,b)} + \overline{(e,f)} = \overline{(c,d)}$.

Demonstração: Para provar a ida, separemos em dois casos:

(i) Se $\overline{(a,b)} = \overline{(c,d)}$ então $\overline{(a,b)} + 0 = \overline{(c,d)}$.

(ii) Se $\overline{(a,b)} < \overline{(c,d)}$, caímos na Proposição 4.4.

Para provar a volta, também separaremos em dois casos:

(i) Se $\overline{(e,f)} = 0$, temos $\overline{(a,b)} + 0 = \overline{(c,d)}$.

(ii) Se $\overline{(e,f)} > 0$, caímos na Proposição 4.4.

■

Vamos relembrar que um número negativo, conforme Definição 2.23, em $\mathbb{Z}$, é qualquer número menor que 0.

Exemplo 4.8. O número $\overline{(1,2)} < \overline{(1,1)} = 0$. De fato, $1 + 1 < 2 + 1$.

Exemplo 4.9. O número $\overline{(4,2)}$ é positivo. Pois de acordo com a Definição 2.22, temos que $\overline{(1,1)} < \overline{(4,2)}$ pois $1 + 2 < 1 + 4$.

Exemplo 4.10. O número $0 = \overline{(1,1)}$ não é nem positivo, nem negativo, conforme as Definições 2.22 e 2.23, pois ele não é maior do que o zero do conjunto, embora ele seja maior do que ou igual.

Exemplo 4.11. Quando quisermos mencionar os números positivos e incluir o zero, chamaremos simplesmente de números não negativos. Analogamente, os números não positivos são os números negativos junto com o zero.

Proposição 4.6. *Um número inteiro é não negativo se, e somente se, a primeira coordenada é maior do que ou igual a segunda coordenada. Isto é, se* $\overline{(a,b)}$ *é um número inteiro, então vale* $0 \leq \overline{(a,b)} \iff b \leq a$.

Demonstração: Seja $0 = \overline{(1,1)}$. Tem-se que:

$$0 = \overline{(1,1)} \leq \overline{(a,b)} \iff 1 + b \leq 1 + a \iff b \leq a.$$

■

Corolário 4.2. *Dado um número inteiro, ou ele é maior do que ou igual a zero, ou seu simétrico aditivo é, ou seja, se* $\overline{(a,b)} \in \mathbb{Z}$, *então* $\overline{(a,b)} \geq 0 = \overline{(1,1)}$ *ou* $-\overline{(a,b)} \geq 0$.

Demonstração: Como a relação de ordem $\leq$ é total conforme o Teorema 4.7, vale que $\overline{(a,b)} \leq \overline{(1,1)}$ ou $\overline{(1,1)} \leq \overline{(a,b)}$. Se $\overline{(a,b)}$ é não negativo é imediato que o corolário é válido. Já no segundo caso, de $\overline{(a,b)} \leq \overline{(1,1)}$ temos $a + 1 \leq b + 1 \implies a \leq b$.
Com isso, $-\overline{(a,b)} = \overline{(b,a)} \geq \overline{(1,1)}$ pela Proposição 4.6. ■

Corolário 4.3. *Um número inteiro é não negativo se, e somente se, seu simétrico aditivo é não positivo.*

Demonstração: Pelo Corolário 4.2, considerando um número x e seu simétrico $-x$, ao menos um deles é não negativo. Caso seja $0 \leq x$ temos $0+(-x) \leq x+(-x)$. Logo $-x \leq 0$, assim $-x$ é não positivo. No outro caso supomos que $0 \leq -x$, daí $0 + x \leq -x + x = 0$, assim $x \leq 0$. ∎

Proposição 4.7. *A soma de dois inteiros não negativos é não negativa, isto é, se $x, y \in \mathbb{Z}$ com $x, y \geq 0$ então $0 \leq x + y$.*

Demonstração: Conforme o Corolário 4.3, como $x, y \geq 0$ temos $-x \leq 0$ e $-y \leq 0$. Como qualquer inteiro não negativo é maior do que ou igual a qualquer inteiro não positivo, temos $-y \leq +x$, e pela compatibilidade da soma com a relação de ordem (Teorema 4.7), temos $-y + y \leq x + y$. Desse modo, $x + y \geq 0$. ∎

Proposição 4.8. *Se $x, x' \in \mathbb{Z}$ com $x' \geq x$, então existe y inteiro, tal que $y \geq 0$ e $x' = x+y$.*

Demonstração: Se $x' = x$ então $y = 0$. Caso contrário, se $x' > x$ então considere $x = \overline{(a, b)}, x' = \overline{(a', b')}$. Temos

$$x < x' \iff a + b' < b + a' \iff b + a' = a + b' + c \text{ para algum } c \in \mathbb{N}.$$

Logo

$$a + c + b' = b + a' \iff (a + c, b) \sim (a', b').$$

Temos também que $\overline{(a + c, b)} = \overline{(a + c + 1, b + 1)} = \overline{(a, b)} + \overline{(c + 1, 1)}$, onde usamos a Definição 4.2 e a Proposição 4.1. Assim $x' = \overline{(a + c, b)} = \overline{(a, b)} + \overline{(c + 1, 1)}$.

O número $\overline{(c + 1, 1)}$ é inteiro, pois suas entradas são números naturais, e é positivo pois $\overline{(1, 1)} \leq \overline{(c + 1, 1)} \iff 1 + 1 \leq 1 + (c + 1)$ e como c é natural, ele não pode ser zero, conforme nossa construção. Dessa forma $\overline{(c + 1, 1)}$ é o y desejado. ∎

Proposição 4.9. *Sejam x, x' números inteiros quaisquer. Se existe y inteiro tal que $y \geq 0$ e $x' = x + y$, então $x \leq x'$.*

Demonstração: Seja $x = \overline{(a, b)}$. Suponhamos $0 \leq y$, assim $y = \overline{(e, f)}$ para e, f naturais tais que $e \geq f$ (Proposição 4.6). De $x' = x + y$ temos que $x' = \overline{(a + e, b + f)}$. Temos que

$$f \leq e$$

assim

$$a + b + f \leq b + a + e$$

e então

$$a + (b + f) \leq b + (a + e).$$

Logo

$$\overline{(a, b)} \leq \overline{(a + e, b + f)}$$

e portanto

$$x \leq x'.$$

■

Proposição 4.10. *O quadrado de um número inteiro é um inteiro não negativo, ou seja, se* $\overline{(a, b)} \in \mathbb{Z}$*, então vale* $0 = \overline{(1, 1)} \leq \overline{(a, b)} \cdot \overline{(a, b)}$.

Demonstração: Temos $\overline{(a, b)} \cdot \overline{(a, b)} = \overline{(aa + bb, ab + ba)}$. Observando a Proposição 4.6, queremos mostrar que $aa + bb \geq ab + ba$. Considerando a tricotomia de $\mathbb{N}$ (aplicada em a e b) dada na Proposição 3.1, separaremos a demonstração em 3 casos:

(i) Caso $a = b$:
Temos $aa + aa \geq aa + aa$.

(ii) Caso $a < b$:
Temos $b = a + c$, com $c \in \mathbb{N}$. Logo

$$aa + bb = aa + (a + c)(a + c) = aa + aa + ac + ac + cc$$

e

$$ab + ba = a(a + c) + (a + c)a = aa + ac + aa + ca$$

Notemos que $aa + bb = ab + ba + cc$, com $cc \in \mathbb{N}$, assim $aa + bb \geq ab + ba$.

(iii) Caso $b < a$:
Temos $a = b + c$, com $c \in \mathbb{N}$. Logo

$$aa + bb = (b + c)(b + c) + bb = bb + bc + cb + cc + bb$$

e

$$ab + ba = (b + c)b + b(b + c) = bb + cb + bb + bc.$$

Como $aa + bb = ab + ba + cc$, com $cc \in \mathbb{N}$, provamos que $aa + bb \geq ab + ba$.

■

Proposição 4.11. *O produto de dois inteiros não negativos é não negativo.*

Demonstração: Seja r um número inteiro, tal que $0 \leq r$. Se s é um inteiro tal que $0 \leq s$, pela compatibilidade do produto com a relação de ordem (Teorema 4.7), então $0 \cdot s \leq r \cdot s$, assim $0 \leq rs$. ∎

Proposição 4.12. *Sejam x, y, x', y' números inteiros não negativos, tais que $x \leq x'$ e $y \leq y'$. Vale que $xy \leq x'y'$.*

Demonstração: Suponhamos $x' \geq x$ e $y' \geq y$. Temos que $x' = x + r$ para algum r inteiro não negativo, e que $y' = y + s$ para algum s inteiro não negativo. Segue que $x'y' = (x + r)(y + s) = xy + xs + ry + rs \geq 0$, pois cada uma dessas parcelas é não negativa. De fato, sendo x, y, r, s todos não negativos, o produto de quaisquer dois deles é não negativo (Proposição 4.11). Pela Proposição 4.9 obtemos $xy \leq x'y'$. ∎

4.4. Imersão de $\mathbb{N}$ em $\mathbb{Z}$

A imersão que trataremos a seguir justificará que utilizemos apenas um símbolo para a adição, quer trabalhemos com $\mathbb{N}$, quer trabalhemos com $\mathbb{Z}$. Isso valerá também para $\mathbb{Q}$ e $\mathbb{R}$, que serão apresentados nos próximos capítulos. A ideia de imersão trata de nos permitir corresponder um conjunto num outro, no caso, $\mathbb{N}$ em $\mathbb{Z}$, e assim trabalhar como se $\mathbb{N}$ fosse um subconjunto de $\mathbb{Z}$.

Teorema 4.8. *Considere a função definida abaixo:*

$$\begin{aligned} f\colon \mathbb{N} &\to \mathbb{Z} \\ x &\mapsto \overline{(x+1,1)}. \end{aligned}$$

Essa função tem as propriedades a seguir:

(i) $f(a+b) = f(a) + f(b)$;

(ii) $f(a \cdot b) = f(a) \cdot f(b)$;

(iii) $a \leq b \implies f(a) \leq f(b)$.

Demonstração:

(i)

$$\begin{aligned} f(a+b) &= \overline{(a+b+1,1)} \\ &= \overline{(a+1+b+1,1+1)} \\ &= \overline{(a+1,1)} + \overline{(b+1,1)} \\ &= f(a) + f(b). \end{aligned}$$

(ii)

$$\begin{aligned} f(a \cdot b) &= \overline{(ab+1,1)} \\ &= \overline{(ab+a+b+1+1, a+1+b+1)} \\ &= \overline{((a+1)(b+1)+1, (a+1)1+1(b+1))} \\ &= \overline{(a+1,1)} \cdot \overline{(b+1,1)} \\ &= f(a) + f(b). \end{aligned}$$

(iii) Se $a = b$ então $f(a) = f(b)$ é óbvio. Suponhamos, por outro lado, $a \neq b$. Então $a < b \iff b = a + m$ para algum $m \in \mathbb{N}$. Temos então $f(a) = \overline{(a+1,1)}$ e $f(b) = f(a+m) = \overline{(a+m+1,1)}$. Vemos que $\overline{(a+1,1)} \leq \overline{(a+m+1,1)}$ porque $a + 1 + 1 \leq 1 + a + m + 1$.

■

Observação 4.4. A partir de agora, temos a liberdade de escrever os números inteiros com a notação usual de $\mathbb{N}$, isto é $1 = \overline{(2,1)}, 2 = \overline{(3,1)}, 3 = \overline{(4,1)}$ e assim por diante, além de representar o $\overline{(1,2)} = -1$, $\overline{(1,3)} = -2$, $\overline{(4,1)} = -3$ e, analogamente, ad infinitum.

Teorema 4.9. *O conjunto* $\mathbb{N}$ *não é limitado superiormente em* $\mathbb{Z}$.

Demonstração: O teorema deve ser entendido no contexto da imersão de $\mathbb{N}$ em $\mathbb{Z}$. Por contradição, vamos supor que $\overline{(a,b)} \in \mathbb{Z}$ seja um número fixo e uma cota superior de $\mathbb{N}$. Sabemos que um número natural em $\mathbb{Z}$ é da forma $\overline{(n+1,1)} \in \mathbb{Z}$, com $n \in \mathbb{N}$. Logo, devemos ter $\overline{(n+1,1)} \leq \overline{(a,b)}$ para qualquer $n \in \mathbb{N}$. Temos $n + 1 + b \leq 1 + a$ e então

$$n + b \leq a, \tag{4.5}$$

em que a e b são naturais fixos e n um natural qualquer.

Substituindo n por n_0 na Inequação 4.5, obtemos $n_0 + b \leq a$. Se for $n_0 + b = a$, tomando $n_1 = n_0 + 1$, obtemos que

$$a = n_0 + b < n_0 + 1 + b = n_1 + b,$$

em que $n_1 + b \in \mathbb{N}$, o que é uma contradição. Se for $n_0 + b < a$, então $a = n_0 + b + m$, para algum $m \in \mathbb{N}$. Tomando $n_1 = n_0 + m + 1$, obtemos

$$a = n_0 + b + m < n_0 + m + 1 + b = n_1 + b,$$

em que $n_1 + b \in \mathbb{N}$, o que é uma contradição. Portanto, em $\mathbb{Z}$ não existe uma cota superior para $\mathbb{N}$.

■

Exemplo 4.12. Considerando a imersão, podemos entender o produto $2 \cdot \overline{(a,b)}$ da seguinte forma: $2 = \overline{(3,1)}$ e $\overline{(3,1)} \cdot \overline{(a,b)} = \overline{(3a+b, 3b+a)} = \overline{(2a, 2b)}$. Essa é a notação usual quando se trabalha com elementos onde a multiplicação por um escalar funciona da maneira usual $k \cdot \overline{(a,b)} = \overline{(ka, kb)}$ quando $k > 0$, já quando $k < 0$ precisamos inverter as coordenadas, o que não é usual.

A imersão de $\mathbb{N}$ em $\mathbb{Z}$ permite-nos interpretar $\mathbb{N}$ como um subconjunto de $\mathbb{Z}$, embora pela nossa construção fique evidente que isso não ocorra, nos termos de elementos dos conjuntos. Mas, por outro lado, as operações de adição e multiplicação e a relação de ordem funcionam analogamente em $\mathbb{Z}$, ou seja, o nosso objetivo do capítulo de construir uma adição, uma multiplicação e uma relação de ordem mantendo certa semelhança com $\mathbb{N}$ foi alcançado.

Essa é uma parte importante da construção dos números inteiros. Em geral não importa o que é um número, mas apenas o que conseguimos fazer com ele, as regras do jogo. Por outro lado, a construção do conjunto dos números inteiros mostra-nos que, a existência de um conjunto $\mathbb{N}$, a lógica e a teoria de conjuntos elementar que assumimos até agora garantem que existe um conjunto $\mathbb{Z}$ que podemos manipular com as regras mostradas.

Por certo ponto de vista, não interessa o que são e como são definidas as operações de soma e produto, mas, admitindo que exista um conjunto A com uma operação de soma e uma operação de produto, ambas tendo certas propriedades, é possível provar teoremas sem levar em conta a *natureza* dos entes matemáticos envolvidos.

A construção de $\mathbb{Z}$, as apresentações e provas das proposições apresentadas caminham nesse sentido de permitir uma abstração do conjunto, para que não seja mais necessário trabalhar com pares ordenados (ainda mais sem o 0 em $\mathbb{N}$!).

Poderíamos desenvolver alguns tópicos importantes levando em conta a natureza dos nossos números inteiros, que são pares ordenados. Isso é satisfatório, se conseguirmos provar o que queremos. Por outro lado, tratar com conjuntos genéricos (independente da construção utilizada) permite uma abstração e uma generalização, mostrando que certas características não dependem de um conjunto específico (no nosso caso $\mathbb{N} \times \mathbb{N} / \sim$). As abstrações permitem formar conclusões dependendo de apenas algumas caracterísitcas/propriedades do conjunto. Dessa maneira, em geral a pergunta "qual é o conjunto de números inteiros?" não faz sentido, pois o que nos importa é o que podemos fazer com ele, e não como ele foi construído. Isso se tornará importante na construção de $\mathbb{R}$, podendo ser feita de dois métodos que formalizam o conjunto, mas nos interessa como $\mathbb{R}$ foi construído porque o tema deste trabalho é a construção dos números, mas na utilização do conjunto, se for feito por sequências ou por cortes de Dedekind, não é relevante.

Tá! Mas e aí, existem muitos números e cadê o 15, o 35, o -351? A resposta é

que nesse momento não possuimos um sistema de numeração, que para ser desenvolvido precisa da divisão euclidiana. O leitor interessado em verificar o sistema de numeração para $\mathbb{Z}$ pode consultar (HEFEZ, 2014b).

5. O CONJUNTO DOS NÚMEROS RACIONAIS

5.1. Ideias iniciais e objetivos

No capítulo anterior, conseguimos criar um conjunto $\mathbb{Z}$ cuja soma tivesse elemento neutro e que todo elemento tivesse um elemento simétrico nessa mesma operaçao. Neste capítulo vamos tentar construir um conjunto tal que para a multiplicação, dado qualquer elemento (exceto o neutro da soma), seja também possível encontrar um simétrico. Para isso a bibliografia utilizada será Domingues (2009) e Ferreira (2013).

O conjunto que criaremos será chamado de conjunto dos números racionais e será denotado por $\mathbb{Q}$.

Para criar os racionais, vamos utilizar o mesmo artifício das classes de equivalência num subconjunto do produto cartesiano. O produto cartesiano que precisaremos excluirá o neutro da soma em $\mathbb{Z}$ da segunda cordenada, que se justificará no próximo teorema.

Nesse sentido, consideramos

$$\mathbb{Z} \times \mathbb{Z}^* = \{\, (a, b) : a \in \mathbb{Z} \wedge b \in \mathbb{Z}^* \,\}.$$

Sobre $\mathbb{Z} \times \mathbb{Z}^*$ vamos considerar a relação definida por $(a, b) \sim (c, d) \iff ad = bc$.

Teorema 5.1. *A relação $\sim$ é de equivalência.*

Demonstração: Sejam $a, c, e \in \mathbb{Z}$ e $b, d, f \in \mathbb{Z}^*$. São válidas as propriedades:

(i) Reflexiva: $(a, b) \sim (a, b)$, pois $a \cdot b = b \cdot a$.

(ii) Simétrica: $(a, b) \sim (c, d) \implies (c, d) \sim (a, b)$.
Temos $(a, b) \sim (c, d) \implies a \cdot d = b \cdot c \implies c \cdot b = d \cdot a \implies (c, d) \sim (a, b)$.

(iii) Transitiva: $(a, b) \sim (c, d) \wedge (c, d) \sim (e, f) \implies (a, b) \sim (e, f)$.
Supondo $(a, b) \sim (c, d)$ e $(c, d) \sim (e, f)$ temos que $ad = bc$ e $cf = de$. Logo $adf = bcf$ e $bcf = bde$. Assim $adf = bde$, ou seja $afd = bed$. Como $d \neq 0$ segue que $af = be$, e então $(a, b) \sim (e, f)$.

■

Definição 5.1. *O conjunto dos números racionais é o conjunto* $\mathbb{Z} \times \mathbb{Z}^*/\sim$*, que será denotado por* $\mathbb{Q}$*.*

Claro que com a Definição 5.1, os números de $\mathbb{Q}$ são classes de equivalência em $\mathbb{Z} \times \mathbb{Z}^*$. Dessa forma, se $x \in \mathbb{Q}$, então $x = \overline{(a,b)}$. Ao invés de utilizar a notação ostensiva de pares ordenados como utilizamos no Capítulo 4, passaremos a utilizar a notação de fração, que consiste em separar os elementos do par, na ordem, por uma barra horizontal, denotada $\frac{a}{b}$ ou por uma barra inclinada denotada a/b. Dessa forma, $x = \overline{(a,b)}$ passará a ser denotado $x = \frac{a}{b}$ ou $x = a/b$. Nesse sentido, também indicamos que $a \in \mathbb{Z}$ e $b \in \mathbb{Z}^*$. Além disso, a é chamado numerador, e b é chamado denominador. Ainda, indicaremos que $\frac{a}{b} = \frac{c}{d}$ se, e somente se, $ad = bc$, isto é, $\overline{(a,b)} \sim \overline{(c,d)}$.

Exemplo 5.1. Representam o mesmo número as notações a seguir: $1/2 = 2/4 = 3/6$. O que também é fácil de provar, vejamos que $1/2 = 2/4$. De fato, em $\mathbb{Z}$ vale $1 \cdot 4 = 2 \cdot 2$. Do mesmo modo para mostrar que $1/2 = 3/6$, pois $1 \cdot 6 = 2 \cdot 3$.

Proposição 5.1. *Seja* $\frac{a}{b}$ *um número racional. Vale que* $\frac{a}{b} = \frac{ac}{bc}$*, para qualquer* $c \in \mathbb{Z}^*$*.*

Demonstração: Basta observar que $a \cdot bc = b \cdot ac$, ou que $(a,b) \sim (ac,bc)$. ∎

5.2. Adição em $\mathbb{Q}$

Definição 5.2. *Sejam* $\frac{a}{b}$ *e* $\frac{c}{d}$ *números racionais. A adição entre* $\frac{a}{b}$ *e* $\frac{c}{d}$*, denotada por* $\frac{a}{b} + \frac{c}{d}$*, é definida como* $\frac{ad+bc}{bd}$*.*

Teorema 5.2. *A adição está bem definida, isto é, se* $\frac{a}{b} = \frac{a'}{b'}$ *e* $\frac{c}{d} = \frac{c'}{d'}$*, então* $\frac{a}{b} + \frac{c}{d} = \frac{a'}{b'} + \frac{c'}{d'}$*.*

Demonstração: Sejam a/b e a'/b' duas representações de um mesmo número racional, tal que $\frac{a}{b} = \frac{a'}{b'}$, isto é, $ab' = ba'$. Do mesmo modo, sejam c/d e c'/d' duas representações de um número racional qualquer, tal que $\frac{c}{d} = \frac{c'}{d'}$, isto é, $cd' = dc'$.

Vamos mostrar que $\frac{a}{b} + \frac{c}{d} = \frac{a'}{b'} + \frac{c'}{d'}$. Pela definição de adição, no primeiro caso temos $\frac{ad+bc}{bd}$, e no segundo caso temos $\frac{a'd'+b'c'}{b'd'}$. Devemos mostrar que $\frac{ad+bc}{bd} = \frac{a'd'+b'c'}{b'd'}$, ou seja, que

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

que equivale a

$$adb'd' + bcb'd' = bda'd' + bdb'c'$$

isto é

$$ab'dd' + cd'bb' = a'bdd' + c'dbb'.$$

Como essa última igualdade é uma tautologia, pois $ab' = a'b$ e $cd' = c'd$, a igualdade desejada é verdadeira. ■

Teorema 5.3. *Para a adição em $\mathbb{Q}$ valem as seguintes propriedades:*

(i) Fechamento;

(ii) Associativa;

(iii) Comutativa;

(iv) Da existência do elemento neutro;

(v) Da existência do elemento simétrico;

(vi) Lei do cancelamento;

Demonstração: Sejam $\frac{a}{b}, \frac{c}{d}, \frac{e}{f}$ números racionais quaisquer, temos:

(i) Fechamento:

$$\frac{a}{b} + \frac{c}{d} = \frac{ad + bc}{bd} \in \mathbb{Q}, \text{ pois } ad + bc \in \mathbb{Z} \text{ e } bd \in \mathbb{Z}^*.$$

(ii) Associativa:

$$\begin{aligned}\left(\frac{a}{b} + \frac{c}{d}\right) + \frac{e}{f} &= \frac{ad + bc}{bd} + \frac{e}{f} \\ &= \frac{(ad + bc)f + bde}{bdf} \\ &= \frac{adf + bcf + bde}{bdf} \\ &= \frac{adf + b(cf + de)}{bdf} \\ &= \frac{a}{b} + \frac{cf + de}{df} \\ &= \frac{a}{b} + \left(\frac{c}{d} + \frac{e}{f}\right).\end{aligned}$$

(iii) Comutativa:

$$\frac{a}{b} + \frac{c}{d} = \frac{ad + bc}{bd} = \frac{cb + da}{db} = \frac{c}{d} + \frac{a}{b}.$$

(iv) Da existência do elemento neutro:
Consideremos o número $\frac{0}{a}$, com $a \neq 0$. Temos:

$$\frac{0}{a} + \frac{c}{d} = \frac{0d + ac}{ad} = \frac{ac}{ad} = \frac{c}{d} \text{ pois } ac \cdot d = ad \cdot c.$$

Portanto $\frac{0}{a}$ é o neutro aditivo em $\mathbb{Q}$, que será denotado por $0 = \frac{0}{a}$.

