Guylherme de Barros Mattos

A Construção dos Números

Volta Redonda, RJ

2020

Guylherme de Barros Mattos

A Construção dos Números

Trabalho de Conclusão de Curso submetido ao Curso de Matemática da Universidade Federal Fluminense como requisito parcial para a obtenção do título de Bacharel em Matemática.

Universidade Federal Fluminense

Instituto de Ciências Exatas

Curso de Matemática

Orientador: Carlos Henrique Pereira do Nascimento

Coorientador: Marina Ribeiro Barros Dias

Volta Redonda, RJ

2020

Ficha catalográfica automática - SDC/BAVR
Gerada com informações fornecidas pelo autor

M435c Mattos, Guylherme de Barros
A Construção dos Números / Guylherme de Barros Mattos ; Carlos Henrique Pereira do Nascimento, orientador ; Marina Ribeiro Barros Dias, coorientadora. Volta Redonda, 2021.
78 f.

Trabalho de Conclusão de Curso (Graduação em Matemática)- Universidade Federal Fluminense, Instituto de Ciências Exatas, Volta Redonda, 2021.

1. Conjuntos Numéricos. 2. Axiomas de Peano. 3. Cortes de Dedekind. 4. Sequências de Cauchy. 5. Produção intelectual. I. Nascimento, Carlos Henrique Pereira do, orientador. II. Dias, Marina Ribeiro Barros, coorientadora. III. Universidade Federal Fluminense. Instituto de Ciências Exatas. IV. Título.

CDD -

Bibliotecário responsável: Debora do Nascimento - CRB7/6368

Guylherme de Barros Mattos

A Construção dos Números

Trabalho de Conclusão de Curso submetido ao Curso de Matemática da Universidade Federal Fluminense como requisito parcial para a obtenção do título de Bacharel em Matemática.

Trabalho aprovado. Volta Redonda, RJ, 03 de maio de 2020:

Prof. Dr. Carlos Henrique Pereira do Nascimento – UFF
Orientador

Profa. Dra. Marina Ribeiro Barros Dias – UFF
Coorientadora

Prof. Dr. Leandro Gines Egea – UFF

Prof. Dr. Miguel Adriano Koiller Schnoor – UFF

Volta Redonda, RJ
2020

Dedico este trabalho à minha querida avó Ligia Gouvea de Barros (in memoriam), cuja presença foi essencial na minha vida.

Agradecimentos

Gostaria de agradecer em primeiro lugar a Deus e a Nossa Senhora, pois graças a eles pude chegar até aqui. Agradeço a toda minha família, de modo muito especial ao meu pai Jamberly e minha mãe Cibele por todo apoio e ajuda que eles me deram. Sem eles eu não teria conseguido até agora. Agradeço aos meus amigos de faculdade e, em especial, agradeço ao Guilherme Saroka, João Pedro, Joel Marques, João Marcos, Lucas Aparecido, Mariana Macedo, Nelson Assis, Orlando Warlem, Patrick Alves, Rayan Gustavo e Tais Letícia, por tanta ajuda e momentos de risos. Agradeço passar por todo esses períodos com vocês. Com certeza esse tempo foi melhor graças a vocês. Obrigado aos professores com quais eu tive aula, obrigado por todos os ensinamentos, preparações, de modo particular agradeço aos meus orientadores Marina Ribeiro e Carlos Henrique por estarem me acompanhando desde o início da faculdade e tanto me ajudaram, aos professores Miguel Schnoor e Leandro Egea por terem aceitado fazer parta da banca do meu TCC. Agradeço também aqueles que me apoiaram durante a faculdade: Beatriz Cheble, Eduardo Carneiro, Gleyciane Jales, Gustavo Couto, Matheus de Paula, Nathalia Ferreira, Leticia Vieira, Luka Nunes, Sami Safatli. Agradeço de coração a cada um de vocês, obrigado por terem feito parte desse momento tão importante em minha vida.

"Dê-me, Senhor, agudeza para entender, capacidade para reter,
método e faculdade para aprender, sutileza para interpretar,
graça e abundância para falar, acerto ao começar,
direção ao progredir e perfeição ao concluir..."
(São Tomás de Aquino)

Resumo

Este trabalho apresenta a construção do conjunto dos números inteiros, racionais e reais, a partir da formalização do conjunto dos números naturais com os Axiomas de Peano. O conjunto dos números inteiros foi construído com base no conjunto dos naturais, utilizando-se o conceito de classes de equivalência. Foram definidas as operações de soma e produto, bem como uma relação de ordem, e foram demonstradas algumas propriedades. Por fim, estabeleceu-se uma relação entre a forma dos números inteiros construídos e a notação usual de números inteiros. A construção dos racionais seguiu o mesmo raciocínio, utilizando o conjunto dos inteiros como base. O conjunto dos números reais foi construído através de dois métodos distintos: os chamados Cortes de Dedekind, que são subconjuntos especiais do corpo ordenado $\mathbb{Q}$, e a construção de Cantor, usando sequências racionais de Cauchy. Provou-se que ambos os métodos dão origem a um mesmo corpo ordenado completo arquimediano, que é único: o corpo dos números reais.

Palavras-chave: Conjuntos numéricos. Axiomas de Peano. Cortes de Dedekind. Sequências de Cauchy.

Abstract

This work presents an integer's, rationals and real set construction from the formalization of the natural numbers set with Peano axioms. The set of integers were built based on the set of natural numbers, using the equivalence class concept. Sum and product operations were defined, as well as an order relationship, and some properties were exemplified. Ultimately, a relationship was established between the constructed integer numbers form and the usual integers notation. The construction of rationals followed the same thinking path, using the set of integers as a basis. The set of real numbers were constructed using two distinct methods: the so-called Dedekind cuts, which are special subsets of the ordered body $\mathbb{Q}$, and the Cantor set, using rational Cauchy sequences. Both methods have proved to give rise to the same complete Archimedean ordered body, which is unique: the body of real numbers.

Keywords: Numeric set. Peano Axioms. Dedekind Cuts. Cauchy Sequences.

Sumário

1 Introdução

A matemática sempre esteve presente na vida humana. A ideia de contagem não surgiu numa época recente, mas sim em um tempo bastante antigo. Já se fazia uso de números, em uma forma ainda primitiva, sem formalização, ao colocar marcas em pedaços de madeiras para identificar a quantidade de ovelhas, ou quantificar alimentos de uma caça.

Mesmo com sua utilização ocorrendo, o estudo teórico e formal sobre o conceito de números não foi feito de uma maneira rápida e prática, mas sim através de um desenvolvimento lento e complexo ao longo dos anos, até começar a ser abordado.

De fato, um marco importante na história dos números ocorreu no século VI $a.C.$, sendo atribuída à escola Pitagórica: a distinção entre números pares e ímpares, e descobriu-se também o resultado de que a soma de dois números pares é um número par, entre outros resultados [1].

Com o passar do tempo surgiram novos questionamentos em relação aos números e é possível perceber que a construção de cada conjunto numérico tem como base um ponto em comum: a construção de um novo conjunto é motivada por alguma limitação dos conjuntos existentes. Segundo [2], a construção formal dos conjuntos numéricos começou a partir do questionamento do que seria um número real.

Visando abordar a construção dos números de uma forma didática, sem preocupação com a ordem cronológica das formulações, este trabalho abordará a construção de três conjuntos básicos que são hoje conhecidos, assumindo a existência dos números naturais ($\mathbb{N}$): os números inteiros ($\mathbb{Z}$), os números racionais ($\mathbb{Q}$) e os números reais ($\mathbb{R}$).

Fazendo uma analogia, imagine a construção dos conjuntos númericos como a construção de uma escada. O primeiro degrau será o conjunto dos números naturais, que se estrutura formalmente com os Axiomas de Giuseppe Peano, através dos quais definiremos soma, multiplicação e relação de ordem. Serão provadas as principais propriedades conhecidas de $\mathbb{N}$.

Avançando para o segundo degrau, serão construídos os números inteiros, a partir da noção de relações de equivalência e utilizando como base o conjunto dos números naturais. Partindo para o terceiro degrau, serão construídos os números racionais de forma semelhante aos inteiros, mas dessa vez utilizando o conjunto $\mathbb{Z}$ como base.

Finalmente será feita a construção do conjunto dos números reais de duas maneiras distintas, sendo estas atribuídas a dois matemáticos: Richard Dedekind e Georg Cantor. Dedekind usa o que chamamos de cortes, sendo esta construção conhecida pelos chamados

Cortes de Dedekind, enquanto Cantor usa a noção de sequências de Cauchy. Definiremos as operações de soma e multiplicação e apresentaremos diversos resultados em ambas as construções. Mostraremos ainda que o conjunto formado pelas classes de equivalência de sequências racionais de Cauchy é um Corpo Ordenado Completo. Por fim, veremos que a existência de um Corpo Ordenado Completo é única a menos de um isomorfismo.

2 Conjunto dos Números Naturais

Faremos neste Capítulo a axiomatização do conjunto dos números naturais, que será o conjunto base para a construção dos demais conjuntos. O conjunto $\mathbb{N}$, o qual chamamos de naturais, será construído a partir de alguns Axiomas pelo método de Giuseppe Peano. Mais informações sobre este tema podem ser encontradas em [3].

2.1 Método de Giuseppe Peano

Esse método se baseia no fato de que podemos definir uma certa ordenação numa sequência, onde cada elemento tem um sucessor, que está bem definido. Por este motivo diz-se uma "teoria ordinal". Uma outra abordagem, chamada "Teoria Cardinal" pode ser usada para construir também os naturais. O leitor interessado pode consultar esta teoria em [4].

Peano, para fundamentar sua teoria, assume três conceitos primitivos: número natural, zero e sucessor, que se relacionam entre si por cinco Axiomas. Vamos usar $\sigma(n)$ como sendo o sucessor do número n, e 0 para indicar o número zero. Assim, os Axiomas são:

1. 0 é um número natural;
2. Todo número natural n tem um sucessor $\sigma(n)$;
3. 0 não é sucessor de nenhum número;
4. Se $\sigma(n) = \sigma(m)$, então $n = m$;
5. Princípio da indução completa: seja S um conjunto natural tal que

   (a) $0 \in S$;

   (b) Se $n \in S$, então $\sigma(n) \in S$

   Então, S é o conjunto de todos os números naturais.

Denotaremos por $\mathbb{N}$ o conjunto de todos os números naturais.

Pensando fundamentalmente em como somos capazes de expressar as ideias matemáticas em termos de conjunto e funções, podemos reescrever os cinco Axiomas citados anteriormente de forma a obter apenas três. Para isso, observe que o conceito de sucessor pode ser entendido como uma função que, a cada número natural, associa um outro número natural. O Axioma 2 afirma que isso está definido para todo $n \in \mathbb{N}$.

Podemos, então, admitir que existe um conjunto $\mathbb{N}$ e $\sigma : \mathbb{N} \longrightarrow \mathbb{N}$, satisfazendo:

A.1 Existe um elemento $0 \in \mathbb{N}$ tal que $0 \notin Im(\sigma)$;

A.2 A função σ é injetora;

A.3 Seja A um subconjunto de $\mathbb{N}$ tal que

(i) $0 \in A$;

(ii) Se $n \in A$, então $\sigma(n) \in A$.

Então, $A = \mathbb{N}$.

Indicaremos por $\mathbb{N}^+$ o conjunto de todos os naturais diferentes de zero. Note que $\sigma(0) \in \mathbb{N}^+$ e pelo Axioma A.2 temos que $0 \neq \sigma(0)$ mostrando que $\mathbb{N}^+$ é não vazio.

Provaremos que todo natural diferente de zero é sucessor de algum número.

Proposição 1. $Im(\sigma) = \mathbb{N}^+$.

Demonstração. Consideremos o conjunto $A = \{0\} \cup Im(\sigma)$. Temos que $0 \in A$ e, se $n \in A$, então $\sigma(n) \in A$, já que $\sigma(n) \in Im(\sigma)$. Logo pelo Axioma $A.3$, devemos ter $A = \mathbb{N}$. Portanto, $A \backslash \{0\} = \mathbb{N} \backslash \{0\}$, isto é, $Im(\sigma) = \mathbb{N}^+$. □

Definição 1. *Dado um natural $n \neq 0$, o número natural m tal que $\sigma(m) = n$, chama-se antecessor de n, e n chama-se o sucessor de m.*

Na próxima seção definiremos as operações de soma e produto em $\mathbb{N}$ e demonstraremos algumas de suas propriedades.

2.2 Operações e Relação de Ordem

Vamos agora definir a soma $m + n$, para quaisquer naturais m e n. Antes, porém, será preciso definir a soma para um natural m fixado.

Definição 2. Seja $m \in \mathbb{N}$ um número natural dado. Então:

$$(i)\ m + 0 = m$$

$$(ii)\ m + \sigma(n) = \sigma(m + n)$$

Observação. Podemos ter a certeza que a operação em 2 está bem definida por consequência direta do axioma $A.3$, já que definimos o que é somar zero e a partir de um n como obtemos o sucessor de n.

A partir disso, propriedades da soma também podem ser verificadas, como por exemplo, associatividade, comutatividade, unicidade do elemento neutro. O leitor interessado pode consultar mais detalhes em [3].

Indicaremos por 1 o número natural sucessor de 0, isto é, $1 = \sigma(0)$.

Proposição 2. *Para todo número natural* m *temos que* $\sigma(m) = m + 1$.

Demonstração. Seja $A = \{m \in \mathbb{N} |\ \sigma(m) = 1{+}m\}$. Temos que $0 \in\ A$, pois $\sigma(0) = 1{+}0 = 1$. Suponhamos então $m \in A$. Mostraremos que $\sigma(m) \in A$. Com efeito, como $\sigma(m) = 1 + m$ temos que:

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

isto é, $\sigma(m) \in A$. Pelo Axioma $A.3$ temos que $A = \mathbb{N}$. □

Vamos definir a multiplicação $m \cdot n$, para quaisquer m e n.

Definição 3. *Seja* $m \in \mathbb{N}$ *um número natural dado. Então:*

$$(i)\ m \cdot 0 = 0$$

$$(ii)\ m \cdot \sigma(n) = m \cdot n + m$$

Observação. Assim como na soma a operação definida em 3 ela está bem definida por consequência direta do axioma $A.3$.

Vamos verificar agora algumas propriedades relacionadas com a operação do produto, e também com a relação menor ou igual, definida no conjunto dos números naturais.

Lema 1. *É válido que* $m \cdot 0 = 0 \cdot m = 0, \forall m \in \mathbb{N}$.

Demonstração. Por definição $m \cdot 0 = 0$, $\forall m \in \mathbb{N}$. Precisamos então provar que $0 \cdot m = 0$, $\forall m \in \mathbb{N}$. Seja $S = \{m \in \mathbb{N} |\ 0 \cdot m = 0\}$. Temos que $0 \in S$, pois $0 \cdot 0 = 0$. Supondo que $m \in S$, provaremos que $\sigma(m) \in S$. Temos:

$0 \cdot \sigma(m) = 0 \cdot m + 0 = 0 + 0 = 0$ e, portanto, $\sigma(m) \in S$. Assim, pelo Axioma A.3, $S = \mathbb{N}$. □

Proposição 3. *O neutro multiplicativo existe e é único. Aqui neutro se refere ao elemento neutro multiplicativo, isto é, existe um único* $1 \in \mathbb{N}$ *tal que* $1 \cdot a = a$.

Demonstração.

i. Considere $A = \{m \in \mathbb{N} \mid 1 \cdot m = m\}$. Vamos usar o Axioma $A.3$ para provar essa propriedade. Temos que $0 \in A$ pois $1 \cdot 0 = 0$. Suponhamos então que $m \in A$, ou seja, $1 \cdot m = m$. Queremos ver que o sucessor de $m \in A$. Assim,

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

Portanto, $\sigma(m) \in A$. Assim, pelo Axioma A.3, $A \in \mathbb{N}$.

ii. Suponhamos agora que p seja um outro elemento neutro da multiplicação. Tomando o produto $p \cdot 1$, temos que $p \cdot 1 = 1$, pois p é um elemento neutro. No item i da demonstração vimos que 1 também é um elemento neutro. Logo, $p \cdot 1 = p$. Temos ainda que $1 \cdot p = p(0+1) = p \cdot 0 + p = 0 + p = p$. Portanto, $p = 1$ e o elemento neutro é único.

□

Proposição 4. *Valem a comutatividade, distributividade e associatividade para a multiplicação.*

Demonstração. 1. (Comutatividade:) $\forall\ m, n \in \mathbb{N}$ vale que $m \cdot n = n \cdot m$.

Seja $A = \{m \in \mathbb{N} \mid m \cdot n = n \cdot m, \forall n \in \mathbb{N}\}$. Então, $0 \in A$ pois $m \cdot 0 = 0 = 0 \cdot m$. Suponhamos agora que $m \in A$. Provaremos que $\sigma(m) \in A$. De fato,

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

Portanto, $\sigma(m) \in A$ e, pelo Axioma A.3, $A = \mathbb{N}$.

2. (Distributividade:) $\forall\ m, n, p \in \mathbb{N}$ vale que $m \cdot (n + p) = m \cdot n + m \cdot p$.

Seja $S = \{p \in \mathbb{N} \mid m \cdot (n+p) = m \cdot n + m \cdot p, \forall m, n \in \mathbb{N}\}$. Temos que $m \cdot (n+0) = m \cdot n = m \cdot n + 0 = m \cdot n + m \cdot 0$, logo $0 \in S$.

Suponhamos que $p \in S$ e provemos que $\sigma(p) \in S$. Temos:

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

Portanto, $\sigma(p) \in S$. Assim, pelo Axioma A.3, temos que $S = \mathbb{N}$.

3. (Associatividade:) $\forall\ m, n, p \in \mathbb{N}$ é válido que $m \cdot (n \cdot p) = (m \cdot n) \cdot p$

Seja $A = \{p \in \mathbb{N} \mid m \cdot (n \cdot p) = (m \cdot n) \cdot p, \forall m, n \in \mathbb{N}\}$. Temos que $m \cdot (n \cdot 0) = m \cdot 0 = (m \cdot n) \cdot 0$, de onde segue que $0 \in A$.

Supondo agora que $p \in A$, vamos provar que $\sigma(p) \in A$. Temos:

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

Assim, $\sigma(p) \in A$. Portanto, pelo Axioma A.3, $A = \mathbb{N}$.

□

Proposição 5. *Sejam a, b, c números naturais. Se $a + c = b + c$, então $a = b$.*

Demonstração. Seja $S = \{c \in \mathbb{N} | \ a + c = b + c \ \Rightarrow \ a = b\}$. Temos que $0 \in S$, pois $a + 0 = b + 0$, isto é, $a = b$. Supondo que $c \in S$, provemos que $\sigma(c) \in S$.

Temos que $a + \sigma(c) = b + \sigma(c)$ é equivalente a $\sigma(a+c) = \sigma(b+c)$. Pelo Axioma $A.2$ temos que $a + c = b + c$ e, como $c \in S$, segue que $a = b$. Pelo Axioma A.3, $S = \mathbb{N}$. □

A seguir, definiremos no conjunto dos naturais a relação menor ou igual.

Definição 4. Sejam m e n naturais. Diremos que m é menor ou igual a n, se existir um outro número natural r tal que $m + r = n$. Em símbolos,

$$m \leq n \text{ se existe } r \in \mathbb{N} \text{ tal que } m + r = n.$$

O resultado a seguir terá sua importância na prova da tricotomia pois nos mostra que dados $a, b \in \mathbb{N}$, apenas uma das condições ocorre $a = b$, existe x tal que $a + x = b$, ou existe y tal que $a = b + y$. Assim o resultado é enunciado da seguinte maneira.

Proposição 6. *Sejam a e b números naturais. Então, uma das seguintes condições está verificada:*

1. *$a = b$;*
2. *Existe $x \in \mathbb{N}$, $x \neq 0$, tal que $a + x = b$;*
3. *Existe $y \in \mathbb{N}$, $y \neq 0$, tal que $a = b + y$.*

Demonstração. Dado $a \in \mathbb{N}$ qualquer, seja S o conjunto

$$S = \{b \in \mathbb{N} |\ a = b \text{ ou } \exists x \in \mathbb{N}, x \neq 0 \text{ tal que } a + x = b \text{ ou } \exists y \in \mathbb{N}, y \neq 0 \text{ tal que } a = b + y\}.$$

1. Temos que $0 \in S$, pois $a = 0 + a$, $\forall a \in \mathbb{N}$.
2. Suponha que $b \in S$. Vamos provar que $\sigma(b) \in S$ e, para isso, dividiremos nossa demonstração em casos:

   (*Caso 1*) Seja $b \in S$, com $a = b$. Temos que $\sigma(b) = b + 1$. Mas, por hipótese, $a = b$, então $\sigma(b) = a + 1$. Portanto, existe $x = 1$ tal que $a + 1 = \sigma(b)$. Assim, $\sigma(b) \in S$.

   (*Caso 2*) Seja $b \in S$, tal que $\exists x \in \mathbb{N}, x \neq 0$ tal que $a + x = b$. Temos que $\sigma(b) = b + 1$. Por hipótese, $b = a + x$, logo, $\sigma(b) = a + x + 1$. Então, para $y = x + 1$, temos que $\sigma(b) = a + y$. Logo, $\sigma(b) \in S$.

   (*Caso 3*) Seja $b \in S$ tal que $\exists y \in \mathbb{N}, y \neq 0$ tal que $a = b + y$. Temos que $\sigma(a) = a + 1 = b + y + 1 = \sigma(b) + y$. Como $y \neq 0$, existe um número natural x tal que $y = \sigma(x) = x + 1$. Logo, $a + 1 = \sigma(b) + x + 1$. Pela propriedade cancelativa da adição obtemos que $a = \sigma(b) + x$, ou seja, $\sigma(b) \in S$.

□

Proposição 7. *Sejam $a, b, c \in \mathbb{N}$. Se $a \leq b$ e $0 \leq c$, então $a \cdot c \leq b \cdot c$.*

Demonstração. Sejam $a \leq b$ e $0 \leq c$. Então, existe r_1 tal que $a + r_1 = b$ e existe r_2 tal que $0 + r_2 = c$, ou seja, $c = r_2$.

Multiplicando ambos os lados por r_2 em $a + r_1 = b$, obtemos $r_2 \cdot (a + r_1) = b \cdot r_2$.

Usando a distributividade no primeiro lado da igualdade temos, $r_2 \cdot a + r_2 \cdot r_1 = b \cdot r_2$. Como $r_2 = c$, então $c \cdot a + c \cdot r_1 = b \cdot c$.

Além disso, sabendo que a multiplicação é comutativa, $c \cdot a + c \cdot r_1 = b \cdot c$ equivale a $a \cdot c + c \cdot r_1 = b \cdot c$.

Logo, existe $r = c \cdot r_1$ tal que $a \cdot c + r = b \cdot c$ e, portanto, $a \cdot c \leq b \cdot c$. □

Proposição 8. *Sejam $a, b, c \in \mathbb{N}$. Se $a \leq b$, então $a + c \leq b + c$.*

Demonstração. Seja $a \leq b$. Então, existe r_1 tal que $a + r_1 = b$. Somando c em ambos os lados, obtemos $(a + r_1) + c = b + c$.

Como a soma é associativa e comutativa, podemos reescrever a igualdade como $(a + c) + r_1 = b + c$.

Logo, existe r_1 tal que $a + c + r_1 = b + c$ e, portanto, $a + c \leq b + c$. □

Proposição 9. *(Tricotomia) Dados dois naturais a, b quaisquer, tem-se que uma e apenas uma das seguintes situações ocorrem, $a < b$ ou $a = b$ ou $b < a$.*

Demonstração. Vamos provar a tricotomia supondo que dois casos aconteçam simultaneamente e concluir um absurdo.

$(a < b)$ e $(a = b)$: Como $a < b$, então existe $x \in \mathbb{N}, x \neq 0$ tal que $a + x = b$. Mas, temos também que $a = b$, de onde segue que $a = a + x$, e isso implica que $x = 0$. Absurdo, pois por hipótese $x \neq 0$. Analogamente, prova-se o caso em que $(b < a)$ e $(a = b)$.

$(a < b)$ e $(b < a)$: Como $a < b$, existe $x \in \mathbb{N}, x \neq 0$ tal que $b = a + x$, e como $b < a$, existe $y \in \mathbb{N}, y \neq 0$ tal que $b + y = a$. Assim, obtemos:

$$b = (b + y) + x = b + (y + x).$$

Logo, $y + x = 0$. Mas, sabemos que $x \neq 0$ e, portanto, $x = \sigma(x')$, para algum $x' \in \mathbb{N}$. Então, $y + x = y + \sigma(x') = \sigma(y + x') = 0$, ou seja, $0 \in Im(\sigma)$. Isso é uma contradição, pois $0 \notin Im(\sigma)$.

Portanto, os casos não podem acontecer simultaneamente e o resultado está provado. □

Proposição 10. *Se $a \leq b$ e $b \leq a$, então $b = a$, $\forall\ a, b \in \mathbb{N}$.*

Demonstração. Suponha $a \geq b$ e $b \geq a$. Sabemos que $a \geq b$ equivale dizer que $a = b$ *ou* $a < b$ e, de forma análoga, $b \geq a$ nos diz que $b < a$ *ou* $b = a$. Agora, usando a Proposição 9, é possível excluir três casos decorrentes das combinações possíveis: $a < b$ *e* $b < a$, $a < b$ *e* $a = b$, $b < a$ *e* $b = a$. Portanto, o único caso restante é termos $b = a$. □

Proposição 11. *Temos que $a \leq a$, $\forall\ a \in \mathbb{N}$.*

Demonstração. Seja $S = \{a \in \mathbb{N} | a \leq a\}$.

Temos que $0 \in S$, pois tomando $r = 0$, temos $0 + r = 0$. Logo, $0 \leq 0$.

Suponha que $a \in S$. Vamos provar que $\sigma(a) \in S$. Temos que $\sigma(a) = a + 1$ mas, por hipótese $\exists r$ tal que $a + r = a$. Logo, $\sigma(a) = a + r + 1 = \sigma(a) + r$. Assim, encontramos um r tal que $\sigma(a) = \sigma(a) + r$. Então, $\sigma(a) \leq \sigma(a)$ e, portanto, $\sigma(a) \in S$. Logo, $S = \mathbb{N}$. □

Proposição 12. *Se $a \leq b$ e $b \leq c$, então $a \leq c$, $\forall\ a, b, c \in \mathbb{N}$.*

Demonstração. Como $a \leq b$, $\exists\ r_1$ tal que $a + r_1 = b$. Da mesma forma, $\exists\ r_2$ tal que $b + r_2 = c$. Logo, $a + r_1 + r_2 = c$, ou seja, $\exists\ r_3 = r_1 + r_2$ tal que $a + r_3 = c$. Portanto, $a \leq c$. □

Todos os axiomas e proposições vistos nessa seção nos garantem a existência dos naturais e nos mostra como operar com os elementos desse conjunto. No próximo capítulo, tendo os números naturais como nossa base, faremos a construção dos inteiros.

3 Construção dos Números Inteiros

Nessa seção estudaremos o que conhecemos como Conjunto dos Números Inteiros. Faremos a construção deste conjunto a partir dos elementos e operações no Conjunto dos Números Naturais, vistos no Capítulo 2, e do conceito de relação de equivalência.

3.1 Preliminares

Veremos aqui conceitos que serão necessários ao longo da construção que estamos abordando.

Definição 5. Seja R um subconjunto de $A \times A$. Diremos que R define uma relação de equivalência em A se

1. $(a, a) \in R$ para todo $a \in A$
2. Se $(a, b) \in R$ então $(b, a) \in R$
3. Se $(a, b) \in R$ e $(b, c) \in R$ então $(a, c) \in R$

Assim, pensaremos nas relações de equivalência como subconjuntos do produto $A \times A$ e olharemos como sendo relações binárias em A. Logo, podemos admitir que a se relaciona com b quando $(a, b) \in R$.