(v) Da existência do elemento simétrico:
Dado $\frac{a}{b} \in \mathbb{Q}$, têm-se que $\frac{-a}{b} \in \mathbb{Q}$ é tal que

$$\frac{a}{b} + \frac{-a}{b} = \frac{ab + (-ab)}{bb} = \frac{0}{bb} = 0.$$

(vi) A lei do cancelamento decorre do Teorema 2.5.

■

5.3. A multiplicação em $\mathbb{Q}$

Definição 5.3. *Sejam $\frac{a}{b}$ e $\frac{c}{d}$ números racionais quaisquer. A multiplicação de $\frac{a}{b}$ por $\frac{c}{d}$ será denotada por $\frac{a}{b} \cdot \frac{c}{d}$ e é definida por $\frac{ac}{bd}$.*

Teorema 5.4. *A multiplicação em $\mathbb{Q}$ está bem definida.*

Demonstração: Sejam $\frac{a}{b} = \frac{a'}{b'}$ e $\frac{c}{d} = \frac{c'}{d'}$ números racionais quaisquer. Então temos $ab' = ba'$ e $cd' = dc'$. Segue que

$$ab'cd' = ba'dc' \iff acb'd' = bda'c',$$

com isso $\frac{ac}{bd} = \frac{a'c'}{b'd'}$, ou seja, $\frac{a}{b} \cdot \frac{c}{d} = \frac{a'}{b'} \cdot \frac{c'}{d'}$. ■

Teorema 5.5. *Para a multiplicação em $\mathbb{Q}$ valem as seguintes propriedades:*

(i) Fechamento;

(ii) Associativa;

(iii) Comutativa;

(iv) Da existência do elemento neutro;

(v) Da existência do elemento simétrico;

(vi) Lei do cancelamento.

Demonstração: Sejam $\frac{a}{b}, \frac{c}{d}, \frac{e}{f} \in \mathbb{Q}$.

(i) Fechamento:
Temos que $\frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bc} \in \mathbb{Q}$, pois $ac \in \mathbb{Z}$ e $bd \in \mathbb{Z}$. Além disso, em $\mathbb{Z}$ vale que

$$bd = 0 \iff b = 0 \vee d = 0,$$

e como originalmente tínhamos b, d ambos não nulos, temos que $bd \neq 0$.

(ii) Associativa:

$$\left(\frac{a}{b} \cdot \frac{c}{d}\right) \cdot \frac{e}{f} = \left(\frac{ac}{bd}\right) \frac{e}{f} = \frac{ace}{bdf} = \frac{a}{b} \cdot \frac{ce}{df} = \frac{a}{b} \cdot \left(\frac{c}{d} \cdot \frac{e}{f}\right).$$

(iii) Comutativa:

$$\frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd} = \frac{ca}{db} = \frac{c}{d} \cdot \frac{a}{b}.$$

(iv) Da existência do elemento neutro:
Afirmamos que o $\frac{1}{1}$ é o neutro do produto, pois: $(1c/1d) = c/d$. Assim, provamos que é neutro pela esquerda. Pela direita é evidente pela comutatividade do produto em $\mathbb{Z}$.

Observação 5.1. Para cada $a \in \mathbb{Z}^*$ tem-se que $\frac{a}{a} = \frac{1}{1}$, pois $a \cdot 1 = 1 \cdot a$.

(v) Da existência do elemento simétrico:
Vamos obter o simétrico de $\frac{a}{b}$. Por hipótese, temos $b \neq 0$. Suponhamos que $a = 0$. Vejamos se algum $\frac{c}{d}$ pode ser simétrico de $\frac{a}{b}$. Temos $\frac{a}{b}\frac{c}{d} = \frac{ac}{bd} = \frac{0}{bd} \neq \frac{1}{1}$. Assim não podemos ter zero no numerador.
Suponhamos por outro lado, $a \neq 0$. Temos $\frac{ac}{bd} = \frac{1}{1} \implies ac = bd$, que é o mesmo que dizer que $\frac{a}{b} = \frac{d}{c}$. Para que a igualdade ocorra, basta tomar $c = b$ e $d = a$, assim, o simétrico do produto de $\frac{a}{b}$, para $a \neq 0$, é $\frac{c}{d} = \frac{b}{a}$.

(vi) A lei do cancelamento é consequência do Teorema 2.5.

■

5.4. A relação de ordem em $\mathbb{Q}$

Para definirmos a relação de ordem em $\mathbb{Q}$ vamos proceder de maneira semelhante à de $\mathbb{Z}$, mas com uma diferença crucial, que exploraremos logo depois da Definição 5.4.

Teorema 5.6. *Sejam a, b números inteiros, sendo b não nulo. As igualdades (em $\mathbb{Q}$) a seguir são válidas:*

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

Demonstração: Para a primeira igualdade, temos

$$\frac{-a}{b} = \frac{a}{-b} \iff (-a)(-b) = ba,$$

que vale conforme Corolário 4.1. Para mostrar a segunda igualdade, consideremos o número racional $\frac{a}{b}$. Ele é simétrico aditivo de $-\frac{a}{b}$, pois a soma é comutativa. Vejamos que ele também é simétrico aditivo de $\frac{-a}{b}$, pois vale que

$$\frac{-a}{b} + \frac{a}{b} = \frac{(-a)b + ba}{bb} = \frac{ab - ab}{bb} = \frac{0}{bb} = \frac{0}{1},$$

pelo Teorema 4.5. ■

Corolário 5.1. *Qualquer que seja o número racional $\frac{a}{b}$, é sempre possível escolher uma representação $\frac{c}{d}$, de tal modo que $\frac{a}{b} = \frac{c}{d}$, com $d > 0$.*

Demonstração: A primeira igualdade do Teorema 5.6 diz que $\frac{-a}{b} = \frac{a}{-b}$. Os denominadores são b e $-b$, ambos não nulos, logo pelo Corolário 4.2, ao menos um deles é positivo. ■

Definição 5.4. *Sejam $\frac{a}{b}$ e $\frac{c}{d}$ números racionais quaisquer, sendo b e d inteiros positivos. A relação de ordem $\leq$ entre $\frac{a}{b}$ e $\frac{c}{d}$ será denotada por $\frac{a}{b} \leq \frac{c}{d}$ para indicar que $ad \leq bc$ e diremos que $\frac{a}{b}$ é menor do que ou igual a $\frac{c}{d}$.*

Observação 5.2. Deve ser notado que a última desigualdade da Definição 5.4, bem como seu produto, são consideradas em $\mathbb{Z}$.

Vamos fazer agora a análise que comentamos no início da seção. Quando definimos a relação de ordem em $\mathbb{Z}$, podíamos utilizar qualquer representante da classe. Nos racionais, por outro lado, devemos restringir que os denominadores sejam positivos.

Afirmação: A Definição 5.4 não pode ser enfraquecida apenas retirando a obrigatoriedade dos denominadores serem positivos.

Demonstração: Observemos que o racional nulo pode ser representado das seguintes maneiras: $\frac{0}{1} = \frac{0}{-1}$ uma vez que $0 \cdot (-1) = 1 \cdot 0$. Seja $\frac{0}{1} \leq \frac{a}{b}$, temos $0b \leq 1a$. Por outro lado, de $\frac{0}{-1} \leq \frac{a}{b}$ temos $0b \leq -1a$, daí pelo Corolário 4.2, temos $a \leq 0$. Note que não fizemos nenhuma suposição sobre $a \in \mathbb{Z}$. Assim, o mesmo método que diz $a \leq 0$ também diz que $0 \leq a$, o que é uma contradição. ■

Com isso, a relação de ordem fica mais limitada no que diz respeito a escolhermos elementos para trabalhar com ela, pois agora não podemos utilizar denominadores negativos. Por outro lado, como o denominador ser negativo ou positivo é uma questão apenas de

representação do número, e não do número em si, isso não danifica o caráter da relação de ordem, que é a de ordenar números e não suas representações.

Devemos notar também que as operações de adição e multiplicação são independentes de representação, ou seja, podemos calcular uma soma ou produto sem receio de usar denominadores negativos, embora o denominador zero não possa ser utilizado, não tanto por questão de representação, mas porque começa a se configurar o conceito de número, e todo número racional precisa ter um denominador não nulo.

Proposição 5.2. *A relação de ordem está bem definida, isto é, se* $\frac{a}{b} = \frac{a'}{b'}$ *e* $\frac{c}{d} = \frac{c'}{d'}$ *com* $\frac{a}{b} \leq \frac{c}{d}$ *e com* $b, b', d, d' > 0$*, então* $\frac{a'}{b'} \leq \frac{c'}{d'}$.

Demonstração: Das hipóteses, temos:

$$ab' = ba',\ cd' = dc',$$

$$ad \leq bc \iff 0 \leq bc - ad.$$

Consideremos a expressão $(b'c' - a'd')bd$, temos:

$$\begin{aligned}(b'c' - a'd')bd &= (c'b' - a'd')bd \\ &= c'b'bd - a'd'bd \\ &= dc'bb' - ba'dd' \\ &= cd'b'b - ab'd'd \\ &= (bc - ad)b'd'.\end{aligned}$$

Então concluímos que,

$$(b'c' - a'd')bd = (bc - ad)b'd'.$$

Devemos observar que $0 < bd$, pois b e d são positivos por hipótese. O lado direito da igualdade é não negativo, pois tanto $bc - ad$ quando $b'd'$ não são negativos. Assim concluímos que o lado esquerdo também não é negativo, logo $b'c' - a'd'$ deve ser não negativo, o que nos dá:

$$0 \leq b'c' - a'd' \iff a'd' \leq b'c' \iff \frac{a'}{b'} \leq \frac{c'}{d'}.$$

■

Proposição 5.3. *A relação de ordem no conjunto dos números racionais tem as seguintes propriedades:*

(i) Reflexiva;

(ii) Antissimétrica;

(iii) Transitiva;

(iv) Totalidade;

(v) Compatibilidade com a adição;

(vi) Compatibilidade com a multiplicação.

Demonstração: Sejam $\frac{a}{b}, \frac{c}{d}, \frac{e}{f}$ números racionais quaisquer tais que $b, d, f > 0$.

(i) Reflexiva:

$$\frac{a}{b} \leq \frac{a}{b} \iff ab \leq ba.$$

(ii) Antissimétrica:
Supondo $\frac{a}{b} \leq \frac{c}{d}$ temos $ad \leq bc$. Por outro lado, $\frac{c}{d} \leq \frac{a}{b}$ implica que $cb \leq da$. Pela antissimetria de $\leq$ em $\mathbb{Z}$, concluímos que $ad = bc$, ou seja, $\frac{a}{b} = \frac{c}{d}$.

(iii) Transitiva:
Supondo $\frac{a}{b} \leq \frac{c}{d}$ e $\frac{c}{d} \leq \frac{e}{f}$, temos $ad \leq bc$ e $cf \leq de$. Pela compatibilidade do produto em $\mathbb{Z}$, temos:

$$adf \leq bcf \text{ e } bcf \leq bde,$$

assim $adf \leq bde$, e como $d \neq 0$, $af \leq be$. Portanto $\frac{a}{b} \leq \frac{e}{f}$.

(iv) Totalidade:
Vamos mostrar que $\frac{a}{b} \leq \frac{c}{d}$ ou $\frac{c}{d} \leq \frac{a}{b}$. Em $\mathbb{Z}$ vale a totalidade da relação de ordem, e assim $ad \leq bc$ ou $bc \leq ad$. Caso seja $ad \leq bc$ temos $\frac{a}{b} \leq \frac{c}{d}$. Por outro lado, se for $bc \leq ad$, temos que $cb \leq da$, e portanto $\frac{c}{d} \leq \frac{a}{b}$.

(v) Compatibilidade com a adição:
Suponha $\frac{a}{b} \leq \frac{c}{d}$. Logo $ad \leq bc$. Como $f \neq 0$, as linhas abaixo são equivalentes:

$$afd \leq bcf$$

$$affd \leq bcff$$

$$affd + bedf \leq bcff + bdef$$

$$(af + be)df \leq bf(cf + de)$$

$$\frac{af + be}{bf} \leq \frac{cf + de}{df}$$

$$\frac{a}{b} + \frac{e}{f} \leq \frac{c}{d} + \frac{e}{f}.$$

(vi) Compatibilidade com a multiplicação:
Se $\frac{a}{b} \leq \frac{c}{d}$ e $\frac{0}{1} \leq \frac{e}{f}$, temos $ad \leq bc$ e $e \geq 0$. Com isso

$$\begin{aligned} ad \leq bc &\iff adef \leq bcef \\ &\iff aedf \leq bfce \\ &\iff \frac{ae}{bf} \leq \frac{ce}{df} \\ &\iff \frac{a}{b}\frac{e}{f} \leq \frac{c}{d}\frac{e}{f}. \end{aligned}$$

■

Proposição 5.4. *Seja $r = \frac{a}{b}$ um racional, em que $b > 0$. Temos que $r \in \mathbb{Q}_+^*$ se, e somente se, $a > 0$.*

Demonstração: Seja $0 = \frac{0}{1}$. Temos $0 < r = \frac{a}{b} \iff 0b \leq 1a \iff 0 \leq a$. Notemos que ambos os denominadores são positivos, o que nos permite efetivamente fazer a comparação por meio da relação de ordem. ■

Proposição 5.5. *Sejam $r, s, r', s' \in \mathbb{Q}_+^*$. Se $r \leq r'$ e $s \leq s'$, então $rs \leq r's'$.*

Demonstração: Sejam $r = \frac{a}{b},\ s = \frac{c}{d},\ r' = \frac{a'}{b'},\ s' = \frac{c'}{d'}$, com todos os denominadores positivos. Pela Proposição 5.4, concluímos que cada numerador também é positivo. Temos por definição

$$\begin{aligned} r \leq r' &\iff ab' \leq ba', \\ s \leq s' &\iff cd' \leq dc'. \end{aligned}$$

Multiplicando os termos à esquerda entre si, e os termos à direita entre si, obtemos:

$$\begin{aligned} ab' \cdot cd' \leq ba' \cdot dc' &\iff acb'd' \leq bda'c' \\ &\iff \frac{ac}{bd} \leq \frac{a'c'}{b'd'} \\ &\iff \frac{a}{b} \cdot \frac{c}{d} \leq \frac{a'}{b'} \cdot \frac{c'}{d'} \\ &\iff rs \leq r's'. \end{aligned}$$

■

Proposição 5.6. *Sejam $r, s \in \mathbb{Q}$ números fixos quaisquer, com $s \neq 0$. A equação $r = s \cdot t$ sempre admite solução para $t \in \mathbb{Q}$.*

Demonstração: De $r = st$, com $s \neq 0$, temos

$$\frac{1}{s}\frac{r}{1} = \frac{1}{s}\frac{st}{1} \iff \frac{r}{s} = \frac{st}{s} = \frac{t}{1} = t.$$

Logo, $t = \frac{r}{s} \in \mathbb{Q}$ é solução de $r = st$. ■

5.5. Imersão de $\mathbb{Z}$ em $\mathbb{Q}$

Teorema 5.7. *Considere a função definida abaixo:*

$$\begin{aligned} f\colon \mathbb{Z} &\to \mathbb{Q} \\ x &\mapsto \frac{x}{1}. \end{aligned}$$

Essa função tem as propriedades a seguir:

(i) $f(a+b) = f(a) + f(b)$;

(ii) $f(a \cdot b) = f(a) \cdot f(b)$;

(iii) $a \leq b \implies f(a) \leq f(b)$.

Demonstração: Temos que

(i) $f(a+b) = \frac{a+b}{1} = \frac{a}{1} + \frac{b}{1} = f(a) + f(b)$;

(ii) $f(a \cdot b) = \frac{ab}{1} = \frac{a}{1}\frac{b}{1} = f(a) \cdot f(b)$;

(iii) Supondo $a \leq b$, tem-se que $\frac{a}{1} \leq \frac{b}{1}$. Logo $a1 \leq 1b$.

■

Na demonstração do resultado a seguir vamos utilizar as imersões de $\mathbb{N}$ em $\mathbb{Z}$ e de $\mathbb{Z}$ em $\mathbb{Q}$ para confirmar uma visão prática. Um exemplo do que quero dizer é que 2 é um número natural com a notação de número natural. Já $\frac{x}{2}$ com $x \in \mathbb{Z}$ é um número racional, mas o 2 que figura no denominador é um número inteiro, com notação de número natural. Como já provamos a imersão de $\mathbb{N}$ em $\mathbb{Z}$, vamos utilizar a notação dos naturais com o sinal de $-$ quando necessário.

Proposição 5.7. *Sejam r, s números racionais positivos e distintos, tal que $s < r$. Então existe um único racional positivo t tal que $r = s + t$.*

Demonstração: Temos que

$$s < r \implies s - s < r - s \iff 0 < r - s.$$

Assim o elemento $r - s$ é positivo, e também $s + (r - s) = r$, dessa forma $r - s$ é um t do enunciado. Para mostrar que nenhum outro $t' \neq t$ satisfaz o enunciado, podemos supor que seja verdade que $r = s+t'$. Daí vem $r-s = t'$, e substituindo $r-s$ por t, obtemos $t = t'$. ■

Proposição 5.8. *Sejam $s, r \in \mathbb{Q}$ com $s < r$. Vale que $2s < s + r < 2r$.*

Demonstração: Como $s < r$ temos que $r = s + t$, para algum t racional positivo (Proposição 5.7). Da compatibilidade da adição $s < r \implies s + s < s + r \implies 2s < s + r$. E para mostrar que $s + r < 2r$, temos

$$0 < t \implies t < t + t = 2t,$$

assim

$$s + r = t + 2s < 2t + 2s = 2(t + s) = 2r.$$

■

Corolário 5.2. *Entre quaisquer dois números racionais distintos há sempre algum racional entre eles. É o mesmo que dizer que se $s, r \in \mathbb{Q}$ com $s < r$ então existe $t \in \mathbb{Q}$ tal que $s < t < r$.*

Demonstração: Supondo $s < r$, temos que $2s < s + r < 2r$, conforme Proposição 5.8, aí multiplicando por $\frac{1}{2} > 0$, obtemos

$$s < \frac{s + r}{2} < r.$$

Logo, existe $t = \frac{s+r}{2}$ tal que $s < t < r$. ■

Teorema 5.8. *O conjunto $\mathbb{Z}$ não é limitado superiormente em $\mathbb{Q}$.*

Demonstração: Vamos argumentar por contradição, para provar que nenhum racional é cota superior de $\mathbb{Z}$. Suponha que $\frac{r}{s}$ é um racional, tal que $s > 0$, em que $\frac{r}{s}$ é cota superior de $\mathbb{Z}$. Tomemos um número inteiro em $\mathbb{Q}$, que é da forma $\frac{a}{1}$, com $a \in \mathbb{Z}$. Devemos ter $\frac{a}{1} < \frac{r}{s}$, pois $\frac{r}{s}$ é uma cota superior de $\mathbb{Z}$. Logo, $as < r$. Mas essa desigualdade, com r e s fixos e a qualquer, é o mesmo que dizer que r é maior do que qualquer produto as, para quaisquer $a, s \in \mathbb{Z}_+$. Mas os inteiros positivos são identificados com os naturais, que por sua vez, são ilimitados em $\mathbb{Z}$. Desse modo, r é uma cota superior de um conjunto ilimitado, o que é uma contradição. ■

6. O CONJUNTO DOS NÚMEROS REAIS

Neste capítulo vamos fazer a construção do conjunto dos números reais. Vamos construir por meio de cortes de Dedekind, e como nos capítulos anteriores, mostrar a cópia algébrica de $\mathbb{Q}$ em $\mathbb{R}$. A propriedade que $\mathbb{R}$ tem que o diferencia de $\mathbb{Q}$ será o fato de ser completo, pois $\mathbb{Q}$ não é completo. As referências principais para este capítulo são Ferreira (2013) e Domingues (2009).

A ideia de completeza é que cada subconjunto de um dado conjunto limitado tem um máximo. Podemos, a título de observação, ver que o conjunto $A = \{x \in \mathbb{Q} : x^2 < 2\}$ não tem um máximo em Q. Vamos provar isso no final desta seção.

Definição 6.1. *Um conjunto α de números racionais será chamado de corte caso ele atenda as condições a seguir:*

(i) $\emptyset \neq \alpha \neq \mathbb{Q}$;

(ii) se $r \in \alpha$ *e* $s < r$, *sendo* s *um racional qualquer, então* $s \in \alpha$;

(iii) o conjunto α *não tem máximo.*

A ideia por trás da Definição 6.1 é que um corte é um subconjunto próprio do conjunto dos números racionais que não admite máximo e tal que, dado qualquer elemento do corte, todos os elementos que o precedem pela relação de ordem nos racionais, também está no corte.

Observação 6.1. Algo importante que devemos ter em mente na definição de corte é o fato do corte ser subconjunto de $\mathbb{Q}$ e, além disso, de que o conjunto $\mathbb{Q}$ é o conjunto universo aqui considerado.

Alguns exemplos de corte são:

Exemplo 6.1. O conjunto $\alpha = \{x \in \mathbb{Q} : x < 5\}$ é um corte.
De fato:

(i) Como $4 \in \mathbb{Q}$ é tal que $4 < 5$, temos $4 \in \alpha$, logo $\alpha \neq \emptyset$. Como $5 \not< 5$, temos que $5 \notin \alpha$, e portanto $\alpha \neq \mathbb{Q}$.

(ii) Suponha s racional tal que $s < r$ e $r \in \alpha$. Temos $s < r < 5$, logo $s \in \alpha$.

(iii) Para mostrar que não há máximo em α, por contradição suponhamos que exista um, que chamaremos de s. Temos que $s < 5$, e assim, pelo Corolário 5.2, $s < \frac{s+5}{2} < 5$. Logo $s < \frac{s+5}{2} \in \alpha$ e s não é máximo de α, o que é uma contradição, e portanto α não tem máximo.

Exemplo 6.2. O conjunto $\alpha = \{x \in \mathbb{Q} : x < 5/2\}$ é um corte.

(i) De fato, $1 \in \mathbb{Q}$ é tal que $1 < 5/2$, temos $1 \in \alpha$, logo $\alpha \neq \emptyset$. Como $10 \not< 5/2$, temos que $10 \notin \alpha$, e portanto $\alpha \neq \mathbb{Q}$.

(ii) Suponha s racional tal que $s < r \in \alpha$. Temos $s < r < 5/2$, logo $s \in \alpha$.

(iii) Para mostrar que não há máximo em α, por contradição suponhamos que exista um, que chamaremos de s. Seja $r = 5/2$. Temos que $s < r$, e assim, pelo Corolário 5.2, $s < \frac{s+r}{2} < r$. Logo, $s < \frac{s+r}{2} \in \alpha$ e s não é máximo de α, o que é uma contradição, e portanto, α não tem máximo.

Exemplo 6.3. O conjunto $\alpha = \mathbb{Q}^*_- \cup \{x \in \mathbb{Q}_+ : x \cdot x < 2\}$ é um corte. Isso será provado na Proposição 6.3.

Alguns exemplos de conjuntos que não são cortes são:

Exemplo 6.4. O conjunto $A = \{x \in \mathbb{Q} : x > 5\}$ não é um corte, pois $4 < 5$ mas $4 \notin A$.

Exemplo 6.5. O conjunto $A = \{x \in \mathbb{Q} : x \leq 5\}$ não é um corte, pois 5 é máximo de A.