Definição 6. A relação binária $\equiv$ sobre A é uma relação de equivalência sobre A se

1. (Reflexiva) $a \equiv a \ \forall a \in A$,
2. (Simétrica) $a \equiv b \Rightarrow b \equiv a, \ \forall a, b \in A$
3. (Transitiva) $a \equiv b \ e \ b \equiv c \Rightarrow a \equiv c \ \forall a, b, c \in A$

Definição 7. Definimos a classe de equivalência de um elemento $a \in A$ como sendo o conjunto

$$\overline{(a)} = \{x \in A; \ x \equiv a\}.$$

Definição 8. O conjunto quociente de A é o conjunto formado por todas as classes de equivalência e será denotado por $A/\equiv$.

Diremos que a relação binária $\equiv$ é antissimétrica se

$$a \equiv b \ e \ b \equiv a \Rightarrow a = b.$$

Definição 9. Seja R uma relação binária definida no conjunto A. Diremos que R é uma relação de ordem parcial não restrita se, e somente se,

1. R é reflexiva;
2. R é antissimétrica;
3. R é transitiva.

Definição 10. Seja R uma relação binária definida no conjunto A. Diremos que R é uma relação de ordem total se, e somente se,

1. R é reflexiva;
2. R é antissimétrica;
3. R é transitiva;
4. $\forall x, y \in A\ x \leq y\ ou\ y \leq x$ (digamos aqui que x, y são elementos comparáveis).

3.2 A Construção do Conjunto dos Números Inteiros

Consideraremos como ponto de partida o conjunto $\mathbb{N} \times \mathbb{N}$, que representa o conjunto de todos os pares ordenados de números naturais. Sobre tal conjunto, definiremos uma relação de equivalência, que representaremos pelo símbolo $\equiv$, da seguinte forma:

Seja o conjunto $\mathbb{N} \times \mathbb{N}$ e sobre ele a relação $\equiv$ dada por $(a, b) \equiv (c, d)$ se, e somente se $a + d = b + c$.

Exemplo 1. Note que $(4, 6) \equiv (7, 9)$, pois $4 + 9 = 6 + 7$ e $(3, 5)$ não equivale à $(5, 6)$, pois $3 + 6 \neq 5 + 5$.

Proposição 13. *A relação $\equiv$ é uma relação de equivalência.*

Demonstração. 1°) **Reflexiva:** seja $(a, b) \in \mathbb{N} \times \mathbb{N}$. Temos que $a + b = b + a$, pela propriedade comutativa da soma para os naturais, logo $(a, b) \equiv (a, b)$ e, portanto, a relação é reflexiva;

2°)**Simétrica:** sejam (a, b) e $(c, d) \in \mathbb{N} \times \mathbb{N}$, e suponha que $(a, b) \equiv (c, d)$. Então, $a + d = b + c$. Usando da comutatividade da soma temos que $c + b = d + a$, logo $(c, d) \equiv (a, b)$ e, portanto, a relação é simétrica;

3°)**Transitiva:** sejam (a, b), (c, d) e (e, f) tais que $(a, b) \equiv (c, d)$ e $(c, d) \equiv (e, f)$, ou seja, $a + d = b + c$ e $c + f = d + e$. Somando as duas equações temos que $a + d + c + f =$

$b+c+d+e$. Usando a cancelativa da soma concluímos que $a+f=b+e$ e, portanto, $(a,b)\equiv(e,f)$.

Como a relação $\equiv$ é reflexiva, simétrica e transitiva, cocluimos que ela é uma relação de equivalência. □

Agora, vamos considerar o conjunto quociente da relação $\equiv$ em $\mathbb{N}\times\mathbb{N}$. Temos assim que:

$$\overline{(a,b)} = \{(x,y)\ \in\ \mathbb{N}\times\mathbb{N}\ |\ \ (x,y)\equiv(a,b)\}.$$

Definição 11. Denotaremos por $\mathbb{Z}$ o conjunto $\mathbb{N}\times\mathbb{N}/\equiv$ e chamaremos de números inteiros os elementos desse conjunto.

3.3 Operações em $\mathbb{Z}$ e Relação de Ordem

Depois de construído o conjunto dos números inteiros, precisamos definir nele as operações de soma e produto, bem como uma relação de ordem em $\mathbb{Z}$. Estes serão os assuntos abordados nesta seção.

Definição 12. Sejam $\alpha=\overline{(a,b)}$ e $\beta=\overline{(c,d)}$ elementos de $\mathbb{Z}$. Definimos a soma $\alpha+\beta$ dos números inteiros α e β por

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

Definição 13. Sejam $\alpha=\overline{(a,b)}$ e $\beta=\overline{(c,d)}$ elementos de $\mathbb{Z}$. Definimos o produto $\alpha\cdot\beta$ dos números inteiros α e β por

$$\alpha\cdot\beta=\overline{(ac+bd,ad+bc)}.$$

Para verificar que as operações de soma e multiplicação em $\mathbb{Z}$ estão bem definidas, é necessário provar que essas operações não dependem da escolha dos elementos das classes de equivalência. Os Lemas 2 e 3 apresentam tais resultados.

Lema 2. *Sejam* $\overline{(a,b)}=\overline{(a',b')}$ *e* $\overline{(c,d)}=\overline{(c',d')}$ *números inteiros. Então,*

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

Demonstração. [3] □

Lema 3. *Sejam* $\overline{(a,b)}=\overline{(a',b')}$ *e* $\overline{(c,d)}=\overline{(c',d')}$ *números inteiros. Então,*

$$\overline{(ab+bd,ad+bc)}=\overline{(a'c'+b'd',a'd'+b'c')}$$

Demonstração. [3] □

Vamos agora definir uma relação de ordem entre os elementos do conjunto $\mathbb{Z}$, da seguinte maneira:

Definição 14. Dados $\alpha = \overline{(a,b)}$ e $\beta = \overline{(c,d)} \in \mathbb{Z}$, diremos que

$$\alpha \leq \beta \quad \text{se} \quad a + d \leq b + c.$$

Dizemos ainda que $a < b$ se $a \leq b$ e $a \neq b$. De forma análoga, definimos "$\geq$" e "$>$".

A fim de exemplificar a Definição 14, suponha dois elementos de $\mathbb{Z}$, $\alpha = \overline{(1,2)}$ e $\beta = \overline{(5,3)}$. Temos que $\alpha \leq \beta$, pois $1 + 3 \leq 2 + 5$.

De posse das operações soma e subtração, e da relação de ordem, podemos enunciar e demonstrar as propriedades básicas do conjunto dos números inteiros. Estes resultados são apresentados a seguir.

Proposição 14. *(Propriedade Associativa) $\forall \alpha, \beta, \gamma \in \mathbb{Z}$ tem-se que $(\alpha + \beta) + \gamma = \alpha + (\beta + \gamma)$.*

Demonstração. Sejam $\alpha = \overline{(a,b)}, \beta = \overline{(c,d)}, \gamma = \overline{(e,f)}$. Temos que

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

Pela associativa da soma temos

$$\overline{a + (c+e), b + (d+f)} = \overline{(a,b)} + \overline{(c+e, d+f)} = \alpha + [\overline{(c,d)} + \overline{(e,f)}] = \alpha + (\beta + \gamma).$$

$\square$

Proposição 15. *(Comutativa) Para todo par $\alpha, \beta \in \mathbb{Z}$ tem-se que $\alpha + \beta = \beta + \alpha$.*

Demonstração. Sejam $\alpha = \overline{(a,b)}$ e $\beta = \overline{(c,d)}$. Então,

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

e pela comutativa da soma,

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

$\square$

Proposição 16. *(Elemento Neutro) Existe um único elemento que denotaremos por $0 \in \mathbb{Z}$, tal que $\alpha + 0 = 0 + \alpha = \alpha, \quad \forall \alpha \in \mathbb{Z}$.*

Demonstração. **Existência:** sejam $\overline{(a,b)}$ e $\overline{(x,y)}$ em $\mathbb{Z}$ tais que $\overline{(a,b)} + \overline{(x,y)} = \overline{(a,b)}$. Temos que,

$$\overline{(a,b)} + \overline{(x,y)} = \overline{(a,b)} \Longrightarrow \overline{(a+x, b+y)} = \overline{(a,b)} \Longrightarrow a+x+b = b+y+a \Longrightarrow x = y.$$

Logo, $\overline{(x,x)}$ é elemento neutro em $\mathbb{Z}$.

Unicidade: seja $\overline{(w,z)}$ um elemento neutro em $\mathbb{Z}$ e tomemos a soma $\overline{(w,z)}+\overline{(x,x)}$. Como $\overline{(w,z)}$ é elemento neutro, $\overline{(w,z)} + \overline{(x,x)} = \overline{(x,x)}$. Como $\overline{(x,x)}$ é elemento neutro, $\overline{(w,z)} + \overline{(x,x)} = \overline{(w,z)}$. Portanto, temos que $\overline{(w,z)} = \overline{(x,x)}$. Logo, o elemento neutro é único. □

Proposição 17. *(Existência do Oposto) Para cada inteiro α existe um único elemento que chamaremos seu oposto, e denotaremos por $-\alpha$, tal que $\alpha + (-\alpha) = (-\alpha) + \alpha = 0$.*

Demonstração. **Existência:** sejam $\alpha = \overline{(a,b)}$ e $\beta = \overline{(c,d)}$ tais que $\overline{(a,b)} + \overline{(c,d)} = \overline{(x,x)}$. Então,

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

Logo, o elemento oposto de $\alpha = \overline{(a,b)}$ é o elemento em $\mathbb{Z}$ de classe $\beta = \overline{(b,a)}$.

Unicidade: suponha que exista $\gamma = \overline{(e,f)}$ um elemento oposto de α. Logo, $\overline{(a,b)} + \overline{(e,f)} = \overline{(x,x)}$. Mas vimos anteriormente que $\overline{(b,a)}$ é o oposto de $\overline{(a,b)}$, então $\overline{(a,b)}+\overline{(b,a)} = \overline{(x,x)}$. Entretanto, isso nos diz que

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

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

$$2^*(a+b) = a+b+e+f$$

$$a+b = e+f$$

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

Portanto, o elemento oposto é único. □

Proposição 18. *(Associativa da Multiplicação) Para toda terna $\alpha, \beta, \gamma \in \mathbb{Z}$ tem-se que $(\alpha\beta)\gamma = \alpha(\beta\gamma)$.*

Demonstração. Sejam $\alpha = \overline{(a,b)}$, $\beta = \overline{(c,d)}$ e $\gamma = \overline{(e,f)}$ em $\mathbb{Z}$. Então

$$(\alpha\beta)\gamma = [\overline{(a,b)(c,d)}]\overline{(e,f)} = [\overline{(ac+bd, ad+bc)}]\overline{(e,f)} =$$

$$\overline{((ac)e + (bd)e + (ad)f + (bc)f, (ac)f + (bd)f + (ad)e + (bc)e)}.$$

Aplicando a associativa da multiplicação em toda a expressão obtemos:

$$\overline{(a(ce) + b(de) + a(df) + b(cf), a(cf) + b(df) + a(de) + b(ce))} =$$

$$\overline{(a,b)(ce + df, cf + de)} = \overline{(a,b)}[\overline{(c,d)(e,f)}] = \alpha(\beta\gamma).$$

□

Proposição 19. *(Comutativa da Multiplicação) Para todo $\alpha, \beta \in \mathbb{Z}$ tem-se que $\alpha\beta = \beta\alpha$.*

Demonstração. Sejam $\alpha = \overline{(a,b)}$ e $\beta = \overline{(c,d)}$ elementos de $\mathbb{Z}$. Temos que

$$\alpha\beta = \overline{(a,b)(c,d)} = \overline{(ac + bd, ad + bc)}.$$

Aplicando a comutativa da multiplicação obtemos

$$\overline{(ca + db, da + bc)} = \overline{(c,d)(a,b)} = \beta\alpha.$$

□

Proposição 20. *(Distributiva) Para toda terna $\alpha, \beta, \gamma \in \mathbb{Z}$ tem-se que $\alpha(\beta+\gamma) = \alpha\beta+\alpha\gamma$.*

Demonstração. Sejam $\alpha = \overline{(a,b)}$,$\beta = \overline{(c,d)}$ e $\gamma = \overline{(e,f)}$ em $\mathbb{Z}$. Temos que

$$\overline{(a,b)}[\overline{(c,d)} + \overline{(e,f)}] = \overline{(a,b)}[\overline{(c+e, d+f)}] = [\overline{a(c+e) + b(d+f), a(d+f) + b(c+e)}]$$

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

$$\alpha\beta + \alpha\gamma.$$

□

Proposição 21. *A relação $\leq$ é uma relação de ordem.*

Demonstração. Seja $\alpha = \overline{(a,b)}$ em $\mathbb{Z}$. Temos que $\alpha \leq \alpha$, pois $a + b \leq b + a = a + b$.

Sejam $\alpha = \overline{(a,b)}$ e $\beta = \overline{(c,d)}$ em $\mathbb{Z}$, e suponhamos que $\alpha \leq \beta$ e $\beta \leq \alpha$. Então,

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

Como já provamos a antissimétrica para os naturais, e $a + d \leq b + c$ e $c + b \leq d + a$, temos que $(a,b) = (c,d)$, que são representantes das classes de equivalência de α e β, respectivamente. Portanto, temos $\alpha = \beta$.

Sejam $\alpha = \overline{(a,b)}$, $\beta = \overline{(c,d)}$ e $\gamma = \overline{(e,f)}$ em $\mathbb{Z}$, e suponha que $\alpha \leq \beta$ *e* $\beta \leq \gamma$. Por definição, temos que

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

Somando as duas relações, obtemos

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

e, pela cancelativa da soma, obtemos que $a+f \leq b+e$ que, por definição, nos diz que $\alpha \leq \gamma$.

Como $\leq$ é reflexiva, antissimétrica e transitiva ela é uma relação de ordem. □

Por fim, para encerrar os resultados de operações e relações no conjunto dos inteiros, vamos apresentar a propriedade de monotonicidade da adição.

Proposição 22. *Dados α,β, $\gamma \in \mathbb{Z}$, se $\alpha \leq \beta$ então $\alpha+\gamma \leq \beta+\gamma$.*

Demonstração. Sejam $\alpha = \overline{(a,b)}$, $\beta = \overline{(c,d)}$ e $\gamma = \overline{(e,f)}$, tal que $\alpha \leq \beta$. Então, $a+d \leq b+c$. Somando $e+f$ em ambos os lados obtemos

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

que, por definição, nos diz que $\alpha+\gamma \leq \beta+\gamma$. □

3.4 Correspondência do conjunto construído com a forma usual dos números inteiros

Apesar de termos definido nas Seções 3.2 e 3.3 o conjunto dos números inteiros, eles não foram introduzidos no formato em que usualmente conhecemos. Antes de apresentar a correspondência existente entre os dois formatos, faz-se necessária a definição de número positivo e negativo. Apenas para relembrar, temos que o elemento neutro em $\mathbb{Z}$ é dado por $0 = \overline{(x,x)}$, para qualquer número natural x. Em particular, $0 = \overline{(0,0)}$.

Definição 15. Um inteiro $\alpha = \overline{(a,b)}$, é dito positivo se $\alpha > 0$ e diz-se negativo se $\alpha < 0$.

Das Definições 14 e 15 decorrem as seguintes observações:

- $\alpha = \overline{(a,b)}$ positivo $\Longleftrightarrow \alpha > 0 \Longleftrightarrow a+0 > b+0 \Longleftrightarrow a > b$
- $\alpha = \overline{(a,b)}$ negativo $\Longleftrightarrow \alpha < 0 \Longleftrightarrow a+0 < b+0 \Longleftrightarrow a < b$

Seja $\alpha = \overline{(a,b)} \in \mathbb{Z}$.

1. $\alpha > 0 \Longleftrightarrow a > b \Longleftrightarrow (a,b) \equiv (a-b,0) \Longleftrightarrow \overline{(a,b)} = \overline{(a-b,0)} = \overline{(m,0)},\ m = a-b.$

2. $\alpha < 0 \Longleftrightarrow a < b \Longleftrightarrow (a,b) \equiv (0, b-a) \Longleftrightarrow \overline{(a,b)} = \overline{(0,b-a)} = \overline{(0,m)},\ m = b-a.$

3. $\alpha = 0 \Longleftrightarrow 0 = \overline{(0,0)}.$

Perceba que, com as observações 1 e 2, já é possível trabalhar com uma forma mais parecida com a notação usual dos inteiros.

Por exemplo, podemos tomar $\alpha = \overline{(3,1)} = \overline{(2,0)} > 0$, pela observação 1, e veremos com o próximo resultado que a classe $\overline{(2,0)}$ tem uma correspondência com o número 2. Um outro exemplo é tomando $\beta = \overline{(2,3)} = \overline{(0,1)} < 0$, pela observação 2.

Observamos a seguir que o conjunto dos inteiros não-negativos é uma *cópia* do conjunto $\mathbb{N}$ dos números naturais.

Seja $\mathbb{Z}^+ = \{(a,0) \mid a \in \ \mathbb{N}\}$ o conjunto dos inteiros não negativos. Definimos

$$\phi : \mathbb{N} \longrightarrow \mathbb{Z}^+$$

$$a \longmapsto \overline{(a,0)}$$

Afirmação: ϕ é bijetora.

Injetora:
Sejam $a, b \in \mathbb{N}$ tais que $\phi(a) = \phi(b)$. Então,

$$\phi(a) = \phi(b) \Longrightarrow \overline{(a,0)} \equiv \overline{(b,0)} \Rightarrow (a,0) = (b,0) \qquad \Longrightarrow a + 0 = b + 0 \Longrightarrow a = b.$$

Sobrejetora:
Seja $\overline{(b,0)} \in \mathbb{Z}^+$. Exibiremos $a \in \mathbb{N}$ tal que $\phi(a) = \overline{(b,0)}$.

Tome $a = b$. Então $\phi(a) = \phi(b) = \overline{(b,0)}$. Portanto, a função ϕ é sobrejetora.

Como ϕ é sobrejetora e injetora, temos que ela é bijetora.

Além disso, essa função preserva as operações e a ordem. Mais precisamente, temos que $\forall a, b \in \mathbb{Z}$:

$$(i) \quad \phi(a+b) = \phi(a) + \phi(b)$$

$$(ii) \quad \phi(ab) = \phi(a) \cdot \phi(b)$$

$$(iii) \quad \text{Se } a \leq b \text{ então } \phi(a) \leq \phi(b)$$

Para finalizarmos esta seção, enunciaremos a seguir o Princípio da Boa Ordem, que possui papel importante em muitas demonstrações matemáticas, como por exemplo, na demonstração do princípio de indução. O Princípio da Boa Ordem afirma que todo subconjunto não-vazio formado por números naturais possui um menor elemento. No que segue, utilizaremos a correspondência vista anteriormente entre $\mathbb{N}$ e o conjunto dos inteiros não negativos e, por isso, não faremos distinção entre esses dois conjuntos.

Proposição 23. *(Princípio da Boa Ordem) Seja $A \subset \mathbb{Z}$ um conjunto não-vazio de inteiros não-negativos. Então A contém um elemento mínimo (isto é, existe a_0 tal que $a_0 \leq a$, $\forall\, a \in A$).*

Demonstração. Consideremos o conjunto I_n dos números naturais menores ou iguais a n. Se $0 \in A$ então 0 será o menor elemento de A. Mas, se $0 \notin A$, então consideremos o conjunto X dos números naturais n tais que $I_n \subset \mathbb{N} - A$. Como $I_0 = \{0\} \subset \mathbb{N} - A$, vemos que $0 \in X$. Mas, como A não é vazio, concluímos que $X \neq \mathbb{N}$. Assim, a conclusão do Axioma 5 não seria válida. Segue, então, que deve existir $n \in X$ tal que $n + 1 \notin X$. Portanto $I_n = \{0, 1, 2, \dots, n\} \subset \mathbb{N} - A$ mas $n_0 = n + 1 \in A$. Portanto n_0 é o menor elemento do conjunto A, pois não existe número natural entre n e $n + 1$. □

4 Construção dos Números Racionais

4.1 Preliminares

Veremos nesta Seção alguns conceitos necessários para a construção do conjunto que denominaremos racionais.

Dizemos que um corpo $(K, +, \cdot)$ é um conjunto $K \neq 0$ munido de duas operações, $+$ e $\cdot$, denominadas como adição e multiplicação, respectivamente, se satisfaz nove Axiomas listados a seguir:

1. Associatividade da Adição: para todo $x, y, z \in K$ temos que $(x+y)+z = x+(y+z)$;
2. Comutatividade da Adição: para todo $x, y \in K$, temos $x + y = y + x$;
3. Existência do elemento neutro: Existe $0 \in K$ tal que $x + 0 = x, \ \forall x \in K$;
4. Existência do inverso aditivo: para todo $x \in K$ existe, $-x \in K$, tal que $x+(-x) = 0$;
5. Associatividade da Multiplicação: para todo $x, y, z \in K$ temos que $(x\cdot y)\cdot z = x\cdot(y\cdot z)$;
6. Comutatividade da Multiplicação: para todo $x, y \in K$, temos $x \cdot y = y \cdot x$;
7. Existência do elemento neutro para a multiplicação: Existe $1 \in K$ tal que $x \cdot 1 = x, \ \forall x \in K$;
8. Existência do inverso multiplicativo: para todo $x \neq 0 \in K$, existe $x^{-1} \in K$, tal que $x \cdot x^{-1} = 1$;
9. Distributividade: para todo $x, y, z \in K$ temos que $x \cdot (y + z) = x \cdot y + x \cdot z$.

Vale observar que se $x, y \in K$, então $x + y$ e $x \cdot y$, podem ser chamadas de soma e produto de x e y, respectivamente. Por ser mais simples, podemos escrever xy ao invés $x \cdot y$.

Observação. Dado um corpo ordenado K. Por um momento, vamos denotar o elemento neutro da multiplicação por e. Já sabemos que $0 < e$. Daí, somando e aos dois membros da desigualdade (já que $<$ é uma relação de ordem), temos:

$$e < e + e$$

Novamente somando e aos dois membros da última desigualdade, teremos

$$e + e < e + e + e \Longrightarrow e < e + e < e + e + e$$

Repetindo esse processo, teremos

$$e < e < e + e < e + e + e < e + e + e + e < \dots$$

Veja que dessa forma, $e, (e+e), (e+e+e), (e+e+e+e), \dots$ são todos elementos diferentes entre si. Considere o conjunto dos números naturais

$$\mathbb{N} = \{1, 2, 3, 4, \dots\}$$

Definindo a função $f : \mathbb{N} \longrightarrow K$ por

$$f(1) = e, f(2) = e + e, f(3) = e + e + e, f(4) = e + e + e + e, \dots$$

temos uma bijeção do conjunto $\mathbb{N}$ sobre o subconjunto $f(\mathbb{N})$ de K. Isso significa dizer que dentro de um corpo ordenado existe um conjunto "muito parecido" com $\mathbb{N}$. Na verdade, dado um corpo ordenado K, costuma-se dizer que $K \supset \mathbb{N}$.

Definição 16. Um corpo ordenado é um corpo K, munido das operações + e $\cdot$, de forma que existe um subconjunto $P \subset K$ onde vale as seguintes propriedades:

1. $\forall\ x, y \in P \Rightarrow x + y \in P$ e $x \cdot y \in P$;

2. $\forall x \in K$ deve ocorrer somente uma das seguintes alternativas: ou $x \in P$ ou $x = 0$ ou $-x \in P$.

O conjunto P é chamado de conjunto dos elementos positivos de K. Se $-P = \{-x; x \in P\}$, então:

$$K = -P \cup \{0\} \cup P \text{ (dois a dois disjuntos).}$$

O conjunto $-P$ é chamado conjunto dos elementos negativos de K.

Podemos afirmar que para todo elemento $a \neq 0$ de um corpo ordenado temos que $a^2 \in P$. De fato, $a \neq 0 \Rightarrow a \in P$ *ou* $-a \in P$. Assim, segue que $a \cdot a \in P$ ou $(-a) \cdot (-a) \in P$. Como $a \cdot a = (-a) \cdot (-a)$, temos que $a \cdot a = a^2 \in P$.

Definição 17. Em um corpo ordenado $\mathbb{K}$, definimos as relações:

$$\begin{aligned} a < b \quad &\Leftrightarrow b - a \in P, \\ a > b \quad &\Leftrightarrow b < a, \quad \text{(ou } a - b \in P) \\ a \leq b \quad &\Leftrightarrow b < a, \text{ ou } a = b \\ a \geq b \quad &\Leftrightarrow b > a, \text{ ou } a = b \end{aligned}$$

Definição 18. Em um corpo ordenado K, definimos o valor absoluto de $x \in K$ como

$$|x| = \begin{cases} x, \text{ se } x \geq 0 \\ -x, \text{ se } x < 0 \end{cases}$$

Da definição, $|x| = x \geq 0$ ou $|x| = -x > 0$. Portanto, $|x| \geq 0$ para todo $x \in K$. Note que, $|x| = x(\text{ se } x \geq 0)$ ou $|x| = -x > x(\text{ se } x < 0)$. Ou seja, $|x| = \max\{x, -x\}$.

O próximo teorema nos mostra algumas propriedades do valor absoluto

Teorema 4.1. Para quaisquer que sejam $x, y \in \mathbb{K}$, tem-se:

1. $|x + y| \leq |x| + |y|$ (Desigualdade Triangular);

2. $|x \cdot y| = |x| \cdot |y|$;

3. $||x| - |y|| \leq |x - y|$.

Demonstração. Veja em [5]. $\square$

Definição 19. Dizemos que um subconjunto X de um corpo ordenado K é limitado superiormente se $\exists\ b \in K$ tal que $x \leq b$, para todo $x \in X$. Dizemos que o elemento b é uma cota superior de X. De forma análoga, podemos definir X limitado inferiormente se $\exists\ a \in K$ tal que $a \leq x$, para todo x em X. O elemento a é dito uma cota inferior de X. Diremos que X é limitado se ele for limitado inferior e superiormente.

Definição 20. (Supremo) Seja K um corpo ordenado e $X \subset K$ limitado superiormente. Diremos que $b \in K$ é supremo de X se é a menor das cotas superiores. Isto é,

i. $x \leq b, \forall x \in X$;

ii. Se $\exists\ c \in K$ tal que $x \leq c, \forall\ x \in X$, então $b \leq c$.

De forma análoga, definimos o ínfimo de um conjunto X.

Definição 21. (Ínfimo) Seja K um corpo ordenado e $X \subset K$ limitado inferiormente. Diremos que $a \in K$ é ínfimo de X se é a maior das cotas inferiores. Isto é,

i. $a \leq x, \forall x \in X$;

ii. Se $\exists\ c \in K$ tal que $c \leq x, \forall\ x \in X$, então $c \leq a$.

Podemos dizer que se o supremo pertence ao conjunto X, ele será o elemento máximo de X e, de forma análog,a se o ínfimo pertence a X, ele será o elemento mínimo de X.

Definição 22. Um corpo ordenado K é arquimediano se, para cada $x \in K$, existe $n \in \mathbb{N}$ de forma que

$$x < \overbrace{1 + 1 + \cdots + 1}^{n \text{ vezes}}.$$

Proposição 24. *(Propriedade arquimediana). As seguintes propriedades num corpo ordenado arquimediano K são equivalentes:*

1. *$\mathbb{N} \subset K$ é ilimitado superiormente;*

2. *Dados $a, b \in K$, com $a > 0$, existe $n \in \mathbb{N}$ tal que $n \cdot a > b$;*

3. *Para cada $a > 0$ de K, existe $n \in \mathbb{N}$ tal que $0 < \dfrac{1}{n} < a$, pensando na existência do inverso multiplicativo como existe uma cópia de $\mathbb{N}$ em $\mathbb{K}$, o elemento n possui inverso multiplicativo, esse sendo $n^{-1} = \dfrac{1}{n}$, assim $\dfrac{1}{n}$ está bem definido.*

Definição 23. Dizemos que um corpo ordenado K é completo, se todo subconjunto não-vazio de K limitado superiormente possui supremo em K.

4.2 A Construção do Conjunto dos Números Racionais

No Capítulo 3 fizemos a construção dos números inteiros. Podemos, então, fazer alguns questionamentos: qual seria a motivação para a extensão deste conjunto? Por que o conjunto construído não é suficiente? O que significa medir algum objeto ou o quanto um comprimento cabe em outro? Particularmente, para esta última pergunta, devemos entender o que é medida. Podemos pensar no conceito milenar que conhecemos, como a ideia de medir uma roupa, alguma obra, etc. Nesse sentido, medir pode ser entendido como comparar duas grandezas da mesma espécie (dois comprimentos, dois pesos, dois volumes). Podemos então considerar uma pergunta fundamental com relação ao comprimento (que será nosso objetivo de estudo, pensando em uma reta numérica): dados dois comprimentos $\overline{AB}$ e $\overline{CD}$ com $\overline{CD} < \overline{AB}$, quantas vezes $\overline{CD}$ cabe em $\overline{AB}$?

Aqui, estamos partindo de um comprimento maior e subdividindo esse comprimento em partes menores. Por exemplo, se temos um comprimento de tamanho 4 e outro de tamanho 2, podemos dividir o maior segmento em duas partes, isto é, estamos fazendo a razão entre os comprimentos. Mas se tivéssemos um comprimento de tamanho 5 e outro de tamanho 3, como dividiríamos o maior em partes iguais, se 5 não é divisível por 3? Então a razão não teria um valor exato, ou seja, no conjunto dos inteiros esse valor seria um número desconhecido, apesar de sabermos que ele está ali. Segundo [3], nós temos um dilema:

1. Ou nós ignoramos o fato de não conseguirmos exprimir um comprimento em função de outro pela questão de divisibilidade entre seus tamanhos;

2. Ou queremos exprimir sempre esses comprimentos, e com isso temos que reconhecer que o instrumento numérico que até aqui conhecemos (números inteiros) é insuficiente para fazer essa medição e é necessário completá-lo. A questão é: como faremos isso?

Iniciaremos a construção desse novo conjunto a partir desse questionamento, definindo sobre o conjunto $\mathbb{Z} \times \mathbb{Z}^*$ uma relação de equivalência, a fim de construir esse "conjunto maior", o qual será chamado de conjunto dos números racionais. Indicaremos por $\mathbb{Z}^*$ o conjunto de todos os inteiros exceto o número 0.

Consideremos o seguinte conjunto:

$$\mathbb{Z} \times \mathbb{Z}^* = \{(a, b) |\ a \in \mathbb{Z}\ e\ b \in \mathbb{Z}^*\},$$

isto é, o conjunto de todos os pares ordenados de números inteiros com segunda componente não-nula. Da mesma forma como fizemos para os inteiros, definiremos uma relação sobre esse conjunto, a qual indicaremos por $\simeq$.

Definição 24. Dado dois elementos (a, b) e $(c, d) \in \mathbb{Z} \times \mathbb{Z}^*$, diremos que

$$(a, b) \simeq (c, d) \text{ se, e somente se, } ad = bc.$$

Exemplo 2. Os pares $(1, 2)$ e $(3, 6)$ se relacionam, pois $1 \cdot 6 = 2 \cdot 3$. Já os pares $(3, 5)$ e $(4, 6)$ não se relacionam, pois $3 \cdot 6 \neq 5 \cdot 4$.

A relação dada na Definição 24 é de equivalência. De fato,

- Para todo par $(a, b) \in \mathbb{Z} \times \mathbb{Z}^*$, temos que $(a, b) \equiv (a, b)$, pois $ab = ba$, logo a relação é reflexiva.
- Sejam agora $(a, b), (c, d)$ pares tais que $(a, b) \equiv (c, d)$. Logo $ad = bc$, donde também temos que $cb = da$, assim $(c, d) \equiv (a, b)$ logo a relação é simétrica.
- Sejam $(a, b), (c, d)$ e (e, f) pares tais que $(a, b) \equiv (c, d)$ e $(c, d) \equiv (e, f)$. Então $ad = bc$ e $cf = de$. Multiplicando a primeira igualdade por f e a segunda por b obtemos:

  $$adf = bcf,$$
  $$bcf = bde,$$

  donde

  $$abf = bde$$

  Como $d \neq 0$ podemos cancelar(pois d é elemento de $\mathbb{Z}^*$), assim $af = de$, o que implica que $(a, b) \equiv (e, f)$, portanto a relação é transitiva.

Portanto $\equiv$ é simétrica.

Vamos considerar agora o conjunto $(\mathbb{Z} \times \mathbb{Z}^*)/ \simeq$.

Para representar a classe do par (a, b) utilizamos o símbolo $\dfrac{a}{b}$. Assim,

$$\frac{a}{b} = \{(x, y) \in \mathbb{Z} \times \mathbb{Z}^* | (x, y) \simeq (a, b)\}.$$

O símbolo $\dfrac{a}{b}$ chama-se uma fração de numerador a e denominador b. Indicaremos por $\mathbb{Q}$ o conjunto $(\mathbb{Z} \times \mathbb{Z}^*)/ \simeq$, e chamaremos de números racionais os elementos de $\mathbb{Q}$.

4.3 Operações e Relação de ordem em $\mathbb{Q}$

Nesta Seção vamos definir a soma e o produto de dois elementos do conjunto $\mathbb{Q}$, bem como uma relação de ordem entre os seus elementos.

Definição 25. Sejam $\alpha = \frac{a}{b}$ e $\beta = \frac{c}{d}$ elementos de $\mathbb{Q}$. Definimos

$$\alpha + \beta = \frac{a}{b} + \frac{c}{d} = \frac{ad + bc}{bd},$$

ou seja, $\alpha + \beta$ é a classe do par $(ad + bc, bd)$.

Definição 26. Sejam $\alpha = \frac{a}{b}$ e $\beta = \frac{c}{d}$ elementos de $\mathbb{Q}$. Definimos o produto $\alpha\beta$ por

$$\alpha\beta = \frac{ac}{bd},$$

ou seja, $\alpha\beta$ é a classe do par (ac, bd).

Podemos perceber que, em primeiro lugar, a soma e a multiplicação parecem depender dos representantes de classe. Entretanto, os Lemas 4 e 5 darão garantia de que as Definições 25 e 26 independem do representante escolhido.

Lema 4. *Sejam* $\alpha = \frac{a}{b} = \frac{a'}{b'}$ *e* $\beta = \frac{c}{d} = \frac{c'}{d'}$ *números racionais. Então,*

$$\frac{ad + bc}{bd} = \frac{a'd' + b'c'}{b'd'}.$$

Demonstração. Sejam $\alpha = \frac{a}{b} = \frac{a'}{b'}$ e $\beta = \frac{c}{d} = \frac{c'}{d'}$ números racionais. Isso nos dá que $ab' = ba'$ e $cd' = dc'$. Assim

$$\frac{a}{b} + \frac{c}{d} = \frac{ad + bc}{bd} \quad \text{e} \quad \frac{a'}{b'} + \frac{c'}{d'} = \frac{a'd' + b'c'}{b'd'}$$

Queremos provar que as duas somas são iguais, ou seja, que $(ad + bc)b'd' = (a'd' + b'c')\,bd$, isto é, $adb'd' + bcb'd' = a'd'bd + b'c'bd$, ou ainda, $(ab')\,(dd') + (cd')\,(bb') = (a'b)\,(dd') + (bb')\,(c'd)$, o que é fato, pois, $ab' = ba'$ e $cd' = dc'$. □

Lema 5. *Sejam* $\alpha = \frac{a}{b} = \frac{a'}{b'}$ *e* $\beta = \frac{c}{d} = \frac{c'}{d'}$ *números racionais. Então,*

$$\frac{ac}{bd} = \frac{a'c'}{b'd'}.$$

Demonstração. Sejam $\alpha = \frac{a}{b} = \frac{a'}{b'}$ e $\beta = \frac{c}{d} = \frac{c'}{d'}$ números racionais, isso nos dá que $ab' = ba'$ e $cd' = dc'$. Assim

$$\frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd} \quad \text{e} \quad \frac{a'}{b'} \cdot \frac{c'}{d'} = \frac{a'c'}{bd'}$$

Da mesma forma, queremos provar que $\frac{ac}{bd} = \frac{a'c'}{b'd'}$, isto é, $acb'd' = bda'c'$, ou, $(ab')\,(cd') = (dc')\,(a'b)$, que é verdadeiro, pela hipótese acima. □

Vamos agora definir uma relação de ordem em $\mathbb{Q}$ e veremos algumas de suas propriedades.

Definição 27. Sejam $\alpha = \frac{a}{b}$, $\beta = \frac{c}{d} \in \mathbb{Q}$. Dizemos que $\alpha \leq \beta$ se $ad \leq bc$.

A definição é análoga para "$\geq$", "$<$" e "$>$".

A relação dada na Definição 27 é uma relação de ordem, ou seja, é reflexiva, antissimétrica e transitiva. A prova desta afirmação pode ser encontrada em [3].

Observações: os próximos três itens se tratam de algumas notações que fixaremos para evitar uma confusão no restante dos resultados.

i. $0 = \frac{0}{x}, \forall\, x \in \mathbb{Z}^*$. Fixemos $0 = \frac{0}{x_0}$, com x_0 inteiro positivo;

ii. $\alpha = \frac{a}{b} > 0 \Longleftrightarrow ax_0 > b.0$. Isto é, $ax_0 > 0$;

iii. $\alpha = \frac{a}{b} < 0 \Longleftrightarrow ax_0 < b.0$. Isto é, $ax_0 < 0$;

Em $\mathbb{Q}$ não vale o Princípio da Boa Ordem (Teorema 23). Para comprovar esta afirmação, basta perceber que $\mathbb{Q}$ é diferente do vazio e que não possui elemento mínimo pois, para qualquer $m > 0 \in \mathbb{Z}$ $\frac{1}{m} \in \mathbb{Q}$, temos que $\frac{1}{m+1} \in \mathbb{Q}$ e $\frac{1}{m+1} < \frac{1}{m}$. Logo, não vale o princípio da boa ordem.

Proposição 25. *Dados $\alpha, \beta \in \mathbb{Q}$, se $\alpha < \beta$ então $\exists\, \gamma \in \mathbb{Q}$ tal que $\alpha < \gamma < \beta$.*

Demonstração. Para esta proposição basta tomar

$$\gamma = \frac{\alpha + \beta}{2} = \frac{ad + bc}{2bd}.$$

Como $\alpha < \beta$, então $ad < bc$, ou seja, $2ad < ad + bc$. Portanto, $2adb < (ad + bc)b$ e, consequentemente, $\frac{a}{b} < \frac{ad + bc}{2bd}$. Logo, $\alpha < \gamma$. De forma análoga, segue que $\gamma < \beta$. □

4.4 Propriedades do Conjunto dos Racionais

Nesta Seção apresentaremos as principais propriedades do conjunto dos números racionais e faremos a demonstração de algumas destas propriedades.

Proposição 26. *(Propriedade Associativa da Soma) $\alpha + (\beta + \gamma) = (\alpha + \beta) + \gamma$, $\forall\, \alpha, \beta, \gamma \in \mathbb{Q}$.*

Demonstração. Sejam $\alpha = \frac{a}{b}, \beta = \frac{c}{d}, \gamma = \frac{e}{f} \in \mathbb{Q}$. Temos que

$$\alpha + (\beta + \gamma) = \frac{a}{b} + \left(\frac{c}{d} + \frac{e}{f}\right) = \frac{a}{b} + \left(\frac{cf + ed}{df}\right) =$$

$$\frac{a(df) + b(cf + ed)}{b(df)} = \frac{(ad + bc)f + (bd)e}{(bd)f} = \left(\frac{ad + bc}{bd}\right) + \frac{e}{f} = \left(\frac{a}{b} + \frac{c}{d}\right) + \frac{e}{f} = (\alpha + \beta) + \gamma$$

□

Proposição 27. *(Comutativa da Soma)* $\alpha + \beta = \beta + \alpha, \ \forall \ \alpha, \beta \in \ \mathbb{Q}$.

Demonstração. Temos que

$$\alpha + \beta = \frac{a}{b} + \frac{c}{d} = \frac{ad + bc}{bd}.$$

Aplicando a propriedade comutativa dos números inteiros em toda a equação, obtemos

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

□

Proposição 28. *(Existência do Neutro da Soma) Existe um único elemento, que chamaremos neutro aditivo ou zero, e indicaremos por* 0*, tal que* $\alpha + 0 = \alpha$*.*

Demonstração. Considere $n = \frac{0}{y}, y \neq 0$. Vamos mostrar que n é elemento neutro. De fato,

$$\alpha + n = \frac{a}{b} + \frac{0}{y} = \frac{ay + b0}{by} = \frac{ay}{by} = \frac{a}{b},$$

pois $ayb = aby$, ou seja, $(ay, by) \equiv (a, b)$. Logo n é elemento neutro.

Suponhamos agora que $d = \frac{g}{h}$ seja um elemento neutro e consideremos a soma $n + d$, onde $n = \frac{0}{y}$. Temos que $n + d = n$, pois d, por hipótese, é neutro e $n + d = d$ (pois p n é um elemento neutro). Logo, $n = d$. Assim, concluímos que o elemento neutro é único. □

Notemos que $\frac{0}{y}$ é elemento neutro de $\mathbb{Q}$, para todo inteiro y não nulo.

Proposição 29. *(Existência do Oposto) Para cada racional* α *existe um único elemento, que chamaremos de oposto de* α*, e indicaremos por* $-\alpha$*, tal que* $\alpha + (-\alpha) = 0$*.*

Demonstração. Da mesma forma que na demonstração do elemento neutro, tomemos $-\alpha = \dfrac{-a}{b}$. Vamos mostrar que $-\alpha$ é o elemento oposto de α. Temos que

$$\alpha + (-\alpha) = \frac{a}{b} + \frac{-a}{b} = \frac{ab + (-ab)}{b^2} = \frac{0}{b^2} = \frac{0}{b}.$$

Portanto, $-\alpha$ é oposto de α.

Agora, seja ϕ um elemento oposto de α. Então, $\alpha + \phi = \dfrac{0}{m}$, $m \neq 0 \in \mathbb{Z}$. Mas vimos que $\alpha + (-\alpha) = \dfrac{0}{m}$, ou seja, $\alpha + \phi = \alpha + -\alpha$ e, consequentemente, $\phi = -\alpha$. Portanto, o oposto é único. □

Proposição 30. *(Associativa da Multiplicação) $\alpha(\beta\gamma) = (\alpha\beta)\gamma$, $\forall\ \alpha, \beta, \gamma \in \mathbb{Q}$.*

Demonstração. Temos

$$\alpha(\beta\gamma) = \frac{a}{b}\left(\frac{c}{d}\frac{e}{f}\right) = \frac{a}{b}\left(\frac{ce}{df}\right) = \frac{a(ce)}{b(df)} = \frac{(ac)e}{(bd)f} = \left(\frac{ac}{bd}\right)\frac{e}{f} = \left(\frac{a}{b}\frac{c}{d}\right)\frac{e}{f} = (\alpha\beta)\gamma.$$

□

Proposição 31. *(Existência do Inverso) Para cada racional $\alpha \neq 0$, existe um único elemento que chamaremos de inverso de α, e denotaremos por α^{-1}, tal que $\alpha\alpha^{-1} = 1$.*

Demonstração. Dado $\alpha = \dfrac{a}{b} \neq 0$, temos que $a \neq 0$. Logo, $\dfrac{b}{a}$ também é um número racional. Mostraremos que $\alpha^{-1} = \dfrac{b}{a}$.

Como efeito temos que

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

Mostraremos a unicidade do inverso de α. Seja α' um elemento de $\mathbb{Q}$ tal que $\alpha\alpha^{'} = 1$. Temos

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

□

Veremos agora que, para todo α em $\mathbb{Q}$, temos que $\alpha \cdot 0 = 0$. De fato, seja $\alpha = \dfrac{a}{b} \in \mathbb{Q}$. Sabemos que o elemento $\dfrac{0}{y}$ é o elemento neutro de $\mathbb{Q}$, para qualquer $y \neq 0$. Assim,

$$\frac{a}{b} \cdot 0 = \frac{a}{b} \cdot \frac{0}{y} = \frac{a0}{by} = \frac{0}{by} = 0.$$

Proposição 32. *(Comutativa da Multiplicação) $\alpha\beta = \beta\alpha$, $\forall\ \alpha, \beta \in \mathbb{Q}$.*

Demonstração. Temos que

$$\alpha\beta = \frac{a}{b} \cdot \frac{c}{d} = \frac{ab}{cd} = \frac{ba}{dc} = \frac{b}{c} \cdot \frac{a}{b} = \beta\alpha.$$

□

No início deste capítulo, foi abordado um pouco de quais teriam sido as motivações para a extensão do conjunto dos inteiros ou porque ele não seria suficiente, dessa maneira podemos pensar que um dos problemas seria como resolver uma equação do tipo $bX = a$, onde a não é múltiplo de b, aqui podemos pensar em $a = 3$ e $b = 2$ qual valor de X teríamos que ter para encontrar a igualdade $bX = a$ se pensarmos nos números inteiros nossa equação não tem solução, já que $X = \frac{3}{2}$ e esse número não pertence a $\mathbb{Z}$. Mas se tratando dos números racionais isso muda e de fato veremos que em $\mathbb{Q}$ se $a, b \in \mathbb{Q}$ a equação $bX = a$ tem solução em $\mathbb{Q}$.

Teorema 4.2. Toda equação da forma $\beta X = \alpha$, onde $\alpha, \beta \in \mathbb{Q}$ e $\beta \neq 0$, tem solução em $\mathbb{Q}$. Além disso, essa solução é única.

Demonstração. Como $\beta \neq 0$, pela Proposição 31 sabemos que ele possui um inverso β^{-1}, tal que $\beta\beta^{-1} = 1 = \beta^{-1}\beta$. Nosso objetivo será mostrar que $\gamma = \beta^{-1}\alpha$ é a solução para a equação.

Primeiramente, vamos substituir γ na equação dada. Temos

$$\beta\gamma = \beta(\beta^{-1}\alpha) = (\beta\beta^{-1})\alpha = 1\alpha = \alpha.$$

Agora, suponhamos que $x \in \mathbb{Q}$ seja outra solução para a equação, ou seja, $\beta x = \alpha$. Multiplicando ambos os lados por β^{-1} obtemos

$$\beta^{-1}\beta x = \beta^{-1}\alpha = \gamma \Longrightarrow x = \gamma.$$

Portanto, a solução é única. □

Provamos que a equação $\beta X = \alpha$ tem solução sempre que $\alpha, \beta \in \mathbb{Q}$ e $\beta \neq 0$. Lembremos que, no caso do conjunto dos inteiros, uma equação do tipo $aX = b$, com $a, b \in \mathbb{Z}$, nem sempre tem solução (apenas quando b *divide* a).

Um solução óbvia para esse caso seria tomarmos $X = \frac{b}{a}$. Mas, olhando com um pouco mais de cuidado, em nenhum momento definimos o que seria o produto entre um inteiro e um racional. O conjunto dos números racionais foi construído a partir de uma relação de equivalência entre números inteiros. Assim, podemos dizer em certo sentido que inteiros e racionais são elementos com uma "natureza" diferente.

Esse impasse pode ser resolvido fazendo algo semelhante com o que aconteceu com os inteiros, onde encontramos neste conjunto uma "cópia" dos naturais. Para isso, consideremos o conjunto

$$\bar{\mathbb{Z}} = \left\{ \frac{a}{1} |\ a \in\ \mathbb{Z} \right\}.$$

Observemos que esse conjunto é um subconjunto de $\mathbb{Q}$. Consideremos a função

$$\phi : \mathbb{Z} \longrightarrow \bar{\mathbb{Z}}$$

$$a \in \mathbb{Z} \longmapsto \frac{a}{1} \in \bar{\mathbb{Z}}$$

Afirmamos que ϕ é bijetora e que ela preserva as operações, isto é

i. $\phi(a + b) = \phi(a) + \phi(b)\ \forall\ a, b \in\ \mathbb{Z}$;

ii. $\phi(ab) = \phi(a)\phi(b)\ \forall\ a, b \in\ \mathbb{Z}$.

Vejamos a prova de que ϕ é bijetora.

Proposição 33. *A função ϕ definida anteriormente é bijetora.*

Demonstração. Sejam $a, b \in \mathbb{Z}$ tais que $\phi(a) = \phi(b)$. Então,$\dfrac{a}{1} = \dfrac{b}{1}$. Mas isso nos diz que

$$\overline{(a, 1)} \equiv \overline{(b, 1)} \Rightarrow a.1 = b.1 \Rightarrow a = b.$$

Logo, ϕ é injetiva.

Agora seja $\dfrac{b}{1} \in\ \bar{\mathbb{Z}}$. Exibiremos $a \in\ \mathbb{Z}$ tal que $\phi(a) = \dfrac{b}{1}$. Para isso, tome $a = b$. Logo, $\phi(a) = \phi(b) = \dfrac{b}{1}$. Portanto, a função ϕ é sobrejetora.

Como ϕ é sobrejetora e injetora, temos que ela é bijetora. □

Dessa forma, sempre que não houver perigo de confusão, não haverá necessidade de distinguirmos m da sua imagem em $\overline{\mathbb{Z}}$, que seria $\dfrac{m}{1}$. Ou seja,

$$m + \frac{a}{b} \quad \text{e} \quad m \cdot \frac{a}{b}$$

indicarão, respectivamente,

$$\frac{m}{1} + \frac{a}{b} \quad \text{e} \quad \frac{m}{1} \cdot \frac{a}{b}.$$

Com base no que foi apresentado podemos concluir que $\mathbb{Q}$ é um corpo. Veremos a seguir um resultado para finalizarmos este capítulo, onde mostraremos que $\mathbb{Q}$ é um corpo ordenado.

Proposição 34. ($\mathbb{Q}$ *é ordenado*). *Seja* $P = \{\overline{(a,b)} \in \mathbb{Q} |\ ab >_{\mathbb{Z}} 0\}$*, onde* $>_{\mathbb{Z}}$ *é a relação de ordem definida nos inteiros. O conjunto* P *faz com que* $\mathbb{Q}$ *seja ordenado.*

Demonstração. Sejam $x = \overline{(a,b)}$ e $y = \overline{(c,d)}$ elementos de P. Assim,

$$ab >_{\mathbb{Z}} 0 \ \text{ e } \ cd >_{\mathbb{Z}} 0.$$

Além disso, sabemos que $d \neq 0$ e $b \neq 0$ e, assim, $d^2 > 0$ e as propriedades de ordem em $\mathbb{Z}$ se verificam, ou seja,

- $x + y = \overline{(ad + bc, bd)} \in P$, pois $(ad + bc)bd = abd^2 + b^2cd$ e, como $cd, ab >_{\mathbb{Z}} 0$, e tendo $b, d \neq 0$ $(b^2, d^2 > 0)$ conclui-se $(ad + bc)bd > 0$
- $x \cdot y = \overline{(ac, bd)} \in P$, pois $(ac)(bd) >_{\mathbb{Z}} 0$, já que $ac, bd >_{\mathbb{Z}} 0$ por hipótese.

Dessa maneira, a adição e multiplicação são fechadas em P. Resta mostrar a tricomia. Seja $\overline{(a,b)} \in \mathbb{Q}$. Então, $ab \in \mathbb{Z}$. Pela tricotomia em $\mathbb{Z}$, temos que

$$\text{ou } ab >_{\mathbb{Z}} 0 \text{ ou } ab = 0 \text{ ou } ab <_{\mathbb{Z}} 0.$$

Por conseguinte,

$$\text{ou } \overline{(a,b)} \in P \text{ ou } \overline{(a,b)} = \overline{(0,b)} = 0 \text{ ou } \overline{(-a,b)} \in P,$$

isto é,

$$\text{ou } \overline{(a,b)} \in P \text{ ou } \overline{(a,b)} = 0 \text{ ou } -\overline{(a,b)} \in P.$$

Portanto, $\mathbb{Q}$ é ordenado.

□

5 Construção dos Números Reais

O objetivo deste capítulo é construir o conjunto dos números reais de uma forma mais rigorosa, comparado ao que é ensinado no contexto escolar, onde diz-se simplesmente que a cada ponto de uma reta está associado um número real. Pensando nos conjuntos já construídos (naturais, inteiros e racionais), pode-se pensar, por exemplo, que há pontos que não correspondem a números racionais (podemos verificar isso utilizando a diagonal de um quadrado de lado 1). A esses pontos correspondem o que chamamos de números irracionais. Assim como nas construções anteriores, utilizaremos um conjunto como base, neste caso o conjunto dos números racionais. Dois matemáticos foram responsáveis por fazer tal construção utilizando métodos diferentes. São eles: Cantor e Dedekind. Enquanto Cantor utilizou **Classes de Equivalência de Sequências de Cauchy**, Dedekind utilizou a noção de **Cortes**, o que deu origem ao que conhecemos por **Cortes de Dedekind**.

5.1 Preliminares

Veremos nesta seção alguns resultados que serão necessários para o bom entendimento da construção dos números reais. Para consultar mais informações sobre o tema, veja [6], [5], [7].

Sejam K *e* K' dois corpos. Dizemos que uma função $f : K \longrightarrow K'$ é um homomorfismo de K em K' se satisfaz as seguintes condições:

1. $f(x + y) = f(x) + f(y), \ \forall \ x, y \in K$
2. $f(x \cdot y) = f(x) \cdot f(y), \ \forall \ x, y \in K$

Se $f : K \longrightarrow K'$ é um homomorfismo bijetivo dizemos que f é um isomorfismo de K sobre K' e dizemos que K e K' são isomorfos (denotamos por $K \simeq K'$) se existir um isomorfismo de K sobre K'.

Definição 28. Um conjunto X é dito enumerável quando é finito ou quando existe uma bijeção $f : \mathbb{N} \longrightarrow X$. Neste caso, dizemos que f é uma enumeração dos elementos de X.

Vamos introduzir agora o conceito de sequência de números racionais. Uma sequência de números racionais é uma função $x : \mathbb{N} \longrightarrow \mathbb{Q}$. Denotaremos uma sequência de números racionais por

$$(x_n) \text{ ou } (x_1, x_2, x_3, \ldots, x_n, \ldots).$$

Exemplo 3. A sequência definida por $x_n = \dfrac{1}{n}$ é uma sequência de números racionais, e será de grande ajuda em muitos exemplos dessa seção.

Exemplo 4. Sabemos que no conjunto dos racionais não existe um número racional cujo quadrado é dois, assim podemos definir duas sequências, z_n e y_n, do seguinte modo: $z_n =$ Maior número racional cujo quadrado é menor que dois. Assim, os números de (z_n) são escritos, na forma de fração utilizando o denominador como potências de dez, como

$$(z_n) = \left(1, \frac{14}{10}, \frac{141}{100}, \frac{1414}{1000}, \frac{14142}{10000}, \frac{141421}{100000}, \frac{1414213}{1000000}, \dots\right)$$

$y_n =$ Menor número racional cujo quadrado é maior que dois. Assim, os números de (y_n) são escritos, na forma de fração utlizando o denominador como potências de dez, como

$$(y_n) = \left(2, \frac{15}{10}, \frac{142}{100}, \frac{1415}{1000}, \frac{14143}{10000}, \frac{141422}{100000}, \frac{1414214}{1000000}, \dots\right)$$

As sequências estão bem definidas, pois tomando um elemento da sequência $z_{n_0} = 1,41\dots a_0$ encontramos o termo seguinte z_{n_0+1} acrescentando um dígito d ao número z_{n_0}. Assim, temos o número $1,41\dots a_0 d$, e o dígito $d \in \{0,1,2,3,4,5,6,7,8,9\}$. Temos dois casos a considerar:

Caso 1: se para todo $d \in \{0,1,2,3,4,5,6,7,8,9\}$ tivermos $z^2_{n_0+1} < 2$ então $d = 9$. Nessa situação já estará definido o número $y_{n_0+1} = 1,41\dots(b_0+1)\,d'$ tal que $d' = 0$.

Caso 2: se para algum dígito $d \in \{0,1,2,3,4,5,6,7,8,9\}$ tivermos $z^2_{n_0+1} > 2$ então $d-1$ será o dígito que devemos acrescentar a z_{n_0}, e também já estaremos definindo o número $y_{n_0+1} = 1,41\dots b_0 d$.