Exemplo 6.6. O conjunto $A = \{x \in \mathbb{Q} : 1 < x < 5\}$ não é um corte, pois $2 \in A$, mas $0 < 2$ e 0 não está em A.

Teorema 6.1. *Todo corte tem uma cota superior.*

Demonstração: Vamos mostrar por contradição, supondo que α seja um corte sem cota superior. Como α é um subconjunto próprio de $\mathbb{Q}$, existe $q \in \mathbb{Q} \setminus \alpha$. Como q não é cota superior de α, deve existir um $r > q$, com $r \in \alpha$. Mas como α é um corte, pelo Item (ii) da Definição 6.1, $q \in \alpha$, o que é uma contradição. ∎

Proposição 6.1. *Sejam α um corte e $r \in \mathbb{Q}$. O número r é cota superior de α se, e somente se, $r \in \mathbb{Q} \setminus \alpha$.*

Demonstração: Primeiro provemos a ida. Por hipótese, r é cota superior de α, desse modo r não pode estar em α, pois se estivesse, seria máximo de α, o que contradiz o

Item (iii) da Definição 6.1. Agora, vamos provar a volta. Por hipótese $r \notin \alpha$. Argumentando por contradição, se r não fosse cota superior de α, existiria um $s > r$ com $s \in \alpha$, e pelo Item (ii), teríamos que $r \in \alpha$, o que é uma contradição. ■

Teorema 6.2. *Sejam r um racional e $\alpha = \{x \in \mathbb{Q} : x < r\}$, então α é um corte e r é a menor cota superior de α.*

Demonstração:

Primeiro vamos provar que α é de fato um corte. Observando que o número $r-1 \in \alpha$, sabemos que α não é vazio, e como $r \not< r$, $r \notin \alpha$, logo α é um subconjunto próprio de $\mathbb{Q}$, assim provamos o Item (i) da Definição 6.1. Para o Item (ii), se $s \in \alpha$, então $s < r$, e para qualquer $q < s$, com q racional, vale que $q < s < r$, logo $q \in \alpha$. Agora mostremos que α não tem máximo. Consideremos um número $s \in \alpha$, assim vale que $s < \frac{s+r}{2}$ conforme Corolário 5.2, e analogamente $\frac{s+r}{2} < r$, assim s não é máximo de α. Como s é arbitrário, α não tem máximo.

Com isso provamos que α é um corte. Provemos agora que r é a menor cota superior de α. Se $x \in \alpha$, então $x < r$ e r é uma cota superior de α. Seja $t < r$, com t racional, pela definição de α sabemos que $t \in \alpha$. Assim t não pode ser máximo, porque um corte não tem máximo. Logo, qualquer $t < r$ não é cota superior de α e r é a menor cota superior de α. ■

Definição 6.2. *Seja $\alpha = \{x \in \mathbb{Q} : x < r\}$, com $r \in \mathbb{Q}$. O conjunto α é chamado de corte racional e é representado por r^*.*

Observação 6.2. O Teorema 6.2 garante que r^* é, de fato, um corte.

Teorema 6.3. *Todo corte com cota superior mínima é racional.*

Demonstração: Sejam α um corte e q a menor cota superior de α. Considere $\beta = \{\, x \in \mathbb{Q} : x < q \,\}$, vamos mostrar que $\alpha = \beta$. Se $r \in \alpha$, temos que $r < q$, pois q é cota superior de α. Logo $\alpha \subset \beta$. Se $x \in \beta$, temos $x < q$. Devemos ter $x \in \alpha$, pois do contrário, q não seria a menor cota superior de α. Assim $\beta \subset \alpha$, e portanto $\alpha = \beta = q^*$ e α é um corte racional. ■

Proposição 6.2. *Não existe um número racional r, tal que $r^2 = 2$.*

Demonstração: A prova será desenvolvida semelhante à feita por Alfeld (1996), que utiliza o Teorema Fundamental da Aritmética, cuja demonstração aqui é omitida, mas pode ser encontrada em Santos (2015, p. 9). Esse teorema garante que todo número

inteiro maior do que 1 pode ser representado de maneira única, a menos de ordem, por um produto de fatores primos.

Suponhamos que $r \in \mathbb{Q}$ seja tal que $r^2 = 2$. Temos $r = \frac{p}{q}$, para $p \in \mathbb{Z}$ e $q \in \mathbb{Z}^*$. Podemos, pelo Teorema Fundamental da Aritmética, supor que p e q sejam números primos entre si (se não forem, basta observar que podemos cancelar o fator comum usando a Proposição 5.1). Temos que $2 = r^2 = \left(\frac{p}{q}\right)^2 = \frac{p^2}{q^2}$, logo, $p^2 = 2q^2$, e portanto p^2 é par, e então p também é par. Seja $p = 2m$, para algum $m \in \mathbb{Z}$, segue que $p^2 = (2m)^2 = 4m^2$. Disso obtemos que $4m^2 = 2q^2$, assim $2m^2 = q^2$. Desse modo, concluímos que são pares os números q^2 e q. Isso é uma contradição, pois supomos que p e q não tinham fatores primos em comum. Portanto, não existe um número racional r, tal que $r^2 = 2$.

■

Observação 6.3. Com uma outra terminologia, a Proposição 6.2 também indica que a raiz quadrada de 2 não é um número racional.

Proposição 6.3. *Seja* $\alpha = \mathbb{Q}_-^* \cup \{\, x \in \mathbb{Q}_+ : x^2 < 2 \,\}$. *Tem-se que* α *é um corte sem cota superior mínima.*

Demonstração: Sabemos que $0 \in \alpha$ e que $3^2 = 9 \notin \alpha$, e portanto α é um subconjunto próprio de $\mathbb{Q}$ e atende ao Item (i) da Definição 6.1. Sejam $s < r$ números racionais, tais que $r \in \alpha$. Se $s \leq 0$ é óbvio que $s \in \alpha$. Se for $s > 0$ temos $0 < s < r$, e pelo Proposição 5.5, obtemos $0 < s^2 < r^2 < 2$. Portanto $s \in \alpha$ e α atende ao Item (ii). Para mostrar que não há máximo em α, tomemos um elemento arbitrário $r \in \alpha$ e provemos que $r < s$ para algum $s \in \alpha$. Se $r \leq 0$, basta tomar $s = 0$, pois $0 \in \alpha$. Caso seja $r > 0$, basta mostrar que existe um $s = r + h \in \alpha$, com $h > 0$. Vamos encontrar um $0 < h < 2$, com $s = r + h$. Tomando $h = 2 - r^2$, temos que

$$s^2 = \left(r + \frac{h}{5}\right)^2 = r^2 + \frac{2rh}{5} + \frac{h^2}{25},$$

e como $r^2 < 2$, temos $r < 2$, daí $2rh < 4h$. Tínhamos que $0 < h < 2$, daí $h^2 < 2h$. Substituindo as desigualdades obtidas, temos

$$s^2 < r^2 + \frac{4h}{5} + \frac{2h}{25} = r^2 + \frac{22h}{25} < r^2 + h = 2.$$

Desse modo, $s^2 < 2$, logo $s \in \alpha$. Também provamos que $s > r$, o que nos mostra que em α não há máximo, e portanto, α é um corte.

Para mostrar que qualquer cota superior r de α não é mínima, notemos que não pode ocorrer $r^2 = 2$, pois essa equação não admite solução racional, pela Proposição 6.2. Se, por outro lado, for $r^2 < 2$, temos $r \in \alpha$, logo r não é uma cota superior. Resta então verificar que $r^2 > 2$ também não ocorre.

Suponhamos, por contradição, que $r^2 = 2 + h$ para algum racional h positivo. Como 2 é uma cota superior de α, pois $2^2 \not< 2$, obtemos que $0 < h < 2$. Além disso, como $r < 2$, temos $rh < 2h$, e então $-2h < -rh$, que equivale a $-h < \frac{-rh}{2}$.

Seja $t = r - \frac{h}{4}$. Assim, $t < r$. Como r e h são positivos, para t temos que

$$t^2 = \left(r - \frac{h}{4}\right)^2 = r^2 - \frac{rh}{2} + \frac{h^2}{16} > r^2 - \frac{rh}{2}.$$

E então

$$t^2 > r^2 - \frac{rh}{2} > r^2 - h = 2.$$

Claramente t é uma cota superior de α, pois $t^2 > 2$. Por outro lado, tínhamos que $t < r$, logo t é uma cota superior menor do que a cota superior mínima, o que é uma contradição. Com isso provamos que α não tem uma cota superior mínima. ■

Definição 6.3. *O conjunto dos números reais, denotado por $\mathbb{R}$, é o conjunto de todos os cortes α, dados pela Definição 6.1.*

6.1. A relação de ordem em $\mathbb{R}$

Definição 6.4. *Sejam α e β cortes. Diremos que α é menor do que β e denotaremos $\alpha < \beta$ quando $\beta \setminus \alpha \neq \emptyset$.*

Observação 6.4. De maneira análoga aos outros conjuntos, temos $\alpha \leq \beta$ quando $\alpha < \beta$ ou $\alpha = \beta$.

Definição 6.5. *Um corte α será chamado de:*

(i) corte positivo, quando $0^* < \alpha$;

(ii) corte negativo, quando $0^* > \alpha$;

(iii) corte não negativo, quando $0^* \leq \alpha$;

(iv) corte não positivo, quando $0^* \geq \alpha$.

Teorema 6.4. *Sejam α e β números reais. Valem:*

(i) $\alpha < \beta \iff \alpha \subset \beta$ e $\alpha \neq \beta$;

(ii) $\alpha \leq \beta \iff \alpha \subset \beta$.

Demonstração:

(i) $\alpha < \beta \iff \alpha \subset \beta$ e $\alpha \neq \beta$:
De $\alpha < \beta$ temos que existe $x \in \beta \setminus \alpha$, logo x é cota superior de α. Sendo assim $x > y$ para qualquer $y \in \alpha$, e ainda, como $\alpha \subset \mathbb{Q}$, temos que $y \in \beta$ para qualquer $y \in \alpha$ (devido ao Item (ii) da Definição 6.1), assim $\alpha \subset \beta$. Obviamente $\alpha \neq \beta$ pois $x \in \beta$ e $x \notin \alpha$. Reciprocamente, se $\alpha \subset \beta$ e $\alpha \neq \beta$, então $\alpha \subset \beta$ e, por definição, $\alpha < \beta$.

(ii) $\alpha \leq \beta \iff \alpha \subset \beta$:
Se $\alpha \leq \beta$ pode ocorrer uma de duas situações: $\alpha < \beta$, o que nos leva ao item anterior. Se por outro lado, $\alpha = \beta$, pela dupla inclusão de conjuntos, $\alpha \subset \beta$. Reciprocamente, se $\alpha \subset \beta$ então, por definição, $\alpha < \beta$. Logo, $\alpha \leq \beta$.

■

Teorema 6.5. *A relação $\leq$ é tricotômica.*

Demonstração: Sejam α e β números reais. Primeiro vamos mostrar que no máximo uma relação entre $=, <$ e $>$ pode ocorrer. Comecemos analisando a igualdade. Se $\alpha = \beta$ então $\alpha \setminus \beta = \beta \setminus \alpha = \emptyset$, logo $\alpha \not< \beta$ e $\beta \not< \alpha$. Agora analisemos as desigualdades $<, >$ e constatemos que elas não podem ocorrer simultaneamente. Se $\alpha < \beta$ existe $x \in \beta \setminus \alpha$. Por contradição, admitamos que possa ocorrer $\beta < \alpha$. Desse modo existe $y \in \alpha \setminus \beta$, mas tal y não pode existir pois, conforme o Teorema 6.4, temos $\alpha \subset \beta$.

Agora vamos mostrar que ao menos uma das relações ocorre. Se $\alpha = \beta$ nada há para provar. Se $\alpha \neq \beta$ então ocorre $\alpha \setminus \beta \neq \emptyset$ ou $\beta \setminus \alpha \neq \emptyset$, assim $\alpha \leq \beta$ ou $\beta \leq \alpha$, o que garante que ao menos uma das três relações ocorre. ■

Teorema 6.6. *A relação $\leq$ é uma relação de ordem total sobre $\mathbb{R}$.*

Demonstração: Sejam α, β e γ números reais, a relação $\leq$ é:

(i) Reflexiva, pois tem-se $\alpha \subset \alpha$, assim $\alpha \leq \alpha$.

(ii) Antissimétrica, pois supondo $\alpha \leq \beta$ e $\beta \leq \alpha$, temos $\alpha \subset \beta$ e $\beta \subset \alpha$, o que pela antissimetria da inclusão de conjuntos, garante que $\alpha = \beta$.

(iii) Transitiva, pois se $\alpha \leq \beta$ e $\beta \leq \gamma$, então $\alpha \subset \beta$ e $\beta \subset \gamma$, e da transitividade da inclusão de conjuntos, $\alpha \subset \gamma$. Assim $\alpha \leq \gamma$.

(iv) Total, pelo Teorema 6.5.

■

6.2. A adição em $\mathbb{R}$

Definição 6.6. *Sejam α e β números reais. A adição de α e β, denotada por $\alpha+\beta$, é definida por $\gamma = \{x+y : x \in \alpha \wedge y \in \beta\}$.*

O lema a seguir terá sua demonstração omitida. O leitor interessado pode consultar Ferreira (2013, p. 73).

Lema 6.1. *O conjunto $\{\, s+mr : n \in \mathbb{Z}_+ \text{ e } r \in \mathbb{Q}_+^* \,\}$ não é limitado superiormente em $\mathbb{Q}$.*

Lema 6.2. *Sejam α um corte e r um número racional positivo. Então existem racionais p, q tais que q é cota superior não mínima de α, $p \in \alpha$ e vale que $q - p = r$.*

Demonstração: Consideremos a sequência de números racionais

$$s, s+r, s+2r, s+3r, ..., s+mr, ...,$$

em que $s \in \alpha$ é um elemento qualquer, $r \in \mathbb{Q}_+^*$ e $m \in \mathbb{Z}_+$. Essa sequência inicia em α mas sai do conjunto em algum valor de m. De fato, α é limitado, mas a sequência não o é. Seja $A = \{\, m \in \mathbb{Z}_+ : s+mr \text{ é cota superior de } \alpha \,\}$. Assim, $A \neq \emptyset$. O conjunto A admite elemento mínimo, basta observar que caso 0 seja elemento de A, então ele será elemento mínimo, e caso 0 não esteja em A, a aplicação do princípio da boa ordem (Teorema 3.6) garante que há tem um elemento mínimo.

Temos então que A tem um elemento mínimo, o chamemos de t. Caso $s+tr$ seja cota superior não mínima de α, tome $q = s+tr$ e $p = s+(t-1)r$, e assim

$$q - p = (s+tr) - (s+(t-1)r) = tr - tr + r = r.$$

Caso $s+tr$ seja cota superior mínima de α, tome $q = s+tr+\frac{r}{2}$ e $p = s+(t-1)r+\frac{r}{2}$, e assim

$$q - p = s+tr+\frac{r}{2} - \left(s+(t-1)r+\frac{r}{2}\right) = s+tr+\frac{r}{2} - s - tr + r - \frac{r}{2} = r.$$

Em ambos os casos q é cota superior não mínima de α e $p \in \alpha$. ∎

Teorema 6.7. *Sejam α, β números reais quaisquer. Para a adição valem as seguintes propriedades:*

(i) Fechamento;

(ii) Associativa;

(iii) Comutativa;

(iv) Da existência do elemento neutro;

(v) Da existência do elemento simétrico;

(vi) Lei do cancelamento.

Demonstração: Sejam α, β números reais quaisquer e considere

$$\gamma = \alpha + \beta = \{x + y : x \in \alpha \wedge y \in \beta\}.$$

(i) Fechamento:
Devemos provar que γ é um número real (ou seja, um corte).

Como α, β são não vazios, $\gamma \neq \emptyset$. Para mostrar que $\gamma \neq \mathbb{Q}$, tomemos a como cota superior de α, e b como cota superior de β. Como $a > x$ e $b > y$, para qualquer $a \in \alpha$ e $b \in \beta$, temos que $a + b > x + y$, logo $a + b \notin \gamma$.

Se $r \in \gamma$ e $s < r$, com $s \in \mathbb{Q}$, mostremos que $s \in \gamma$. Temos $r = x + y$, com $x \in \alpha$ e $y \in \beta$. Como $s < r = x + y$ temos $s = x + y'$ para algum $y' < y$. Logo $y' \in \beta$, $s = x + y'$, com $x \in \alpha$ e $y' \in \beta$. Com isso, concluímos que $s \in \gamma$.

Para mostrar que em γ não há máximo, suponhamos que $a = x + y$ seja máximo de γ. Como existe $x' \in \alpha$ com $x' > x$, temos $a = x + y < x' + y$, com $x' + y \in \gamma$, o que contradiz nossa suposição de que a é máximo de γ.

Com isso provado, observando a Definição 6.1, concluímos que γ é um corte, ou seja, um número real.

(ii) Associativa[(1)]:

$$\begin{aligned}(\alpha + \beta) + \gamma &= \{x + y : x \in \alpha \wedge y \in \beta\} + \gamma \\ &= \{(x + y) + z : (x \in \alpha \wedge y \in \beta) \wedge z \in \gamma\} \\ &= \{x + (y + z) : x \in \alpha \wedge (y \in \beta \wedge z \in \gamma)\} \\ &= \alpha + (\beta + \gamma).\end{aligned}$$

(iii) Comutativa:
$\alpha + \beta = \{x + y : x \in \alpha \wedge y \in \beta\} = \{y + x : y \in \beta \wedge x \in \alpha\} = \beta + \alpha.$

(iv) Da existência do elemento neutro:
Vamos mostrar que 0^* é o elementro neutro para a adição. Para isso, mostraremos que dado $\alpha \in \mathbb{R}$, temos $\alpha + 0^* \subset \alpha$ e também que $\alpha \subset \alpha + 0^*$.

(1) Pode ser útil ao leitor algumas propriedades da conjunção (como a comutatividade e a associatividade). Mortari (2016, p. 147) apresenta métodos para demonstrar tais propriedades.

Seja $r \in \alpha + 0^*$. Temos que $r = x + y$ com $x \in \alpha$ e $y \in 0^*$. De $y \in 0^*$ sabemos que $y < 0 \in \mathbb{Q}$. Desse modo $r < x$ e portanto $r \in \alpha$, logo $\alpha + 0^* \subset \alpha$.

Para mostrar que $\alpha \subset \alpha + 0^*$, tomemos $a, b \in \alpha$ tal que $a < b$. Consideremos a soma $b + (a - b) = a$, temos $b \in \alpha$ e $a - b \in 0^*$, pois $a - b < 0$. Portanto $a \in \alpha + 0^*$ e $\alpha \subset \alpha + 0^*$.

(v) Da existência do elemento simétrico:
Seja $\delta = \{p \in \mathbb{Q} : -p \text{ é cota superior não mínima de } \alpha\}$. Denotaremos o conjunto das cotas superiores não mínimas de α por $\mathbb{S}_\alpha$. Vamos mostrar que δ é um número real e que $\alpha + \delta = 0^*$.

Pelo Item (i) da Definição 6.1, devemos mostrar que δ é um subconjunto próprio de $\mathbb{Q}$. Um corte sempre admite uma infinidade de cotas superiores, e alguma delas não será mínima, assim $\delta \neq \emptyset$. Para mostrar que $\delta \neq \mathbb{Q}$, pegue um número $-a \in \alpha$, logo $-a$ não é cota superior de α e assim $a \notin \delta$.

Antes de prosseguir com a demonstração, vejamos um exemplo que ilustra a ideia da demonstração. Sejam $\alpha = 5^*$ e $\delta = \{b \in \mathbb{Q} : -b \in \mathbb{S}_\alpha\}$. Sabemos que o $-(-7) = 7 \in \mathbb{S}_\alpha$. Daí vem que $-7 \in \delta$. Por outro lado o $-(-3) = 3 \notin \mathbb{S}_\alpha$, daí $-3 \notin \delta$.

Para provar o Item (ii) da Definição 6.1, devemos mostrar que se $a < b$ e $b \in \delta$, então $a \in \delta$. Basta observar que $a < b \iff -b < -a$, logo tanto $-b$ quanto $-a$ são cotas superiores de α e não são mínimas, pois $-b$ já não era mínima, assim $-a \in \mathbb{S}_\alpha$. Portanto $a \in \delta$.

Para verificar o Item (iii) da Definição 6.1, seja $-a \in \mathbb{S}_\alpha$. Assim $-a$ é uma cota superior não mínima de α. Seja $-b$ uma outra cota superior de α, tal que $-b < -a$. Para $-b$ não precisamos da exigência de não ser mínima. Pegamos $-c = \frac{-a-b}{2}$, daí $-b < -c < -a$, desse modo $b > c > a$. Note que $-c$ é cota superior não mínima de α, pois $-b < -c$ e $-b$ é cota superior de α. Desse modo, para qualquer $a \in \delta$ existirá algum $b \in \delta$ com $b > a$, assim δ não possuí máximo.

Com isso, provamos que $\delta \in \mathbb{R}$. Vamos mostrar que δ é o simétrico de α, isto é, $\alpha + \delta = 0^*$. Vamos iniciar pela inclusão $\alpha + \delta \subset 0^*$. Seja $c \in \alpha + \delta$, assim $c = a + d$, com $a \in \alpha$ e $d \in \delta$, logo $-d \in \mathbb{S}_\alpha$ e $-d > a$. Com isso, $0 > a + d$ e $a + d \in 0^*$. Assim está provada a primeira inclusão.

Agora vamos mostrar que $0^* \subset \alpha + \delta$. Seja $c \in 0^*$, então $c \in \mathbb{Q}^*_-$. Pelo Lema 6.2 sabemos que existem d, d' tais que $d' - d = -c$, com $d' \in \mathbb{S}_\alpha$ e $d \in \alpha$. Assim $d' \in \delta$, mas de $-c = d' - d$ temos $c = -d' + d = d - d'$, com $d \in \alpha,\ d' \in \delta$ assim $c \in \alpha + \delta$.

(vi) Lei do cancelamento, é válida conforme a Teorema 2.5, pois a adição é associativa e admite simétrico.

■

Observação 6.5. Além de existir um elemento simétrico para a adição, ele é único, como visto no Teorema 2.4. Isso nos permite utilizar a notação usual, e então denotar o simétrico de α por $-\alpha$.

Teorema 6.8. *A relação $\leq$ é compatível com a adição.*

Demonstração: Vamos mostrar que $\alpha \leq \beta \implies \alpha + \gamma \leq \beta + \gamma$. Primeiro observemos que se $x \in \alpha + \gamma$ então $x = r + s$ com $r \in \alpha$ e $s \in \gamma$. Por outro lado temos $\alpha \subset \beta$, então $r \in \beta$, desse modo $r + s \in \beta + \gamma$. Com isso concluímos que $\alpha + \gamma \subset \beta + \gamma$, o que nos mostra que $\alpha + \gamma \leq \beta + \gamma$. ■

Definição 6.7. *Sejam α e β números reais. A subtração de α por β, denotada por $\alpha - \beta$ é definida como $\alpha + (-\beta)$, em que $-\beta$ é o simétrico aditivo de β.*

Proposição 6.4. *A subtração é fechada em $\mathbb{R}$.*

Demonstração: Basta observar que a subtração é uma adição, que é fechada conforme o Teorema 6.7. ■

Teorema 6.9. *Sejam α, β números reais. Vale:*

(i) $-(-\alpha) = \alpha$;

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

Demonstração: Sejam $\alpha, \beta \in \mathbb{R}$.

(i) $-(-\alpha) = \alpha$, pois a adição admite neutro e é associativa, conforme a Proposição 2.1.

(ii) Vamos provar que ambos são simétricos de $(\alpha + \beta)$. Temos

$$-(\alpha + \beta) + (\alpha + \beta) = (\alpha + \beta) - (\alpha + \beta) = 0^*.$$

Por outro lado,

$$(-\alpha - \beta) + (\alpha + \beta) = \alpha + (-\alpha) + \beta + (-\beta) = 0^* + 0^* = 0^*.$$

■

Proposição 6.5. *Se* $0^* \leq \alpha$ *então* $-\alpha \leq 0^*$.

Demonstração: De $0^* \leq \alpha$ e do Teorema 6.8 obtemos

$$0^* + (-\alpha) \leq \alpha + (-\alpha) \iff -\alpha \leq 0^*.$$

■

Proposição 6.6. *Se* $\alpha \neq 0^*$, *então* $-\alpha \neq 0^*$.

Demonstração: Sabemos que $\alpha + (-\alpha) = 0^*$. Se admitíssemos que pudesse ocorrer $-\alpha = 0^*$, teríamos $\alpha + 0^* = 0^*$, o que contradiz a hipótese. ■

Corolário 6.1. *Se* $0^* < \alpha$ *então* $-\alpha < 0^*$.

Demonstração: Como $0^* < \alpha \implies 0^* \leq \alpha$, pela Proposição 6.5 obtemos que $-\alpha \leq 0^*$. Como $\alpha \neq 0^*$, temos $-\alpha \neq 0^*$, assim $-\alpha < 0^*$. ■

Teorema 6.10. *Sejam* $\alpha, \beta \in \mathbb{R}$. *Vale que* $\alpha \leq \beta \iff -\beta \leq -\alpha$.

Demonstração: Utilizando a compatibilidade da adição com a relação de ordem (Teorema 6.8), temos que

$$\begin{aligned} \alpha \leq \beta &\iff \alpha - \alpha \leq \beta - \alpha \\ &\iff -\beta + 0^* \leq -\beta + \beta - \alpha \\ &\iff -\beta \leq -\alpha. \end{aligned}$$

■

Definição 6.8. *O módulo de um corte* α, *denotado por* $|\alpha|$, *é definido por*

$$|\alpha| = \begin{cases} \alpha & , \text{ se } \alpha \geq 0^* \\ -\alpha & , \text{ se } \alpha < 0^* \end{cases}.$$

Teorema 6.11. *Para qualquer número real* α, *vale* $|\alpha| \geq 0^*$.

Demonstração: Se $\alpha \geq 0^*$, então $|\alpha| = \alpha \geq 0^*$. Se $\alpha \leq 0^*$, então $|\alpha| = -\alpha \geq 0^*$, conforme a Proposição 6.5. ■

Proposição 6.7. *Para qualquer número real α, vale $|\alpha| = 0^* \iff \alpha = 0^*$.*

Demonstração: Se $\alpha = 0^*$ então obtemos $|0^*| = 0^*$. Se $\alpha \neq 0^*$ então, ou $\alpha > 0^*$ ou $\alpha < 0^*$. No primeiro caso, temos $|\alpha| = \alpha > 0^*$. No segundo, temos $|\alpha| = -\alpha$, como $\alpha \leq 0^*$, pela Proposição 6.5, temos $-\alpha \geq 0^*$, mas tínhamos $\alpha \neq 0^*$, assim $-\alpha \neq 0^*$ onde concluímos que $-\alpha > 0^*$. ■

Observação 6.6. Considerando a Proposição 6.7, podemos considerar uma segunda versão da definição de módulo, como abaixo:

Definição 6.9. *Versão equivalente da Definição 6.8:*

$$|\alpha| = \begin{cases} \alpha & , \text{ se } \alpha \geq 0^* \\ -\alpha & , \text{ se } \alpha \leq 0^* \end{cases}.$$

Proposição 6.8. *Para qualquer número real α, vale $|\alpha| \geq \alpha$.*

Demonstração: Se $\alpha \geq 0^*$ então $|\alpha| = \alpha$. Se $\alpha < 0^*$ então $|\alpha| = -\alpha \geq 0^* > \alpha$. ■

Proposição 6.9. *Se $\alpha, \beta \in \mathbb{R}$, com $\alpha \geq |\beta|$, então $\alpha + \beta \geq 0^*$.*

Demonstração: Notando que $\alpha \geq 0^*$, caso $\beta \geq 0^*$ então $\alpha + \beta \geq 0^*$. Já se $\beta < 0^*$, temos $\alpha \geq |\beta| = -\beta$, assim $\alpha \geq -\beta \iff \alpha + \beta \geq 0^*$. ■

Proposição 6.10. *Se $\alpha \in \mathbb{R}$ então $|\alpha| = |-\alpha|$.*

Demonstração: Façamos a demonstração em três casos.

(i) Caso $\alpha = 0^*$:
Como 0^* é neutro da soma, temos $0^* = -0^*$, assim $|-\alpha| = |\alpha|$.

(ii) Caso $\alpha > 0^*$:
Temos $|\alpha| = \alpha$ e $|-\alpha| = -(-(\alpha)) = \alpha$, porque $-\alpha < 0^*$ conforme Corolário 6.1.

(iii) Caso $\alpha < 0^*$:
Temos $|\alpha| = -\alpha$ e $|-\alpha| = -\alpha$, pois $-\alpha > 0$, pelo Corolário 6.1.

■

Definição 6.10. *A multiplicação de dois números reais α e β, denotada por $\alpha \cdot \beta$, é definida por:*

$$\alpha \cdot \beta = \begin{cases} \mathbb{Q}^*_- \cup \{rs : r \in \alpha \text{ e } s \in \beta, 0 \leq r, 0 \leq s\}, \text{ se} & \alpha \geq 0^*, \beta \geq 0^* \\ -(|\alpha||\beta|) \quad , \text{ se} & \alpha < 0^*, \beta \geq 0^* \\ -(|\alpha||\beta|) \quad , \text{ se} & \alpha \geq 0^*, \beta < 0^* \\ (|\alpha||\beta|) \quad , \text{ se} & \alpha < 0^*, \beta < 0^* \end{cases}.$$

Essa definição faz com que a multiplicação fique "fundamentada" no produto de dois números não negativos, e quando um dos fatores for negativo, utilizamos o módulo para obter um número não negativo para calcular o produto, e depois aplicamos uma regra de sinal.

Proposição 6.11. *A multiplicação de dois números reais é fechada, isto é, também é um número real (corte).*

Demonstração: Vamos primeiro mostrar que quando α e β são ambos não negativos, o resultado da multiplicação é um número real.

Seja $\alpha \cdot \beta = \mathbb{Q}^*_- \cup \{rs : r \in \alpha \text{ e } s \in \beta, 0 \leq r, 0 \leq s\}$.

Vamos mostrar que $\alpha\beta$ é um conjunto próprio de $\mathbb{Q}$. Sabemos que $\mathbb{Q}^*_- \subset \alpha\beta$, assim o produto é não vazio. Sejam r' uma cota superior de α e s' uma cota superior de β, assim ficamos com $0 \leq r < r'$ para qualquer r não negativo de α (caso exista, isto é, $\alpha \neq 0^*$). Analogamente para β, temos $0 \leq s < s'$ para qualquer s não negativo de β. Pela Proposição 5.5, temos $rs < r's'$, desse modo $r's' \notin \alpha\beta$, assim $\alpha \cdot \beta \neq \mathbb{Q}$.

Para verificar o segundo item da Definição 6.1, observamos que o conjunto $\alpha \cdot \beta$ é uma união dos racionais negativos com outro conjunto (que pode ter alguns racionais não negativos). Desse modo, qualquer número racional negativo está em $\alpha\beta$. Vejamos agora o que ocorre com a parte não negativa. Se dados r, s com $0 \leq s < r$ e $r \in \alpha\beta$, vamos provar que $s \in \alpha\beta$. Temos que $r = xy$, com $0 \leq x \in \alpha$ e $0 \leq y \in \beta$, assim $s < xy$. Se $x = 0$, então $s < 0y = 0$ e $s \in \mathbb{Q}^*_- \subset \alpha \cdot \beta$. Se $x \neq 0$, usando a compatibilidade do produto com a relação de ordem (Proposição 5.3), obtemos $\frac{s}{x} < y$. Como $s = x \cdot \frac{s}{x}$, e $x \in \alpha, \frac{s}{x} < y \in \beta$, segue que $\frac{s}{x} \in \beta$ e $s \in \alpha\beta$.

Para mostrar que não há máximo em $\alpha\beta$ usamos o fato de que não há máximo nem em α, nem em β. Sejam $r \in \alpha$ e $s \in \beta$. Em α existe $r' > r$ e em β existe $s' > s$, dessa forma, pela Proposição 5.5, obtemos $rs < r's' \in \alpha\beta$.

Desse modo, concluímos que quando α e β são não negativos, o resultado $\alpha \cdot \beta$ é um corte.

Para os outros casos, observemos que o módulo de um número real é um número real, bem como o simétrico. Com isso, independentemente de α, β serem positivos ou não, sempre temos $\alpha \cdot \beta \in \mathbb{R}$. ■

Proposição 6.12. *Sejam α e β números reais. Vale que $(-\alpha)\,\beta = \alpha\,(-\beta) = -\,(\alpha\beta)$.*

Demonstração: Consideremos quatro casos distintos, que contemplem todas as combinações de α, β sendo maiores do que ou iguais a 0^*, ou sendo menores do que 0^*. Vamos utilizar a Proposição 6.10 e a Definição 6.9 (a segunda definição de módulo) porque ela é conveniente quando trabalhamos com, digamos, $\gamma \geq 0^*$ e obtemos $-\gamma \leq 0^*$. Com isso evitamos separar em dois casos ($-\gamma = 0^*$ e $-\gamma < 0^*$) para aplicar a definição de módulo inicial (Definição 6.8).

1. $\alpha \geq 0^*$ e $\beta \geq 0^*$:
   Temos $-\alpha \leq 0^*$ e $-\beta \leq 0^*$. Assim
   $$(-\alpha)\beta = -(|-\alpha||\beta|) = -(|\alpha||\beta|),$$
   e
   $$\alpha(-\beta) = -(|\alpha||-\beta|) = -(|\alpha||\beta|).$$
   Como $-(|\alpha||\beta|) = -(\alpha\beta)$, o resultado é válido.

2. $\alpha \geq 0^*$ e $\beta < 0^*$:
   Temos $-\alpha \leq 0^*$ e $-\beta > 0^*$. Assim
   $$(-\alpha)\beta = |-\alpha||\beta| = |\alpha||\beta| = \alpha(-\beta).$$
   Temos também que $-(\alpha\beta) = -(-(|\alpha||\beta|)) = |\alpha||\beta| = \alpha(-\beta)$ e o resultado é válido.

3. $\alpha < 0^*$ e $\beta \geq 0^*$:
   Temos $-\alpha > 0^*$ e $-\beta \leq 0^*$. Assim
   $$\alpha(-\beta) = |\alpha||-\beta| = (-\alpha)\beta.$$
   Temos também que $-(\alpha\beta) = -(-(|\alpha||\beta|)) = |\alpha||\beta| = (-\alpha)\beta$.

4. $\alpha < 0^*$ e $\beta < 0^*$:
   Temos $-\alpha > 0^*$ e $-\beta > 0^*$. Assim
   $$(-\alpha)\beta = -(|-\alpha||\beta|) = -((-\alpha)(-\beta)),$$
   $$\alpha(-\beta) = -(|\alpha||-\beta|) = -((-\alpha)(-\beta)),$$
   e
   $$-(\alpha\beta) = -(|\alpha||\beta|) = -((-\alpha)(-\beta)).$$
   Logo, o resultado também é válido.

■

Proposição 6.13. *Sejam α e β números reais, vale que $(-\alpha)\,(-\beta) = \alpha\beta$.*

Demonstração: Vamos utilizar a Definição 6.9 e a Proposição 6.10, analogamente à prova anterior (Proposição 6.12).

1. $\alpha \geq 0^*$ e $\beta \geq 0^*$:
   Temos $-\alpha \leq 0^*$ e $-\beta \leq 0^*$. Assim
   $$(-\alpha)(-\beta) = |-\alpha||-\beta| = \alpha\beta.$$

2. $\alpha \geq 0^*$ e $\beta < 0^*$:
   Temos $-\alpha \leq 0^*$ e $-\beta > 0^*$. Assim
   $$(-\alpha)(-\beta) = -(|-\alpha||-\beta|) = -(|\alpha||\beta|) = \alpha\beta.$$

3. $\alpha < 0^*$ e $\beta \geq 0^*$:
   Temos $-\alpha > 0^*$ e $-\beta \leq 0^*$. Assim
   $$(-\alpha)(-\beta) = -(|-\alpha||-\beta|) = -(|\alpha||\beta|) = \alpha\beta.$$

4. $\alpha < 0^*$ e $\beta < 0^*$:
   Temos $-\alpha > 0^*$ e $-\beta > 0^*$. Assim
   $$\alpha\beta = |\alpha||\beta| = (-\alpha)(-\beta).$$

■

Proposição 6.14. *A multiplicação de números reais é associativa.*

Demonstração: Vamos provar que $(\alpha\beta)\gamma = \alpha(\beta\gamma)$, separando em casos.

1. Se $\alpha,\ \beta,\ \gamma \geq 0^*$:
   Como $\alpha\beta = \mathbb{Q}^*_- \cup \{ab : a \in \alpha \wedge b \in \beta\}$ segue que:
   $$(\alpha\beta)\gamma = \mathbb{Q}^*_- \cup \{(ab)c : (a \in \alpha \wedge b \in \beta) \wedge c \in \gamma\},$$
   $$\alpha(\beta\gamma) = \mathbb{Q}^*_- \cup \{a(bc) : a \in \alpha \wedge (b \in \beta \wedge c \in \gamma)\}.$$
   Como a associatividade vale tanto para o produto em $\mathbb{Q}$ quanto para a conjunção $\wedge$, obtemos que $(\alpha\beta)\gamma = \alpha(\beta\gamma)$.

2. Se qualquer um dos números α, β ou γ é nulo, a associatividade é trivial.

3. Se $\alpha,\ \beta > 0^*,\ \gamma < 0$:

$$\begin{aligned}(\alpha\beta)\gamma &= -((\alpha\beta)|\gamma|)\\ &= -(\alpha(|\beta||\gamma|))\\ &= \alpha(-(|\beta||\gamma|)) \text{ (Proposição 6.12)}\\ &= \alpha(\beta\gamma).\end{aligned}$$

4. Se $\alpha,\ \gamma > 0^*,\ \beta < 0^*$:

$$\begin{aligned}(\alpha\beta)\gamma &= (-(|\alpha||\beta|))\gamma\\ &= -((|\alpha||\beta|)\gamma) \text{ (Proposição 6.12)}\\ &= -(|\alpha|(|\beta|\gamma))\\ &= |\alpha|(-(|\beta|\gamma))\\ &= \alpha(\beta\gamma).\end{aligned}$$

5. Se $\alpha > 0^*,\ \beta,\ \gamma < 0^*$:

$$\begin{aligned}(\alpha\beta)\gamma &= (-(|\alpha||\beta|)\gamma\\ &= \Big| -(|\alpha||\beta|)\Big||\gamma| \text{ (Definição 6.10 para } -(|\alpha||\beta|) < 0^* \text{ e } \gamma < 0^*)\\ &= (|\alpha||\beta|)|\gamma|\\ &= |\alpha|(|\beta||\gamma|)\\ &= \alpha(\beta\gamma).\end{aligned}$$

6. Se $\alpha < 0^*,\ \beta,\ \gamma > 0^*$:

$$\begin{aligned}(\alpha\beta)\gamma &= (-(|\alpha||\beta|))\gamma\\ &= -((|\alpha||\beta|)\gamma) \text{ (Proposição 6.12)}\\ &= -(|\alpha|(|\beta|\gamma))\\ &= \alpha(\beta\gamma).\end{aligned}$$

7. Se $\alpha,\ \gamma < 0^*,\ \beta > 0^*$:

$$\begin{aligned}(\alpha\beta)\gamma &= \Big(- \big(|\alpha||\beta|\big)\Big)\gamma \\ &= \Big| - \big(|\alpha||\beta|\big)\Big|\gamma\Big| \\ &= \Big|\big(|\alpha||\beta|\big)\Big|\gamma\Big| \\ &= |\alpha|\big(|\beta||\gamma|\big) \\ &= -\alpha(|\beta||\gamma|) \\ &= \alpha(-|\beta||\gamma|) \\ &= \alpha(\beta\gamma).\end{aligned}$$

8. Se $\alpha,\ \beta < 0^*,\ \gamma > 0^*$:

$$\begin{aligned}(\alpha\beta)\gamma &= \big(|\alpha||\beta|\big)|\gamma| \\ &= |\alpha||\beta||\gamma| \\ &= (-\alpha)\big(|\beta||\gamma|\big) \\ &= \alpha\Big(- \big(|\beta||\gamma|\big)\Big) \\ &= \alpha(\beta\gamma).\end{aligned}$$

9. Se $\alpha,\ \beta,\ \gamma < 0^*$:

$$\begin{aligned}(\alpha\beta)\gamma &= \big(|\alpha||\beta|\big)\gamma \\ &= -\Big(\big||\alpha||\beta|\big|\gamma|\Big) \\ &= -\big(|\alpha||\beta||\gamma|\big) \\ &= -\big(|\alpha|(\beta\gamma)\big) \\ &= \alpha(\beta\gamma).\end{aligned}$$

■

Proposição 6.15. *A multiplicação de números reais é comutativa.*

Demonstração: Também dividiremos em casos:

1. Se $\alpha, \beta \geq 0^*$, temos:

$$\alpha\beta = \mathbb{Q}^*_- \cup \{ab : a \in \alpha \wedge b \in \beta\} = \mathbb{Q}^*_- \cup \{ba : b \in \beta \wedge a \in \alpha\} = \beta\alpha.$$

2. Se $\alpha \geq 0^*$ e $\beta < 0^*$, temos:

$$\alpha\beta = -(|\alpha||\beta|) = -(\alpha(-\beta)) = -((-\beta)\alpha) = -(-\beta\alpha) = \beta\alpha.$$

3. Se $\alpha < 0^*$ e $\beta \geq 0^*$, temos:

$$\alpha\beta = -(|\alpha||\beta|) = -((-\alpha)\beta) = -(\beta(-\alpha)) = -(-\beta\alpha) = \beta\alpha.$$

4. Se $\alpha, \beta < 0^*$, temos:

$$\alpha\beta = |\alpha||\beta| = (-\alpha)(-\beta) = (-\beta)(-\alpha) = \beta\alpha.$$

■

Teorema 6.12. *O número $1^* \in \mathbb{R}$ é o elemento neutro do produto, isto é, para qualquer $\alpha \in \mathbb{R}$ vale $\alpha \cdot 1^* \subset \alpha$ e $\alpha \subset \alpha \cdot 1^*$.*

Demonstração: Vamos primeiro considerar $\alpha \geq 0^*$. Mostremos que $\alpha \cdot 1^* \subset \alpha$. Temos $\alpha \cdot 1^* = \mathbb{Q}^*_- \cup \{rs : 0^* \leq r \in \alpha \wedge 0^* \leq s \in 1^*\}$. Nessas condições $0 \leq s < 1$ assim pela compatibilidade do produto em $\mathbb{Q}$, obtemos $rs < r \cdot 1 = r \in \alpha$, portanto $\alpha \cdot 1^* \subset \alpha$.

Para mostrar que $\alpha \subset \alpha \cdot 1^*$, seja $r \in \alpha$. Como α não tem máximo, podemos escolher um $r' > r$. Pela Proposição 5.6, temos que a expressão $r = r' \cdot b$ sempre tem uma solução para b, dada por $\frac{r}{r'} = b$. Basta mostrar que $b < 1$, que ocorre devido à compatibilidade do produto com a relação de ordem em $\mathbb{Q}$, pois $r < r' \iff \frac{r}{r'} < \frac{r'}{r'} = 1$. Assim $b < 1$ e temos $r = r' \cdot b$, com $r' \in \alpha$ e $b \in 1^*$. Logo $r \in \alpha \cdot 1^*$. ■

Proposição 6.16. *No conjunto dos números reais, a multiplicação é distributiva em relação à adição, isto é, se α, β e γ são números reais, então $\alpha(\beta + \gamma) = \alpha\beta + \alpha\gamma$.*

Demonstração: Sejam α, β, γ números reais. Inicialmente vamos supor que sejam todos não negativos. Temos que

$$\beta + \gamma = \{y + z \in \mathbb{Q} : y \in \beta \wedge z \in \gamma\}.$$

Seja $A = \alpha(\beta + \gamma) = \mathbb{Q}^*_- \cup \{r \in \mathbb{Q} : r = pq, \text{ com } 0 \leq p \in \alpha \wedge 0 \leq q \in \beta + \gamma\}$.
Assim, de $q \in \beta + \gamma$ temos que $q = y + z$ com $y \in \beta$ e $z \in \gamma$.
Os elementos de A são ou racionais negativos, ou da forma $r = p(y + z) = py + pz$ com $0 \leq p \in \alpha$, $y \in \beta$ e $z \in \gamma$ tais que $0 \leq y + z$. Já para $B = \alpha\beta + \alpha\gamma$ temos:

$$\alpha\beta = \mathbb{Q}^*_- \cup \{r' = p'y', \text{ com } 0 \leq p' \in \alpha \text{ e } 0 \leq y' \in \beta\}$$

e

$$\alpha\gamma = \mathbb{Q}^*_- \cup \{r'' \in \mathbb{Q} : r'' = p''z'' \text{ com } 0 \leq p'' \in \alpha \text{ e } 0 \leq z'' \in \gamma.$$

Assim

$$B = \alpha\beta + \alpha\gamma = \{s + t \in \mathbb{Q} : s \in \alpha\beta \text{ e } t \in \alpha\gamma\}.$$

Desse modo, os elementos de B são de uma das formas:

(i) $a + b$, com $a, b \in \mathbb{Q}^*_-$;

(ii) $a + p''z''$, com $a \in \mathbb{Q}^*_-$, $0 \leq p'' \in \alpha$ e $0 \leq z'' \in \gamma$;

(iii) $p'y' + b$, com $b \in \mathbb{Q}^*_-$, $0 \leq p' \in \alpha$, $0 \leq y' \in \beta$;

(iv) $p'y' + p''z''$, com $0 \leq p' \in \alpha$, $0 \leq y' \in \beta$, $0 \leq p'' \in \alpha$ e $0 \leq z'' \in \gamma$.

Para provar que $A \subset B$, observemos que A é a união de dois conjuntos. Assim:

1. se r é um número negativo de A, então r está em B , pois o elemento r se caracteriza pela forma (i).
2. se $r \in A$ é da forma $r = py + pz$, com $0 \leq p \in \alpha$ e $0 \leq y + z$, com $y \in \beta$ e $z \in \gamma$, dividimos em quatro subcasos:
   a) se $y \geq 0$ e $z \geq 0$ então r está em B na forma (iv).
   b) se $y \leq 0$ e $z \geq 0$ então $r = py + pz = a + pz$ com $a \leq 0$. Se $a = 0$, então r está em B na forma (iv). Caso $a < 0$ então r está em B na forma (ii).
   c) se $y \geq 0$ e $z \leq 0$ então $r = py + pz$. Se $z = 0$, então $r = py + 0$ está em B na forma (iv). Caso $z < 0$, temos $r = py + b, b < 0$, aí $r \in B$ é da forma (iii).
   d) para $y < 0$ e $z < 0$ temos um caso impossível, pois temos necessariamente $0 > y + z$.

Assim concluímos que $A \subset B$.

Para mostrar que $B \subset A$ vamos provar que o caso da forma (iv) está em A, e também que, para qualquer elemento s que esteja representado em uma das outras três formas de B, existirá um elemento r na forma (iv) com $r > s$.

Tomemos um elemento da forma (iv), dado por $p'y' + p''z''$ com $0 \leq p' \in \alpha$, $0 \leq y' \in \beta, 0 \leq p'' \in \alpha, 0 \leq z'' \in \gamma$. Sabemos que pela tricotomia de $\mathbb{Q}$, vale $p' \geq p''$ ou $p'' > p'$. Assim:

1. Se $p' \geq p''$ então:

$$\begin{aligned} r = p'y' + p''z'' &= p'y' + p'z'' - p'z'' + p''z'' \\ &= p'(y' + z'') + z''(p'' - p'). \end{aligned}$$

Sabemos que $p' \in \alpha$ e $y' + z'' \in \beta + \gamma$. Logo $p'(y' + z'') \in A = \alpha(\beta + \gamma)$. Além disso, $z''(p'' - p') \leq 0$ e como A é um corte, então $z''(p'' - p') \in A$, e também $p'(y' + z'') + z''(p'' - p') < p'(y' + z'')$. Assim $r = p'(y' + z'') + z''(p'' - p') \in A$.