As duas sequências são construídas recursivamente por meio do processo explicado acima.

O procedimento teria fim se existisse um número racional cujo quadrado é dois, mas isso é um absurdo.

Dada uma sequência racional (x_n), se existir um número racional M de modo que todo elemento da sequência racional (x_n), for menor ou igual a M, diremos que (x_n) é uma sequência limitada superiormente e M é uma cota superior do conjunto formado pelos elementos da sequência.

Exemplo 5. A sequência racional definida por $x_n = \dfrac{1}{n}$ é limitada superiormente, pois todos os seus termos são menores que 2, logo o número racional 2 é uma cota superior para o conjunto $X = \left\{1, \dfrac{1}{2}, \dfrac{1}{4}, \dots\right\}$.

De forma análoga podemos dizer que uma sequência racional (x_n) é limitada inferiormente se existe um m de modo que todo elemento da sequência (x_n) for maior ou igual a m, diremos que m é uma cota inferior do conjunto formado pelos elementos da sequência.

Uma sequência racional (x_n) será limitada quando for simultaneamente limitada superiormente e inferiormente.

Algumas sequências apresentam um comportamento regular quando as observamos através da relação de ordem. Considerando (x_n) uma sequência, ela pode se comportar de diversas maneiras, em particular veremos quatro dessas. São elas:

1. Para todo $n \in \mathbb{N}$, $x_n < x_{n+1}$. Sequências que apresentam esse comportamento são ditas monótonas crescentes.

2. Para todo $n \in \mathbb{N}$, $x_n \leq x_{n+1}$. Sequências que apresentam essa estrutura são ditas monótonas não-decrescentes.

3. Para todo $n \in \mathbb{N}$, $x_n > x_{n+1}$. Tais sequências são ditas monótonas decrescentes.

4. Para todo $n \in \mathbb{N}$, $x_n \geq x_{n+1}$. Sequências que apresentam esse comportamento são ditas monótonas não-crescentes.

Definição 29. Uma sequência racional de Cauchy é uma sequência de números racionais (x_n) tal que, dado qualquer número racional positivo ϵ, todos os termos a partir de um certo termo de índice n_ϵ diferem entre si por um número racional inferior a ϵ. Matematicamente,

$$\text{Dado } \epsilon > 0 \text{ existe } n_\epsilon \in \mathbb{N} \text{ tal que } n, m > n_\epsilon \Rightarrow |x_m - x_n| < \epsilon.$$

Exemplo 6. A sequência $(x_n)_n$ tal que $x_n = \dfrac{1}{n}$ é de Cauchy. De fato, dado $0 < \epsilon \in \mathbb{Q}$, pela propriedade arquimediana existe um número natural n_e tal que $n_e \cdot \epsilon > 2$. Ou, ainda, temos que $n_e > \dfrac{2}{\epsilon}$, que por sua vez equivale a $\dfrac{1}{n_e} < \dfrac{\epsilon}{2}$. Portanto, para todo $m, n > n_e$ tem-se

$$|x_m - x_n| = |x_m + (-x_n)| \leq |x_m| + |-x_n| = |x_m| + |x_n|,$$

pela desigualdade triângular dos números racionais e a propriedade de módulo, $|-r| = |r|$, onde $r \in \mathbb{Q}$. Por outro lado, como $m > n_\epsilon$ e $n > n_\epsilon$ equivalem a $\dfrac{1}{m} < \dfrac{1}{n_\epsilon}$ e $\dfrac{1}{n} < \dfrac{1}{n_e}$, conclui-se que

$$|x_m - x_n| = |x_m + (-x_n)| \leq |x_m| + |x_n| = \frac{1}{m} + \frac{1}{n} < \frac{\epsilon}{2} + \frac{\epsilon}{2} = \epsilon.$$

Portanto, $(x_n)_n$ é de Cauchy.

Teorema 5.1. Toda sequência racional monótona limitada é de Cauchy.

Demonstração. Ver **Teorema** 1.1 em [6]. □

Teorema 5.2. Toda sequência de Cauchy é limitada.

Demonstração. Ver em [6]. □

Existem algumas sequências racionais cujos termos apresentam uma propriedade com relação a um número racional de modo específico. Tal propriedade é o que chamamos de convergência. Diremos que uma sequência racional (x_n) é convergente se:

$$\forall\ \epsilon > 0,\ \exists n_\epsilon \in \mathbb{N}\ \textit{tal que}\ n > n_\epsilon \Rightarrow |x_n - r| < \epsilon.$$

Assim, $r \in \mathbb{Q}$ é chamado limite da sequência racional (x_n) e dizemos que a sequência (x_n) converge para o número racional r. Assim, se r existir, diremos que a sequência $(x_n)_n$ converge para o número racional r ou que o número racional r é limite da sequência racional $(x_n)_n$. Outras notações para essa propriedade são: $\lim\limits_{n\to\infty} x_n = r$ ou $x_n \longrightarrow r$.

Exemplo 7. A sequência racional (x_n) definida por $x_n = \dfrac{1}{n}$ converge para o número racional zero. De fato, dado o número racional $\epsilon > 0$, tomando $n_e = \left\lfloor \dfrac{1}{\epsilon} \right\rfloor + 1$ teremos que, se $n > n_e$ então

$$n > n_e \Rightarrow n > \left\lfloor \frac{1}{\epsilon} \right\rfloor + 1 \Rightarrow n > \frac{1}{\epsilon} \Rightarrow n \cdot \epsilon > 1 \Rightarrow \frac{1}{n} < \epsilon \Rightarrow \left|\frac{1}{n}\right| < \epsilon \Rightarrow \left|\frac{1}{n} - 0\right| < \epsilon.$$

Portanto, $\lim\limits_{n\to\infty} \dfrac{1}{n} = 0$.

Teorema 5.3. Toda sequência racional convergente é de Cauchy.

Demonstração. Ver em [6]. □

Seja (x_n) uma sequência de números racionais, diremos que uma subsequência de (x_n) é a restrição da função (x_n) a um subconjunto infinito $\mathbb{N}' = \{n_1 < n_2 < n_3 < \ldots < n_i < \ldots\}$ de números naturais. Indicamos uma subsequência de (x_n) por (x_{n_k}).

Teorema 5.4. Uma sequência de Cauchy que possui uma subsequência convergente para um número racional é convergente (este resultado é mais geral e conhecido como Teorema de Bolzano-Weierstrass).

Demonstração. Ver em [6]. □

5.2 Método de Dedekind

A primeira forma de construção dos reais será feita através do chamado método de Dedekind. Para isso, precisaremos definir o que é um corte, suas propriedades, e consideraremos o conjunto de todos os Cortes. Para tal conjunto definiremos duas operações, adição e multiplicação, e uma relação de ordem. Mostraremos que esse conjunto possui as propriedades aritméticas de $\mathbb{Q}$ e uma propriedade que $\mathbb{Q}$ não possui, que é a propriedade de ser completo. A esse conjunto de cortes chamaremos de números reais e ele será representado por $\mathbb{R}$. Como nas construções anteriores, veremos que $\mathbb{R}$ contém uma cópia de $\mathbb{Q}$.

Definição 30. Um conjunto α de números racionais diz-se um corte se satisfizer as seguintes condições:

i. $\emptyset \neq \alpha \neq \mathbb{Q}$;

ii. se $r \in \alpha$ e $s < r$ (s racional), então $s \in \alpha$;

iii. em α não existe elemento máximo.

Exemplo 8. O conjunto $A = \left\{x \in \mathbb{Q} \mid x < \frac{3}{5}\right\}$ é um corte.

Vamos verificar que realmente o conjunto A satisfaz as propriedades de corte:

i. $A \neq \emptyset$, pois $0 \in A$; $A \neq \mathbb{Q}$ pois $1 \in \mathbb{Q}$, e $1 \notin A$;

ii. Seja $r \in A$ e $s < r$. Assim, $s < r < \frac{3}{5}$, ou seja, $s < \frac{3}{5}$. Portanto $s \in A$;

iii. Suponhamos que em A exista um elemento máximo m. Logo $r < m, \forall r \in A$, e $m < \frac{3}{5}$, já que $m \in A$. Mas, já vimos na Proposição 25, que entre dois números racionais existe um outro racional. Neste caso,

$$m < \frac{m + \frac{3}{5}}{2} < \frac{3}{5},$$

o que contradiz a maximalidade de m. Logo, A não tem elemento máximo e, portanto, A é um corte.

Exemplo 9. O conjunto $B = \left\{x \in \mathbb{Q} \mid x > \frac{3}{5}\right\}$ não é um corte. De fato vamos ver qual propriedade esse conjunto não satisfaz.

i. $B \neq \emptyset$, pois $1 \in B$; $B \neq \mathbb{Q}$, pois $0 \notin B$;

ii. Seja $r \in B$ e $s < r$. Tomemos $r = 1$ e $s = 0$, assim $s < r$ mas $s \notin B$.

Portanto, B não é um corte.

Exemplo 10. O conjunto $C = \left\{x \in \mathbb{Q} \mid x \leq \frac{3}{5}\right\}$ não é um corte.

Pois $x = \frac{3}{5}$ é elemento máximo de C contradizendo o item (*iii.*) da Definição 30.

Proposição 35. *Sejam α um corte e $r \in \mathbb{Q}$. Então r é cota superior de α se, e somente se, $r \in \mathbb{Q} \backslash \alpha$.*

Demonstração. Se r é cota superior de α, temos que r não pode pertencer a α, pois, se pertencesse, ele seria o elemento máximo de α, o que contradiz a definição de corte. Assim, $r \in \mathbb{Q} \backslash \alpha$. Reciprocamente, suponhamos que $r \in \mathbb{Q} \backslash \alpha$, mas r não é cota superior de α. Então, existe $s \in \alpha$ tal que $r < s$. Mas pela definição de corte, segue que $r \in \alpha$, uma contradição. $\square$

Proposição 36. *Se $r \in \mathbb{Q}$ e $\alpha = \{x \in \mathbb{Q} \mid x < r\}$, então α é um corte e r é a menor cota superior de α.*

Demonstração. Vamos demonstrar que α satisfaz as condições necessárias para ser um corte:

1. $\alpha \neq \emptyset$ pois $x = r - 1 \in \alpha$ e $r \neq \mathbb{Q}$ pois $r \notin \alpha$;
2. Seja $s \in \alpha$ e $t < s$. Como $s \in \alpha$ temos que $s < r$. Mas $t < s$, o que implica $t < r$. Logo $t \in \alpha$;
3. Basta observamos que, dado $s \in \alpha$, $s < \dfrac{s+r}{2} < r$. Mas como $\dfrac{s+r}{2} \in \mathbb{Q}$, segue que $\dfrac{s+r}{2} \in \alpha$. Assim, s não é o elemento máximo de α.

Agora, seja t uma cota superior de α tal que $t < r$. Por definição de α, temos que $t \in \alpha$ é cota superior, então t é o elemento máximo. Mas isso contradiz a condição de um corte não ter elemento máximo, ou seja, $r \leq t$ para toda cota superior t de α e, portanto, r é a menor cota superior de α. $\square$

Definição 31. Os cortes definidos pela Proposição 36 são chamados de cortes racionais e serão representados por r^*.

Proposição 37. *Todo corte que possui cota superior mínima é racional.*

Demonstração. Suponha α um corte com cota superior mínima r, ou seja, $x \leq r,\ \forall\, x \in \alpha$. Sabemos que $r \notin \alpha$, pois sendo cota superior mínima e pertencendo a α, ele seria o elemento máximo do conjunto, contradizendo a definição de corte. Logo, $x < r\ \forall,\ x \in \alpha$. Além disso, como r é a menor das cotas superiores, dado qualquer $s \in \mathbb{Q}$ tal que $s < r$, s não será cota superior de α, ou seja, $s \in \alpha$. Portanto, se r é cota superior mínima, temos que $\alpha = \{t \in \mathbb{Q} \mid t < r\}$, ou seja α é um corte racional. $\square$

Teorema 5.5. Seja $\alpha = \{x \in \mathbb{Q}_+ \mid x^2 < 2\} \cup \mathbb{Q}_-^*$. Então α é um corte que não é racional.

Demonstração. Vamos demonstrar que α é um corte:

1. $\alpha \neq \emptyset$, pois $0 \in \alpha$, e $\alpha \neq \mathbb{Q}$, pois $2 \in \mathbb{Q}$ e $2 \notin \alpha$;

2. Seja $r \in \alpha$ e $s < r$. Assim,

   - Se $s \leq 0$ então $s \in \alpha$;
   - Se $s > 0$, como $s < r$ e $r^2 < 2$, então $s^2 < 2$, pois $s^2 < rs$ e $rs < r^2$, logo $s^2 < r^2 < 2$. Portanto, $s \in \alpha$.

3. Vamos mostrar que, para cada $r \in \alpha$, conseguimos encontrar um racional $s \in \alpha$ tal que $r < s$. Suponhamos, então, que $r \in \alpha$, ou seja, $r^2 < 2$.

   - Se $r \leq 0$, então $s = 1 \in \alpha$ e $r < s$.
   - Suponhamos então $r \geq 0$ e $r^2 < 2$. Seja $h \in \mathbb{Q}$ tal que $0 < h < 1$ e $h < \dfrac{2 - r^2}{2r + 1}$. Podemos afirmar que tal h existe pelo fato de $\mathbb{Q}$ ser arquimediano. Seja agora $s = r + h$. Assim, $s \in \mathbb{Q}$ e $s > r$.

     Temos que $s^2 = r^2 + h^2 + 2rh$.

     Como $0 < h < 1$, $s^2 < r^2 + (1 + 2r)h$, e tomando $h < min\left\{1, \dfrac{2 - r^2}{2r + 1}\right\}$, obtemos que $s^2 < r^2 + (2 - r^2) = 2$. Logo, $s \in \alpha \; e \; s > r$. Assim, α não possui elemento máximo.

Dessa maneira, temos que α é um corte.

Agora precisamos provar que α não possui cota superior mínima. Observemos que os racionais que não pertencem a α são os positivos que possuem quadrado maior ou igual a 2. Sabemos ainda que não existe racional cujo quadrado é 2. Assim,

$$y \in \mathbb{Q} \backslash \alpha \Leftrightarrow y > 0, \; y^2 > 2.$$

Pela Proposição 35, todo elemento $y \in \mathbb{Q} \backslash \alpha$ é maior que qualquer elemento $w \in \alpha$. Mostraremos então que, dado $y \in \mathbb{Q} \backslash \alpha$, existe $t \in \mathbb{Q} \backslash \alpha$, com $t < y$, sendo exatamente o que queremos mostrar. Vamos buscar um h racional positivo tal que $(y - h)^2 > 2$, e seja $t = y - h$. Suponhamos, sem perda de generalidade, $h < 1$. Sabemos que $(y - h)^2 > 2$ equivale a $y^2 - 2rhy + h^2 > 2$, ou $y^2 - h(2y - h) > 2$, ou ainda $h < \dfrac{y^2 - 2}{2y - h}$, pois $2y - h > 0$ (basta ver que $y > 1$ e $h < 1$). Como $h > 0$, temos que $\dfrac{y^2 - 2}{2y - h} > \dfrac{y^2 - 2}{2y}$. Assim, tomando $h < min\left\{1, \dfrac{y^2 - 2}{2y}\right\}$ (podemos fazer isso pois $\mathbb{Q}$ é arquimediano), obtemos

$$(y - h)^2 = y^2 - 2hy + h^2 > y^2 - 2y\frac{y^2 - 2}{2y} + h^2 = 2 + h^2 > 2.$$

□

5.2.1 Relação de ordem e operações com cortes

Vamos denotar por C o conjunto de todos os corte e nele definir duas operações, "+" e "." e uma relação de ordem. Começaremos introduzindo a relação de ordem, já que ela será indispensável para a definição da multiplicação.

Definição 32. Sejam $\alpha, \beta \in \mathsf{C}$. Dizemos que α é menor do que β e escrevemos $\alpha < \beta$ quando $\beta \backslash \alpha \neq \emptyset$. Nos casos "$\geq$", "$\leq$" e "$>$", a definição é análoga.

Exemplo 11. a) $4^* > \left(\frac{3}{5}\right)^*$, pois $2 \in 4^* \backslash \left(\frac{3}{5}\right)^*$;

b) $(-3)^* < 0^*$, pois $-1 \in 0^* \backslash (-3)^*$;

c) Se α é o corte dado no Teorema 5.5, então $\alpha < 2^*$, pois $\frac{18}{10} \in 2^* \backslash \alpha$.

Definição 33. Um corte $\alpha \in \mathsf{C}$ é chamado de corte positivo se $\alpha > 0^*$. Se $\alpha < 0^*$, α é dito corte negativo. Se $\alpha \geq 0^*$, chama-se não negativo. Se $\alpha \leq 0^*$, α é dito corte não positivo.

Proposição 38. *Para $\alpha, \beta \in \mathsf{C}$ valem as seguintes equivalências:*

1. $\alpha < \beta \Leftrightarrow \alpha \subset \beta$ *e* $\alpha \neq \beta$;

2. $\alpha \leq \beta \Leftrightarrow \alpha \subset \beta$.

Demonstração. Vamos demonstrar o item 1:

($\Rightarrow$) Suponha $\alpha < \beta$. Então existe $p \in \beta$ tal que $p \notin \alpha$. Claramente, temos $\alpha \neq \beta$. Suponha agora que $\alpha \not\subset \beta$, ou seja, existe $p \in \alpha$ tal que $p \notin \beta$. Mas isso é um absurdo pois, por definição, se isso ocorre, $\beta < \alpha$. Portanto, $\alpha \subset \beta$.

($\Leftarrow$) Se $\alpha \subset \beta$ e $\alpha \neq \beta$, então existe p em β tal que p não está em α, ou seja, $\alpha < \beta$.

Agora vamos demonstrar o item 2:

($\Leftarrow$) Suponhamos $\alpha \leq \beta$, isto é $\alpha = \beta$ ou $\alpha < \beta$. Se $\alpha < \beta$, pelo item anterior, $\alpha \subset \beta$. Agora, se $\alpha = \beta$, claramente $\alpha \subset \beta$.

($\Rightarrow$) Supondo que $\alpha \subset \beta$, pelo item anterior $\alpha < \beta$, isto é, $\alpha \leq \beta$. □

Teorema 5.6. Tricotomia: Para $\alpha, \beta \in \mathsf{C}$, temos que uma, e apenas uma, das possibilidades a seguir ocorre:

$$\alpha = \beta \text{ ou } \alpha < \beta \text{ ou } \alpha > \beta.$$

Demonstração. Notemos que $\alpha = \beta$ exclui as outras duas possibilidades, pela definição de igualdade de conjuntos. Da mesma forma, $\alpha < \beta$ e $\alpha > \beta$ excluem a possibilidade de $\alpha = \beta$ pela Proposição 38. Queremos mostrar, então, que as desigualdades se excluem mutuamente. Para isso, suponhamos o contrário, isto é, que $\alpha < \beta$ e $\alpha > \beta$ ocorram de forma simultânea. Assim, existem $t \in \beta \backslash \alpha$ e $u \in \alpha \backslash \beta$. De $t \in \beta$ e $u \notin \beta$, temos que $t < u$. Por outro lado, de $u \in \alpha$ e $t \notin \alpha$, resulta em $u < t$, contradizendo a lei da tricotomia em $\mathbb{Q}$. Logo, ocorre no máximo uma das três possibilidades. Precisamos ainda verificar que, necessariamente, uma delas ocorre. Se $\alpha = \beta$, não é necessário provar nada. Suponhamos, então, que $\alpha \neq \beta$. Então, $\alpha \backslash \beta \neq \emptyset$ ou $\beta \backslash \alpha \neq \emptyset$ (pois, caso contrário $\alpha = \beta$). No primeiro caso temos que $\beta > \alpha$ e, no segundo, $\alpha < \beta$. □

Teorema 5.7. A relação $\leq$ é uma relação de ordem em C.

Demonstração. Provaremos que as propriedades reflexiva, antissimétrica e transitiva valem.

1. Reflexiva: seja $\alpha \in \mathsf{C}$. Facilmente percebemos que $\alpha = \alpha$, portanto $\alpha \leq \alpha$;

2. Antissimétrica: sejam $\alpha, \beta \in \mathsf{C}$ tal que $\alpha \leq \beta$ e $\beta \leq \alpha$. Pela tricotomia temos que $\alpha = \beta$;

3. Transitiva: sejam α, β *e* $\gamma \in \mathsf{C}$, tais que $\alpha \leq \beta$ e $\beta \leq \gamma$. Assim:

$$\begin{cases} \alpha \leq \beta \Rightarrow \alpha \subset \beta \\ \beta \leq \gamma \Rightarrow \beta \subset \gamma \end{cases}.$$

   Como a inclusão de conjuntos é transitiva, de $\alpha \subset \beta$ e $\beta \subset \gamma$ segue que $\alpha \subset \gamma$. Logo $\alpha \leq \gamma$.

□

Vamos introduzir agora as operações de adição e multiplicação em C. Começamos com o seguinte teorema:

Teorema 5.8. Sejam $\alpha, \beta \in \mathsf{C}$. Se $\gamma = \{r + s |\ r \in \alpha \ e \ s \in \beta\}$, então $\gamma \in \mathsf{C}$.

Demonstração. Queremos mostrar que γ satisfaz as três condições para ser corte.

1. Como $\alpha \neq \emptyset$ e $\beta \neq \emptyset$, então $\gamma \neq \emptyset$. Tomemos $t \in \mathbb{Q} \backslash \alpha$ e $u \in \mathbb{Q} \backslash \beta$. Assim, $t > r$, $\forall r \in \alpha$ e $u > s$, $\forall s \in \beta$. Portanto, $t + u > r + s$, $\forall r \in \alpha$, $s \in \beta$. Assim, $t + u \notin \gamma$ e, consequentemente, $\gamma \neq \mathbb{Q}$;

2. Sejam $r \in \gamma$ e $s \in \mathbb{Q}$ tais que $s < r$. Veremos que $s \in \gamma$. Sabemos que r é do tipo $p + q$, onde $p \in \alpha$ e $q \in \beta$. Então, $s < p + q$ e podemos escrever $s = p + q'$, com $q' < q$ e, portanto, $q' \in \beta$. Logo $s = p + q'$, com $p \in \alpha$ e $q' \in \beta$, ou seja, $s \in \gamma$;

3. Provemos que γ não possui elemento máximo. Seja $r \in \gamma$. Temos que $r = p + q$, com $p \in \alpha$ e $q \in \beta$. Como existe $p' \in \alpha$ tal que $p < p'$, o racional $s = p' + q \in \gamma$ e $s > r$.

□

Definição 34. Para $\alpha, \beta \in \mathsf{C}$, definimos $\alpha + \beta$ como sendo o corte dado no Teorema 5.8, isto é,

$$\alpha + \beta = \{r + s | \ r \in \alpha \text{ e } s \in \beta\}.$$

Teorema 5.9. A adição em C é comutativa, associativa e tem 0^* como elemento neutro.

Demonstração.

1. Comutatividade: sejam $\alpha, \beta \in \mathsf{C}$. Queremos mostrar que $\alpha + \beta = \beta + \alpha$. Dessa forma, seja $r + s \in \alpha + \beta$, assim $r \in \alpha$ e $s \in \beta$. Mas sabemos que a propriedade comutativa é válida em $\mathbb{Q}$, ou seja, $r + s = s + r$ em $\mathbb{Q}$. Além disso, $s + r \in \beta + \alpha$, ou seja, temos que $r + s \in \beta + \alpha$. Portanto, $\alpha + \beta \subset \beta + \alpha$. De forma análoga vemos que $\beta + \alpha \subset \alpha + \beta$. Logo, $\alpha + \beta = \beta + \alpha$.

2. Associatividade: sejam α, β *e* $\gamma \in \mathsf{C}$. Queremos provar que $\alpha + (\beta + \gamma) = (\alpha + \beta) + \gamma$. Seja $r + (s + t) \in \alpha + (\beta + \gamma)$ $r \in \alpha, \ s \in \beta, \ t \in \gamma$. Temos que a propriedade associativa é válida em $\mathbb{Q}$, isto é, $r + (s + t) = (r + s) + t$. Temos ainda que $(r + s) + t \in (\alpha + \beta) + \gamma$, dessa maneira $r + (s + t) \in (\alpha + \beta) + \gamma$, portanto $\alpha + (\beta + \gamma) \subset (\alpha + \beta) + \gamma$. De forma análoga concluimos que $(\alpha + \beta) + \gamma \subset \alpha + (\beta + \gamma)$. Logo, $\alpha + (\beta + \gamma) = (\alpha + \beta) + \gamma$.

3. Elemento Neutro: queremos provar que $\alpha + 0^* = \alpha, \ \forall \alpha \in \mathsf{C}$. Seja $r \in \ \alpha + 0^*$. Então, $r = p + q$, onde $p \in \alpha$ *e* $q \in 0^*$, isto é, $q < 0$. Dessa forma $r < p \in \alpha$, ou seja, $r \in \alpha$. Portanto $\alpha + 0^* \subset \alpha$. Agora, seja $r \in \alpha$. Tome $s > r$ e podemos escrever r como $r = s + (r - s)$, onde $r - s < 0$, donde $r - s$ irá pertencer a 0^*. Assim, $r \in \alpha + 0^*$ e $\alpha \subset \alpha + 0^*$. Logo $\alpha = \alpha + 0^*$.

□

Proposição 39. *Se* $s \in \mathbb{Q}$ *e* $r \in \mathbb{Q}^*_+$, *então* $\{s + mr | \ m \in \mathbb{N}\}$ *não é limitado superiormente em* $\mathbb{Q}$.

Demonstração. Sejam $s \in \mathbb{Q}$ e $r \in \mathbb{Q}^*_+$, e, por absurdo, suponhamos que $\alpha = \{s + mr | \ m \in \mathbb{N}\}$ é limitado superiormente. Então, $\exists \ p \in \alpha$ tal que $q \leq p, \ \forall \ q \in \alpha$ (pois α é limitado superiormente). Como $p \in \alpha, \ p = r + m_1 r, \ m \in \mathbb{N}$. Se tomarmos $k = s + m_2 r, \ m_2 > m_1$, teremos que $k \in \alpha$ e $k > p$, pois $m_2 r > m_1 r$. Absurdo, pois por hipótese, p é o elemento máximo de α. Portanto, α não é limitado superiormente. □

Lema 6. *Sejam* $\alpha \in \mathsf{C}$ *e* $r \in \mathbb{Q}^*_+$. *Então existem números racionais* p *e* q *tais que* $p \in \alpha$, $q \notin \alpha$, *q não é cota superior mínima de α e* $q - p = r$.

Demonstração. Seja s arbitrário em α e considere a sequência

$$s, \ s + r, \ s + 2r, \ s + 3r, \ldots, \ s + nr, \ldots \ .$$

Como essa sequência não é limitada superiormente, pela Proposição 39, α é limitado superiormente e $s \in \alpha$. Assim, existe um único inteiro $m \geq 0$ tal que $s + mr \in \alpha$ e $s + (m+1)r \notin \alpha$. Se $s + (m+1)r$ não for cota superior mínima de α, devemos tomar $p = s + mr$ e $q = s + (m+1)r$, daí, $q - p = r$. Se $s + (m+1)r$ for cota superior mínima de α, devemos tomar $p = s + mr + \dfrac{r}{2}$ e $q = s + (m+1)r + \dfrac{r}{2}$, daí, $q - p = r$. □

Teorema 5.10. Seja $\alpha \in \mathsf{C}$. Existe um único $\beta \in \mathsf{C}$ tal que $\alpha + \beta = 0^*$. Como nos casos dos inteiros e racionais, tal β denota-se por $-\alpha$ e se chama simétrico (ou inverso aditivo) de α.