2. Se $p'' > p'$ então:

$$\begin{aligned} r = p'y' + p''z'' &= p'y' + p''y' - p''y' + p''z'' \\ &= p''y' + p''z'' + p'y' - p''y' \\ &= p''(y' + z'') + y'(p' - p''). \end{aligned}$$

Analogamente ao caso anterior, a primeira parcela da soma está em A e a segunda parcela é um número negativo, então r está no corte A.

Agora vamos mostrar que sempre podemos escolher um elemento em B na forma (iv) em que ele é maior do que algum elemento com uma representação fixa em alguma das outras três formas.

Para mostrar que podemos escolher tal elemento, basta observar que as demais formas são tais que $a, b \in \mathbb{Q}^*_-$, $0 < p', p'' \in \alpha$, $0 < y' \in \beta$, $0 < z'' \in \gamma$. Desse modo, em cada uma das demais formas temos:

(i) $p'y' + p''z'' > a + b$;

(ii) $p'y' + p''z'' > a + p''z''$;

(iii) $p'y' + p''z'' > p'y' + b$.

Com isso, provamos a distributividade no caso em que α, β e γ são não negativos.

Vamos mostrar agora que ela vale também para os casos em que α, β e γ possam ser negativos também. Analisaremos cada situação:

1. $\alpha < 0^*$ e $\beta, \gamma \geq 0^*$:

$$\begin{aligned}\alpha(\beta+\gamma) &= -(|\alpha||\beta+\gamma|)\\ &= -((-\alpha)(\beta+\gamma))\\ &= -((-\alpha)\beta+(-\alpha)\gamma)\\ &= -(-\alpha\beta-\alpha\gamma)(\text{pela Proposição 6.13})\\ &= -((-\alpha\beta)+(-\alpha\gamma))\\ &= -(-\alpha\beta)-(-\alpha\gamma)(\text{pelo Teorema 6.9})\\ &= \alpha\beta+\alpha\gamma.\end{aligned}$$

2. $\alpha \geq 0^*$ e $\beta, \gamma < 0^*$:

$$\begin{aligned}\alpha(\beta+\gamma) &= -(|\alpha||\beta+\gamma|)\\ &= -(\alpha\cdot(-(\beta+\gamma)))\\ &= -(\alpha((-\beta)+(-\gamma)))(\text{pelo Teorema 6.9})\\ &= -(\alpha(-\beta)+\alpha(-\gamma))\\ &= -\alpha(-\beta)-\alpha(-\gamma)\\ &= \alpha\beta+\alpha\gamma.\end{aligned}$$

3. $\alpha, \beta \geq 0^*$ e $\gamma < 0^*$:
   Vamos separar em dois casos, considerando a desigualdade entre β e $|\gamma|$.

   a) Se $\beta \geq |\gamma| = -\gamma$:

$$\begin{aligned}\alpha\beta &= \alpha(\beta+\gamma-\gamma)\\ &= \alpha((\beta+\gamma)+(-\gamma))(\text{pela Proposição 6.9})\\ &= \alpha(\beta+\gamma)-\alpha\gamma.\end{aligned}$$

   Assim, $\alpha\beta = \alpha(\beta+\gamma)-\alpha\gamma$ e então $\alpha\beta+\alpha\gamma = \alpha(\beta+\gamma)$.

   b) Se $\beta < |\gamma| = -\gamma$:

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

   Assim, $\alpha\gamma = \alpha(\gamma+\beta)-\alpha\beta$ e então $\alpha\gamma+\alpha\beta = \alpha(\gamma+\beta)$.

4. $\alpha, \beta, \gamma < 0^*$:

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

■

Teorema 6.13. *Seja $\alpha \in \mathbb{R}$, vale que $\alpha \cdot 0^* = 0^*$.*

Demonstração: Primeiro notemos que $0^* = \mathbb{Q}^*_-$, ou seja, todos os racionais negativos. Sabemos que se $\alpha \geq 0^*$, então $\alpha \cdot 0^* = \mathbb{Q}^*_- \cup \{rs : 0 \leq r \in \alpha \text{ e } 0 \leq s \in 0^*\}$, mas como não existe elemento em 0^* que seja maior do que ou igual a zero, a segunda parcela da união é vazia, desse modo $\alpha \cdot 0^* = 0^* = \mathbb{Q}^*_-$ para $\alpha \geq 0^*$.

Por outro lado, se $\alpha < 0$, temos $\alpha \cdot 0^* = -(|\alpha| \cdot |0^*|) = -(|\alpha| \cdot 0^*) = 0^*$. Note que na última igualdade usamos a primeira parte dessa demonstração e na penúltima igualdade usamos a Proposição 6.7. ■

Teorema 6.14. *O produto em $\mathbb{R}$ é compatível com a relação de ordem.*

Demonstração: Sejam $\alpha, \beta \in \mathbb{R}$ e $0^* \leq \gamma \in \mathbb{R}$. Vamos provar que se $\alpha \leq \beta$, então $\alpha\gamma \leq \beta\gamma$, separando em três casos:

1. $0^* \leq \alpha \leq \beta$: Temos

$$\alpha\gamma = \mathbb{Q}^*_- \cup \{rs : 0 \leq r \in \alpha \text{ e } 0 \leq s \in \gamma\},$$

e

$$\beta\gamma = \mathbb{Q}^*_- \cup \{r's' : 0 \leq r' \in \beta \text{ e } 0 \leq s' \in \gamma\}.$$

Obviamente, $\mathbb{Q}^*_-$ está contido em $\alpha\gamma$ e em $\beta\gamma$. Para a segunda parcela da união em $\alpha\gamma$, como ocorre que $r \in \alpha \implies r \in \beta$, temos também que para $s \in \gamma$, $rs \in \alpha\gamma \implies rs \in \beta\gamma$. Logo $\alpha\gamma \subset \beta\gamma$ e $\alpha\gamma \leq \beta\gamma$.

2. $\alpha \leq \beta \leq 0^*$:

Pelo Teorema 6.10, temos

$$\alpha \leq \beta \iff -\beta \leq -\alpha.$$

Como $-\alpha \geq 0^*$ e $-\beta \geq 0^*$, pelo caso anterior temos

$$(-\beta)\gamma \leq (-\alpha)\gamma$$

isto é,

$$-\beta\gamma \leq -\alpha\gamma$$

e pelo Teorema 6.10

$$\alpha\gamma \leq \beta\gamma.$$

3. $\alpha \leq 0^* \leq \beta$:

   Basta observar a Definição 6.10, pois $\alpha\gamma = -(|\alpha||\gamma|) \leq 0^*$ e $\beta\gamma \geq 0^*$. Logo $\alpha\gamma \leq \beta\gamma$.

■

Teorema 6.15. *Se $0^* \neq \alpha \in \mathbb{R}$ então α admite um inverso, isto é, existe um $\beta \in \mathbb{R}$ tal que $\alpha \cdot \beta = 1^*$.*

Demonstração: A demonstração é semelhante com a da simetria no Teorema 6.7, mas com algumas diferenças que aparecem também devido ao fato de um número racional ser uma fração com denominador não nulo.

Seja $\mathbb{S}_\alpha = \{a \in \mathbb{Q} : a \text{ é cota superior não mínima de } \alpha\}$.

Vamos supor inicialmente que $\alpha > 0^*$. Consideremos

$$\beta = \mathbb{Q}^*_- \cup \{0\} \cup \{b \in \mathbb{Q}^*_+ : \frac{1}{b} \in \mathbb{S}_\alpha\}$$

e mostremos que $\beta \in \mathbb{R}$.

Para mostrar que β é subconjunto próprio de $\mathbb{Q}$, iniciamos notando que $0 \in \beta$. Para mostrar que $\beta \neq \mathbb{Q}$ podemos escolher um elemento racional que não está em β da seguinte forma: escolha $\frac{1}{b} \in \alpha$ sendo $\frac{1}{b} > 0$, assim $\frac{1}{b} \notin \mathbb{S}_\alpha$, isto é, $\frac{1}{b}$ não está no conjunto das cotas superiores não mínimas de α, daí $b \notin \beta$, desse modo $\beta \neq \mathbb{Q}$.

Para mostrar o Item (ii) da Definição 6.1, seja $r \in \beta$. É imediato que qualquer racional negativo, ou nulo está em β. Consideremos então o último caso, $0 < s < r$. Temos que

$$s < r \iff \frac{s}{sr} < \frac{r}{sr} \iff \frac{1}{r} < \frac{1}{s},$$

assim $\frac{1}{s}$ é maior do que uma cota superior que não é mínima de α, então $\frac{1}{s} \in \mathbb{S}_\alpha$ e $s \in \beta$.

Para mostrar o Item (iii) da Definição 6.1, devemos mostrar que dado $r \in \beta$, existe $s > r$ com $s \in \beta$. Qualquer racional não positivo está em β, por construção. Se, por outro lado, escolhermos um $r > 0$ de β, então $\frac{1}{r} \in \mathbb{S}_\alpha$, e como $\frac{1}{r}$ é cota superior não mínima de α, existe uma cota superior $s' < \frac{1}{r}$, e podemos obter o inverso s de s', pois qualquer racional diferente de 0 possui um inverso, como diz o Teorema 5.5. Assim, $s' = \frac{1}{s}$ é uma cota superior de α, podendo ser mínima ou não. Temos então $\frac{1}{s} < \frac{1}{r}$, aí podemos escolher um terceiro elemento entre eles, como provado no Corolário 5.2. Pode ser, usando a mesma expressão do Corolário 5.2,

$$\frac{1}{t} = \frac{\frac{1}{s} + \frac{1}{r}}{2},$$

assim $\frac{1}{s} < \frac{1}{t} < \frac{1}{r}$ e, portanto, $s > t > r$, uma vez que o produto é compatível com a relação de ordem em $\mathbb{Q}$. Observando que $\frac{1}{t} \in \mathbb{S}_\alpha$ concluímos que $t \in \beta$, com $t > r$, desse modo β não tem máximo.

Para mostrar o caso em que $\alpha < 0$, observemos a Definição 6.10, pois o produto de dois números não negativos é não negativo, e o produto de dois não positivos é não negativo. Como 1^* é positivo, se o inverso de α existir, ele deve ser negativo. Aí temos $\alpha \cdot \beta = |\alpha||\beta|$, com β igual no caso anterior, quando $\alpha > 0$. Como o inverso é único conforme Teorema 2.4, concluímos que apenas esse β é o inverso de α, ou seja, $\beta < 0^*$ é o inverso de $\alpha < 0^*$, em que $|\beta|$ é inverso de $|\alpha|$.

■

6.4. Imersão de $\mathbb{Q}$ em $\mathbb{R}$

Teorema 6.16. *Considere a função definida abaixo:*

$$\begin{aligned} {}^*\colon \mathbb{Q} &\to \mathbb{R} \\ x &\mapsto x^*. \end{aligned}$$

Essa função tem as propriedades a seguir:

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

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

(iii) $p \leq q \implies p^* \leq q^*$.

Demonstração: Sejam $p^* = \{\, x \in \mathbb{Q} : x < p \,\}$ e $q^* = \{\, x \in \mathbb{Q} : x < q \,\}$.

(i) Vamos provar que $(p+q)^* \subset p^* + q^*$ e em seguida que $p^* + q^* \subset (p+q)^*$. Temos que $(p+q)^* = \{\, x \in \mathbb{Q} : x < p+q \,\}$, e que $p^* + q^* = \{\, x + y : x \in p^* \text{ e } y \in q^* \,\}$. Logo, se $x \in (p+q)^*$, então $x < p+q$. Seja $h > 0$ um racional tal que $x + h = p + q$. Assim, $x = p + q - h = \left(p - \frac{h}{2}\right) + \left(q - \frac{h}{2}\right)$. Tomando $a = p - \frac{h}{2} < p$ e $b = q - \frac{h}{2}$, temos que $a \in p^*$ e $b \in q^*$. Portanto, se $x = a + b \in (p+q)^*$, então $x \in p^* + q^*$.

Vamos mostrar que $p^* + q^* \subset (p+q)^*$. Considere $r = x + y \in p^* + q^*$, com $x \in p^*$ e $y \in q^*$. Assim $x < p$ e $y < q$. Sejam h_1 e h_2 tais que $x + h_1 = p$ e $y + h_2 = q$. Temos que $x + h_1 + y + h_2 = p + q$, logo, $x + y < p + q$. Desse modo, $r = x + y \in (p+q)^*$.

(ii) Para provar que $(pq)^* = p^* \cdot q^*$, notemos inicialmente que, para $p = 0$, temos

$$p^* \cdot q^* = 0^* \cdot q^* = 0^* = (0q)^* = (pq)^*.$$

Para $q = 0$ é análogo. Resta mostrar para os casos onde p e q são ambos não nulos.

a) Caso $p, q > 0$:
Provemos que $(pq)^* \subset p^* \cdot q^*$. Temos que

$$p^* \cdot q^* = \mathbb{Q}^*_- \cup \{\, rs : 0 \leq r \in p^* \text{ e } 0 \leq s \in q^* \,\},$$

e que

$$(pq)^* = \{\, x \in \mathbb{Q} : x < pq \,\}.$$

Seja $x \in (pq)^*$. Logo $x < pq$. Se $x < 0$, então $x \in \mathbb{Q}^*_- \subset (pq)^*$ e a inclusão é imediata. Se $x \geq 0$, tomemos $y = \frac{1}{2}\left(\frac{x}{q} + p\right)$. Como $x \geq 0$, $p > 0$ e $q > 0$, temos que $y > 0$. Pelo Corolário 5.2, concluímos que $\frac{x}{q} < y < p$. Assim, $y < p$, portanto $y \in p^*$. Como $\frac{x}{q} < y$, temos que $\frac{x}{y} < q$, pois $y, q > 0$. Desse modo, $s = \frac{x}{y} \in q^*$. Assim, $x = y \cdot \frac{x}{y} = ys$, com $0 \leq y \in p^*$ e $0 \leq s \in q^*$, ou seja, $x \in p^* \cdot q^*$.

Para mostrar a inclusão $p^* \cdot q^* \subset (pq)^*$, seja $x \in p^* \cdot q^*$. Notemos que se $x < 0$, então $x < pq$, e assim $x \in (pq)^*$ e a inclusão desejada é imediata. Se for $x \geq 0$, então $x = rs$, com $r \in p^*$ e $s \in q^*$. Logo, $r < p$ e $s < q$. Pela Proposição 5.5, obtemos que $x = rs < pq$, e portanto $x \in (pq)^*$, como queríamos mostrar.

b) Caso $p < 0$ e $q > 0$:
Temos $-p^* > 0^*$ e, pela Definição 6.8:

$$\begin{aligned} p^* \cdot q^* &= -(|p^*| \cdot |q^*|) \\ &= -((-p^*) \cdot q^*) \\ &= -((-p^* \cdot q^*)) \\ &= -((-p \cdot q)^*) \\ &= -(-(pq)^*) \\ &= (pq)^*. \end{aligned}$$

c) Caso $p > 0$ e $q < 0$:
Basta usar a comutatividade do produto e aplicar o item anterior.

d) Caso $p, q < 0$:
Temos $-p^* > 0$ e $-q^* > 0$, pela Definição 6.8, segue que

$$\begin{aligned} p^* \cdot q^* &= |p^*||q^*| \\ &= ((-p)(-q))^* \\ &= (pq)^*. \end{aligned}$$

Portanto, em todos os casos, $p^* \cdot q^* = (pq)^*$.

(iii) Para mostrar que * preserva a relação de ordem, considere $p < q$. Temos que $p^* = \{\, x \in \mathbb{Q} : x < p \,\}$ e que $q^* = \{\, x \in \mathbb{Q} : x < q \,\}$. Temos assim que existe r tal que

$p < r < q$, e portanto $r \in q^*$ mas $r \notin p^*$. Portanto $r \in q^* \setminus p^*$, e pela Definição 6.4, $p^* < q^*$.

■

Teorema 6.17. *O conjunto $\mathbb{Q}$ não é limitado superiormente em $\mathbb{R}$.*

Demonstração: Faremos a demonstração por contradição. Suponha que $L \in \mathbb{R}$ seja uma cota superior de $\mathbb{Q}$. Assim, L é um corte (Definição 6.1) que não tem cota superior em $\mathbb{Q}$, o que contraria o Teorema 6.1. ■

Observação 6.7. É imediato que $\mathbb{N}$ também não é limitado superiormente em $\mathbb{R}$, em vista de $\mathbb{N}$ ser ilimitado em $\mathbb{Z}$ (Teorema 4.9), de $\mathbb{Z}$ ser ilimitado em $\mathbb{Q}$ (Teorema 5.8), e de $\mathbb{Q}$ ser ilimitado em $\mathbb{R}$ (Teorema 6.17).

Proposição 6.17. *Se $\alpha, \beta \in \mathbb{R}$ com $\alpha < \beta$, então existe um corte racional r^* tal que $\alpha < r^* < \beta$.*

Demonstração: De $\alpha < \beta$ sabemos que existe $s \in \beta \setminus \alpha$. Como β não tem máximo, existe $s' \in \beta$ com $s' > s$. Pelo Corolário 5.2, sabemos que existe um racional entre outros dois fixados, $s < \frac{s+s'}{2} < s'$. Tome $r = \frac{s+s'}{2}$. Temos que $\alpha < r^*$ pois $s \in r^* \setminus \alpha$. Também temos que $r^* < \beta$ pois $s' \in \beta \setminus r^*$. ■

Teorema 6.18. *Sejam $A, B \subset \mathbb{R}$ tais que:*

(i) $\mathbb{R} = A \cup B$;

(ii) $A \cap B = \emptyset$;

(iii) $A \neq \emptyset \neq B$;

(iv) Se $\alpha \in A$ e $\beta \in B$ então $\alpha < \beta$.

Nestas condições existe um único γ, tal que $\alpha \leq \gamma \leq \beta$, para quaisquer $\alpha \in A$ e $\beta \in B$.

Demonstração: Primeiro vamos provar a unicidade. Suponhamos que existam γ_1, γ_2 (distintos) nestas condições. Sem perda de generalidade suponhamos $\gamma_1 < \gamma_2$. Pela Proposição 6.17 existe r^* tal que $\gamma_1 < r^* < \gamma_2$. De $\gamma_1 < r^*$ obtemos que $r^* \in B$, pois caso contrário, por hipótese ocorreria que $r^* \in A$ e, portanto, $r^* \leq \gamma_1$ o que contradiz $\gamma_1 < r^*$. Analogamente, se $r^* < \gamma_2$ temos que $r^* \in A$, pois de outro modo, pela hipótese, ocorreria $r^* \in B$ e teríamos $r^* \geq \gamma_2$, o que contradiz $r^* < \gamma_2$. Portanto γ é único.

Considere $\gamma = \{r \in \mathbb{Q} : r \in \alpha, \text{ para algum } \alpha \in A\}$. Vamos mostrar que γ é um número real, isso vem claramente pelo fato de α ser também um número real.

Para mostrar que γ é um subconjunto próprio de $\mathbb{Q}$, observemos que $A \neq \emptyset$ e que os elementos de A são conjuntos não vazios (conjuntos de números racionais). Para mostrar que $\gamma \neq \mathbb{Q}$, fixemos algum $\beta \in B$. Como $\alpha < \beta \iff \alpha \subset \beta$, podemos escolher $s \notin \beta$, isso garante que $s \notin \alpha$, qualquer que seja $\alpha \in A$, assim $\gamma \neq \mathbb{Q}$.

Para mostrar o Item (ii) da Definição 6.1, se $r \in \gamma$ então $r \in \alpha$ para algum $\alpha \in A$. Como α é um número real, qualquer racional $s < r$ também está em α e, portanto, está em γ.

Para mostrar que não há máximo em γ, seja $r \in \gamma$. Logo $r \in \alpha$ para algum $\alpha \in A$, e como α é um número real, existe $r' \in \alpha$ com $r' > r$. Assim $r' \in \gamma$ é tal que $r' > r$ e γ não tem máximo.

Com isso concluímos que γ é de fato um número real.

Vamos mostrar que $\alpha \leq \gamma \leq \beta$, quaisquer que sejam $\alpha \in A$ e $\beta \in B$. Como γ tem qualquer racional de qualquer α de A, temos que $\alpha \subset \gamma$, daí $\alpha \leq \gamma$. Para mostrar que $\gamma \leq \beta$, por contradição, suponhamos que $\beta < \gamma$. Aí temos que existe $s \in \gamma \setminus \beta$, mas temos $s \in \gamma \implies s \in \alpha$ para algum $\alpha \in A$ (devido à definição do conjunto γ). Temos então $s \in \alpha$ e $s \notin \beta$, o que é uma contradição, pois implicaria $\beta < \alpha$.

Portanto, mostramos que existe um único γ tal que

$$\alpha \leq \gamma \leq \beta.$$

■

O Teorema 6.18 é a principal diferença entre $\mathbb{Q}$ e $\mathbb{R}$. Esse resultado às vezes é substituído pelo Teorema do Supremo, que veremos no capítulo seguinte. Ao se trabalhar de maneira axiomática com esses conjuntos, os axiomas que os caracterizam são os mesmos, exceto pelo axioma relacionado à completude. Numa abordagem axiomática da geometria euclidiana plana, os números reais podem ser colocadas em correspondência biunívoca com os pontos de uma reta (BARBOSA, 2012, p. 16). Isso permite que posteriormente seja obtido o teorema conhecido popularmente como Teorema de Pitágoras. Esse teorema diz que num triângulo retângulo, se a é a hipotenusa, e c, d os catetos, então $a^2 = b^2 + c^2$ (BARBOSA, 2012, p. 133). Isso, todavia, só ganha significado completo com os números reais, pois os racionais não são adequados para medir nem mesmo a diagonal de um quadrado de lado 1.

7. SOBRE A ENUMERABILIDADE E UNICIDADE DE $\mathbb{R}$

Neste capítulo estudaremos a enumerabilidade de conjuntos, com o intuito de compreender como comparar a quantidade de elementos de um conjunto com outro. Após estabelecermos como comparar quantidades de conjuntos, por meio do conceito de enumerabilidade, vamos mostrar que os conjuntos $\mathbb{Z}$ e $\mathbb{Q}$ são enumeráveis. Isso servirá para que possamos nos questionar sobre a enumerabilidade de $\mathbb{R}$, de uma maneira significativa. Uma maneira não significativa seria assumir, por exemplo, que a quantidade de elementos de $\mathbb{Z}$ é maior do que a de $\mathbb{N}$, caso olhássemos para esses conjuntos como uma inclusão própria $\mathbb{N} \subset \mathbb{Z}$, e ainda mais, $\mathbb{Z} \setminus \mathbb{N} \neq \emptyset$, e por fim $\mathbb{Z} \setminus \mathbb{N}$ é um conjunto infinito!!!

Olhando por esse lado intuitivo, fica explícito alguns motivos que levam a ideias equivocadas[1] à respeito da quantidade de elementos de conjuntos infinitos. Mas não é só na questão de quantidades de elementos, o infinito também acarreta imprecisões quando é operado da mesma forma que um número real, por exemplo, ao somar como se fossem números reais $+\infty + (-\infty) = 0$. Seria bom se sempre soubéssemos em que ponto a intuição passará a falhar.

Para este capítulo as referências utilizadas serão Lima (2016) e Bartle e Sherbert (1927).

7.1. Conjuntos finitos

Definição 7.1. *Considere* $C_n = \{1, 2, ..., n\} = \{x \in \mathbb{N} : 1 \leq x \leq n\}$. *Diremos que um conjunto* A *é finito se:*

(i) $A = \emptyset$, *ou*

(ii) existe uma função bijetora $\phi \colon C_n \to X$.

Observação 7.1. Note que apesar de a notação $\{1, 2, ..., n\}$ sugerir que sempre o 2 está em C_n, isso não ocorre quando $n = 1$, pois temos $C_1 = \{\, 1 \,\}$.