Demonstração. Vamos provar inicialmente a unicidade. Suponhamos que $\alpha + \beta = \alpha + \beta' = 0^*$. Então,

$$\beta' = \beta' + 0^* = \beta' + (\alpha + \beta) = \left(\beta' + \alpha\right) + \beta = 0^* + \beta = \beta.$$

Provemos agora a existência de um corte β que satisfaça $\alpha + \beta = 0^*$. O primeiro passo é tomar um β e mostrar que é corte. Seja

$$\beta = \{p \in \mathbb{Q} \mid -p \notin \alpha \ \text{ e } \ -p \ \text{ não é cota superior mínima de } \alpha\}.$$

1. Vamos mostrar que $\beta \neq \emptyset$ em dois casos:

   - α não possui cota superior mínima: como α é um corte então $\alpha \neq \mathbb{Q}$, e $\exists\, q \in \mathbb{Q}$ tal que $q \notin \alpha$. Dessa forma, tome $p = -q \in \mathbb{Q}$. Assim, $-p = q \notin \alpha$. Logo, $p \in \beta$ e, portanto, $\beta \neq \emptyset$;
   - α possui cota superior mínima m: como m é cota superior mínima de α, $m \notin \alpha$ e, com isso, $m + 1 \notin \alpha$. Seja $p = -m - 1 \in \mathbb{Q}$ e $-p = m + 1 \notin \alpha$, além disso, $-p = m + 1 \neq m$. Portanto, $p \in \beta$ e $\beta \neq \emptyset$.

   Agora precisamos mostrar que $\beta \neq \mathbb{Q}$, considerando os mesmos dois casos.

   - α não possui cota superior mínima: como α é corte, então $\alpha \neq \emptyset$ e, portanto, existe $r \in \alpha$ (daí $r \in \mathbb{Q}$). Tomemos $p = -r \in \mathbb{Q}$. Segue que $-p = r \in \alpha$. Logo, $p \notin \beta$ e $p \in \mathbb{Q}$, isto é, $\beta \neq \mathbb{Q}$;
   - α possui cota superior mínima m: como m é cota superior mínima de α, então $m - 1 \in \alpha$ (caso contrario, $m - 1$ seria uma cota superior de α menor do que m, contradizendo a minimalidade de m). Seja $p = -m + 1 \in \mathbb{Q}$ e $-p = m - 1 \in \alpha$. Portanto, $p \notin \beta$ e $p \in \mathbb{Q}$, isto é, $\beta \neq \mathbb{Q}$.

2. Seja agora $p \in \beta$ e $q \in \mathbb{Q}$ tal que $q < p$. Queremos ver que $q \in \beta$. Como $p \in \beta$, $-p \notin \alpha$ e $-p$ não é cota superior mínima de α. Como $q < p$, temos:

$$-p < -q \tag{5.1}$$

dessa maneira $-q \notin \alpha$. Além disso, $-q$ não é cota superior mínima de α (pois caso contrário, sabendo que $-p \notin \alpha$, ou seja, é uma cota superior de α, teríamos $-q \leq -p$ (contradizendo a desigualdade (5.1)). Como $q \in \mathbb{Q}$, $-q \notin \alpha$ e $-q$ não é cota superior mínima de α, temos que $q \in \beta$.

3. Queremos ver agora que dado $p \in \beta$ existe um $q \in \beta$ tal que $p < q$. Dividiremos a demonstração também em dois casos:

   - α não possui cota superior mínima: como $-p \notin \alpha$ e α não possui cota superior mínima, temos que existe uma cota superior q de α (isto é, $q \notin \alpha$), de forma que $q < -p$. Assim, $-q \in \beta$ e $p < -q$, logo β não possui máximo.
   - α possui cota superior mínima m: seja $r = \dfrac{-m+p}{2} \in \mathbb{Q}$. Como $p \in \beta$, temos que $-p \notin \alpha$, ou seja, é uma cota superior de α, mas não é cota superior mínima de α, portanto, $m < -p$, daí, $p < -m$. Sendo assim,

     $$r = \frac{-m+p}{2} = \frac{-m}{2} + \frac{p}{2} > \frac{p}{2} + \frac{p}{2} = p.$$

     Porém, temos:

     $$-r = \frac{m-p}{2} = \frac{m}{2} - \frac{p}{2} > \frac{m}{2} + \frac{m}{2} = m$$

     e, portanto, $-r \neq m$. Como $-r > m$, então $-r \notin \alpha$. Finalmente, como $r \in \mathbb{Q}$, $r \notin \alpha$ e $-r$ não é cota superior mínima de α, temos que $r \in \beta$ e $p < r$, logo, β não possui máximo.

Agora precisamos mostrar que $\alpha + \beta = 0^*$. Para isso devemos mostrar duas contingências.

- Seja $r + q \in \alpha + \beta$, com $r \in \alpha$ e $q \in \beta$. Como $r \in \alpha$ e $-q \notin \alpha$, então $r < -q$, ou seja $r + q < 0$, isto é, $r + q \in 0^*$.
- $p \in 0^* \Rightarrow p \in \mathbb{Q}$ e $p < 0$ $(-p > 0)$. Sejam $r \in \alpha$ e $r' \notin \alpha$ $\left(r'\right.$ não sendo cota superior mínima de $\left.\alpha\right)$, tais que $r' - r = -p$ (pelo Lema 6). Segue que $p = r + \left(-r'\right)$, com $r \in \alpha$ e $-r' \in \beta$, ou seja, $p \in \alpha + \beta$.

□

Definição 35. Como nos casos de $\mathbb{Z}$ e $\mathbb{Q}$, definimos a subtração em C por $\alpha - \beta = \alpha + (-\beta)$, $\forall\ \alpha, \beta \in \mathsf{C}$.

Proposição 40. *Se $\alpha \in \mathsf{C}$, então $\alpha = -(-\alpha)$.*

Demonstração. Sabemos que o oposto de α é $-\alpha$. Assim,

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

Por outro lado, sabemos também que o oposto de $(-\alpha)$ é $-(-\alpha)$. Assim,

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

Além disso, o elemento neutro é único. Portanto, $\alpha = -(-\alpha)$.

$\square$

Teorema 5.11. (Compatibilidade da relação de ordem com a adição) Sejam $\alpha, \beta, \gamma \in \mathsf{C}$, tais que $\alpha \leq \beta$. Então, $\alpha + \gamma \leq \beta + \gamma$.

Demonstração. $\alpha \leq \beta \Leftrightarrow \alpha \subset \beta$. Tome $t \in \alpha + \gamma$, isto é, $t = r + s$, com $r \in \alpha$ e $s \in \gamma$. Como $\alpha \subset \beta$, temos que $r \in \beta$ e $t = r + s \in \beta + \gamma$, logo $\alpha + \gamma \subset \beta + \gamma$. Portanto, $\alpha + \gamma \leq \beta + \gamma$. $\square$

Para definir a multiplicação em C, procederemos de forma análoga aos passos realizados na definição da adição e suas propriedades. Pela definição de adição, $3^* + 5^* = 8^*$. Uma boa definição de multiplicação seria $3^*.5^* = 15^*$. Num primeiro momento, poderíamos tentar transferir a definição de adição para o caso da multiplicação, de forma que: $3^*.5^* = \{p.q|\ p \in 3^* \text{ e } q \in 5^*\}$. Porém, não obteríamos 15^* como resultado, já que o racional $(-10).(-5) = 50$ é elemento do conjunto anterior, mas não é elemento de 15^*. Percebemos então que essa transferência direta do caso aditivo não funciona bem. Entretanto, fazendo alguns ajustes, teremos uma definição satisfatória.

Proposição 41. *Para $\alpha, \beta \in \mathsf{C}$, com $\alpha \geq 0^*$ e $\beta \geq 0^*$, seja*

$$\gamma = \mathbb{Q}_-^* \cup \{r \in \mathbb{Q}|\ r = pq,\ com\ p \in \alpha,\ q \in \beta,\ p \geq 0\ e\ q \geq 0\}.$$

Então, γ é um corte e $\gamma \geq 0$.

Demonstração.

- Como $p = -1 \in \gamma$, $\gamma \neq \emptyset$. Temos ainda que,

$$\begin{cases} \alpha \neq \mathbb{Q} & \Rightarrow \exists\ p_0 \in \mathbb{Q} \text{ tal que } p_0 \notin \alpha \\ \beta \neq \mathbb{Q} & \Rightarrow \exists\ q_0 \in \mathbb{Q} \text{ tal que } q_0 \notin \beta \end{cases}.$$

  Logo, $p_0q_0 \in \mathbb{Q}$. Mostremos que $p_0q_0 \notin \gamma$. Suponhamos que $p_0q_0 \in \gamma$, isto é, existem $p \in \alpha, q \in \beta, p \geq 0$ e $q \geq 0$ tal que $p_0q_0 = pq$. Não podemos ter $p_0 \leq p$ (pois teríamos $p_0 \in \alpha$), nem $q_0 \leq q$ (pois teríamos $q_0 \in \beta$). Assim, $p < p_0$ e $q < q_0$, daí, $pq < p_0q_0$, o que é uma contradição com $p_0q_0 = pq$. Portanto, $p_0q_0 \notin \gamma$ e, assim, $\gamma \neq \mathbb{Q}$.

- Sejam $r \in \gamma$ e $s < r$. Queremos ver que $s \in \gamma$. Se $s < 0$, então $s \in \gamma$. Suponha $s \geq 0$, logo $r > 0$. Como $r \in \gamma$, existem $p \in \alpha$ e $q \in \beta$, tais que $r = pq$, com $p \geq 0$ e $q \geq 0$. Como $r > 0$, segue que $p > 0$ e $q > 0$. Seja $t = \dfrac{s}{p}(s \geq 0, p > 0 \Rightarrow t \geq 0)$. Se $q \leq t$ teríamos $pq \leq pt$, isto é, $r \leq s$, o que é um absurdo, já que $s < r$. Portanto, devemos ter $t < q$ e, como $q \in \beta$, então $t \in \beta$. Assim, como $s = pt, p \in \alpha, t \in \beta, p > 0$ e $t \geq 0$, então $s \in \gamma$.

- Tome $r \in \gamma$ e mostremos que existe $s \in \gamma$ tal que $r < s$. De fato, se $r < 0$, basta tomar $s = \frac{r}{2} < 0$, daí $s > r$. Suponhamos $r \geq 0$. Neste caso, $r \in \gamma$ significa que $r = pq$, com $p \in \alpha, q \in \beta, p \geq 0$ e $q \geq 0$. Existem $t \in \alpha$ e $u \in \beta$ tais que $p < t$ e $q < u$ (pois α e β não possuem máximo). Logo, $r = pq < tu$. Tomando $s = tu$, temos $s \in \gamma$ (pois $s = tu$ com $t \in \alpha, u \in \beta, t > 0$ e $u > 0$) e $s > r$. Portanto, γ não tem máximo.

Dessa forma temos que γ é um corte. □

Definição 36. Se $\alpha, \beta \in \mathsf{C}$ e $\alpha \geq 0,\ \beta \geq 0$, definimos o produto $\alpha\beta$ como sendo o corte γ dado na Proposição 41.

Para a definição de produto de cortes que contêm fatores negativos, introduziremos a noção de valor absoluto de um corte.

Definição 37. Dado $\alpha \in \mathsf{C}$, definimos o valor absoluto de α, representado por $|\alpha|$, da seguinte forma:

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

Proposição 42. *1.* $|\alpha| \geq 0$*;*

2. $|\alpha| = 0^* \Leftrightarrow \alpha = 0^*$.

Demonstração. 1. • Se $\alpha \geq 0^*$, então $|\alpha| = \alpha \geq 0^*$, portanto $|\alpha| \geq 0^*$.

- Se $\alpha < 0^*$, então $|\alpha| = -\alpha$. Além disso, $-\alpha > 0^*$. Assim, $|\alpha| > 0^*$.

2. ($\Rightarrow$) Suponha $|\alpha| = 0^*$.

   - Se $\alpha > 0^*$, então $|\alpha| = \alpha > 0^*$, absurdo pois $|\alpha| = 0^*$.
   - Se $\alpha < 0^*$, temos que $-\alpha > 0^*$. Logo, por definição, $|\alpha| = -\alpha > 0^*$. Absurdo, pois $|\alpha| = 0^*$.

   ($\Leftarrow$) Se $\alpha = 0^*$, temos que $|\alpha| = \alpha = 0^*$.

□

Definição 38. Se $\alpha, \beta \in \mathsf{C}$, definimos:

$$\alpha\beta = \begin{cases} -(|\alpha||\beta|) & \text{se} \quad \alpha < 0^* \quad \text{e} \quad \beta \geq 0^*; \\ -(|\alpha||\beta|) & \text{se} \quad \alpha \geq 0^* \quad \text{e} \quad \beta < 0^*; \\ |\alpha||\beta| & \text{se} \quad \alpha < 0^* \quad \text{e} \quad \beta < 0^*. \end{cases}$$

Teorema 5.12. Sejam $\alpha, \beta, \gamma \in \mathsf{C}$. Valem:

1. Comutatividade: $\alpha\beta = \beta\alpha$;

2. Associatividade: $(\alpha\beta)\gamma = \alpha(\beta\gamma)$;

3. Elemento Neutro 1^* : $\alpha \cdot 1^* = \alpha$.

Demonstração. Vamos supor $\alpha, \beta, \gamma \geq 0^*$

1. Tome $r \in \alpha\beta$. Se $r < 0$, então $r \in \beta\alpha$ por definição do produto. Suponhamos então $r \geq 0$. Assim $r = pq,\ p \in \alpha,\ q \in \beta,\ p, q \geq 0$. Dessa forma, temos que $r = pq = qp,\ q \in \beta,\ p \in \alpha,\ q, p \geq 0$. Ou seja, $r \in \beta\alpha$. Analogamente, para o caso $r \in \beta\alpha \Rightarrow\ r \in \alpha\beta$.

2. É de forma análoga ao item anterior, usando a associatividade dos racionais, isto é, $(\alpha\beta)\gamma = \mathbb{Q}^*_- \cup \{q \in \mathbb{Q} |\ q =\ (rs)t,\ r \in \alpha,\ s \in \beta,\ t \in \gamma,\ r, s, t \geq 0\}\ =\ \mathbb{Q}^*_- \cup \{q \in \mathbb{Q} |\ q = r(st),\ r \in \alpha,\ s \in \beta,\ t \in \gamma,\ r, s, t \geq 0\}$.

3. Seja $r \in \alpha \cdot 1^*$ e $r < 0$. Se $\alpha = 0^*, r < 0$, então $r \in 0^* = \alpha$, portanto, $r \in \alpha$. Se $\alpha > 0^*$, temos que existe $p \in \alpha$ tal que $p \notin 0^*$, daí $p \geq 0$. Dessa maneira, $r < 0 \leq p$, logo $r \in \alpha$. Suponhamos agora $r \geq 0$ e $r \in \alpha \cdot 1^*$. Assim, $r = pq$ com $p \in \alpha, q \in 1^*, p \geq 0$ e $q \geq 0$. Como $q \in 1^*$, temos que, $q < 1$, daí $pq < p \cdot 1$, isto é, $r = pq < p$. Como $p \in \alpha, r = pq < p$ e α é corte, então $r \in \alpha$. Logo, $\alpha \cdot 1^* \subset \alpha$.

   Por outro lado, tome $r \in \alpha$. Se $r < 0$ então $r \in \alpha$, por definição de produto. Suponha $r \geq 0$. Tome $p \in \alpha$ tal que $0 \leq r \leq p$ (pois α não tem máximo). Se $q = \dfrac{r}{p}$ então $0 \leq q < 1$ e portanto $q \in 1^*$. Concluímos que, como $r = pq,\ p \in \alpha, q \in 1^*, p > 0, q \geq 0$ então $r \in \alpha \cdot 1^*$. Portanto $\alpha \subset \alpha \cdot 1^*$. Logo $\alpha = \alpha \cdot 1^*$.

□

Teorema 5.13. Seja $\alpha \in \mathsf{C}$ com $\alpha > 0^*$. O conjunto $\beta = \{p \in \mathbb{Q} |\ p \leq 0$ *ou* $p^{-1} \notin \alpha$ *e existe* $q \notin \alpha$ *tal que* $q < p^{-1}\}$ é corte.

Demonstração.

1. Como $0 \in \beta$, temos que $\beta \neq \emptyset$. Seja $p \in \alpha$ tal que $p > 0$ (este p existe pois, como $\alpha > 0^*$ existe $q \in \mathbb{Q},\ q \in \alpha$ *e* $q \notin 0^*$, isto é $q \geq 0$). Precisamos mostrar agora que $p^{-1} \notin \beta$. De fato, se $p^{-1} \in \beta$, teríamos que $(p^{-1})^{-1} = p \notin \alpha$, absurdo, pois $p \in \alpha$. Logo, $p^{-1} \notin \beta$, ou seja, $\beta \neq \mathbb{Q}$.

2. Seja $p \in \beta$ e $q \in \mathbb{Q}$ com $q < p$. Queremos mostrar que $q \in \beta$. Se $q \leq 0$, então $q \in \beta$, pela definição de β. Suponha então $q > 0$. Assim, temos $0 < q < p$. Como $p, q \in \mathbb{Q}^*_+$ e $q < p$, usando as propriedades dos racionais, $p^{-1} < q^{-1}$. Como $p^{-1} \notin \alpha$, segue que $q^{-1} \notin \alpha$. Assim, $p^{-1} \notin \alpha,\ q^{-1} \notin \alpha,\ p^{-1} < q^{-1}$, o que nos diz que q^{-1} não é cota superior mínima de α. Logo, $q \in \beta$.

3. Seja $p \in \beta$. Vamos mostrar que existe $q \in \beta$ tal que $p < q$. Sem perda de generalidade, vamos supor $p > 0$. Como $p \in \beta$ e $p > 0$, então $p^{-1} \notin \alpha$ e existe $r \notin \alpha$ tal que

$r < p^{-1}$. Tomemos $s = \dfrac{r+p^{-1}}{2}$. Assim, temos $r < s < p^{-1}$. Tomando $q = s^{-1}$ temos $q = s^{-1} > p > 0$, portanto, $q > 0$. De fato, $q^{-1} = s \notin \alpha$ (pois $s > r$ e $r \notin \alpha), q^{-1} = s > r$ e $r \notin \alpha$. Logo, $q \in \beta$, isto é, β não possui máximo.

□

Definição 39. Seja α um corte tal que $\alpha \neq 0^*$. Se $\alpha > 0^*$, então o corte β do Teorema 5.13 é denotado por α^{-1} e chamado de inverso de α. Se $\alpha < 0^*$, então definimos o inverso de α como $\alpha^{-1} = -|\alpha|^{-1}$.

Teorema 5.14. Seja α um corte tal que $\alpha \neq 0^*$. Então $\alpha\alpha^{-1} = 1^*$. Além disso, o inverso de α é unico.

Demonstração. Vamos considerar dois casos, $\alpha > 0^*$ e $\alpha < 0^*$.

- $\alpha > 0^*$: tome $r \in \alpha.\alpha^{-1}$. Se $r \leq 0$, temos que $r \in 1^*$. Suponha então $r > 0$. Como $r \in \alpha\alpha^{-1}$ existem $s \in \alpha,\ p \in \alpha^{-1}$ tal que $r = sp,\ s \geq 0,\ p \geq 0$. Mas $r > 0$, portanto devemos ter $s > 0,\ p > 0$. Como $p \in \alpha^{-1}$ *e* $p > 0$, existe $q \notin \alpha$ tal que $q < p^{-1}$. Como $s \in \alpha$ *e* $q \notin \alpha$, temos que $s < q$. De $q < p^{-1}$, temos $p < q^{-1}$, segue então que $sp < sq^{-1}$. Logo, como $s < q$, temos que $sq^{-1} < 1$, e assim, $r = sp < sq^{-1} < 1$, isto é $r \in 1^*$.

  Reciprocamente, seja $r \in 1^*$, isto é, $r < 1$. Se $r < 0$, então $r \in \alpha\alpha^{-1}$, por definição de produto. Agora, se $r = 0$, temos $r = p \cdot 0$, onde $p \in \alpha,\ 0 \in \alpha^{-1}$ e $p > 0$. Logo, $r \in \alpha\alpha^{-1}$. Suponha agora $0 < r < 1$. Tome $s \in \alpha$ com $s > 0$. Seja n o maior natural que satisfaz $s(r^{-1})^n \notin \alpha$ (existe n, pois $r^{-1} > 1$ e se $s(r^{-1})^n \in \alpha\ \forall\ n \in \mathbb{N}$, teríamos $\alpha = \mathbb{Q}$, absurdo pois α é corte). Tomemos $p_1 = s(r^{-1})^{n-1} \in \alpha$ e $t = s(r^{-1})^n \notin \alpha$. Seja $p \in \alpha$ tal que $p_1 < p$ (α não possui máximo). Tome $q = t^{-1}p^{-1}p_1$, isto é, $q^{-1} = tpp_1^{-1}$. Assim, podemos ter:

  $$p_1 < p \Rightarrow p_1p_1^{-1} < pp_1^{-1} \Rightarrow 1 < pp_1^{-1} \Rightarrow t < tpp_1^{-1} \Rightarrow t < q^{-1}.$$

  Como $t \notin \alpha, q^{-1} \notin \alpha$ e q^{-1} não é a menor cota superior de α. Temos ainda,

  $$\begin{aligned} q = t^{-1}p^{-1}p_1 &\Rightarrow pq = pt^{-1}p^{-1}p_1 \Rightarrow pq = t^{-1}p_1 \\ &\Rightarrow pq = \left(s\left(r^{-1}\right)^n\right)^{-1} s\left(r^{-1}\right)^{n-1} \\ &\Rightarrow pq = s^{-1}r^n sr^{-n+1} \Rightarrow pq = r. \end{aligned}$$

  Desta forma, $p \in \alpha$ e, como $q^{-1} \notin \alpha$ e existe $t \notin \alpha$ tal que $t < q^{-1}$, então, $q \in \alpha^{-1}$. Portanto, $r \in \alpha\alpha^{-1}$. Logo, concluímos que, se $\alpha > 0^*$, então $\alpha\alpha^{-1} = 1^*$.

- $\alpha < 0^*$: se $\alpha < 0^*$, por definição, $\alpha^{-1} = -|\alpha|^{-1}$. Sabemos que $|\alpha|^{-1} > 0^*$ e, portanto, $-|\alpha|^{-1} < 0^*$, ou seja, $\alpha^{-1} < 0^*$. Assim, pela definição de produto, $\alpha\alpha^{-1} = |\alpha||\alpha^{-1}| = |\alpha|| - |\alpha|^{-1}| = |\alpha||\alpha|^{-1} = 1^*$.

Vamos provar a unicidade de α^{-1}. Suponhamos que existam α_1^{-1} *e* α_2^{-1}, tais que $\alpha\alpha_1^{-1} = 1^*$ e $\alpha\alpha_2^{-1} = 1^*$. Assim,

$$\alpha_1^{-1} = \alpha^{-1} \cdot 1^* = \alpha_1^{-1}(\alpha\alpha_2^{-1}) = (\alpha_1^{-1}\alpha)\alpha_2^{-1} = 1^* \cdot \alpha_2^{-1} = \alpha_2^{-1}.$$

□

Teorema 5.15. (Distributividade). Se $\alpha, \beta, \gamma \in \mathsf{C}$, então $\alpha(\beta + \gamma) = \alpha\beta + \alpha\gamma$.

Demonstração. Demonstraremos inicialmente para α, β, γ maiores que 0^*. Os outros casos serão consequências deste que provaremos. Primeiro vamos mostrar que $\alpha(\beta+\gamma) \subset \alpha\beta+\alpha\gamma$. De fato,

$$\alpha(\beta + \gamma) = \{q \in \mathbb{Q} |\ q < 0\} \cup \{p \in \mathbb{Q} |\ p = rs\ onde\ r \in \alpha,\ s \in (\beta + \gamma),\ r \geq 0,\ s \geq 0\}.$$

Assim, se $x \in \alpha(\beta + \gamma)$ então, ou $\in 0^*$ ou $x = rs$ com $r \in \alpha,\ s \in (\beta + \gamma),\ r \geq 0,\ s \geq 0$. Se $x \in 0^*$, então $\dfrac{x}{2} \in 0^*$ e $\dfrac{x}{2} + \dfrac{x}{2} = x$, ou seja, $x \in \alpha\beta + \alpha\gamma$. Agora, se $x = rs\ com\ r \in \alpha,\ s \in (\beta+\gamma),\ r \geq 0,\ s \geq 0$, então $s = q+p$, onde $q \in \beta,\ p \in \gamma,\ q, p \geq 0$. Portanto, $x = rs = r(q + p) = rq + rp$, logo $x \in \alpha\beta + \alpha\gamma$. Dessa maneira, temos que $\alpha(\beta + \gamma) \subset \alpha\beta + \alpha\gamma$.

Devemos mostrar agora que $\alpha\beta + \alpha\gamma \subset \alpha(\beta + \gamma)$. De fato,

$$\alpha\beta + \alpha\gamma = \{t \in \mathbb{Q} |\ t = ps + pq \text{ onde } ps \in \alpha\beta, pq \in \alpha\gamma\}.$$

Seja $u \in \alpha\beta + \alpha\gamma$, isto é, $u = ps + pq$, com $ps \in \alpha\beta,\ pq \in \alpha\gamma$.

- $ps \in \alpha\beta \Rightarrow\ ps < 0$ ou $p \in \alpha$ e $s \in \beta\ com\ p, s \geq 0$;
- $pq \in \alpha\gamma \Rightarrow\ pq < 0$ ou $p \in \alpha$ e $q \in \gamma\ com\ p, q \geq 0$.

Desta maneira, teremos quatro casos:

1. Suponha $ps < 0$ e $pq < 0$. Temos que, $u \in \alpha(\beta + \gamma)$ pois $u = ps + pq < 0$;
2. Suponha $ps < 0$ e $p \in \alpha$ e $q \in \gamma$, com $p, q \geq 0$. Como $ps < 0$ e $p \geq 0$, temos $s < 0$, daí, se $-s > q$, então $s + q < 0$, portanto $u = ps + pq = p(s + q) < 0$. Se $-s \leq q$, então $s + q \geq 0$, e como $p \geq$, temos $u = p(s + q) \in \alpha(\beta + \gamma)$, já que $p \in \alpha\ e\ s + q \in \beta + \gamma$, com $p, q \geq 0$;
3. Suponha $p \in \alpha$, $s \in \beta$ com $p, q \geq 0$ e $pq < 0$. De forma análoga ao caso anterior conluímos que $u = ps + pq \in \alpha(\beta + \gamma)$;
4. Suponha agora que $p \in \alpha$, $s \in \beta$ e $q \in \gamma$, com $p, s, q \geq 0$. Dessa forma, $u = ps+pq = p(s + q)$, onde $p \in \alpha$ e $s + q \in \beta + \gamma$, com $p, s + q \geq 0$, logo $u \in \alpha(\beta + \gamma)$.

Portanto, provada as duas inclusões, temos $\alpha\beta + \alpha\gamma = \alpha(\beta + \gamma)$ $\square$

Teorema 5.16. Para $\alpha, \beta \in \mathsf{C}$, temos $(-\alpha)\beta = \alpha(-\beta) = -(\alpha\beta)$ e $(-\alpha)(-\beta) = \alpha\beta$.

Demonstração. Com efeito, temos,

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

Isso nos diz ainda que $(-\alpha)\beta = -(\alpha\beta)$, pois, o oposto de um corte é único (Teorema 5.10). Temos também que,

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

Da mesma maneira, $\alpha(-\beta) = -(\alpha\beta)$. Ainda temos,

$$\begin{aligned}(-\alpha)(-\beta) &= -(\alpha(-\beta)) \text{ por } (*)\\ &= -(-(\alpha\beta)) \text{ por } (**)\\ &= \alpha\beta, \text{ pela Proposicao 40.}\end{aligned}$$

$\square$

Assim como no caso da adição, o teorema a seguir trata da compatibilidade da relação de ordem com a multiplicação.

Teorema 5.17. Se $\alpha \leq \beta$ e $\gamma > 0^*$, então, $\alpha\gamma \leq \beta\gamma$.

Demonstração. Como $\alpha \leq \beta$, temos que $0^* = \alpha + (-\alpha) \leq \beta + (-\alpha)$ e, portanto, $\beta + (-\alpha) \geq 0^*$. Além disso, como $\gamma \geq 0^*$, temos $(\beta + (-\alpha))\gamma \geq 0^*$, pela Definição 36. Portanto, $\beta\gamma + (-\alpha)\gamma \geq 0^*$, dessa maneira temos que $\beta\gamma \geq \alpha\gamma$, isto é, $\alpha\gamma \leq \beta\gamma$. $\square$

Proposição 43. *Seja α um corte qualquer, então $\alpha \cdot 0^* = 0^*$.*

Demonstração. Temos que

$$\alpha \cdot 0^* = \alpha(0^* + 0^*) = \alpha \cdot 0^* + \alpha \cdot 0^*,$$

daí

$$\alpha \cdot 0^* - \alpha \cdot 0^* = \alpha \cdot 0^* + \alpha \cdot 0^* - \alpha \cdot 0^*.$$

Portanto, $0^* = \alpha \cdot 0^*$, como queríamos demonstrar. $\square$

Proposição 44. *Sejam α e β cortes. Temos que $\alpha\beta = 0^*$, se e somente se, $\alpha = 0^*$ ou $\beta = 0^*$.*

Demonstração. Se $\alpha = 0^*$ *ou* $\beta = 0^*$, pelo resultado anterior segue que $\alpha\beta = 0^*$. Suponhamos agora que $\alpha\beta = 0^*$. Sem perda de generalidade tome $\alpha \neq 0^*$, isto é, existe $\gamma \in \mathsf{C}$, tal que $\alpha\gamma = 1^*$. Dessa forma,

$$\beta = \beta \cdot 1^* = \beta(\alpha\gamma) = (\alpha\beta)\gamma = 0^*\gamma = 0^*.$$

Da mesma forma concluímos que se $\beta \neq 0^*$, temos $\alpha = 0^*$. □

Proposição 45. *Seja* $\alpha \in \mathsf{C}$. *Temos que* $r \in \alpha$ *se, e somente se,* $r^* < \alpha$.

Demonstração. Se $r \in \alpha$, como $r \notin r^*$, então $r^* < \alpha$. Reciprocamente, se $r^* < \alpha$, existe $s \in \alpha \backslash r^*$. Temos que $s \geq r$ *e* $s \in \alpha$. Logo $r \in \alpha$. □

Teorema 5.18. Se $\alpha, \beta \in \mathsf{C}$ e $\alpha < \beta$, então existe um corte racional r^* tal que $\alpha < r^* < \beta$.

Demonstração.

1. Suponha α um corte racional, isto é, $\alpha = s^*$. Como $\alpha < \beta$, existe $r \in \beta \backslash \alpha$, com $r > s$. De $r \in \beta$ e $r \notin r^*$, obtemos que $r^* < \beta$. Como $s < r$, temos que $\alpha = s^* < r^*$.

2. Suponha agora que α não é um corte racional. Sabendo que $\alpha < \beta$, então existe $r \in \beta \backslash \alpha$. Além disso temos que $r \in \beta \backslash r^*$, daí obtemos $r^* < \beta$. Como r é cota superior de α e α não é um corte racional, então r não é a cota superior mínima de α. Portanto existe $s \in r^* \backslash \alpha$, ou seja $\alpha < r^*$.

□

Construímos um conjunto C, munido de duas operações e uma relação de ordem, de forma que C é um corpo ordenado, assim como $\mathbb{Q}$. Em particular, definimos também a divisão em C e adotamos a notação de fração como nos racionais $\dfrac{\alpha}{\beta}$. Veremos a seguir um resultado que nos mostra uma aplicação injetora de $\mathbb{Q}$ em C, semelhante ao que foi feito em $\mathbb{Z}$ e $\mathbb{Q}$, o Capítulo 4.

Teorema 5.19. A aplicação j: $\mathbb{Q} \longrightarrow C$, dada por $j(r) = r^*$ é injetora e preserva adição, multiplicação e ordem, isto é, as seguintes afirmações são válidas:

1. $j(p) + j(q) = j(p+q)$, ou seja, $p^* + q^* = (p+q)^*$;

2. $j(p)j(q) = j(pq)$, isto é, $p^*q^* = (pq)^*$;

3. $j(p) < j(q)$ se, e somente se $p < q$, ou ainda, $p^* < q^*$ se, e somente se $p < q$;

4. $j(p) = j(q)$ se, e somente se $p = q$, ou seja, $p^* = q^*$ se, e somente se, $p = q$.

Demonstração. 1. Tome $u \in p^* + q^*$, ou seja, $u = t + w$ com $t \in p^*,\ w \in q^*$ e ainda, $t < p$ e $w < q$. Daí, temos que $u = t + w < p + q$, isto é, $u = t + w \in (p + q)^*$.

Seja agora $r \in (p + q)^*$, isto é, $r < p + q$. Tome $h = p + q - r$, $s = p - \dfrac{h}{2}$ e $t = q - \dfrac{h}{2}$. Dessa forma, temos $s < p$ e $t < q$, ou seja, $s \in p^*$ e $t \in q^*$. Portanto, $u = s + t \in p^* + q^*$.

2. Faremos a prova para o caso $p > 0$ e $q > 0$, e os outros casos podem ser provados de maneira análoga.

   Se $r \in p^*q^*$, então, ou $r < 0$ ou $r = st$, com $p \geq 0, q \geq 0$ e $q > t \geq 0$, de modo que, ou $r < 0$ ou $r = st < pq$ e assim, $r \in (pq)^*$.

   Agora, seja $r \in (pq)^*$. Então podemos afirmar que ou $r < 0$ ou $0 \leq r < pq$. Se $r < 0$, claramente $r \in p^*q^*$, pela definição de corte positivos. Se $0 \leq r < pq$, então existem $p_1,\ q_1 \in \mathbb{Q}$, tais que $0 < p_1 < p,\ 0 < q_1 < q$, e ainda, $r < p_1q_1 < pq$. Além disso, $p_1 \in p^*,\ q_1 \in q^*,\ p_1q_1 \in p^*q^*$ e, portanto, $r \in p^*q^*$.

3. Se $p < q$, então $p \in q^*$. Como $p \notin p^*$, concluímos que $p^* < q^*$. Analogamente, se $p^* < q^*$, existe um racional s, tal que $s \in q^*$ *e* $s \notin p^*$, ou seja, $r < q$ e $r \geq p$. Portanto, $p \leq r < q$, ou seja, $p < q$.

4. Se $p = q$, obviamente $p^* = q^*$. Suponhamos então $p^* = q^*$. Como $p \notin p^*$, segue que $p \notin q^*$, logo $p \geq q$. Mas, como $q \notin q^*$, segue que $q \notin p^*$, então $p \leq q$. Pela tricotomia segue que, $p = q$.

□

Novamente, obtivemos uma cópia de um conjunto em outro, mais precisamente um homomorfismo injetor. Desta vez, $j(\mathbb{Q})$ é uma cópia de $\mathbb{Q}$ em C, sendo $j(\mathbb{Q})$ precisamente o conjunto dos cortes racionais. Além disso, o Teorema 5.5, nos mostra que existem cortes não racionais em C. Portanto, $\mathsf{C} \backslash j(\mathbb{Q}) \neq \emptyset$.

Podemos notar ainda que o corpo ordenado dos números racionais é isomorfo ao corpo ordenado de todos os cortes racionais (C^*) (isto é, existe um homomorfismo de corpos que é bijetor e preserva a soma, o produto e a ordem), permitindo assim identificar um corte racional r^* com o número racional r. Porém, naturalmente r^* não é, de modo algum, o mesmo número racional, mas as propriedades que interessam são as mesmas nos dois corpos ordenados.

Definição 40. O conjunto C dos cortes será, a partir de agora, denominado de conjunto dos números reais e denotado por $\mathbb{R}$. Os cortes racionais serão identificados, via a injeção j, com os números racionais. Além disso, todo corte que não for racional será denominado número irracional.

A identificação de $j(\mathbb{Q})$ com $\mathbb{Q}$, nos permite dizer que $\mathbb{Q} \subset \mathbb{R}$. E o conjunto $\mathbb{R}\backslash\mathbb{Q}$, representa o conjunto dos números irracionais.

Teorema 5.20. (Dedekind). Sejam A e B subconjuntos de $\mathbb{R}$ tais que:

1. $\mathbb{R} = A \cup B$
2. $A \cap B = \emptyset$
3. $A \neq \emptyset$ e $B \neq \emptyset$
4. Se $\alpha \in A$ e $\beta \in B$, então $\alpha < \beta$.

Nestas condições, existe um, e apenas um, número real γ tal que $\alpha \leq \gamma \leq \beta$, para todo $\alpha \in A$ e para todo $\beta \in B$.

Demonstração. Vamos provar primeiro a unicidade: suponhamos que existam dois números γ_1 e γ_2, tais que $\gamma_1 > \gamma_2$ nas condições do enunciado. Agora, tome γ_3 de forma que $\gamma_1 < \gamma_3 < \gamma_2$, o que é possível pelo Teorema 5.18. Sabendo que $\gamma_3 < \gamma_2$, temos que $\gamma_3 \in A$, pois $\beta \geq \gamma_2 (> \gamma_3)$, para todo $\beta \in B$ e $A \cup B = \mathbb{R}$. Analogamente, de $\gamma_1 < \gamma_3$, temos que $\gamma_3 \in B$. Ou seja, $\gamma_3 \in A \cup B$, contradição.

Vamos provar a existência: considere $\gamma = \{r \in \mathbb{Q}|\ r \in \alpha,\ \textit{para algum}\ \alpha \in A\}$. Mostraremos que γ é um corte nas condições requeridas.

1. Como $A \neq \emptyset$, temos que $\gamma \neq \emptyset$. Para ver que $\gamma \neq \mathbb{Q}$, tomemos $\beta \in B$. Seja $s \in \beta$ um racional. Como $\alpha \subset \beta$, para todo $\alpha \in A$, concluímos que, $s \notin \alpha$ para todo $\alpha \in A$, o que nos diz que $s \notin \gamma$;
2. Suponha $r \in \gamma$ e $s < r$. Então $r \in \alpha$ para algum $\alpha \in A$ e, como $s < r$, então $s \in \alpha$, assim $s \in \gamma$;
3. Sabemos que $r \in \alpha$ para algum $\alpha \in A$, e como α é um corte, temos que existe $s > r$ em α, logo $s \in \gamma$.

Portanto, γ é um número real e temos ainda que $\alpha \leq \gamma\ \forall \alpha \in A$, pois pela definição de γ, sabemos que $\alpha \subset \gamma,\ \forall \alpha \in A$.

Nos falta mostrar que $\gamma \leq \beta$, para todo $\beta \in B$. Suponha que exista $\beta \in B$ com $\beta < \gamma$. Com isso, existe um racional $r \in \gamma$, tal que $r \notin \beta$. Como $r \in \gamma$, temos que r pertence a algum $\alpha \in A$ e, não sendo elemento de β, obtemos que $\beta < \alpha$, entrando em contradição com a última hipótese do teorema. Logo, $\alpha \leq \beta$, para todo $\beta \in B$. $\square$

O Teorema 5.20 fornece a grande essência da diferença entre $\mathbb{Q}$ e $\mathbb{R}$, que vamos verificar através do exemplo a seguir.

Exemplo 12. Consideremos os seguintes subconjuntos de $\mathbb{Q}$:

$$A = \{x \in \mathbb{Q}_+ |\ x^2 < 2\} \cup \mathbb{Q}_-^* \text{ e } B = \{x \in \mathbb{Q}_+ |\ x^2 > 2\}.$$

Podemos perceber que A e B satisfazem as hipóteses do Teorema 5.20 anterior, com $\mathbb{Q}$ no lugar de $\mathbb{R}$, mas que não existe $r \in \mathbb{Q}$ satisfazendo $s \leq r$ para todo $s \in A$ e $r \leq t$ para todo $t \in B$.

Tendo em vista o Exemplo 12, podemos dizer que em $\mathbb{R}$, não há "lacunas", enquanto que em $\mathbb{Q}$ há. Por este motivo, dizemos que $\mathbb{R}$ possui a propriedade da completude ou que $\mathbb{R}$ é completo.

Corolário 1. *Nas condições do Teorema 5.20, ou existe em A um número máximo, ou, em B, um número mínimo.*

Demonstração. Seja γ como no Teorema 5.20. Temos que γ está em A ou em B, pela hipótese (1) e, por (2), que está em apenas em um desses conjuntos. Se $\gamma \in A$, então γ é elemento máximo de A; se $\gamma \in B$, γ é elemento mínimo de B. □

Notemos ainda que se o conjunto A do Teorema 5.20 não contiver γ, então ele é um corte em $\mathbb{R}$, no sentido da defnição inicial de cortes que vimos em $\mathbb{Q}$ (Definição 30). A diferença entre ambas as situações é que em $\mathbb{Q}$ não se tem, necessariamente, como no Teorema 5.20 para os números reais, um elemento γ. Essas lacunas é que geram os cortes (números) irracionais. Como essas lacunas não ocorrem em $\mathbb{R}$, então cortes em $\mathbb{R}$ não geram elementos novos.

Adotaremos também a usual notação para intervalos de números reais, que são os subconjuntos de $\mathbb{R}$ dos seguintes tipos, onde a e b são reais com $a < b$:

1. $(a, b) = \{x \in \mathbb{R}|\ a < x < b\}$;
2. $[a, b) = \{x \in \mathbb{R}|\ a \leq x < b\}$;
3. $(a, b] = \{x \in \mathbb{R}|\ a < x \leq b\}$;
4. $[a, b] = \{x \in \mathbb{R}|\ a \leq x \leq b\}$;
5. $(a, +\infty) = \{x \in \mathbb{R}|\ x > a\}$, e de forma análoga para os intervalos:

$$[a, +\infty)\ ;\ (-\infty, a)\ ;\ (-\infty, a] \text{ e } (-\infty, +\infty) = \mathbb{R}.$$

O próximo teorema é de extrema importância na Análise Matemática. A partir dele decorrem os famosos Teorema do Valor Intermediário e o Teorema Weierstrass. Desses dois teoremas, decorrem todos os demais teoremas do Cáculo Diferencial e Integral de funções reais a valores reais. Mas antes de enunciarmos, vejamos algumas definições:

i. Seja A um subconjunto de $\mathbb{R}$. Dizemos que A é limitado superiormente se $k \in \mathbb{R}$ tal que $k \geq x$, $\forall\, x \in A$. Um tal k diz-se cota superior de A;

ii. De modo análogo, define-se um subconjunto de $\mathbb{R}$ limitado inferiormente e cota inferior;

iii. A diz-se limitado se for limitado superiormente e inferiormente;

iv. Suponhamos que A seja limitado superiormente e que exista uma cota superior de A, digamos s, que seja mínima. Neste caso s diz-se supremo de A e é denotado por $supA$;

v. De modo análogo, define-se ínfimo de A (para conjuntos A limitados inferiormente), denotado por $infA$, como sendo uma cota inferior máxima para o conjunto A.

Teorema 5.21. Se $X \subset \mathbb{R}$ é um conjunto não vazio e limitado superiormente, então existe $supX$.

Demonstração. Seja $A = \{\alpha \in \mathbb{R}|\ \alpha < x,\ \text{para algum } x \in X\}$, ou seja, A é o conjunto constituído precisamente pelos números reais que não são cotas superiores de X. Tome $B = \mathbb{R}\backslash A$, isto é, B é o conjunto constituído pelas cotas superiores de X. Vamos verificar que A e B satisfazem as condições do Teorema 5.20. As duas primeiras condições do teorema são válidas. Para a terceira condição, temos que, sendo $X \neq \emptyset$, existe $x \in X$, e portanto qualquer $\alpha < x$ é elemento de A, logo $A \neq \emptyset$. Ainda, como X é limitado superiormente, $B \neq \emptyset$.

Para verificarmos a quarta condição, consideremos $\alpha \in A$ e $\beta \in B$. Assim, existe $x \in X$ tal que $\alpha < x$. Como $\beta \geq x$, otemos que $\beta > \alpha$, e pelo Corolário 1, ou A possui máximo, ou B possui mínimo. Vamos mostrar que a primeira alternativa não pode ocorrer, dessa forma decorre que B possuí mínimo, provando o teorema.

Tomemos, então, $\alpha \in A$ arbitrário. Existe $x \in X$ tal que $\alpha < x$. Considere $\alpha^{'}$ tal que $\alpha < \alpha^{'} < x$. Como $\alpha^{'} < x$, então $\alpha^{'} \in A$ e é maior do que α, ou seja, nenhum elemento de A é maior do que os demais, como queríamos demonstrar. □

Essa propriedade, válida para $\mathbb{R}$, não se verifica em $\mathbb{Q}$, isto é, não é verdade que todo subconjunto de números racionais não vazio e limitado superiormente em $\mathbb{Q}$ sempre admita supremo em $\mathbb{Q}$. Por exemplo, o conjunto $A = \{x \in \mathbb{Q}_+ \mid x^2 < 2\}$ não possui supremo racional, mas tem supremo, se considerado como subconjunto de $\mathbb{R}$.

Teorema 5.22. O conjunto $\mathbb{N}$ dos naturais é ilimitado em $\mathbb{R}$.

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

Definição 41. Seja $a \in \mathbb{R}$ e $n \in \mathbb{N}$. Definimos a potencia a^n, recursivamente, como sendo:

$$a^n = \begin{cases} 1, \text{ se} & n = 0 \\ a \cdot a^{n-1}, \text{ se} & n > 1 \end{cases}.$$

Finalmente, se $a \neq 0$, definimos:

$$a^{-n} = \left(a^{-1}\right)^n.$$

Proposição 46. *Se a e b são reais e n, m são inteiros positivos, são válidos:*

1. $(ab)^n = \ a^n \cdot b^n$;
2. $a^n a^m = a^{n+m}$;
3. $(a^n)^m = a^{mn}$.

Demonstração. Realizaremos a demonstração do primeiro item, visto que os outros se dão de modo análogo. Usemos indução finita.

Seja $n = 0$. Por definição, $(ab)^0 = 1$ e $a^0 \cdot b^0 = 1 \cdot 1 = 1$. Logo, $(ab)^0 = a^0 \cdot b^0$.

Suponhamos que a igualdade vale para n, provemos então que vale para $n + 1$. Nossa hipótede de indução nos diz que $(ab)^n = a^n \cdot b^n$.

Por definição, $(ab)^{n+1} = (ab)(ab)^{n+1-1} = (ab)(ab)^n$. Pela hipótese de indução temos que:

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

Por definição novamente,

$$a^{n+1}b^{n+1} = aa^{n+1-1}bb^{n+1-1} = aa^n bb^n = (ab)a^n b^n.$$

Portanto, por indução, a igualdade é válida. $\square$

Tais propriedades também são válidas para $m, n \in \mathbb{Z}$, bastando notar que se $m < 0$, então $m = -n$, para algum $n \in \mathbb{N}$. Daí, $a^m = a^{-n} = (a^{-1})^n$, voltando aos itens da Proposição 46. Para expoentes negativos, a base deve ser não nula.

Teorema 5.23. Seja a um real positivo e $n > 0$ natural. Existe um único número real positivo que é solução da equação $x^n = a$.

Demonstração. A prova deste teorema pode ser encontrada em [8]. $\square$

Definição 42. Dado um número real positivo a, o único número real positivo que é solução da equação $x^n = a$, estabelecido pelo teorema anterior, chama-se raiz n-ésima de a e é denotado por $\sqrt[n]{a}$ ou por $a^{\frac{1}{n}}$. A raiz n-ésima de a permite que se defina expoente racional do seguinte modo: se m, n são inteiros positivos, $a^{\frac{m}{n}} = (a^{\frac{1}{n}})^m$ e, como para expoentes inteiros, $a^{\frac{-m}{n}} = (a^{-1})^{\frac{m}{n}}$

Proposição 47. *Se a e b säo reas positivos, n inteiro positivo e r, s racionais positivos, temos que:*

1. $(ab)^{\frac{1}{n}} = a^{\frac{1}{n}} b^{\frac{1}{n}}$;
2. $a^r a^s = a^{r+s}$;
3. $(a^r)^s = a^{rs}$;
4. $(ab)^r = a^r b^r$.

Demonstração. Mostraremos novamente o primeiro item, tendo em vista que os seguintes decorrem do mesmo modo usando manipulações algébricas com uso de propriedades já demonstradas. Sejam a, b reais positivos e $n \in \mathbb{N}^*$. Se temos $\alpha^n = a$ e $\beta^n = b$, por definição existem as seguintes soluções reais: $\alpha = a^{\frac{1}{n}}$ e $\beta = b^{\frac{1}{n}}$. Assim,

$$ab = \alpha^n \beta^n = (\alpha\beta)^n.$$

Por definição, $\alpha\beta = (ab)^{\frac{1}{n}}$, daí $a^{\frac{1}{n}} b^{\frac{1}{n}} = \alpha\beta = (ab)^{\frac{1}{n}}$, como queríamos mostrar. □

Vamos trazer um resultado análogo ao que vimos no Teorema 5.21, mas o teorema em questão trata do ínfimo.

O próximo teorema trata do ínfimo de um subconjunto de $\mathbb{R}$ limitado inferiormente, de forma análoga ao que vimos no caso do supremo de um subconjunto de $\mathbb{R}$ limitado superiormente.

Teorema 5.24. Todo subconjunto não vazio de números reais, limitado inferiormente, possui ínfimo.

Demonstração. Suponhamos $X \subset \mathbb{R}$ limitado inferiormente e consideremos o conjunto $-X = \{-x \in \mathbb{R} |\ x \in X\}$. Temos que $-X \subset \mathbb{R}$. Como X é limitado inferiormente, então existe $M \leq x$ para todo $x \in X$. Daí, temos que $-M \geq -x$, $\forall -x \in -X$, ou seja $-X$ é limitado superiormente e portanto, possui supremo.

Seja $c = sup(-X)$. Queremos mostrar que $-c = inf(X)$. De fato $c \geq -x$, $\forall\ -x \in -X$, ou ainda, $-c \leq x$, $\forall\ x \in X$. Logo, $-c$ é uma cota inferior de X. Suponhamos agora que exista d tal que $-c < d \leq x$ para todo $x \in X$. Sabemos de $d \leq x$, que $-d \geq -x$ para todo $-x \in -X$, isto é, $-d$ é cota superior de $-X$. Porém, temos que $-c < d \Rightarrow c > -d$, o que é uma contradição pois c é supremo de $-X$. Logo, $-c$ é a maior das cotas inferiores de X, ou seja $-c = inf(X)$, como queríamos. $\square$

5.2.2 Representação decimal dos números reais

Assumindo conhecida a representação dos inteiros em base dez, estudaremos a representação decimal dos números reais. Para isso, trataremos de um resultado a respeito da representação dos números reais não negativos menores do que 1, a partir do qual obteremos a representação decimal dos demais números reais.

Proposição 48. *Dado um número real não negativo α, existe um número natural n_0 máximo que é menor ou igual a α. Além disso $0 \leq \alpha - n_0 < 1$.*

Demonstração. Tome $\alpha \in \mathbb{R}_+$. Considere o conjunto $A = \{n \in \mathbb{N} |\ n \leq \alpha\}$. Queremos mostrar que A possui um elemento máximo. De fato, seja $B = \{p \in \mathbb{N} |\ p > \alpha\}$. Claramente $B \subset \mathbb{N}$ e, ainda $B \neq \emptyset$, pois, como já vimos $\mathbb{N}$ é ilimitado em $\mathbb{R}$. Assim, pelo Princípio da Boa Ordem, B possui um elemento mínimo, digamos p_0. Dessa forma, $p_0 \leq p$ para todo $p \in B$. Assim, $\alpha < p_0 \leq p$, para todo $p \in B$. Dessa maneira, $p_0 - 1 \notin B$, ou seja, $p_0 - 1 \leq \alpha$, logo $p_0 - 1 \in A$. Afirmamos que $p_0 - 1$ é o máximo de A. Com efeito, suponhamos que $p_0 - 1 < n$ para algum $n \in A$. Daí, $p_0 - 1 < n \leq \alpha$, ou ainda $p_0 \leq n \leq \alpha$, sendo uma contradição, pois $p_0 > \alpha$. Agora, tendo que n_0 é o máximo de A, claramente $n_0 \leq \alpha < n_0 + 1$, donde $0 \leq \alpha - n_0 < 1$. $\square$

Teorema 5.25. (Representação decimal dos números reais.)

1. A cada número real α, näo negativo e menor do que 1, corresponde uma única sequência de digitos $(n_k)_{k\in\mathbb{N}^*}$, satisfazendo :

   a) $0 \leq n_k \leq 9$, para todo $k \in \mathbb{N}^*$;

   b) $(n_k)_{k\in\mathbb{N}^*}$ não possui infinitos dígitos consecutivos iguais a 9;

   c) definindo, para cada $k \in \mathbb{N}, S_k$ como a soma $\dfrac{n_1}{10} + \dfrac{n_2}{10^2} + \ldots + \dfrac{n_k}{10^k}, \alpha$ será supremo do conjunto $S = \{S_k \mid k \in \mathbb{N}^*\}$.

2. Reciprocamente, a cada sequência de digitos $(n_k)_{k\in\mathbb{N}*}$, satisfazendo $1a$ e $1b$, e definindo S_k como em $1c$, corresponde um único número real α, não negativo e menor do que 1, que é o supremo do conjunto limitado superiormente $S = \{S_k \mid k \in \mathbb{N}^*\}$.

Demonstração. A prova está feita em [3]. $\square$

Definição 43. 1. Dado um número real α, com $0 \leq \alpha < 1$, seja $(n_k)_{k\in\mathbb{N}^*}$, a sequência de dígitos correspondentes a α, sem infinitos noves consecutivos, construída na primeira parte do Teorema 5.25, a representação decimal de α, se define como sendo a expressão $0, n_1n_2n_3\ldots$. Se $n_k \neq 0$ e $n_l = 0$, para todo $l > k$, convenciona-se a representação por $0, n_1n_2n_3\ldots$ por $0, n_1n_2n_3\ldots n_k$, que será dita representação decimal finita de α.

2. Se $\alpha \geq 1$, seja n_0 o maior número natural que é menor ou igual a α, dado na Proposição 48. Seja, $0, n_1n_2n_3\ldots n_k\ldots$ a representação decimal de $\alpha - n_0$ definida em (1). Definimos a representação decimal de α como sendo a expressão $n_0, n_1n_2n_3\ldots n_k\ldots$

3. Se $\alpha < 0$, definimos sua representação decimal como sendo $-r$, onde r é a representação de $-\alpha$.

Sabemos que as representações decimais não consideram expressões com infinitos noves consecutivos. Porém, é possível atribuir a elas um significado semelhante aos das expressões sem infinitos noves consecutivos. Seja a expressão $0, 99999\ldots$ Vamos estender o que vimos para representações sem infinitos noves sucessivos. O número real α a ela associado deverá ser o supremo do conjunto $S = \{S_k |\ k \in \mathbb{N}^*\}$, onde $S_k = \dfrac{9}{10} + \dfrac{9}{10^2} + \cdots + \dfrac{9}{10^k}$ que é, pelo Teorema 5.25, o número real 1. Por outro lado, a representação decimal de 1 é, pela Definição 43, $1, 0000\ldots$, que convencionamos representar pelo própiro 1. Com efeito, tem-se como resultado, que tais expressões também representam números reais com representação decimal finita, e de forma recíproca, qualquer representação decimal finita diferente da do número 0 admite uma representação com infnitos noves consecutivos nos termos acima. Para isso, vejamos o seguinte exemplo.

Exemplo 13. A representação decimal $2, 79999\ldots$ também representa o número $2, 8$. De fato, neste caso $n_0 = 2$ e o número real $\alpha - n_0$ deve ser o supremo do conjunto $S = \{S_k |\ k \in \mathbb{N}^*\}$, onde $S_k = \dfrac{7}{10} + \dfrac{9}{10^2} + \cdots + \dfrac{9}{10^k} + \cdots$. Analogamente ao que foi visto acima, $\dfrac{9}{10^2} + \cdots + \dfrac{9}{10^k} + \cdots$ converge para $0, 1$, daí S_k converge para $0, 8$, ou seja, a representação deste α, segundo a Definição 43, é $2, 8$. Do mesmo modo, a representação decimal com infinitos noves de $0, 47$ é representada por $0, 46999\ldots$.