Utilizamos a notação C_n para dar a entender uma contagem em X.

[1] Na verdade, nem se poderia dizer equivocadas antes de ser estabelecido um critério formal para a comparação de quantidades de elementos de um conjunto.

Quando $A = \emptyset$ diremos que ele não tem elementos ou, alternativamente, que tem zero elementos. Caso $A \neq \emptyset$, diremos que o número de elementos de A (também chamada de quantidade de elementos de A) é o número $n \in \mathbb{N}$ tal que $\phi\colon C_n \to A$ é uma bijeção.

Estabeleçamos que numa função, o seu domínio e contradomínio sejam sempre não vazios.

São por meio de bijeções entre conjuntos que compararemos a quantidade de seus elementos. Isso é o que diferenciará a comparação formal da quantidade de elementos, de uma abordagem leiga e intuitiva.

Definição 7.2. *Um conjunto A é chamado de infinito quando ele não é finito.*

Teorema 7.1. *Sejam $A, B \neq \emptyset$ e $f\colon A \to B$ uma bijeção. O conjunto A é finito se, e somente se, B também é finito.*

Demonstração: Seja $f\colon A \to B$ uma bijeção. Suponhamos que A seja finito. Então existe uma bijeção
$\phi\colon C_n \to A$ para algum $n \in \mathbb{N}$. Fazendo a composição de funções $f \circ \phi\colon C_n \to B$ obtemos uma função bijetora (pois a composição de funções bijetoras é uma função bijetora). Desse modo, B é finito.

Por outro lado, suponha B finito. Sabemos que existe uma função bijetora $\psi\colon C_m \to B$. Como f é bijetora, ela admite uma função inversa também bijetora, denotada por f^{-1}, cujo domínio é B e contradomínio é A. Fazendo a composição $f^{-1} \circ \psi\colon C_m \to A$, obtemos uma função bijetora, logo A também é finito. ∎

Teorema 7.2. *Se $A \subset C_n$ e existir uma bijeção $f\colon C_n \to A$, então $A = C_n$.*

Demonstração: Os índices usados na demonstração a seguir são para ajudar a distinguir os conjuntos e funções, mas eles atendem às hipóteses do teorema.

Provaremos por induçao em n. Para $n = 1$ temos $C_1 = \{\, 1 \,\}$ e como $A_1 \subset C_1$, então $A_1 = \emptyset$ ou $A_1 = \{\, 1 \,\}$. Se fosse $A_1 = \emptyset$ teríamos um contradomínio vazio (o que não pode ocorrer), então $A_1 = C_1 = \{\, 1 \,\}$. Suponhamos então que seja válido para algum $k \in \mathbb{N}$ que, se $A_k \subset C_k$ e existir uma bijeção $f\colon C_k \to A_k$ então $A_k = C_k$, queremos mostrar que vale o mesmo para $k + 1$.

Dessa forma, suponha que $A_{k+1} \subset C_{k+1}$ e que $f_{k+1}\colon C_{k+1} \to A_{k+1}$ seja uma bijeção (que não precisa ser uma extensão da bijeção da hipótese de indução!), e tomemos $a = f_{k+1}(k + 1)$. Se restringirmos o domínio e contradomínio de f_{k+1} para $f'_{k+1}\colon C_k \to A_{k+1} \setminus \{\, a \,\}$, obtemos que f'_{k+1} é bijetora.

Caso $A_{k+1} \setminus \{ a \} \subset C_k$ teremos que $A_{k+1} \setminus \{ a \} = C_k$ o que leva a

$$f_{k+1}(k+1) = k+1 \in A_{k+1},$$

assim concluímos que $A_{k+1} = C_{k+1}$.

Caso $A_{k+1} \setminus \{ a \} \not\subset C_k$ (f_{k+1} não é extensão de f_k) teremos $k+1 \in A_{k+1} - \{ a \}$, ou seja, existe $p \in C_k \subset C_{k+1}$ com $f(p) = k+1$. Vamos definir uma nova bijeção $g\colon C_{k+1} \to A_{k+1}$ tal que

$$\begin{aligned} &g(x) = f(x), \text{ se } x \neq p \text{ e } x \neq k+1, \\ &g(p) = a = f(k+1), \\ &g(k+1) = k+1. \end{aligned}$$

Assim temos que a restrição de g para $g'\colon C_k \to A_{k+1} \setminus \{ k+1 \}$ é uma bijeção, com $A_{k+1} \setminus \{ k+1 \} \subset C_k$ e, pela hipótese de indução, temos $A_{k+1} \setminus \{ k+1 \} = C_k$, o que leva a $A_{k+1} = C_k \cup \{ k+1 \} = C_{k+1}$.

■

Teorema 7.3. *Sejam dados dois conjuntos C_m, C_n. Se existir uma bijeção $f\colon C_m \to C_n$ então $m = n$.*

Demonstração: Suponhamos, sem perda de generalidade, que $m \leq n$. Desse modo $C_m \subset C_n$, pois caso não fosse, ao observarmos a Definição 7.1, exisitiria $p \in C_m \setminus C_n$, daí $n < p \leq m$, o que é contraditório.

Supondo que existe uma bijeção $f\colon C_m \to C_n$, pelo Teorema 7.2, como $C_m \subset C_n$ temos que $C_m = C_n$. Observando novamente a Definição 7.1, que se refere ao C_n, concluímos que $m = n$. ■

Com esse resultado sobre a unicidade de n numa bijeção $f : C_n \to A$, não há qualquer risco de ambiguidade quando dizemos que um conjunto A tem uma quantidade n de elementos.

Teorema 7.4. *Qualquer subconjunto de um conjunto finito também é finito. Isto é, dado um conjunto finito A, se $B \subset A$, então B é finito.*

Demonstração: Suponha A finito, com n elementos, e $B \subset A$. Vamos supor que possa ocorrer de B ser um conjunto infinito, e então chegar numa contradição. Devemos observar que B tem ao menos n elementos (pois se tivesse menos, necessariamente seria finito). Seja $B' = \{ b_1, b_2, b_3, ..., b_n \}$ com $b_i \neq b_j$, elementos distintos quaisquer de B. Desse modo existe uma bijeção $g\colon C_n \to B'$.

Queremos mostrar que nesse cenário, existe ao menos um $b \in B \setminus A$. Temos que $B' \subset B \subset A$, e que B' e A tem ambos n elementos. Ao colocarmos $A = \{ a_1, a_2, a_3, ..., a_n \}$ podemos concluir que dado um número natural $i \leq n$, vale que $a_i = b_j$ para algum natural $j \leq n$. Se isso fosse falso existiria algum $b_j \in B$ com $b_j \notin A$, o que é uma contradição. Seja $b_{n+1} \in B \setminus B'$ (podemos pegar um elemento qualquer, pois se não houvesse qualquer outro elemento B seria finito). Se fosse o caso de $b_{n+1} \in A$, teríamos que $b_{n+1} = a_i = b_j$ para algum par de i, j naturais menores do que ou iguais a n, mas daí $b_{n+1} \in B'$ o que é uma contradição. ■

Teorema 7.5. *Seja $A \subset \mathbb{N}$ um conjunto não vazio. O conjunto A é limitado se, e somente se, A é finito.*

Demonstração: Seja $A \subset \mathbb{N}$ limitado. Então existe $\alpha \in \mathbb{R}$ em que α é uma cota superior de A. Considere o conjunto $B = \{ n \in \mathbb{N} : \alpha \leq n \}$. Sabemos que pelo Teorema 3.6, o conjunto B tem um menor elemento, digamos b. Temos $A \subset C_b$, pois se não fosse, teríamos algum $a \in A$ com $a > b$, daí b não seria uma cota superior de A, o que é uma contradição. E como C_b é finito, pelo Teorema 7.4, concluímos que A é finito.

Por outro lado, considere A finito (e não vazio). Então A tem alguma quantidade n de elementos. Suponha $A = \{ a_1, a_2, ..., a_n \}$, com $a_i \in \mathbb{N}$. O número

$$k = \sum_{i=1}^{n} a_i$$

é uma cota superior para A, pois para qualquer $a \in A$ tem-se

$$a = a_i \leq \sum_{i=1}^{n} a_i = k.$$

Dessa forma, A é limitado. ■

7.2. Conjuntos enumeráveis

Definição 7.3. *Um conjunto é A é dito enumerável se ele é finito ou se existe uma bijeção $f : \mathbb{N} \to A$.*

Note que às vezes ocorre de um conjunto ser infinito e também ser enumerável, mas por outro lado, se ele não é enumerável então necessariamente ele é infinito.

Quando A é infinito e enumerável, uma bijeção $f \colon \mathbb{N} \to A$ é dita uma enumeração dos elementos de A. Tomando $f(n) = a_n$ para cada $n \in \mathbb{N}$, tem-se que $A = \{ a_1, a_2, a_3, ..., a_n, ... \}$.

Proposição 7.1. *Seja $f\colon A \to B$ uma função bijetora. O conjunto A será enumerável se, e somente se, B também for enumerável.*

Demonstração: Seja $f\colon A \to B$ bijetora. Se A for finito, existe uma bijeção $g\colon C_n \to A$, e portanto $f \circ g\colon C_n \to B$ é bijetora, daí B é finito enumerável. Se B for finito, existe uma bijeção $h\colon B \to C_n$ (pois uma bijeção sempre admite inversa), assim $h \circ f\colon A \to C_n$ é uma bijeção, e $(h \circ f)^{-1}\colon C_n \to A$ é uma enumeração finita de A.

Caso A seja infinito enumerável, existe uma bijeção $g\colon \mathbb{N} \to A$, daí $f \circ g\colon \mathbb{N} \to B$ é uma enumeração de B. Caso B seja infinito enumerável, ao considerarmos f^{-1}, caímos no caso anterior. ∎

Teorema 7.6. *Qualquer subconjunto $A \subset \mathbb{N}$ é enumerável.*

Demonstração: Se A for finito é imediato que é enumerável. Se A for infinito, vamos construir uma bijeção crescente $f\colon \mathbb{N} \to A$. Pelo Teorema 3.6 (Princípio da boa ordem) qualquer subconjunto não vazio de $\mathbb{N}$ tem um elemento mínimo. Definamos como $f(1)$ o menor elemento em A (que denotaremos por a_1). Seja $f(2)$ o menor elemento de $A \setminus \{ a_1 \}$, que denotaremos por a_2.

Suponhamos que estejam definidos $a_1 = f(1), a_2 = f(2), a_3 = f(3), ..., a_n = f(n)$, de modo a estender a ideia anterior, de que $a_1 < a_2 < ... < a_n$, e tentemos definir a partir daí o elemento de A que será $f(n+1)$. Primeiro definamos $B_n = A \setminus \{ a_1, a_2, ..., a_n \}$. Sabemos que $B_n \neq \emptyset$ pois se fosse $A \setminus \{ a_1, a_2, a_3, ..., a_n \} = \emptyset$ teríamos $A \subset \{ a_1, a_2, a_3, ..., a_n \}$ e daí pelo Teorema 7.4 teríamos que A é finito, o que é uma contradição.

Definiremos $f(n+1)$ como o menor elemento de B_n. Com isso terminamos a definição de f, basta mostrar que é bijetora.

Para mostrar que f é injetora, basta observar que $a_1 < a_2 < ... < a_n < a_{n+1}$, ou seja, dados $m, n \in \mathbb{N}$ com $m < n$ temos $a_m < a_n$, ou seja, $f(m) < f(n)$. Mostraremos que é sobrejetora por contradição. Suponha que exista algum elemento $a \in A$ com $f(n) \neq a$ para qualquer $n \in \mathbb{N}$. Desse modo $a \in B_n$ para qualquer $n \in \mathbb{N}$, o que acarreta $a > a_n$ para qualquer $n \in \mathbb{N}$ e portanto A é limitado. Como A é infinito, obtemos uma contradição pelo Teorema 7.5. ∎

Teorema 7.7. *Todo subconjunto de um conjunto enumerável também é enumerável.*

Demonstração: Seja $A \subset B$, com B enumerável. Se A for finito então é enumerável. Se A for infinito, considere uma bijeção $f\colon B \to \mathbb{N}$ (o que podemos fazer pois uma bijeção é sempre inversível). Temos $f(B) = \mathbb{N}$.

Vamos provar que $f(A) \subset \mathbb{N}$. Uma vez que $A \subset B$, se existisse $a \in A$ com $f(a) \notin \mathbb{N}$, como $a \in B$ teríamos $f(a) \in \mathbb{N}$, o que é uma contradição. Desse modo $f(A) \subset \mathbb{N}$, e pelo Teorema 7.6, concluímos que $f(A)$ é enumerável.

Como sabemos que $f(A)$ é enumerável, seja $g\colon f(A) \to \mathbb{N}$ uma bijeção. Ao considerarmos a composta de g com a f restrita a A, temos que $g \circ f\colon A \to \mathbb{N}$ é uma bijeção, pois tanto f quanto g são bijetoras. Assim provamos que A é enumerável. ■

Proposição 7.2. *Se $f\colon A \to B$ é injetora e B é enumerável, então A é enumerável.*

Demonstração: Seja B enumerável e $f\colon A \to B$ injetora. Se A é finito, então é enumerável. Se A é infinito, então considerando a restrição $f'\colon A \to f(A)$, obtemos que f' é bijetora. Temos $f(A) \subset B$, e pelo Teorema 7.7, $f(A)$ é enumerável, assim A é enumerável. ■

Observação 7.2. Não vamos fazer a demonstração de duas proposições que utilizaremos, por se tratarem dos requisitos iniciais que supomos de lógica e teoria de conjuntos básica. Caso haja interesse em ver a demonstração, o leitor pode consultar Lima (2016, p. 22).

(i) Uma função $f\colon A \to B$ admite inversa à direita se, e somente se, é sobrejetora.

(ii) Uma função $f\colon A \to B$ admite inversa à esquerda se, e somente se, é injetora.

Proposição 7.3. *Se $f\colon A \to B$ é sobrejetora e A é enumerável, então B é enumerável.*

Demonstração: Como f é sobrejetora ela admite uma inversa à direita, $g\colon B \to A$, com $f \circ g = id_B$. Assim g admite inversa à esquerda e portanto g é injetora. Aplicando a Proposição 7.2 para g, concluímos que B é enumerável. ■

Para o próximo teorema vamos assumir algumas proposições que não demonstramos ao longo deste trabalho. Isso não prejudica o desenvolvimento do trabalho pois o foco desta seção é provar a não enumerabilidade de $\mathbb{R}$. Já a enumerabilidade de outros conjuntos tem caráter mais ilustrativo do que essencial. Ainda assim ficaria mais elegante trabalhar com a enumerabilidade de conjuntos somente com o que já vimos em relação aos números naturais, só que isso é muito restritivo para este objetivo. Por causa disso, trabalharemos com a imersão de $\mathbb{N}$ em $\mathbb{Q}$.

Teorema 7.8. *O conjunto $\mathbb{N} \times \mathbb{N}$ é enumerável.*

Demonstração: Vamos inicialmente considerar a função

$$\phi(k) = 1 + 2 + ... + k = \frac{k(k+1)}{2}.$$

Essa função ϕ é estritamente crescente, pois em $\mathbb{Q}$ a multiplicação é compatível com a relação de ordem, ou seja, $p < q \implies \frac{1}{2}p(p+1) < \frac{1}{2}q(q+1)$ quando $p, q \in \mathbb{N}$.

Vamos considerar a função

$$\begin{aligned} f\colon \mathbb{N} \times \mathbb{N} &\to \mathbb{N}, \\ (a,b) &\mapsto \phi(a+b-2)+a, \end{aligned}$$

e provar que ela é bijetora.

Para mostrar a injetividade, vamos mostrar que

$$(a,b) \neq (a',b') \implies f(a,b) \neq f(a',b').$$

De $(a,b) \neq (a',b')$ temos $(a+b \neq a'+b')$ ou $(a+b = a'+b'$ e $a \neq a'$ e $b \neq b')$. Consideremos $a+b < a'+b'$, e portanto $a+b+r = a'+b'$ para algum $r \in \mathbb{N}$. Temos:

$$\begin{aligned} f(a,b) &= \phi(a+b-2)+a \\ &\leq \phi(a+b-2)+(a+b-1) \quad (\text{pois } b \geq 1) \\ &= \phi(a+b-1). \end{aligned}$$

Note que a última igualdade vem de

$$\begin{aligned} \phi(a+b-1) - \Big(\phi(a+b-2)+(a+b-1)\Big) & \\ &= \frac{1}{2}(a+b-1)(a+b) - \frac{1}{2}(a+b-2)(a+b-1) - a - b + 1 \\ &= \frac{1}{2}(a+b-1)(a+b-a-b+2) - a - b + 1 \\ &= a+b-1-a-b+1 = 0. \end{aligned}$$

Tínhamos que $f(a,b) \leq \phi(a+b-1)$ e assim:

$$\begin{aligned} f(a,b) &\leq \phi(a+b-1) \\ &\leq \phi(a'+b'-2) \text{ (pois } \phi \text{ é estritamente crescente)} \\ &< \phi(a'+b'-2)+a' \\ &= f(a',b'). \end{aligned}$$

Consideremos agora $a+b = a'+b'$ com $a \neq a'$. Temos:

$$f(a,b) = \phi(a+b-2)+a$$

e

$$f(a',b') = \phi(a'+b'-2)+a'.$$

Obviamente, os valores de ϕ, nesse caso são iguais. Por outro lado os valores para f são diferentes pois $a \neq a'$. Vale notar que se $a+b = a'+b'$, com $a \neq a'$, então $b \neq b'$. Portanto, obtemos em qualquer caso que:

$$(a,b) \neq (a',b') \implies f(a,b) \neq f(a',b').$$

Para mostrar que f é sobrejetora, observemos que $f(1,1) = 1$. Tomemos então um elemento $p \in \mathbb{N}$ com $p \geq 2$. Queremos encontrar $a_p, b_p \in \mathbb{N}$ tais que $f(a_p, b_p) = p$. Observemos que $p < \frac{p(p+1)}{2} = \phi(p)$. Isso porque:

$$\begin{aligned} 2 \leq p &\implies 2 < p+1 \\ &\implies 1 < \frac{p+1}{2} \\ &\implies p < \frac{p(p+1)}{2} = \phi(p). \end{aligned}$$

Consideremos o conjunto $E_p = \{\, k \in \mathbb{N} : p \leq \phi(k) \,\}$. Pelo Teorema 3.6, o conjunto E_p admite um elemento mínimo, que chamaremos de k_p.
Temos $\phi(k_p - 1) < p$ porque $k_p - 1$ é um natural com $k_p - 1 < k_p$, pois se fosse $k_p - 1 \geq p$ então $k_p - 1$ seria elemento de E_p menor que o mínimo, uma contradição. Também pela definição de E_p, temos $p \leq \phi(k_p) = \phi(k_p - 1) + (k_p - 1) + 1$. Notemos que para a função ϕ vale:

$$\phi(k+1) = \frac{1}{2}(k+1)(k+2) = \frac{1}{2}(k^2+3k+2) = \frac{1}{2}(k)(k+1) + \frac{2k+2}{2} = \phi(k) + k + 1.$$

Temos, agregando esses dados, que $\phi(k_p - 1) < p \leq \phi(k_p) = \phi(k_p - 1) + k_p$.

Definamos $a_p = p - \phi(k_p - 1)$ e $b_p = k_p - a_p + 1$. Disso concluímos que

$$a_p + b_p - 2 = a_p + (k_p - a_p + 1) - 2 = k_p - 1.$$

E por fim, temos

$$f(a_p, b_p) = \phi(a_p + b_p - 2) + a_p = \phi(k_p - 1) + a_p = \phi(k_p - 1) + (p - \phi(k_p - 1)) = p.$$

Isso prova que f é sobrejetora, e portanto é bijetora. Logo $\mathbb{N} \times \mathbb{N}$ é enumerável. ■

Observação 7.3. Vamos fazer outra demonstração do Teorema 7.8, admitindo-se o Teorema Fundamental da Aritmética, que pode ser encontrado em Santos (2015, p. 9). Para esta demonstração, é considerada a função injetora

$$\begin{aligned} f \colon \mathbb{N} \times \mathbb{N} &\to \mathbb{N} \\ (a,b) &\mapsto 2^a \cdot 3^b. \end{aligned}$$

O fato dessa função ser injetora já garante que $\mathbb{N} \times \mathbb{N}$ é enumerável, em vista da Proposição 7.2.

Teorema 7.9. *Se A, B são dois conjuntos enumeráveis, então o conjunto $A \times B$ também é enumerável.*

Demonstração: Sejam $\phi\colon \mathbb{N} \to A$ e $\psi\colon \mathbb{N} \to B$ enumerações de A, B. A função

$$\begin{aligned} g\colon \mathbb{N} \times \mathbb{N} &\to A \times B \\ (m, n) &\mapsto (\phi(a), \psi(b)) \end{aligned}$$

é bijetora.

Ela é injetora pois se $(m, n) \neq (m', n')$ então $m \neq m'$ ou $n \neq n'$. Sem perda de generalidade, considere $m \neq m'$. Temos então $g(m, n) = (\phi(m), \psi(n))$ e $g(m', n') = (\phi(m'), \psi(n'))$. Só que $(\phi(m), \psi(n)) \neq (\phi(m'), \psi(n'))$ pois $\phi(m) \neq \phi(m')$. O caso $n \neq n'$ é análogo. Portanto $g(m, n) \neq g(m', n')$ e g é injetora.

Para mostrar que g é sobrejetora, considere $(a, b) \in A \times B$, como ϕ e ψ são sobrejetoras, existem $m, n \in \mathbb{N}$ com $a = \phi(m)$ e $b = \psi(n)$. Daí

$$(a, b) = (\phi(m), \psi(n)) = g(m, n),$$

portanto g é sobrejetora.

Como g é bijetora, e $\mathbb{N} \times \mathbb{N}$ é enumerável (Teorema 7.8), concluímos que $A \times B$ é enumerável. ∎

Corolário 7.1. *Os conjuntos $\mathbb{Z}$ e $\mathbb{Q}$ são enumeráveis.*

Demonstração: Consideremos as definições dos conjuntos:

$$\mathbb{Z} = \mathbb{N} \times \mathbb{N}/\sim$$

e

$$\mathbb{Q} = \mathbb{Z} \times \mathbb{Z}^*/\sim,$$

cada um com sua respectiva relação de equivalência, conforme vimos nos Capítulos 4 e 5. Pelo Teorema 7.8 sabemos que $\mathbb{N} \times \mathbb{N}$ é enumerável. Por outro lado a relação $\sim$, em cada caso, não adiciona elementos nos conjuntos $\mathbb{Z}$ e $\mathbb{Q}$. Mais precisamente, temos que a função

$$\begin{aligned} f\colon \mathbb{N} \times \mathbb{N} &\to \mathbb{N} \times \mathbb{N}/\sim \\ (m, n) &\mapsto \overline{(m, n)} \end{aligned}$$

é uma função sobrejetora, assim com a Proposição 7.3 concluímos que $\mathbb{Z} = \mathbb{N} \times \mathbb{N}/\sim$ é enumerável.

Para os racionais o argumento da enumerabilidade é análogo. ∎

Definição 7.4. *Seja A um conjunto qualquer. Uma função $f : \mathbb{N} \to A$ é chamada de sequência de elementos de A, e o elemento $a \in A$ que é imagem de um número natural n, é frequentemente denotado a_n.*

Observação 7.4. Às vezes omite-se o caráter da função e opta-se pela representação de uma sequência só pela exibição dos elementos da imagem, $a_1, a_2, a_3, ...a_n, ...$ na ordem crescente de n.

Definição 7.5. *Seja A um conjunto limitado superiormente. Um número s chama-se supremo de A se for a menor das suas cotas superiores e é denotado por $sup(A)$.*

Exemplo 7.1. Ao falarmos de supremo, estamos falando sobre a completude dos números reais. No conjunto dos números racionais, que não é completo, nem todo subconjunto limitado superiormente admite um supremo. Por exemplo, o conjunto

$$\{ r \in \mathbb{Q}_+ : r^2 < 2 \} \subset \mathbb{Q},$$

não admite supremo em $\mathbb{Q}$.

Teorema 7.10. *Qualquer conjunto não vazio e limitado superiormente de números reais admite um supremo.*

Demonstração: Seja $X \subset \mathbb{R}$ um conjunto não vazio e limitado superiormente. Definamos $A = \{ \alpha \in \mathbb{R} : \alpha < x \text{ para algum } x \in X \}$, e $B = \mathbb{R} \setminus A$. Vamos usar o Teorema 6.18 para provar que existe um supremo para X.

Na definição de A, observemos que seus elementos são números que não são cotas superiores de X (essa observação se aplica mesmo que X tenha máximo). Por outro lado, em B estão os elementos complementares de A em relação à $\mathbb{R}$, assim B tem todas as cotas superiores de X.

Devemos observar que os Itens (i) e (ii) do Teorema 6.18 são imediatos da definição de AeB. Para mostrar o Item (iii) do Teorema 6.18, basta observar que dado $x \in X$, $x - 1 < x$ portanto $x - 1 \in A \neq \emptyset$. Para mostrar que $B \neq \emptyset$ basta observar que se algum elemento $L \in \mathbb{R}$ é cota superior de X, então $L + 1 \in B$. Para mostrar o Item (iv), consideremos $\alpha \in A$ e $\beta \in B$. De $\alpha \in A$ sabemos que $\alpha < x_0$ para algum $x_0 \in X$. Por outro lado, $\beta \in B$ é uma cota superior de X, pois se não fosse, ocorreria $\beta < x$ para algum $x \in X$ e daí β seria elemento de A, o que é contraditório. Temos que $x \leq \beta$ para qualquer $x \in X$, e substituindo x por x_0, obtemos $\alpha < x_0 \leq \beta$.

Concluímos que A e B atendem todas as condições do Teorema 6.18, e portanto existe um único número real tal que $\alpha \leq \gamma \leq \beta$, para quaisquer $\alpha \in A, \beta \in B$.

Devemos mostrar que $\gamma \in B$. Vamos supor que tivesse um máximo em A, digamos M. Teríamos $M < x$ para algum $x \in X$, mas como sempre existe um número real y tal

que $M < y < x$ (pela Proposição 6.17), teríamos que $y \in A$ o que é uma contradição, pois $y > M$.

Isso acarreta que de $\alpha \leq \gamma \leq \beta$ não pode ocorrer que $\gamma = \alpha$ para algum $\alpha \in A$, pois desse modo γ seria máximo de A, o que não pode ocorrer. Temos então $\alpha < \gamma \leq \beta$. Como $A \cup B = \mathbb{R}$ e $\gamma \notin A$, então $\gamma \in B$. Obviamente γ é a menor das cotas superiores, pois para qualquer $\beta \in B$ vale $\gamma \leq \beta$. Portanto, γ é o supremo de X. ■

Definição 7.6. *Seja A um conjunto limitado inferiormente. Um número i chama-se ínfimo de A se for a maior das cotas inferiores e é denotado por $inf(A)$.*

Definição 7.7. *Um conjunto $I \subset \mathbb{R}$ é chamado de intervalo fechado de extremos a e b (com $a < b$), denotado por $[a, b]$ quando*

$$I = [a, b] = \{\, x \in \mathbb{R} : a \leq x \leq b \,\}.$$

Teorema 7.11. *(Intervalos Encaixados) Seja $I_1 \supset I_2 \supset I_3 \cdots \supset I_n \supset \ldots$ uma sequência de intervalos limitados e fechados $I_n = [a_n, b_n]$. A interseção*

$$\bigcap_{n=1}^{\infty} I_n$$

tem ao menos um elemento.

Demonstração: De acordo com as hipóteses, para um dado n natural, temos $I_{n+1} \subset I_n$, o que acarreta $a_{n+1} \leq a_n \leq b_n \leq b_{n+1}$. Como cada intervalo é limitado, então o conjunto dos a_n é limitado (inferiormente por a_1 e superiormente por b_n) para qualquer n natural. Denotando por A o conjunto de todos os a_i, e denotando por B o conjunto de todos os b_i, temos que o conjunto A admite supremo em $\mathbb{R}$, conforme o Teorema 7.10. Analogamente, se considerarmos o conjunto dos b_n, ele é limitado superiormente por b_1 e inferiormente por a_n. Seja $a = sup(A)$ e $b = inf(B)$, como a é sempre maior do que a_n, para todo $n \in \mathbb{N}$ e $a \leq b_n$ para todo $n \in \mathbb{N}$, concluímos que $a \in I_n$ para qualquer $n \in \mathbb{N}$. ■

Teorema 7.12. *O conjunto dos números reais não é enumerável.*

Demonstração: A ideia nesta demonstração é criar intervalos e utilizar o Teorema 7.11 para garantir a existência de um número real, que terá a característica de não ser um elemento de qualquer subconjunto enumerável de $\mathbb{R}$.

Vamos iniciar ilustrando como serão criados os intervalos. Considere $I = [a, b]$, com $a < b$ e um número real x. Então existe um intervalo $J = [a', b'] \subset I$, com $a' < b'$, $J \neq I$ e $x \notin [a', b']$. Caso $x \notin I$, basta pegar $J = [a, b']$ com $a < b' < b$, isso já garante que $J \subset I$ e

$J \neq I$. Se x estiver nos extremos do intervalo, isto é, caso $x = a$ ou $x = b$, se for $x = a$ pegue $J = [a', b]$, com $a < a' < b$. Caso seja $x = b$, pegue $J = [a, b']$, com $a < b' < b$. Resta a situação $x \in I$, em que x não está nos extremos do intervalo. Pegue o intervalo $J = \left[a + \frac{x-a}{3}, a + \frac{x-a}{2}\right]$, como $x > a \iff x - a > 0$, temos $a + \frac{x-a}{3} > a$ e $a + \frac{x-a}{3} < b$, pois $b - a > x - a > \frac{x-a}{3}$. Analogamente, $a + \frac{x-a}{2} > 0$. Temos que $x \notin J$ e $J \subset I$ com $J \neq I$.

Seja $X = \{ x_1, x_2, x_3, ..., x_n, ... \} \subset \mathbb{R}$. Vamos mostrar que existe um $x \in \mathbb{R}$ que não é nenhum dos x_n. Vamos construir os intervalos assim, seja $I_0 = [a_0, b_0]$ um intervalo limitado e fechado, com $a_0 < b_0$. Sejam definidos indutivamente os $I_n = [a_n, b_n]$ assim: $I_1 \subset I_0$ tal que $x_1 \notin I_1$, $I_2 \subset I_1$ tal que $x_2 \notin I_2$, $I_3 \subset I_2$ tal que $x_3 \notin I_3$, e assim por diante, sempre com $a_n < b_n$. Isso cria uma sequência de intervalos $I_n \subset I_{n-1} \subset \cdots \subset I_2 \subset I_1$.

Podemos observar que qualquer x_n não está no intervalo I_n, por outro lado, pelo Teorema 7.11 (Teorema dos Intervalos Encaixados), existe pelo menos um número real $x \in I_n$, dessa maneira $x \neq x_n$ para qualquer $n \in \mathbb{N}$. Dessa maneira, qualquer que seja o conjunto enumerável X (e qualquer enumeração $x_1, x_2, ..., x_n, ...$ de X), existe algum número real $x \notin X$. Portanto não existe uma função sobrejetora $f \colon \mathbb{N} \to \mathbb{R}$. Desse modo $\mathbb{R}$ é não enumerável. ∎

7.3. A unicidade de $\mathbb{R}$

O objetivo dessa seção é apresentar $\mathbb{R}$ como o único corpo ordenado completo a menos de isomorfismo. A Definição 2.26 apresenta o que é um corpo. Nós vamos definir o que é um corpo ordenado completo e, em seguida, mostrar que quaisquer corpos ordenados completos são isomorfos entre si, isto é, preservam a adição, a multiplicação e a relação de ordem. O método de provar essa unicidade lembra, intuitivamente, dos cortes de Dedekind que vimos no Capítulo 6, pegando um subconjunto próprio de $\mathbb{Q}$, sem máximo, e que para qualquer racional no corte, todos os racionais que o precedem também estejam no corte. Uma abordagem da unicidade via sequências pode ser encontrada em Hefez (2014b).

Definição 7.8. *Um corpo ordenado é um corpo K, no qual existe um subconjunto $P \subset K$ de número que são chamados de positivos, em que são satisfeitas as condições a seguir:*

1. *A adição e a multiplicação de elementos de P estão em P, isto é,*

$$x, y \in P \implies x + y \in P$$

e

$$x, y \in P \implies x \cdot y \in P.$$

2. Dado $x \in K$ uma, e apenas uma, das seguintes situações ocorre:

$$x = 0,\ x \in P,\ -x \in P.$$

Observação 7.5. Caso o leitor queira mais informações e propriedades a respeito da ordenação em um corpo ordenado, pode consultar Lima (2016, p. 65). Vamos usar o fato que a Definição 7.8 implica que o corpo ordenado K tem uma relação de ordem total, que é compatível com sua adição e sua multiplicação.

Observação 7.6. Para esta seção, vamos também assumir que num corpo ordenado completo, o neutro da adição e o neutro da multiplicação são elementos distintos, e portanto o corpo não é composto de apenas um elemento, com $1 = 0$.

Definição 7.9. *Um corpo ordenado K é chamado de corpo ordenado completo se, para qualquer conjunto $A \subset K$, em que A é limitado superiormente, A admite um supremo em K.*

Agora vamos mostrar que um corpo ordenado completo qualquer X contém um subconjunto imergido de $\mathbb{N}$, isto é, existe uma imersão de $\mathbb{N}$ em X.

Sejam 0_X o elemento neutro da adição de X, e 1_X o neutro da multiplicação de X.

Lema 7.1. *Sejam X, Y, conjuntos com uma adição que admite a lei do cancelamento, e qualquer elemento possui um simétrico para a adição. Se $f\colon X \to Y$ é uma função aditiva, então $f(0_X) = 0_Y$.*

Demonstração: Temos que $f(0_X) + 0_Y = f(0_X) = f(0_X + 0_X) = f(0_X) + f(0_X)$. Pela lei do cancelamento da adição, $f(0_X) = 0_Y$. ∎

Teorema 7.13. *Seja X um corpo ordenado completo. Definamos uma função*

$$\begin{aligned} i\colon \mathbb{N} &\to X \\ 1 &\mapsto 1_X \\ m+1 &\mapsto i(m) + i(1). \end{aligned}$$

A função i tem as propriedades a seguir, para todos os $m, n \in \mathbb{N}$:

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

(ii) $i(m \cdot n) = i(m) \cdot i(n)$;

(iii) $m \leq n \implies i(m) \leq i(n)$.

Demonstração: As provas serão por indução.

(i) Temos pela definição de i, que $i(m+1) = i(m) + i(1)$. Assim nossa hipótese de indução é que $i(m+k) = i(m) + i(k)$ para $k \in \mathbb{N}$. Daí temos

$$i(m+k+1) = i((m+k)+1) = i(m+k)+i(1) = i(m)+i(k)+i(1) = i(m)+i(k+1).$$

(ii) Temos que, pela definição de i, que $i(m \cdot 1) = i(m) = i(m) \cdot 1_X = i(m) \cdot i(1)$. Assim nossa hipótese de indução é que $i(m \cdot k) = i(m) \cdot i(k)$ para $k \in \mathbb{N}$. Assim temos

$$\begin{aligned} i(m \cdot (k+1)) = i(m \cdot k + m) &= i(m \cdot k) + i(m) \\ &= i(m) \cdot i(k) + i(m) = i(m)(i(k) + 1_X) \\ &= i(m)(i(k) + i(1)) \ = i(m)i(k+1). \end{aligned}$$

Portanto i preserva a multiplicação.

(iii) Para mostrar que i preserva a relação de ordem, iniciemos mostrando que $i(m) > 0$, para todo $m \in \mathbb{N}$. Temos que $i(1) = 1_X > 0_X$. Suponhamos que vale $i(k) > 0_X$ para algum $k \in \mathbb{N}$. Temos que $i(k+1) = i(k) + i(1)$, e como $i(k)$ e $i(1)$ são ambos positivos, e num corpo ordenado a adição é compatível com a relação de ordem, temos que $i(k+1) > 0_X$.

Suponha que $m < n$, temos que $n = m + k$ com algum k natural. Assim $i(n) = i(m+k) = i(m) + i(k)$. Como num corpo ordenado a adição e a multiplicação são compatíveis com a relação de ordem, e temos que $i(m), i(k) > 0$, então $i(m) + i(k) > i(m)$. Logo, $i(m) < i(n)$.

■

Vamos utilizar a seguinte notação, $1 \mapsto 1_X, 2 \mapsto 2_X$, e assim sucessivamente, para indicar a imagem da imersão de $\mathbb{N}$ no conjunto X. A notação é análoga para outro corpo ordenado completo qualquer, Y. Além disso, quando conveniente, usaremos a notação $\mathbb{N}_X$ para indicar o conjunto dos números naturais em X. O que nos permite fazer isso é o Teorema 7.13, que garante que todo corpo ordenado completo tem um subconjunto imergido de $\mathbb{N}$.

Teorema 7.14. *Se X, Y são corpos ordenados completos, então existe um isomorfismo entre eles que preserva a relação de ordem. É o mesmo que dizer que existe uma função bijetora $f\colon X \to Y$ tal que, para $x_1, x_2 \in X$ sejam válidas*

$$\begin{aligned} f(x_1 + x_2) &= f(x_1) + f(x_2), \\ f(x_1 \cdot x_2) &= f(x_1) \cdot f(x_2), \\ x_1 \leq x_2 \implies f(x_1) &\leq f(x_2). \end{aligned}$$

Observação 7.7. Também é usado para descrever o isomorfismo do Teorema 7.14, que esse isomorfismo preserva a adição, a multiplicação e a relação de ordem.

Demonstração: Separaremos essa demonstração em quatro casos, a fim de mostrar que $\mathbb{N}_X$ é isomorfo à $\mathbb{N}_Y$, que $\mathbb{Z}_X$ é isomorfo à $\mathbb{Z}_Y$, $\mathbb{Q}_X$ é isomorfo à $\mathbb{Q}_Y$ e por último, que X é isomorfo à Y.

1. Para verificar as propriedades em $\mathbb{N}$, considere a função

$$\begin{aligned} f_1 &\colon \mathbb{N}_X \to \mathbb{N}_Y, \\ f_1(a_X) &= a_Y. \end{aligned}$$

   a) A função f_1 é bijetora.
   Basta observar que existe uma imersão i de $\mathbb{N}$ em X que é uma bijeção se restringirmos o contradomínio para $\mathbb{N}_X$. Analogamente, existe uma imersão j de $\mathbb{N}$ em Y, que é uma bijeção de $\mathbb{N}$ em $\mathbb{N}_Y$. Assim, temos bijeções $i\colon \mathbb{N} \to \mathbb{N}_X$ e $j\colon \mathbb{N} \to \mathbb{N}_Y$. Fazendo a composta $j \circ i^{-1}\colon \mathbb{N}_X \to \mathbb{N}_Y$, obtemos uma função bijetora como queríamos.

   b) Vamos provar agora f_1 preserva a adição. Usaremos indução. Temos que

$$\begin{aligned} f_1(a_X + 1_X) &= f_1((a+1)_X) \\ &= (a+1)_Y \\ &= a_Y + 1_Y. \end{aligned}$$

   Nossa hipótese de indução é que vale $f_1(a_X + k_X) = f_1(a_X) + f_1(k_X)$ para $k \in \mathbb{N}$. Vejamos o que ocorre para $k+1$:

$$\begin{aligned} f_1(a_X + (k+1)_X) &= f_1(a_X + k_X + 1_X) \\ &= f_1(a_X + k_X) + f(1_X) \\ &= f_1(a_X) + f_1(k_X) + 1_Y \\ &= f_1(a_X) + f_1(k_X + 1_X) \\ &= f_1(a_X) + f_1((k+1)_X). \end{aligned}$$

   Dessa maneira a adição é preservada por f_1.

   c) Para mostrar que a multiplicação é preservada, também usaremos indução. Temos que

$$f_1(a_X \cdot 1_X) = f_1(a_X) = f_1(a_X) \cdot 1_Y = f_1(a_X) \cdot f_1(1_X).$$

Nossa hipótese de indução é que vale $f_1(a_X \cdot k_X) = f_1(a_X) \cdot f_1(k_X)$ para $k \in \mathbb{N}$. Assim

$$\begin{aligned} f_1(a_X \cdot (k+1)_X) &= f_1(a_X \cdot (k_X + 1_X)) \\ &= f_1(a_X \cdot k_X + a_X \cdot 1_X) \\ &= f_1(a_X \cdot k_X + a_X) \\ &= f_1(a_X \cdot k_X) + f_1(a_X) \\ &= f_1(a_X \cdot k_X) + f_1(a_X) \cdot 1_Y \\ &= f_1(a_X) \cdot f_1(k_X) + f(a_X) \cdot 1_Y \\ &= f_1(a_X)(f_1(k_X) + 1_Y) \\ &= f_1(a_X)(f_1(k_X) + f_1(1_X)) \\ &= f_1(a_X)\Big(f_1((k+1)_X\Big). \end{aligned}$$

Assim, f_1 preserva a multiplicação.

d) Para mostrar que a relação de ordem é preservada, observemos que $f_1(c_X) > 0_Y$, para todo $c_X \in \mathbb{N}_X$. Isso vem da imersão i, dada no Teorema 7.13 ser estritamente crescente (pela preservação da relação de ordem) e de $f_1 \colon \mathbb{N}_X \to \mathbb{N}_Y$ ser uma bijeção. Assim, supondo $a_X < b_X$ temos $b_X = a_X + c_X$ para algum $c_X \in \mathbb{N}_X$, com $c_X \neq 0_X$. E então

$$\begin{aligned} f_1(b_X) &= f_1(a_X + c_X) \\ &= f_1(a_X) + f_1(c_X). \end{aligned}$$

Como $f_1(c_X) > 0_Y$, e num corpo ordenado completo a adição é compatível com a relação de ordem, segue que $f_1(a_X) < f_1(b_X)$. Portanto a desigualdade é mantida como queríamos mostrar.

2. Para $\mathbb{Z}$, queremos estender a função f_1 para uma função f_2, definida em um conjunto que, a partir dos inteiros positivos, tenha os inteiros negativos e o zero.

a) Definamos o conjunto

$$\mathbb{Z}_X = \{\, m_X - n_X : m_X, n_X \in \mathbb{N}_X \,\}.$$

Esse conjunto tem o zero, basta tomar $m_X = n_X$, e também qualquer inteiro negativo, quando $n_X > m_X$. Temos também a situação de que a representação de um elemento de $\mathbb{Z}_X$ não é única. Observemos que a subtração indicada é a do corpo X. Analogamente, define-se $\mathbb{Z}_Y$.

Sendo $m_X, n_X \in \mathbb{N}_X$ e $m_Y = f_1(m_X), n_Y = f_1(n_X) \in \mathbb{N}_Y$ podemos agora definir f_2 do seguinte modo:

$$\begin{aligned} f_2 &\colon \mathbb{Z}_X \to \mathbb{Z}_Y \\ m_X - n_X &\mapsto m_Y - n_Y. \end{aligned}$$

Note que $f_2(m_X - n_X) = f_1(m_X) - f_1(n_X)$. Devemos mostrar que a função f_2 está bem definida, isto é, dados $m_X - n_X = m'_X - n'_X$ com $m_X, n_X, m'_X, n'_X \in \mathbb{N}_X$ teremos um mesmo $m_Y - n_Y = m'_Y - n'_Y$ em Y. De fato, temos que

$$m_X - n_X = m'_X - n'_X \iff m_X + n'_X = n_X + m'_X$$

e assim

$$\begin{aligned} f_1(m_X + n'_X) &= f_1(n_X + m'_X), \\ f_1(m_X) + f_1(n'_X) &= f_1(n_X) + f_1(m'_X), \\ f_1(m_X) - f_1(n_X) &= f_1(m'_X) - f_1(n'_X), \\ f_2(m_X - n_X) &= f_2(m'_X - n'_X). \end{aligned}$$

E portanto a função f_2 está bem definida.

Devemos mostrar que a função f_2 é bijetora. Sejam $m_X, m'_X, n_X, n'_X \in \mathbb{N}_X$, temos

$$\begin{aligned} f_2(m_X - n_X) = f_2(m'_X - n'_X) &\implies f_1(m_X) - f_1(n_X) = f_1(m'_X) - f_1(n'_X) \\ &\implies f_1(m_X) + f_1(n'_X) = f_1(n_X) + f_1(m'_X) \\ &\implies f_1(m_X + n'_X) = f_1(n_X + m'_X) \\ &\implies m_X + n'_X = n_X + m'_X \ \text{ pois } f_1 \text{ é bijetora} \\ &\implies m_X - n_X = m'_X - n'_X. \end{aligned}$$

E portanto a função f_2 é injetora.

Para ver que f_2 é sobrejetora, seja $a_Y = m_Y - n_Y \in \mathbb{Z}_Y$ um elemento qualquer de $\mathbb{Z}_Y$. Basta considerar o elemento $m_X - n_X \in \mathbb{Z}_X$, pois

$$f_2(m_X - n_X) = f_1(m_X) - f_1(n_X) = m_Y - n_Y = a_Y.$$

Dessa forma f_2 também é sobrejetora e portanto é bijetora.

b) f_2 é aditiva. Dados $a_X = m_X - n_X$ e $b_X = p_X - q_X$ com $a_X, b_X \in \mathbb{Z}_X$, temos:

$$\begin{aligned} f_2(a_X + b_X) &= f_2(m_X - n_X + p_X - q_X) \\ &= f_2((m_X + p_X) - (n_X + q_X)) \\ &= f_1(m_X + p_X) - f_1(n_X + q_X) \\ &= f_1(m_X) + f_1(p_X) - (f_1(n_X) + f_1(q_X)) \\ &= f_1(m_X) - f_1(n_X) + f_1(p_X) - f_1(q_X) \\ &= f_2(m_X - n_X) + f_2(p_X - q_X) \\ &= f_2(a_X) + f_2(b_X). \end{aligned}$$

Assim provamos que f_2 é aditiva.

c) f_2 é multiplicativa. Dados $a_X = m_X - n_X$ e $b_X = p_X - q_X$ com $a_X, b_X \in \mathbb{Z}_X$, temos:

$$\begin{aligned}
f_2(a_X \cdot b_X) &= f_2((m_X - n_X) \cdot (p_X - q_X)) \\
&= f_2(m_X p_X - m_X q_X - n_X p_X + n_X q_X) \\
&= f_2((m_X p_X + n_X q_X) - (m_X q_X + n_X p_X)) \\
&= f_1(m_X p_X + n_X q_X) - f_1(m_X q_X + n_X p_X) \\
&= f_1(m_X) f_1(p_X) + f_1(n_X) f_1(q_X) - (f_1(m_X) f_1(q_X) + f_1(n_X) f_1(p_X)) \\
&= f_1(m_X)[f_1(p_X) - f_1(q_X)] - f_1(n_X)[f_1(p_X) - f_1(q_X)] \\
&= f_1(m_X) f_2(p_X - q_X) - f_1(n_X) f_2(p_X - q_X) \\
&= [f_1(m_X) - f_1(n_X)][f_2(p_X - q_X)] \\
&= f_2(m_X - n_X) \cdot f_2(p_X - q_X) \\
&= f_2(a_X) \cdot f_2(b_X).
\end{aligned}$$

Dessa forma concluímos que f_2 é multiplicativa.

d) f_2 preserva a relação de ordem. Dados $a_X = m_X - n_X$ e $b_X = p_X - q_X$ com $a_X, b_X \in \mathbb{Z}_X$, temos:

$$\begin{aligned}
a_X < b_X &\implies m_X - n_X < p_X - q_X \\
&\implies m_X + q_X < n_X + p_X \\
&\implies f_1(m_X + q_X) < f_1(n_X + p_X) \\
&\implies f_1(m_X) + f_1(q_X) < f_1(n_X) + f_1(p_X) \\
&\implies f_1(m_X) - f_1(n_X) < f_1(p_X) - f_1(q_X) \\
&\implies f_2(m_X - n_X) < f_2(p_X - q_X) \\
&\implies f_2(a_X) < f_2(b_X).
\end{aligned}$$

Dessa forma a função f_2 também preserva a relação de ordem, o que conclui a bijeção aditiva, multiplicativa e que preserva a ordem, de $\mathbb{Z}_X$ em $\mathbb{Z}_Y$.