Deste modo, estamos apontando que as representações decimais finitas ou periódicas correspondem a números racionais. De fato, seja $\alpha = 0, a_1a_2\ldots a_n$ um número real com representação decimal finita. Vamos multiplicar por 10^n ambos os lados da igualdade. Assim:

$$10^n\alpha = a_1a_2\ldots a_n \Rightarrow \alpha = \frac{a_1a_2\ldots a_n}{10^n},$$

o que nos garante que α é um número racional.

Do mesmo modo, podemos garantir que se α é um número real com representação decimal periódica ($n \geq 1$), então ele será um número racional. Basta vermos que se $\alpha = 0, a_1a_2\ldots a_na_1a_2\ldots a_n$, multiplicando por 10^n em ambos os lados da igualdade obtemos, $10^n\alpha = a_1a_2\ldots a_na_1a_2\ldots a_n$ e subtraindo os lados destas duas igualdades na ordem dada, temos:

$$10^n\alpha - \alpha = a_1a_2\ldots a_n \Rightarrow (10^n-1)\alpha = \frac{a_1a_2\ldots a_n}{10^n-1}.$$

De forma recíproca, podemos provar que todo número racional possui uma representação decimal finita ou periódica.

5.2.3 $\mathbb{R}$ não é enumerável

A representação decimal dos números reais nos permite mostrar que $\mathbb{R}$ não é enumerável (ver a definição 49). Para tal, precisamos antes de dois resultados.

Proposição 49. *Todo subconjunto infinito de um conjunto enumerável é enumerável.*

Demonstração. Seja X um conjunto enumerável e Y um subconjunto infinito de X. Como X é enumerável, existe $f : X \longrightarrow \mathbb{N}$ bijetora. Dessa forma, $f|_Y : Y \longrightarrow \mathbb{N}$ e, com isso, $f(Y) \subset \mathbb{N}$. Usando o resultado que todo subconjunto infinito de $\mathbb{N}$ é enumerável temos que $f(Y)$ é enumerável (ver em [5]), ou seja, existe $g : f(Y) \longrightarrow \mathbb{N}$ bijetora. Sabendo que g *e* $f|_Y$ são bijetoras, obtemos que $g \circ f|_Y : Y \longrightarrow \mathbb{N}$ é bijetora, portanto, Y é enumerável, como queríamos. □

Lema 7. *O intervalo* $I = (0,1)$ *não é enumerável.*

Demonstração. Queremos mostrar que, para qualquer que seja a enumeração estabelecida para os elementos de I, sempre existirá um elemento de I não considerado na dada enumeração, ou seja, qualquer subconjunto enumerável de I é diferente de I e obteremos, portanto, que I não pode ser enumerável. Seja então I' um conjunto enumerável constituído de elementos de I, ou seja que, pode ser escrito como $I' = \{x_0, x_1, x_2, \ldots\}$, onde para cada $n \in \mathbb{N}$, x_n representa a imagem de n por uma certa bijeção de $\mathbb{N}$ em I'. Vamos representar cada elemento de I' pela sua representação decimal dada acima, sem infinitos noves consecutivos e dispô-las na forma de uma "Matriz Infinita", assim:

$$\begin{aligned}
x_0 &= 0, x_{00}x_{01}x_{02}\ldots \\
x_1 &= 0, x_{10}x_{11}x_{12}\ldots \\
x_2 &= 0, x_{20}x_{21}x_{22}\ldots \\
&\vdots \\
x_k &= 0, x_{k0}x_{k1}x_{k2}\ldots
\end{aligned}$$

Agora vamos construir um número real $x \in I$, diferente de todos os elementos de I' usando a seguinte representação decimal: $0, a_0a_1a_2a_3\ldots$, onde, para cada $n \in \mathbb{N}$, o digito decimal a_n dessa representação é diferente de 9, de 0 e do dígito decimal x_{nn}

da representação de x_n. Pela correspondência bijetora que foi estabelecida acima entre números reais e representações decimais sem infinitos noves, a representação decimal $0, a_0a_1a_2a_3\ldots$, corresponde a um único número real de I, que é diferente de todos os elementos de I', como queríamos. Este belo argumento se deve a Cantor, e é chamado também método da diagonal de Cantor. □

Teorema 5.26. O conjunto dos números reais não é enumerável;

Demonstração. O subconjunto I de $\mathbb{R}$ dado pelo Lema 7 é não enumerável, e pela Proposição 49, $\mathbb{R}$ não pode ser enumerável. □

5.3 Construção de Cantor

Nesta seção abordaremos a segunda forma de construção do conjunto dos números reais. A princípio o conjunto que construiremos será chamado de Conjunto de Cauchy e representado por $\mathbb{S}$. Mostraremos que esse conjunto é um corpo ordenado completo e que existe um isomorfismo entre $\mathbb{S}$ e o conjunto construído na Seção 5.2, via cortes de Dedekind. Utilizaremos sequências de Cauchy e, novamente, o conceito de relação de equivalência, semelhante ao que foi feito na construção dos inteiros e dos racionais (Capítulos 3 e 4, respectivamente).

5.3.1 Relação no conjunto $\mathbb{S}$

Seja $\mathbb{S}_{\mathbb{Q}}$ o conjunto definido por

$$\{x : \mathbb{N} \to \mathbb{Q}; (x_n)_n \text{ é de Cauchy}\},$$

isto é, $\mathbb{S}_{\mathbb{Q}}$ é o conjunto das sequências racionais de Cauchy. Sobre esse conjunto definiremos uma relação, tendo como base a convergência de uma sequência racional.

Definição 44. Sejam x, y duas sequências em $\mathbb{S}_{\mathbb{Q}}$. Diremos que a sequência x se relaciona com a sequência y se

$$\lim_{n\to\infty} (x_n - y_n) = 0.$$

Quando x se relacionar com y utilizaremos a notação $x \sim y$.

Exemplo 14. Sejam x, y as sequências racionais tais que: $x_n = 1$ e $y_n = \dfrac{10^n - 1}{10^n}$. Ou ainda:

$$x = (1, 1, \ldots, 1, \ldots),\ y = \left(\frac{9}{10}, \frac{99}{100}, \ldots, \frac{10^n - 1}{10^n}, \ldots\right).$$

Essas sequências são monótonas, limitadas e, pelo Teorema 5.1, são de Cauchy. Mais ainda, tomando a diferença entre as duas sequências, temos:

$$(x_n - y_n) = \left(\frac{1}{10}, \frac{1}{100}, \ldots, \frac{1}{10^n}, \ldots\right).$$

Queremos ver que a sequência x se relaciona com a sequência y. Para isso, devemos ver que a sequência $z_n = \dfrac{1}{10^n}$ converge para zero. Assim, dado $\epsilon > 0$, consideremos a sequência $w = \dfrac{1}{n}$. Existe um $n_\epsilon \in \mathbb{N}$ tal que $n > n_\epsilon \Rightarrow \left|\dfrac{1}{n} - 0\right| < \epsilon$. Mas usando indução, podemos concluir que: $\left|\dfrac{1}{10^n} - 0\right| < \left|\dfrac{1}{n} - 0\right|$. Assim,

$$n > n_\epsilon \Rightarrow \left|\frac{1}{n} - 0\right| < \epsilon \Rightarrow \left|\frac{1}{10^n} - 0\right| < \epsilon.$$

Portanto, temos $\lim\limits_{n\to\infty} z_n = \lim\limits_{n\to\infty} (x_n - y_n) = 0$.

A relação que definimos em $\mathbb{S}_\mathbb{Q}$ é uma relação de equivalência, isto é, é **reflexiva, simétrica, transitiva**. Vamos, de fato, mostrar que são válidas essas propriedades.

- Reflexiva: consideremos $x \in \mathbb{S}_\mathbb{Q}$, onde cada termo da sequência é representado por x_n. Assim,

$$x_n - x_n = 0, \ \forall \ n \in \mathbb{N} \Rightarrow \lim_{n\to\infty}(x_n - x_n) = 0 \Rightarrow x \sim x.$$

- Simétrica: sejam duas sequências $x, y \in \mathbb{S}_\mathbb{Q}$ tais que $x \sim y$. Temos então que: $\lim\limits_{n\to\infty} (x_n - y_n) = 0$. Ou seja, dado $\epsilon > 0$, existe n_e tal que $n > n_e \Rightarrow |(x_n - y_n) - 0| < \epsilon$. Por outro lado,

$$|(x_n - y_n) - 0| < \epsilon \Leftrightarrow |x_n - y_n| < \epsilon \Leftrightarrow |y_n - x_n| < \epsilon \Leftrightarrow |(y_n - x_n) - 0| < \epsilon.$$

Portanto, é válido também que

$$\lim_{n\to\infty} (y_n - x_n) = 0 \Rightarrow y \sim x.$$

- Transitiva: sejam $x,\ y,\ z \in \mathbb{S}_\mathbb{Q}$, de forma que $x \sim y,\ y \sim z$, e mostremos que $x \sim z$. Dado $\dfrac{\epsilon}{2} > 0$, existe $n_{\epsilon_1}, n_{\epsilon_2} \in \mathbb{N}$ tais que $n > n_{\epsilon_1} \Rightarrow |(x_n - y_n) - 0| < \dfrac{\epsilon}{2}$ e $n > n_{\epsilon_2} \Rightarrow |(y_n - z_n) - 0| < \dfrac{\epsilon}{2}$. Agora, seja $n_\epsilon = \max\{n_{\epsilon_1}, n_{\epsilon_2}\}$. Utilizando a desigualdade triangular temos

$$n > n_\epsilon \Rightarrow |x_n - z_n| = |(x_n - y_n) + (y_n - z_n)| \leq |x_n - y_n| + |y_n - z_n| < \frac{\epsilon}{2} + \frac{\epsilon}{2} = \epsilon.$$

Assim,

$$\lim_{n\to\infty} (x_n - z_n) = 0 \Rightarrow x \sim z.$$

Dessa maneira, provamos que a relação definida no início deste capítulo é, de fato, uma relação de equivalência.

Definição 45. Dada uma sequência $(x_n) \in \mathbb{S}_\mathbb{Q}$, chamaremos o conjunto

$$\{y \in \mathbb{S}_\mathbb{Q} : \ y \sim x\}$$

de classe de equivalência da sequência (x_n) e denotaremos por $\overline{(x_n)}$, isto é:

$$\overline{(x_n)} = \{y \in \mathbb{S}_\mathbb{Q} : \ y \sim x\}.$$

O principal conjunto deste capítulo será definido via classes de equivalência.

Definição 46. Chamaremos de **Conjunto de Cauchy** o conjunto

$$\mathbb{S} = \{\overline{(x_n)} : \ (x_n) \in \mathbb{S}_{\mathbb{Q}}\}.$$

Notemos que $\mathbb{S} \neq \emptyset$ pois $\mathbb{S}_{\mathbb{Q}} \neq \emptyset$.

5.3.2 Adição no conjunto de Cauchy

Vejamos que é possível, a partir de duas sequências de Cauchy, definirmos uma outra sequência de Cauchy. Sejam (x_n) e $(y_n) \in \mathbb{S}_{\mathbb{Q}}$. Vamos provar que a sequência

$$(x_1 + y_1, x_2 + y_2, \ldots, x_n + y_n, \ldots)$$

também é de Cauchy. De fato, dado $\epsilon > 0$, $\exists n_\epsilon \in \mathbb{N}$ tal que:

$$m, n > n_\epsilon \Rightarrow |(x_m + y_m) - (x_n + y_n)| = |(x_m - x_n) + (y_m + y_n)| \leq \ldots$$
$$\ldots \leq |x_m - x_n| + |y_m - y_n| < \frac{\epsilon}{2} + \frac{\epsilon}{2} = \epsilon.$$

Logo, a sequência obtida pela adição termo a termo de duas sequências de cauchy também é de Cauchy.

Definição 47. Sejam $t = \overline{(x_n)}$ e $u = \overline{(y_n)}$ duas classes de equivalência em $\mathbb{S}$. Definimos a adição de t e u por

$$t + u = \overline{(x_n + y_n)}.$$

Agora é necessário provarmos que a operação está bem definida. Devemos verificar que, dadas duas classes de equivalência $t, u \in \mathbb{S}$ tais que $t = \overline{(x_n)} = \overline{(x_n^{'})}, u = \overline{(y_n)} = \overline{(y_n^{'})}$, teremos

$$\overline{(x_n + y_n)} = \overline{(x_n^{'} + y_n^{'})}.$$

Como $\overline{(x_n)} = \overline{(x_n^{'})}$, temos que $\left(x_n - x_n^{'}\right) \to 0$. Analogamente, $\left(y_n - y_n^{'}\right) \to 0$. Assim, dado $\epsilon > 0$, $\exists n_1 \in \mathbb{N}$ tal que $n > n_1 \Rightarrow |x_n - y_n| < \dfrac{\epsilon}{2}$ e $\exists n_2 \in \mathbb{N}$ tal que $n > n_2 \Rightarrow |x_n^{'} - y_n^{'}| < \dfrac{\epsilon}{2}$. Agora, utilizando a desigualdade triangular, obtemos

$$|(x_n + y_n) - (x_n^{'} + y_n^{'})| = |(x_n - x_n^{'}) + (y_n - y_n^{'})| \leq |x_n - x_n^{'}| + |y_n - y_n^{'}| < \frac{\epsilon}{2} + \frac{\epsilon}{2} = \epsilon.$$

Portanto, $(x_n + y_n) \sim (x_n^{'} + y_n^{'})$ e a soma $t + u$ independe das sequências representantes das classes de equivalência. Dessa maneira, a adição em $\mathbb{S}$ está bem definida.

A seguir, provaremos algumas propriedades relativas à adição.

- (Propriedade Associativa) Dadas t, u e $v \in \mathbb{S}$ é sempre válida a relação:

$$(t + u) + v = t + (u + v).$$

Demonstração. Como $t, u, v \in \mathbb{S}$, existem sequências $(x_n), (y_n), (z_n) \in \mathbb{S}_{\mathbb{Q}}$, tais que $t = \overline{(x_n)},\ u = \overline{(y_n)}$ e $v = \overline{(z_n)}$. Agora, utilizando a definição de adição (Definição 47) temos

$$(t + u) + v = \overline{(x_n + y_n)} + \overline{(z_n)} = (\overline{(x_n + y_n) + z_n}).$$

Usando o fato de $\mathbb{Q}$ ser um corpo, temos

$$((x_n + y_n) + z_n)_n = (x_n + (y_n + z_n))_n\,.$$

Logo,

$$(t + u) + v = (\overline{(x_n + y_n) + z_n}) = (\overline{x_n + (y_n + z_n)}) = \overline{(x_n)} + \overline{(y_n + z_n)} = t + (u + v).$$

Portanto, a propriedade associativa é válida para a adição em $\mathbb{S}$. □

- (Existência do Elemento Neutro da Adição) Existe o elemento $0 \in \mathbb{S}$ tal que $0 = \overline{(\theta_n)}$, onde $(\theta_n) = (0, 0, 0, \ldots)$ é um representante da classe de equivalência do elemento neutro da adição, isto é, dada $t \in \mathbb{S}$, temos que $t + 0 = 0 + t = t,\ \forall\, t \in \mathbb{S}$.

  Demonstração. Primeiro, lembremos que toda sequência racional constante é convergente, e que toda sequência convergente é de Cauchy. Portanto, $\theta_n \in \mathbb{S}_{\mathbb{Q}}$ e $0 \in \mathbb{S}$. Agora, sejam $t = \overline{(x_n)}$ *e* $0 = \overline{(\theta_n)}$. Assim,

  $$t{+}0 = \overline{(x_n + \theta_n)} = [(x_1{+}0, x_2{+}0, \ldots, x_n{+}0, \ldots)] = [(x_1, x_2, \ldots, x_n, \ldots)] = \overline{(x_n)} = t.$$

  Como t é um elemento arbitrário, então isso é válido para todo elemento do conjunto de Cauchy. O caso de $0 + t$ é análogo ao anterior. É importante notarmos a difereça entre o símbolo 0 em $\mathbb{Q}$ e em $\mathbb{S}$, sendo feita a distinção pelos termos envolvidos. □

- (Existência do Elemento Inverso Aditivo) Para cada $t \in \mathbb{S}$ existe um elemento que será denotador por $-t \in \mathbb{S}$ tal que $t + (-t) = 0$, onde $0 = \overline{(\theta_n)}$.

  Demonstração. Observe inicialmente que se uma sequência $(x_n) \in \mathbb{S}_{\mathbb{Q}}$, então $(-x_n) \in \mathbb{S}_{\mathbb{Q}}$, pois se $|x_n - x_m| < \epsilon$ então $|(-x_m) - (-x_n)| < \epsilon \Rightarrow |(-x_n) - (-x_m)| < \epsilon \Rightarrow (-x_n) \in \mathbb{S}_{\mathbb{Q}}$. Portanto, dada $t = \overline{(x_n)} \in \mathbb{S}$, existe $\overline{(-x_n)} \in \mathbb{S}$, a qual denotaremos por $-t = \overline{(-x_n)}$. Logo, $t + (-t) = t = \overline{(x_n + (-x_n))} = \overline{(0, 0, \ldots)} = \overline{(\theta_n)} = 0$. Portanto $\forall\ t \in \mathbb{S}$, existe um elemento $-t \in \mathbb{S}$ cuja adição resulta no elemento neutro da adição. □

- (Propriedade Comutativa) Para quaisquer $u, t \in \mathbb{S}$ temos que $t + u = u + t$.

Demonstração. Sejam $t, u \in \mathbb{S}$ tais que $t = \overline{(x_n)}$ e $u = \overline{(y_n)})$. Temos que

$$t + u = \overline{(x_n + y_n)} = \overline{(y + n + x_n)} = u + t.$$

A segunda igualdade decorre do fato do conjunto dos números racionais ser um corpo, e as demais, apenas pela definição da soma. Portanto, o conjunto de Cauchy $\mathbb{S}$ possui a propriedade comutativa da adição. □

Provadas algumas das propriedades para adição, podemos tratar da próxima operação em $\mathbb{S}$.

5.3.3 Multiplicação no conjunto de Cauchy

Semelhante ao que fizemos no caso da adição, vamos provar que dadas duas sequências de Cauchy, a nova sequência dada pelo produto termo a termo dessas sequências também será de Cauchy. Isto é, dadas (x_n) e $(y_n) \in \mathbb{S}_{\mathbb{Q}}$, a sequência

$$(x_1 \cdot y_1, x_2 \cdot y_2, \ldots, x_n \cdot y_n, \ldots)$$

é de Cauchy. Com efeito, sabemos pelo Teorema 5.2 que toda sequência de Cauchy é limitada. Portanto, existem M e M' tais que, para todo $n, m \in \mathbb{N}$ temos $|y_m| \leq M$ e $|x_n| \leq M'$. Consideremos as seguintes igualdades:

$$x_m \cdot y_m - x_n \cdot y_n = x_m \cdot y_m + (y_m \cdot x_n - y_m \cdot x_n) - x_n \cdot y_n$$

$$= (x_m \cdot y_m - y_m \cdot x_n) + (y_m \cdot x_n - x_n \cdot y_n) = y_m(x_m - x_n) + x_n(y_m - y_n).$$

Agora, utilizando o fato de serem sequências de Cauchy, temos que dado $\epsilon > 0$,

$$\exists n_\epsilon \in \mathbb{N};\ m, n > n_\epsilon \Rightarrow |x_m - x_n| < \frac{\epsilon}{2 \cdot R} \text{ e } |y_m - y_n| < \frac{\epsilon}{2 \cdot R}.$$

Tomando $R = M + M'$ e utilizando a desigualdade triangular teremos

$$|x_m \cdot y_m - x_n \cdot y_n| \leq |y_m||x_m - x_n| + |x_n||y_m - y_n|$$

$$\leq R \cdot |x_m - x_n| + R \cdot |y_m - y_n| = R \cdot (|x_m - x_n| + |y_m - y_n|)$$
$$\Rightarrow |x_m \cdot y_m - x_n \cdot y_n| < R \cdot \left(\frac{\epsilon}{2 \cdot R} + \frac{\epsilon}{2 \cdot R}\right) = \epsilon, \forall\ m, n > \epsilon.$$

Definição 48. Dadas as classes de equivalência $t, u \in \mathbb{S}$ tais que $t = \overline{(x_n)}$ e $u = \overline{(y_n)}$, definimos a multiplicação de t por u por

$$t \cdot u = \overline{(x_n \cdot y_n)}.$$

Assim como na adição, é necessário verificarmos se a aplicação de multiplicação está bem definida, ou seja, se a multiplicação independe da escolha do represetante da classe. Isto é, dadas duas classes de equivalência $t, u \in \mathbb{S}$ tais que $t = \overline{(x_n)} = \overline{(x_n')}$ e $u = (\overline{y_n}) = (\overline{y_n'})$, deverá ocorrer a igualdade

$$\overline{(x_n \cdot y_n)} = \overline{(x_n' \cdot y_n')}.$$

Sabemos que se $\overline{(x_n)} = \overline{(x_n')}$, então $(x_n - x_n') \to 0$. Da mesma forma, $(y_n - y_n') \to 0$. Agora, utilizando a desigualdade triangular obtemos

$$\begin{aligned}\left|x_n \cdot y_n - x_n' \cdot y_n'\right| = \left|y_n \left(x_n - x_n'\right) + x_n' \left(y_n - y_n'\right)\right| \leq \left|y_n \left(x_n - x_n'\right)\right| + \left|x_n' \left(y_n - y_n'\right)\right| = \\ = |y_n| \left|x_n - x_n'\right| + \left|x_n'\right| \left|y_n - y_n'\right|.\end{aligned}$$

Sabemos que toda sequência de Cauchy é limitada. Então, existem M e M' tais que para todo $n \in \mathbb{N}$ tem-se $|y_n| \leq M$ e $|x_n'| \leq M'$. Tomando $R = M + M'$ teremos

$$\left|x_n \cdot y_n - x_n' \cdot y_n'\right| \leq |y_n| \left|x_n - x_n'\right| + \left|x_n'\right| \left|y_n - y_n'\right| \leq R \cdot \left(\left|x_n - x_n'\right| + \left|y_n - y_n'\right|\right).$$

Como $(x_n - x_n') \to 0$ e $(y_n - y_n') \to 0$, então $(x_n \cdot y_n - x_n' \cdot y_n') \to 0$. Portanto,

$$\overline{(x_n \cdot y_n)} = \overline{(x_n' \cdot y_n')}.$$

Desta maneira, vemos que o produto $t \cdot u$ independe das sequências representantes das classes. Logo, a operação de multiplicação em $\mathbb{S}$ está bem definida. Provaremos a seguir algumas propriedades desta operação.

- (Propriedade Associativa da Multiplicação) Dados quaisquer $t, u, v \in \mathbb{S}$, é válido que

$$(t \cdot u) \cdot v = t \cdot (u \cdot v).$$

Como $t, u, v \in \mathbb{S}$ existem sequências $(x_n), (y_n), (z_n) \in \mathbb{S}_{\mathbb{Q}}$ tais que $t = \overline{(x_n)},\ u = \overline{(y_n)}$ e $v = \overline{(z_n)}$. Utilizando a definição de multiplicação, temos

$$(t \cdot u) \cdot v = \overline{(x_n \cdot y_n)} \cdot \overline{(z_n)} = \overline{((x_n \cdot y_n) \cdot z_n)}.$$

Como $\mathbb{Q}$ é um corpo, temos

$$\overline{((x_n \cdot y_n) \cdot z_n)} = \overline{(x_n \cdot (y_n \cdot z_n))}.$$

Logo,

$$(t \cdot u) \cdot v = \overline{((x_n \cdot y_n) \cdot z_n)} = \overline{(x_n \cdot (y_n \cdot z_n))} = \overline{(x_n)} \cdot \overline{(y_n \cdot z_n)} = t \cdot (u \cdot v).$$

Assim, é válida a propriedade associativa para a operação de multiplicação no conjunto de Cauchy.

- (Existência do Elemento Neutro da Multiplicação) Existe o elemento $1 \in \mathbb{S}$, $1 = \overline{(i_n)}$, tal que $(i_n) = (1, 1, 1, \ldots)$ é um representante da classe de equivalência do elemento neutro da multiplicação em $\mathbb{S}$ e $t \cdot 1 = 1 \cdot t = t$, para todo $t \in \mathbb{S}$.

  Usando o fato de que toda sequência racional constante é convergente e que toda sequência racional convergente é de Cauchy, temos de fato que $1 \in \mathbb{S}$. Sejam $(x_n) \in \mathbb{S}_{\mathbb{Q}}$ tal que $t = \overline{(x_n)}$ e $1 = \overline{(i_n)}$. Assim,

$$t \cdot 1 = \overline{(x_n \cdot i_n)} = \overline{(x_1 \cdot 1, x_2 \cdot 1, \ldots, x_n \cdot 1, \ldots)} =$$

$$= \overline{(x_1, x_2, \ldots, x_n, \ldots)} = \overline{(x_n)} = t.$$

  Como t foi escolhido arbitrariamente, a proposição é válidada para todo elemento em $\mathbb{S}$. De maneira análoga é válido também que $1 \cdot t = 1$.

  Como no caso da adição, observamos que é necessário cuidado com relação ao símbolo 1 como elemento neutro do conjunto $\mathbb{Q}$ e agora do conjunto $\mathbb{S}$. A distinção é dada observando-se os termos envolvidos.

- (Propriedade Comutativa da Multiplicação) Para quaisquer $u, v \in \mathbb{S}$, temos que $u \cdot t = t \cdot u$.

  Sejam $t, u \in \mathbb{S}$ tais que $t = \overline{(x_n)}$ e $u = \overline{(y_n)}$. Temos que

$$t \cdot u = \overline{(x_n \cdot y_n)} = \overline{(y_n \cdot x_n)} = u \cdot t.$$

  A segunda igualdade decorre de $\mathbb{Q}$ ser um corpo e as demais utilizando a definição de multiplicação. Portanto, o conjunto $\mathbb{S}$ possui a propriedade comutativa com relação a multiplicação.

  Antes de verificarmos a existência do inverso multiplicativo, vejamos um lema que será necessário para tal resultado.

Lema 8. *Se uma sequência racional de Cauchy não tende para o número racional* 0*, então a partir de um certo termo com índice suficientemente grande todos os demais termos da sequência serão não-nulos.*

Demonstração. Seja $x \in \mathbb{S}_{\mathbb{Q}}$ tal que $x = (x_n)$ não tenha limite igual a zero. Suponha que

$$\begin{aligned}
&\text{dado } 0 < \epsilon_1 = 1 \in \mathbb{Q} \text{ exista } x_{n_1} \in \{x_1, x_2, x_3, \ldots\} \text{ tal que } |x_{n_1} - 0| < 1,\\
&\text{dado } 0 < \epsilon_2 = \frac{1}{2} \in \mathbb{Q} \text{ exista } x_{n_2} \in \{x_1, x_2, x_3, \ldots\} \text{ tal que } |x_{n_2} - 0| < \frac{1}{2},\\
&\text{dado } 0 < \epsilon_3 = \frac{1}{3} \in \mathbb{Q} \text{ exista } x_{n_3} \in \{x_1, x_2, x_3, \ldots\} \text{ tal que } |x_{n_3} - 0| < \frac{1}{3},
\end{aligned}$$

$$0 < \epsilon_k = \frac{1}{k} \in \mathbb{Q} \text{ exista } x_{n_k} \in \{x_1, x_2, x_3, \ldots\} \text{ tal que } |x_{n_k} - 0| < \frac{1}{k}.$$

Enquanto existir x_{n_p} nas condições acima, para algum ϵ_p, pode-se continuar esse processo. Mas esse processo é finito, pois caso contrário poderíamos construir uma subsequência da sequência (x_n) tal que a mesma convergiria para zero. Porém, pelo Teorema 5.4, isso implicaria que a sequência (x_n) também convergiria para zero, contradizendo nossa hipótese. Portanto $\exists \epsilon > 0$ e $\exists n_0 \in \mathbb{N}$ tal que $\forall\ n > n_0$, é válido que $|x_n| \leq \dfrac{1}{n_0}$. Dessa maneira, a partir de n_0, todos os termos da sequência são não nulos. $\square$

- (Existência do Elemento Inverso Multiplicativo) Para cada $t \in \mathbb{S} - \{0\}$, existe um elemento t^{-1} tal que $t \cdot t^{-1} = 1$.