3. Para $\mathbb{Q}$, vamos estender os inteiros para todas as frações $\frac{a_X}{b_X}$ em $a_X, b_X \in \mathbb{Z}_X$ e $b_X \neq 0$. Analogamente, definimos $\mathbb{Q}_Y$. Façamos uma observação no que diz respeito à notação que podemos utilizar para trabalhar com frações, por exemplo, $\frac{a}{b} + \frac{c}{d}$ onde a, b, c, d são elementos de algum corpo, com denominadores não nulos, temos

$$\frac{ad + bc}{bd} = \frac{a}{b} + \frac{c}{d} = ab^{-1} + cd^{-1} = ab^{-1}dd^{-1} + cd^{-1}bb^{-1} = b^{-1}d^{-1}(ad + bc).$$

a) Sendo $a_X, b_X \in \mathbb{Z}_X$ e $a_Y, b_Y \in \mathbb{Z}_Y$ podemos agora definir f_3 do seguinte modo:

$$\begin{aligned}
f_3 \colon \mathbb{Q}_X &\to \mathbb{Q}_Y, \\
\frac{a_X}{b_X} &\mapsto \frac{f_2(a_X)}{f_2(b_X)}.
\end{aligned}$$

Sendo assim,

$$f_3\left(\frac{a_X}{b_X}\right) = \frac{f_2(a_X)}{f_2(b_X)}.$$

Note que, como $b_X \neq 0_X$, e como f_2 é aditiva, e injetora, temos que $f_2(b_X) \neq f_2(0_X) = 0_Y$. A função f_3 está bem definida, pois

$$\frac{a_X}{b_X} = \frac{c_X}{d_X} \iff a_X d_X = b_X c_X,$$

e assim

$$\begin{aligned} f_2(a_X d_X) = f_2(b_X c_X) &\iff f_2(a_X)f_2(d_X) = f_2(b_X)f_2(c_X) \\ &\iff \frac{f_2(a_X)}{f_2(b_X)} = \frac{f_2(c_X)}{f_2(d_X)} \\ &\implies f_3\left(\frac{a_X}{b_X}\right) = f_3\left(\frac{c_X}{d_X}\right). \end{aligned}$$

b) Para mostrar que f_3 é injetora, sejam $a_X, c_X \in \mathbb{Z}_X$, $b_X, d_X \in \mathbb{Z}_X^*$ e $p_X, q_X \in \mathbb{Q}_X$ tais que $p_X = \frac{a_X}{b_X}$ e $q_X = \frac{c_X}{d_X}$. Temos que

$$\begin{aligned} f_3(p_X) = f_3(q_X) &\iff \frac{f_2(a_X)}{f_2(b_X)} = \frac{f_2(c_X)}{f_2(d_X)} \\ &\iff f_2(a_X)f_2(d_X) = f_2(b_X)f_2(c_X) \\ &\iff f_2(a_X d_X) = f_2(b_X c_X) \\ &\iff a_X d_X = b_X c_X \\ &\iff \frac{a_X}{b_X} = \frac{c_X}{d_X}. \end{aligned}$$

Para mostrar que f_3 é sobrejetora, considere um elemento $p_Y \in \mathbb{Q}_Y$. Assim, $p_Y = \frac{a_Y}{b_Y}$, para $a_Y, b_Y \in \mathbb{Z}_Y$ com $b_Y \neq 0_Y$. Como f_2 é sobrejetora, existe $a_X, b_X \in \mathbb{Z}_X$ tais que $f_2(a_X) = a_Y$ e $f_2(b_X) = b_Y$. Como f_2 é bijetora e preserva o 0_X (Lema 7.1), como $b_Y \neq 0_Y$, temos $b_X \neq 0_X$. Dessa maneira,

$$f_3\left(\frac{a_X}{b_X}\right) = \frac{f_2(a_X)}{f_2(b_X)} = \frac{a_Y}{b_Y} = p_Y,$$

e f_3 é sobrejetora, logo, também é bijetora.

c) Vamos mostrar que f_3 é aditiva. Temos que

$$\begin{aligned} f_3\left(\frac{a_X}{b_X} + \frac{c_X}{d_X}\right) &= f_3\left(\frac{a_X d_X + b_X c_X}{b_X d_X}\right) \\ &= \frac{f_2(a_X d_X + b_X c_X)}{f_2(b_X d_X)} \\ &= \frac{f_2(a_X d_X) + f_2(b_X c_X)}{f_2(b_X)f_2(d_X)} \\ &= \frac{f_2(a_X)f_2(d_X)}{f_2(b_X)f_2(d_X)} + \frac{f_2(b_X)f_2(c_X)}{f_2(b_X)f_2(d_X)} \\ &= \frac{f_2(a_X)}{f_2(b_X)} + \frac{f_2(c_X)}{f_2(d_X)}. \end{aligned}$$

d) Vamos provar que f_3 preserva a multiplicação. De fato, temos que

$$\begin{aligned} f_3\left(\frac{a_X}{b_X}\cdot\frac{c_X}{d_X}\right) = f_3\left(\frac{a_Xc_X}{b_Xd_X}\right) &= \frac{f_2(a_Xc_X)}{f_2(b_Xd_X)} \\ = \frac{f_2(a_X)f_2(c_X)}{f_2(b_X)f_2(d_X)} &= \frac{f_2(a_X)}{f_2(b_X)}\cdot\frac{f_2(c_X)}{f_2(d_X)} \\ = f_3\left(\frac{a_X}{b_X}\right)\cdot f_3\left(\frac{c_X}{d_X}\right). & \end{aligned}$$

e) Vamos provar que f_3 também preserva a ordem. Observemos que $\frac{a_X}{b_X} = a_Xb_X^{-1}$ é positivo se, e somente se, ambos são positivos ou ambos são negativos, e é nulo caso $a_X = 0_X$. Sem perda de generalidade, suponhamos $b_X > 0_X$, o que podemos fazer conforme o Corolário 5.1.

Tomemos $a_X, c_X \in \mathbb{Z}_X$ e $b_X, d_X \in \mathbb{Z}_X^*$, e considere $p_X = \frac{a_X}{b_X}$ e $q_X = \frac{c_X}{d_X}$. Temos que

$$\begin{aligned} p_X < q_X &\implies a_Xd_X < b_Xc_X \\ &\implies f_2(a_Xd_X) < f_2(b_Xc_X) \\ &\implies f_2(a_X)f_2(d_X) < f_2(b_X)f_2(c_X) \\ &\implies \frac{f_2(a_X)}{f_2(b_X)} < \frac{f_2(c_X)}{f_2(d_X)} \\ &\implies f_3\left(\frac{a_X}{b_X}\right) < f_3\left(\frac{c_X}{d_X}\right) \\ &\implies f_3(p_X) < f_3(q_X). \end{aligned}$$

4. Vamos provar, usando os isomorfismos nos subconjuntos de X e de Y, que os corpos ordenados completos X e Y são isomorfos. Vamos continuar usando a notação com índices, e neste caso vamos incluir também $\mathbb{R}_X$. Deixamos claro, entretanto, que $X = \mathbb{R}_X$. Assim, quando dissermos que $x \in \mathbb{R}_X$, estamos dizendo que x é um elemento qualquer de X, sem necessariamente estar num dos conjuntos trabalhados anteriormente, como $\mathbb{N}_X, \mathbb{Z}_X$ e $\mathbb{Q}_X$.

a) Para qualquer $r \in \mathbb{R}_X$ vamos denotar o conjunto $D(r) = \{\, q \in \mathbb{Q}_X : q < r \,\}$. A ideia é a de corte, como já fizemos no capítulo dos números reais. Vamos definir $f\colon \mathbb{R}_X \to \mathbb{R}_Y$ por $f(r) = sup_{q<r}(f_3(q))$, em que $q \in \mathbb{Q}_X$ e $r \in \mathbb{R}_X$. O índice, depois da notação do supremo, deve ser compreendida como todos os racionais q, que são menores do que r. Podemos também usar a notação $f(r) = sup(f_3(D(r)))$.

Num primeiro cenário, vamos mostrar que caso r seja um racional, teremos $f(r) = f_3(r)$. Para qualquer $q \in \mathbb{Q}_X$ com $q < r$, temos $f_3(q) < f_3(r)$, pois f_3 preserva a ordem. Assim, $f_3(r)$ é cota superior do conjunto $f_3(D(r))$.

Para mostrar que $f_3(r)$ é o supremo de $f_3(D(r))$, suponhamos por contradição que $f_3(r)$ não seja a cota superior mínima de $f_3(D(r))$. Temos, pela definição de $f(r)$, que $f(r) < f_3(r)$ e também que $f(r) < f_3(t) < f_3(r)$ para algum $t \in \mathbb{Q}_X$. Como f_3 preserva a ordem (de $\mathbb{R}_Y$ para $\mathbb{R}_X$ também) temos $t < r$, o que leva a $t \in D(r)$ e $f_3(t) \leq f(r)$ (pois $f(r)$ é supremo de $f_3(D(r))$), o que é uma contradição, portanto $f_3(r) = f(r)$.

b) Devemos provar agora que f é injetora (e concluiremos que também preserva a relação de ordem). Sejam $r, s \in \mathbb{R}_X$ com $r < s$. Existem $p, q \in \mathbb{Q}_X$ tal que $r < p < q < s$.

Temos que $f_3(p)$ é uma cota superior de $f_3(D(r))$ e daí $f(r) \leq f_3(p) = f(p)$. Como $f = f_3$ para números racionais, obtemos $f(p) < f(q)$, e como $q \in D(s)$ temos $f(q) = f_3(q) \leq f(s)$, desse modo $f(r) < f(s)$. Isso mostra que além de injetora, f preserva a relação de ordem.

c) Devemos mostrar agora que f é sobrejetora. Seja $y \in \mathbb{R}_Y$ um elemento qualquer. Denotaremos como $D^*(y) = \{\, q \in \mathbb{Q}_Y : q < y \,\}$. Temos então por definição que y é uma cota superior de $D^*(y)$. Além disso, y é supremo de $D^*(y)$, pois se pudesse ocorrer de $z < y$ ser uma cota superior, existiria $r \in \mathbb{Q}_Y$ com $z < r < y$, e daí $r \in D^*(y)$, logo z não é cota superior de $D^*(y)$, uma contradição.

Como o conjunto $\mathbb{N}_X$ é ilimitado no corpo dos números reais, dado qualquer y de $\mathbb{R}_Y$, existe n_Y natural com $y < n_Y$. Definamos $n_X = f_3^{-1}(n_Y)$. Tínhamos $n_Y > q_Y$ para qualquer $q_Y \in D^*(y)$, daí para qualquer $q_X \in f_3^{-1}(D^*(y))$ teremos $q_X < n_X$, e portanto n_X é uma cota superior de $f_3^{-1}(D^*(y))$, que então admite algum supremo em $\mathbb{R}_X$. Vamos denotar esse supremo por $x = sup(f_3^{-1}(D^*(y)))$.

Afirmamos que $f(x) = y$, e a ideia como vamos mostrar isso é provar que $y \leq f(x)$, mas que $y < f(x)$ não pode ocorrer. Seja então $q_Y < y$, podemos escolher em $\mathbb{R}_Y$ um p_Y qualquer, com $q_Y < p_Y < y$, e se definirmos $q_X = f_3^{-1}(q_Y)$ e $p_X = f_3^{-1}(p_Y)$ teremos $q_X < p_X < x$, o que implica $q_Y < p_Y < f(x)$ e portanto $f(x)$ é uma cota superior de $D^*(y)$. Observando que o supremo é a menor cota superior, e que $y = sup(D^*(y))$, temos que $y \leq f(x)$, pois $f(x)$ é uma cota superior qualquer.

Para mostrar que $y < f(x)$ não ocorre, por contradição vamos supor que possa ocorrer. Isso acarreta que existe $q_Y \in \mathbb{Q}_Y$ tal que $y < q_Y < f(x)$. Como f preserva a ordem temos $q_X < x$, pois se não fosse assim teríamos $q_Y = f(x)$ ou $q_Y > f(x)$. Como x é o supremo de $f_3^{-1}(D^*(y))$, temos que existe $p_X \in \mathbb{Q}_X$ com $q_X < p_X < x$ e também que $f_3(p_X) = p_Y \in D^*(y)$, desse modo $p_Y < y$. Para concluir, tínhamos suposto que $y < q_Y$ e agora obtivemos que $p_Y < y$, logo $p_Y < y < q_Y$, o que contradiz com $q_Y < p_Y$. Assim provamos que $y = f(x)$.

d) Vamos mostrar que f é aditiva.

Vamos primeiro considerar o caso particular em que uma das parcelas é racional. Sejam $u \in \mathbb{R}_X$ arbitrário, e $r \in \mathbb{Q}_X$. Temos que

$$\begin{aligned} f(u+r) &= sup_{q<u+r} f_3(q) \\ &= sup_{p<q} f_3(p) + f(r) \\ &= f(u) + f(r). \end{aligned}$$

Desse modo, provamos que a aditividade para f vale caso uma das parcelas seja racional. Para mostrar o caso geral que $f(u+v) = f(u) + f(v)$, considere um racional $q \in \mathbb{Q}_X$, em que $q < v$. Pela compatibilidade de f com a relação de ordem, temos

$$f(u) + f(q) = f(u+q) < f(u+v).$$

Somando $-f(u)$ em ambos os lados, segue que

$$f_3(q) = f(q) < f(u+v) - f(u)$$

e portanto

$$f(v) = sup_{q<v} f_3(q) \leq f(u+v) - f(u).$$

Vamos mostrar que a desigualdade não ocorre, e o faremos por absurdo. Suponha então que

$$f(v) = sup_{q<v} f_3(q) < f(u+v) - f(u)$$

Então existe um racional r_Y tal que

$$f(v) < r_Y < f(u+v) - f(u).$$

Como f é sobrejetora, temos que $r_Y = f(p)$ para algum $p \in \mathbb{Q}_X$.
Como f preserva a ordem, $v < p$, e da aditividade parcial que acabamos de provar, segue que

$$f(p) = r_Y < f(u+v) - f(u) < f(u+p) - f(u) = f(u) + f(p) - f(u) = f(p),$$

o que é um absurdo. Logo, a desigualdade não ocorre, e assim

$$f(u+v) = f(u) + f(v),$$

quaisquer que sejam $u, v \in \mathbb{R}_X$.

e) Vamos mostrar que f preserva a multiplicação. Queremos mostrar que em qualquer caso vale que $f(u \cdot v) = f(u) \cdot f(v)$. Vamos iniciar mostrando que se um dos fatores for $0_X, +1_X, -1_X$, então a multiplicação é preservada. De fato, dado $u \in \mathbb{R}_X$, temos que $f(u \cdot 0_X) = f(0_X) = 0_Y = f(u) \cdot 0_Y$.
Para $f(u \cdot 1_X) = f(u) = f(u) \cdot 1_Y = f(u) \cdot f(1_X)$ e a multiplicação também é

preservada. Para o -1_X, primeiro provemos que $f(-u) = -f(u)$. Temos que $f(0_X) = f(u + (-u)) = f(u) + f(-u)$, logo, $f(u) + f(-u) = 0_Y$, assim temos $f(-u) = -f(u)$.

Para mostrar o caso $f((-1_X) \cdot u)$, temos que

$$f((-1_X) \cdot u) = f(-u) = -f(u) = (-1_Y) \cdot f(u) = f(-1_X) \cdot f(u).$$

Vamos mostrar agora que, dados $u, v \in \mathbb{R}_X$, com $u, v > 0_X$, a multiplicação é preservada. Como f preserva a ordem, $f(u) > 0_Y$ e $f(v) > 0_Y$. Faremos uma prova parcial com v racional, como no caso da adição. Temos que

$$f(u \cdot v) = sup_{q<u+v} f_3(q) = (sup_{p<u} f_3(p)) \cdot f(v) = f(u) \cdot f(v).$$

Desse modo, f preserva a multiplicação se ao menos um dos fatores for racional, e ambos forem positivos.

Vamos agora, estender para v positivo qualquer, não apenas para racionais. Seja $q \in \mathbb{Q}_X$, com $0 < q < v$. Como num corpo ordenado completo a multiplicação preserva a relação de ordem, temos que $u \cdot q < u \cdot v$, e portanto

$$f(u) \cdot f(q) = f(u \cdot q) < f(u \cdot v).$$

Assim, multiplicando por $\frac{1}{f(u)} > 0_Y$ obtemos

$$f(q) < \frac{f(u \cdot v)}{f(u)}.$$

Para $f(v)$ temos que

$$f(v) = sup_{q<v} f_3(q) \leq \frac{f(u \cdot v)}{f(u)}.$$

Vamos mostrar que a desigualdade não ocorre, supondo, por absurdo, que ela ocorra. Temos então $r_Y \in \mathbb{Q}_Y$, tal que $f(v) < r_Y < \frac{f(u \cdot v)}{f(u)}$. Como f é sobrejetora, temos que $r_Y = f(p)$ para algum $p \in \mathbb{Q}_X$. Em vista de f preservar a ordem, e de que $f(v) < r_Y = f(p)$, temos que $v < p$. Temos então que

$$f(p) = r_Y < \frac{f(u \cdot v)}{f(u)} < \frac{f(u \cdot p)}{f(u)} = \frac{f(u) \cdot f(p)}{f(u)} = f(p),$$

o que é uma contradição.

Para mostrar que f é multiplicativa no caso geral, onde pode haver negativos, considere a função sinal σ, definida como $\sigma(u) = 1$, se $u > 0$, e $\sigma(u) = -1$, se $u < 0$. Como f preserva a ordem, se $u \in \mathbb{R}_X$ for positivo, $f(u) \in \mathbb{R}_Y$ também será, e a função $\sigma(u) = 1 = \sigma(f(u))$. Essa notação tem a vantagem de propiciar que qualquer número $u \in \mathbb{R}_X$ seja representado como $u = \sigma(u) \cdot |u|$, em que o

módulo em $\mathbb{R}_X$ ou em $\mathbb{R}_Y$ é análogo ao definido na Definição 6.8. Temos então que

$$\begin{aligned} f(u \cdot v) &= f((\sigma(u) \cdot |u|) \cdot ((\sigma(v) \cdot |v|))) \\ &= f(\sigma(u) \cdot \sigma(v) \cdot |u| \cdot |v|) \\ &= \sigma(u) \cdot \sigma(b) \cdot f(|u| \cdot |v|) \\ &= \sigma(u) \cdot \sigma(b) \cdot f(|u|) \cdot f(|v|) \\ &= f(\sigma(u) \cdot |u|) \cdot f(\sigma(v) \cdot |v|) \\ &= f(u) \cdot f(v). \end{aligned}$$

Assim, f preserva a multiplicação em todos os casos.

Dessa forma, provamos que dados dois corpos ordenados completos $X = \mathbb{R}_X$ e $Y = \mathbb{R}_Y$, existe uma função bijetora $f\colon X \to Y$, tal que f preserva a adição, a multiplicação, e a relação de ordem desse conjunto. Dessa maneira, concluímos que X e Y são isomorfos, e assim, existe apenas um corpo ordenado completo, que chamamos *o corpo dos números reais*.

■

CONSIDERAÇÕES FINAIS

Ao longo deste trabalho muitos pontos importantes foram colocados em questão. Um deles era verificar se poderíamos desenvolver este trabalho sem considerar o 0 como um número natural. Isso foi possível e não impediu o desenvolvimento dos assuntos abordados, embora tenha sido necessário fazer pequenos ajustes, mas nada substancial.

Conseguimos estender o conceito de número a partir dos números naturais até os números reais. Mostramos também que a interpretação, a nível de ensino básico, da inclusão dos conjuntos $\mathbb{N} \subset \mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R}$ é correta, por causa das imersões, e é conveniente, porque simplifica a notação para os números.

Foram provadas muitas proposições, algumas com caráter essencial para o desenvolvimento do trabalho, tais como a completude e a não enumerabilidade de $\mathbb{R}$, e outras com caráter mais ilustrativo, tais como a enumerabilidade de $\mathbb{Z}$ e de $\mathbb{Q}$ e que a equação $r^2 = 2$ não admite solução em $\mathbb{Q}$. Como principais resultados, destacamos a demonstração de que o conjunto $\mathbb{Q}$ é um corpo ordenado, e que o conjunto $\mathbb{R}$ é o único corpo ordenado completo existente, a menos de isomorfismos.

A compreensão dos temas estudados neste trabalho nos permite almejar novas pesquisas, como a extensão para além do conjunto dos números reais, tais como números complexos ou octónios. Números complexos podem ser compreendidos como pares de números reais, mas que não possuem uma relação de ordem total. Octónios por sua vez, podem ser considerados octetos de números reais cuja álgebra, baseada na álgebra dos quaternários, é não comutativa e não associativa. Como temas de interesse para estudos futuros, destacamos a fundamentação para os axiomas de Peano, através da teoria de conjuntos e da lógica clássica e a investigação à respeito da possibilidade de obtenção dos axiomas de Peano por meio de uma lógica não clássica.

REFERÊNCIAS

ALFELD, Peter. **Why is the square root of 2 irrational?** 1996. Disponível em: <https://www.math.utah.edu/~pa/math/q1.html>. Acesso em: 5 jun. 2023.

BARBOSA, João Lucas Marques. **Geometria euclidiana plana**. 11. ed. Rio de Janeiro: SBM, 2012.

BARTLE, Robert Gardner; SHERBERT, Donald R. **Introduction to real analysis**. 3. ed. [S.l.]: John Wiley e Sons, 1927.

BOYER, Carl B. **História da matemática**. 2. ed. São Paulo: Edgard Blucher, 1996.

DOMINGUES, Hygino Hugueros. **Fundamentos de Aritmética**. Florianópolis: Ed. da UFSC, 2009.

DOMINGUES, Hygino Hugueros; IEZZI, Gelson. **Álgebra Moderna**. 5. ed. São Paulo: Saraiva, 2018.

FERREIRA, Jamil. **A construção dos números**. Rio de Janeiro: SBM, 2013.

GUIDORIZZI, Hamilton Luiz. **Um curso de cálculo**. 6. ed. Rio de Janeiro: LTC, 2018. v. 1.

HEFEZ, Abramo. **Aritmética**. Rio de Janeiro: SBM, 2014.

_____. **Curso de álgebra**. 5. ed. Rio de Janeiro: IMPA, 2014.

LIMA, Elon Lages. **Conceitos e controvérsias**. Disponível em: <https://www.rpm.org.br/cdrpm/1/2.htm>. Acesso em: 3 fev. 2023.

_____. **Curso de análise**. 14. ed. Rio de Janeiro: IMPA, 2016. v. 1.

MORTARI, Cezar A. **Introdução à lógica**. 2. ed. São Paulo: Unesp, 2016.

PEANO, Ioseph. **Arithmetices principia**: nova methodo exposita. Turim: Fratres Bocca, 1889. Disponível em: <https://ia903400.us.archive.org/12/items/arithmeticespri00peangoog/arithmeticespri00peangoog.pdf>. Acesso em: 5 jun. 2023.

ROQUE, Tatiana. **História da matemática**: uma visão crítica, desfazendo mitos e lendas. Rio de Janeiro: Zahar, 2012.

SANTOS, José Plínio de Oliveira. **Introdução à teoria dos números**. 3. ed. Rio de Janeiro: IMPA, 2015.

SUPPES, Patrick. **Axiomatic set theory**. 2. ed. Nova Iorque: Dover, 1972.

UNIQUENESS of the Real Numbers. Disponível em: <https://math.ucr.edu/~res/math205A/uniqreals.pdf>. Acesso em: 29 mai. 2023.