Demonstração. Seja $t \in \mathbb{S} - \{0\}$ tal que $t = \overline{(x_n)}$ e isso nos diz que (x_n) não converge para 0 pois, se convergisse, teríamos que $\lim\limits_{n\to\infty} (x_n - 0) = 0 \Rightarrow \lim\limits_{n\to\infty} (x_n) = 0$, ou seja, a classe de equivalência de $\overline{(x_n)}$ é a mesma que a classe do elemento neutro 0. Absurdo, pois $t \in \mathbb{S} - \{0\}$. Pelo Lema 8 , existe $n_0 \in \mathbb{N}$ tal que $n > n_0 \Rightarrow x_n \neq 0$. Agora, seja (y_n) tal que $y_n = 0$, se $n \leq n_0$, e $y_n = \dfrac{1}{x_n}$, se $n > n_0$. Logo, se $m, n > n_0$, temos que

$$|y_m - y_n| = \left|\frac{1}{x_m} - \frac{1}{x_n}\right| = |x_n - x_m| \cdot \frac{1}{|x_m| \cdot |x_n|} < \frac{1}{|x_{n_0}|^2} \cdot |x_n - x_m| \,.$$

Como (x_n) é de Cauchy então (y_n) também é. Dessa forma, $x_n \cdot y_n = 0$ se $n \leq n_0$ e $x_n \cdot y_n = 1$ se $n > n_0$. Portanto, $(y_n) \in \mathbb{S}_{\mathbb{Q}}$ e

$$\overline{(x_n \cdot y_n)} = \overline{(0, 0, \ldots, 0, 0_{n_0}, 1, 1, \ldots, 1, 1, \ldots)}.$$

Assim, teremos que

$$(i_n - (x_n \cdot y_n)) \to 0;\ i_n = 1,\ \forall\ n \in \mathbb{N}.$$

Isso implica que

$$1 = \overline{(i_n)} = \overline{(x_n \cdot y_n)}.$$

Portanto $t^{-1} = \overline{(y_n)}$ é o inverso multiplicativo do elemento t, e podemos dizer que o conjunto de Cauchy é tal que todo elemento não nulo possui inverso multiplicativo. $\square$

- (Distributividade) Dadas quaisquer $t, u, s \in \mathbb{S}$ é sempre válido que $t \cdot (u + s) = t \cdot u + t \cdot s$.

Demonstração. Sejam $t, u, s \in \mathbb{S}$. Então existem sequências racionais de Cauchy tais que $t = \overline{(x_n)},\ u = \overline{(y_n)}$ e $s = \overline{(z_n)}$. Assim,

$$t \cdot (u + s) = \overline{(x_n)} \cdot \overline{(y_n + z_n)} = \overline{(x_n \cdot (y_n + z_n))}.$$

Como o conjunto dos números racionais é um corpo, segue que

$$\overline{(x_n \cdot (y_n + z_n))} = \overline{(x_n \cdot y_n + x_n \cdot z_n)}.$$

Portanto,

$$t \cdot (u + s) = \overline{(x_n \cdot (y_n + z_n))} = \overline{(x_n \cdot y_n + x_n \cdot z_n)} = \overline{(x_n \cdot y_n)} + \overline{x_n \cdot z_n)} = t \cdot u + t \cdot s.$$

Dessa maneira, o conjunto de Cauchy $\mathbb{S}$ é um corpo. □

5.3.4 O Conjunto de Cauchy é um Corpo Ordenado

Pensar na noção de ordem no conjunto de Cauchy significa pensar no conceito de sequência positiva. Para isso vamos definir a seguir o que é uma classe de equivalência positiva. Depois, consideraremos o conjunto das classes de equivalência positivas no conjunto de Cauchy. Tal conjunto terá as propriedades necessárias para caracterizarmos uma relação de ordem em $\mathbb{S}$.

Definição 49. Uma sequência $(x_n) \in \mathbb{S}_{\mathbb{Q}}$ é dita positiva se existem n_0, $M \in \mathbb{N}$ tais que $x_n > \dfrac{1}{M}$, para todo $n > n_0$.

Definição 50. Um elemento $t \in \mathbb{S}$ será dito positivo se existe uma sequência positiva $(x_n) \in \mathbb{S}_{\mathbb{Q}}$ tal que $t = \overline{(x_n)}$.

Exemplo 15. Consideremos a sequência $x_n = \dfrac{n+1}{n}$. Essa sequência é positiva. De fato, $\forall\ n > 1$, temos que $n + 1 > n$, donde segue que $x_n = \dfrac{n+1}{n} > 1$. Dessa maneira, podemos tomar $n_0 = M = 1$. Assim, concluímos também que a classe de equivalência $\overline{\left(\dfrac{n+1}{n}\right)}$ é positiva.

Teorema 5.27. Se $t \in \mathbb{S}$ é tal que $t = \overline{(x_n)} = \overline{(x_n^{'})}$ e (x_n) é positiva, então a sequência $(x_n^{'})$ também é positiva.

Demonstração. Como (x_n) é positiva, existem $n_0, M \in \mathbb{N}$ tais que $x_n > \dfrac{1}{M}$ para todo $n > n_0$. Por outro lado, dado $\epsilon = \dfrac{1}{2M}$ existe $n_\epsilon \in \mathbb{N}$ tal que $n > n_\epsilon \Rightarrow |x_n - x_n^{'}| < \epsilon$, pois sabemos que $\overline{(x_n)} = \overline{(x_n^{'})}$ e isso nos diz que $(x_n - x_n^{'}) \to 0$. Tomando $n > max\{n_0, n_\epsilon\} = n_1$, teremos que

$$\left|x_n - x_n^{'}\right| < \epsilon \Rightarrow \left|x_n^{'} - x_n\right| < \epsilon \Rightarrow -\epsilon < x_n^{'} - x_n < \epsilon$$
$$\Rightarrow x_n - \epsilon < x_n^{'} < \epsilon + x_n.$$

Como $x_n > \dfrac{1}{M}$ e $\epsilon = \dfrac{1}{2M}$, segue que

$$\frac{1}{2M} = \frac{1}{M} - \frac{1}{2M} < x_n^{'}, \forall\ n > n_1.$$

Portanto $(x_n^{'})$ é positiva. □

Desta maneira, se uma classe de equivalência é positiva é porque todas as sequências que pertencem a esta classe também são positivas.

Seja $P \subset \mathbb{S}$ tal que, para todo $t \in P$, temos que t é positivo. A fim de que o conjunto P possa caracterizar uma relação de ordem em $\mathbb{S}$, devemos demonstrar as seguintes propriedades:

- Propriedade do Fechamento para Multiplicação: se duas classes de equivalência $t, s \in P$, então $t \cdot p \in P$.

Demonstração. Sejam $t, s \in P$ tais que $t = \overline{(x_n)}$ e $s = \overline{(y_n)}$. Então, existem $n_1, n_2, M, N \in \mathbb{N}$ tais que

$$n > n_1 \Rightarrow x_n > \frac{1}{M}$$

e também

$$n > n_2 \Rightarrow y_n > \frac{1}{N}.$$

Tome $n > max\{n_1, n_2\}$. Assim,

$$x_n \cdot y_n > \frac{1}{M} \cdot \frac{1}{N} = \frac{1}{M \cdot N} = \frac{1}{K}.$$

Dessa maneira, existem $n_0, K \in \mathbb{N}$ tais que $n > n_0 \Rightarrow (x_n \cdot y_n) > \dfrac{1}{K}$, onde $n_0 = max\{n_1, n_2\}$ e $K = M \cdot N$. Logo $\overline{(x_n \cdot y_n)}$ é positiva e, portanto, $t \cdot p \in P$. $\square$

- Lei da Tricotomia: dada uma classe de equivalência $t \in \mathbb{S}$, então ou $t \in P$, ou $t = 0$ ou $-t \in P$.

Demonstração. Suponhamos que $t \in \mathbb{S}$ não pertença ao conjunto P, ou seja que $\forall\ M, n_0 \in \mathbb{N}$ existe um x_{n_M} tal que $n_M > n_0$ mas $x_{n_M} \geq \dfrac{1}{M}$. Portanto,

$$M = 1 \Rightarrow \exists\ n_1;\ x_{n_1} \geq 1$$

$$M = 2 \Rightarrow \exists\ n_2;\ x_{n_2} \geq \frac{1}{2}$$

$$M = 3 \Rightarrow \exists\ n_3;\ x_{n_3} \geq \frac{1}{3}$$

$$\vdots$$

$$M = k \Rightarrow \exists\ n_k;\ x_{n_k} \geq \frac{1}{k}$$

Agora vamos olhar para a subsequência (x_{n_k}). Temos duas possibilidades: (x_{n_k}) converge para um certo racional r ou não. Caso essa subsequência venha a convergir para um racional r, então toda a sequência iria convergir para r. Logo, $t = \overline{(x_n)} = \overline{(x_{n_k})} = \overline{(r, r, r, \ldots)}$. Nesse caso teríamos $\left(x_{n_k} - \dfrac{1}{k}\right) \geq 0$, portanto $r \geq 0$. Se $r = 0$

teremos $t = \overline{(\theta_n)} = \overline{(0, 0, 0, \ldots)} = 0$. Se $r < 0$ então $-r > 0$. Neste caso, $-t = \overline{(-x_n)} = \overline{(-r, -r, -r, \ldots)}$ será positiva, pois a sequência constante $(-r, -r, -r, \ldots)$ é positiva. Isto é, $-t \in P$. No segundo caso, a subsequência não converge para nenhum número natural e, em particular, não convergirá para 0. Pelo Lema 8, todos os termos da subsequência, para $n \in \mathbb{N}$ suficientemente grande, serão não nulos, pois $|x_{n_k}| \leq c > 0, \forall\ k > k_0$. Dessa forma, a partir de um certo $n_0 \in \mathbb{N}$ todos os termos serão positivos. Com isso, $(-x_n)$ será positiva e, consequentemente, $-t = \overline{(-x_n)}$ também será positivo. Portanto $-t \in P$.

O caso $-t \in \mathbb{S}$, mas não pertence ao conjunto P, é análogo ao caso anterior.

Agora se $t = \overline{(-x_n)}$ não é zero, certamente a sequência (x_n) não tende a zero, e como se trata de uma sequência de Cauchy, para $n \in \mathbb{N}$ suficientemente grande, os termos seriam todos maiores que zero ou todos menores que zero. Portanto (x_n) é positiva ou $(-x_n)$ é positiva. Assim, temos que $t \in P$ ou $-t \in P$. $\square$

Diremos que $t \in \mathbb{S}$ é maior que $s \in \mathbb{S}$ e escreveremos $t > s$ se, e somente se, $(t - s) \in P$, ou seja, se $(t - s)$ é positiva.

5.3.5 O Conjunto de Cauchy é um Corpo Ordenado Completo

Definiremos agora o que é uma cota superior de um subconjunto do conjunto de Cauchy para depois verificarmos que qualquer subconjunto do conjunto de Cauchy, limitado superiormente, terá a propriedade de existência da menor das cotas superiores. Para tal, utilizaremos sequências de classes de equivalência, ou seja, aplicações do tipo $x : \mathbb{N} \longrightarrow \mathbb{S}$. Usaremos a mesma notação de sequência de números racionais, e a distinção será feita mediante o contexto. Falaremos também sobre a noção de monotonicidade de uma sequência de classes de equivalência, visto que já estabelecemos uma relação de ordem em $\mathbb{S}$.

Definição 51. Seja $T \subset \mathbb{S}$ tal que $T \neq \emptyset$. Se existir um elemento $c \in \mathbb{S}$ tal que, $\forall\ t \in T$ tivermos $t \leq c$, então o elemento $c \in \mathbb{S}$ será chamado de cota superior do conjunto T. Nessa situação diremos que o conjunto T é limitado superiormente.

Seja $T \subset \mathbb{S}$, $T \neq \emptyset$ e suponhamos que $c \in \mathbb{S}$ seja uma cota superior de T. Construiremos duas sequências de classes de equivalência de forma conveniente. Seja $s_0 \in T$. Então, faremos

- $t_1 = c$ e $u_1 = s_0$.
- Supondo que já estejam definidos t_n e u_n consideremos $v_n = \dfrac{t_n + u_n}{2}$.
- Se v_n é uma cota superior para T definiremos $t_{n+1} = v_n$ e $u_{n+1} = u_n$.

- Se v_n não é uma cota superior para T, definiremos $t_{n+1} = t_n$ e $u_{n+1} = v_n$.

Como $s_0 \leq c$ provemos que a sequência (t_n) é não-crescente e a sequência (u_n) não-decrescente. Das definições de (t_n) e (u_n), temos que $u_n \leq t_n, \forall\, n \in \mathbb{N}$. Assim,

$$t_{n+1} = t_n$$

ou então,

$$t_{n+1} = v_n = \frac{t_n + u_n}{2} \leq \frac{t_n + t_n}{2} = \frac{2t_n}{2} = t_n.$$

Portanto, a sequência (t_n) é não-crescente. De forma análoga,

$$u_{n+1} = u_n$$

ou ainda,

$$u_{n+1} = v_n = \frac{t_n + u_n}{2} \geq \frac{u_n + u_n}{2} = \frac{2u_n}{2} = u_n.$$

Assim, a sequência (u_n) é não-decrescente.

Podemos observar ainda que a sequência (t_n) é formada apenas por cotas superiores do conjunto T. Logo, decorre da definição da sequência (u_n) que, para todo elemento da sequência u_{n_0}, existe um elemento x_0 em T tal que $u_{n_0} \leq x_0$. Vemos ainda que

$$s_0 = u_1 \leq u_2 \leq \ldots \leq u_n \leq \ldots \leq t_n \leq \ldots \leq t_2 \leq t_1 = c.$$

Para as próximas demonstrações serão utilizadas propriedades da relação de ordem, entre outras do conjunto de Cauchy. Tais propriedades serão demonstradas na próxima seção, mas a ordem nas demonstrações não afetará os resultados aqui provados.

Teorema 5.28. O conjunto de Cauchy $\mathbb{S}$ tem a propriedade da menor cota superior, isto é, dado um conjunto $T \subset \mathbb{S}$ tal que T seja limitado superiormente, existe $k \in \mathbb{S}$ tal que:

1. k é uma cota superior de T.

2. Se $c \in \mathbb{S}$ é uma cota superior de T então $k \leq c$.

Demonstração. Sejam (t_n) e (u_n) as sequências de classes de equivalência construídas acima. Temos três casos a analisar.

1. Se a sequência de classes de equivalência (u_n) ficar constante a partir de um certo n_0, isto é, se existir $n_0 \in \mathbb{N}$ tal que $n > n_0 \Rightarrow u_n = k$, então k será a menor cota superior do conjunto T. Além disso, sabemos que

$$t_p - u_p = \frac{1}{2^{p-1}}(t_0 - u_0).$$

Então, dado $\epsilon > 0$ e denotando $\epsilon = t_p - u_p$, para p suficientemente grande $\epsilon_p < \epsilon$. Assim,

$$t_p - k = \epsilon_p < \epsilon.$$

- Primeiro, sabemos que qualquer cota superior do conjunto T será maior ou igual a k, pois dada uma cota superior c temos que existe $x_0 \in T$ tal que $k \leq x_0$ mas por outro lado $x_0 \leq c$. Então, por transitividade da relação de ordem temos que $k \leq c$.

- Por outro lado a sequência (t_n) será decrescente, pela definição da construção da mesma. Assim, supondo que exista um elemento $w \in T$ tal que $w > k \Longrightarrow w - k > 0$. Contudo, podemos definir $\epsilon_p = t_p - k$ e, é claro que, para valores de p suficientemente grande, o valor de ϵ_p é arbitrariamente pequeno. Logo, existe p_0 tal que
$$\epsilon_{p_0} < w - k \Longrightarrow t_{p_0} - k < w - k \Longrightarrow t_{p_0} < w.$$
Mas isso é um absurdo, pois t_{p_0} é cota superior do conjunto T e $w \in T$. Portanto, k é a menor cota superior do conjunto T.

2. De forma análoga, se existir um n_0 tal que a sequência (t_n) se torne constante, isto é, $n > n_0 \Rightarrow t_n = k$, então k será a menor cota superior do conjunto T. Sabemos que $t_p - u_p = \dfrac{1}{2^{p-1}}(t_0 - u_0)$. Então, dado $\epsilon > 0$ e denotando $\epsilon_p = t_p - u_p$, para p suficientemente grande $\epsilon_p < \epsilon$ e assim teremos que
$$k - u_p = \epsilon_p < \epsilon.$$

- k é uma cota superior, pois é uma elemento da sequência (t_n).

- Seja $c \in \mathbb{S}$ uma cota superior. Como a sequência (t_n) é constante, para $n \in \mathbb{N}$ suficientemente grande, a sequência (u_n) é crescente, o que decorre da construção de ambas sequências. Suponhamos agora que $k > c$ e observemos a diferença $k - u_p$. Para p suficientemente grande essa diferença será arbitrariamente pequena, portanto existe $p_0 \in \mathbb{N}$ tal que
$$\epsilon_{p_0} = k - u_{p_0} < k - c \Longrightarrow -u_{p_0} < -c \Longrightarrow u_{p_0} > c.$$
No entanto, pela construção da (u_n), existe um $x_0 \in T$ tal que $x_{p_0} \geq u_{p_0}$. Mas isso implicaria que $x_{p_0} > c$, o que é um absurdo pois, por hipótese, c é uma cota superior. Então, temos que $k \leq c$. Assim, k é a menor cota superior do conjunto $T \subset \mathbb{S}$.

3. Agora suponhamos que as sequências (u_n) *e* (t_n) não se tornem constantes. Então existe n_0 tal que $u_{n_0+1} > u_{n_0} \Longrightarrow u_{n_0+1} - u_{n_0} > 0$. Vamos construir uma subsequência decrescente (t_{n_k}), pois a sequência (t_n) não se torna constante. Supondo agora que não exista a menor cota superior, para cada t_{n_k} existe uma cota superior q_k tal que $q_k < t_{n_k}$. Seja $\epsilon = u_{n_0+1} - u_{n_0}$. Sabemos que $t_p - u_p = \dfrac{1}{2^{p-1}}(t_1 - u_1)$. Em particular, para $p = n_0$ temos que
$$t_{n_0} - u_{n_0} = \frac{1}{2^{n_0-1}}(t_1 - u_1).$$

Por outro lado, temos

$$q_0 < t_{n_0} \Rightarrow q_0 - u_{n_0} < t_{n_0} - u_{n_0} = (t_{n_0} - u_{n_0+1}) + (u_{n_0+1} - u_{n_0}).$$

Como $t_{n_0} - u_{n_0+1} \geq 0$, pois existe $x_0 \in T$ tal que $t_{n_0} \geq x_0 \geq u_{n_0+1}$, então

$$q_0 - u_0 < \epsilon \Rightarrow q_0 - u_{n_0} < u_{n_0+1} - u_{n_0} \Rightarrow q_0 < u_{n_0}.$$

Mas isso é um absurdo, pois existe $x_1 \in T$ tal que $x_1 \geq u_{n_0}$. Isso implicaria que $q_0 < x_1$, o que contraria o fato que q_k é cota superior do conjunto T e $x_1 \in T$. Portanto, existe a menor cota superior.

□

Portanto o conjunto de Cauchy $\mathbb{S}$, é um corpo ordenado completo.

5.4 O Corpo Ordenado Completo $\mathbb{R}$ dos Números Reais

5.4.1 Um Corpo Ordenado Completo $\mathbb{K}$

Nesta seção provaremos que só existe um corpo ordenado completo, a menos de isomorfismo. Assim, tanto o conjunto de Cauchy $\mathbb{S}$ quanto o conjunto de cortes de Dedekind, construídos de maneiras diferentes, representam o mesmo conjunto. A fim de garantir a existência desse isomorfismo, veremos inicialmente alguns resultados referentes a corpos ordenados completos.

Observemos primeiro o fato de que todo corpo ordenado $\mathbb{K}$ possui uma "cópia" dos números naturais, inteiros e racionais. Denotando por $1_{\mathbb{K}}$ a unidade do corpo ordenado completo $\mathbb{K}$, escreveremos

$$n_{\mathbb{K}} = \sum_{i=1}^{n} 1_{\mathbb{K}} = 1_{\mathbb{K}} + 1_{\mathbb{K}} + 1_{\mathbb{K}} \ldots + 1_{\mathbb{K}}.$$

Usamos o fato de $\mathbb{K}$ ser ordenado pois a propriedade de monotonicidade da soma garante que ao ir somando 1 nunca voltamos a um número "menor". Ou seja, $n_{\mathbb{K}}$ é a soma em $\mathbb{K}$ de n parcelas das unidades de $\mathbb{K}$. Assim, temos uma bijeção entre os naturais e um subconjunto de $\mathbb{K}$, o qual denotaremos por $\mathbb{N}_{\mathbb{K}}$.

Definição 52. Diremos que um conjunto $X \subset \mathbb{K}$ é denso em $\mathbb{K}$ se, dados quaisquer $x < y$ com $x, y \in \mathbb{K}$, existe um $r \in X$ tal que $x < r < y$.

Teorema 5.29. O conjunto cópia dos racionais $\mathbb{Q}_{\mathbb{K}}$ é denso em qualquer corpo ordenado arquimediano $\mathbb{K}$.

Demonstração. Sejam $x, y \in \mathbb{K}$ distintos. Podemos, sem perda de generalidade, supor que $x < y$. Assim, das propriedades de corpo ordenado são válidas as seguintes equivalências:

$$x < y \Leftrightarrow y - x > 0 \Leftrightarrow (y - x)^{-1} > 0.$$

Como por hipótese $\mathbb{K}$ é arquimediano, temos que existe um $m \in \mathbb{N}_{\mathbb{K}}$ tal que

$$(y - x)^{-1} < m \Rightarrow 1 < my - mx.$$

Usando novamente a hipótese do conjunto $\mathbb{K}$ ser arquimediano e usando o princípio da boa ordenação, tomemos

$$n = min\{z \in \mathbb{N}_{\mathbb{K}};\ mx < z\}.$$

Assim, temos que $mx < n$ e $n - 1 < mx$, pois n é mínimo, e duas desigualdades devem ser consideradas. A primeira é:

$$1 < my - mx \Rightarrow (n - 1) + 1 < my - mx + (n - 1).$$

A segunda é:

$$n - 1 < mx \Rightarrow n - 1 + (my - mx) < mx + (my - mx) \Rightarrow n - 1 + (my - mx) < my.$$

Pela transitividade da relação de ordem em $\mathbb{K}$ temos:

$$(n - 1) + 1 < my \Rightarrow n < my.$$

Portanto, é válida a desigualdade a seguir:

$$mx < n < my \Leftrightarrow x < n \cdot m^{-1} < y.$$

Tomando $r = nm^{-1}$ temos que $r \in \mathbb{Q}_{\mathbb{K}}$ e $x < r < y$, como queríamos demonstrar. Logo, o conjunto cópia dos racionais $\mathbb{Q}_{\mathbb{K}}$ é denso no corpo ordenado arquimediano $\mathbb{K}$. □

Teorema 5.30. Todo corpo ordenado completo $\mathbb{K}$ é arquimediano.

Demonstração. Suponhamos que o conjunto cópia dos naturais $\mathbb{N}_{\mathbb{K}}$ seja limitado. Pela completeza do corpo ordenado $\mathbb{K}$, deve existir um $m = sup\mathbb{N}_{\mathbb{K}}$. Assim o elemento $m - 1 \in \mathbb{K}$ não é cota superior do conjunto $\mathbb{N}_{\mathbb{K}}$. Portanto, $\exists n_0 \in \mathbb{N}_{\mathbb{K}}$ tal que $n_0 > m - 1$, mas isso equivale a $n_0 + 1 > m$, ou seja, existe $p \in \mathbb{N}_{\mathbb{K}}$ tal que $p = n_0 + 1$ e $p > m$. Porém, isso contraria o fato de m ser o supremo desse conjunto. Logo, $\mathbb{N}_{\mathbb{K}}$ é um conjunto ilimitado em $\mathbb{K}$ e, assim, concluímos que o corpo ordenado completo $\mathbb{K}$ também é arquimediano. □

Vale a observação de que a recíproca do teorema 5.30 não vale, já que $\mathbb{Q}$ é um corpo ordenado não completo mas arquimediano.

5.4.2 Unicidade do Corpo Ordenado Completo

Nesta seção representaremos o conjunto de cortes de Dedekind por $\mathbb{D}$. Seja $\mathbb{K}$ um corpo ordenado completo. Usando o fato de que $\mathbb{K}$ é um corpo ordenado completo e portanto contém uma cópia do números racionais, conseguimos pensar na definição de cortes para o corpo $\mathbb{K}$. Assim dado $x \in \mathbb{K}$, vamos definir a aplicação

$$\phi(x) = C_x, \quad \text{com} \quad C_x = \{r \in \mathbb{Q}_{\mathbb{K}} = \mathbb{Q};\ r < x\}.$$

Daqui em diante, não faremos a distinção entre os números racionais $\mathbb{Q}$ e os elementos de $\mathbb{Q}_{\mathbb{K}}$, pois é possível ver que existe um isomorfismo entre ambos. Ademais, iremos considerar $\mathbb{Q} \subset \mathbb{K}$.

Primeiro verifiquemos que o conjunto C_x é de fato um corte de Dedekind.

1. Se dado $x \in \mathbb{K}$ o conjunto C_x fosse vazio, teríamos $r \geq x$ para todo r racional. Neste caso, $\mathbb{Q}$ seria limitado inferiormente, absurdo. Portanto C_x não é vazio, e de forma análago $\mathbb{Q} - C_x$ não é vazio.

2. Seja $s \in C_x$ e $q < s$. Como $s \in C_x$, então $s < x$. Assim, pela transitividade de relação de ordem e usando que $q < s$, temos $q < x$. Portanto, $q \in C_x$.

3. Seja $s \in C_x$. Então $s < x$ e usando o fato que $\mathbb{K}$ é arquimediano, pelo Teorema 5.29 sabemos que $\exists\ r \in \mathbb{Q} \subset \mathbb{K}$ tal que $s < r < x$. Assim, $r < x \Rightarrow r \in C_x$. Mas $r > s$, ou seja, C_x não possui elemento máximo. Portanto $C_x \in \mathbb{D}$, $\forall\ x \in \mathbb{K}$.

Vamos mostrar agora que a aplicação ϕ está bem definida. Se $C_x \neq C_y$, deve existir um elemento que pertence a um deles mas não pertença ao outro conjunto. Sem perda de generalidade suponhamos que existe $z \in C_x$ tal que $z \notin C_y$. Assim, temos que $z < x$ e $z \geq y$. Pela transitivdade da relação de ordem temos que $y < x$, o que implica $x \neq y$. Portanto a aplicação ϕ está bem definida.

Temos que a aplicação ϕ é injetiva. De fato, sejam $C_x, C_y \in \mathbb{D}$ tais que $C_x = C_y$. Se $x < y$, pela propriedade arquimediana exitiria $r \in \mathbb{Q}$ tal que $x < r < y$ e assim, $r \in C_y$ mas $r \notin C_x$, contrariando a hipótese. Analogamente, não pode ocorrer $y < x$. Portanto, devemos ter $x = y$ e, dessa maneira, a função ϕ é injetiva.

A aplicação ϕ é sobrejetiva. Dado $C \in \mathbb{D}$, temos que $C \subset \mathbb{Q} \subset \mathbb{K}$. Como o conjunto C é limitado superiormente e $\mathbb{K}$ é um corpo ordenado completo, podemos tomar $x = sup(C)\ em\ \mathbb{K}$. Vejamos que $C_x = C$, ou seja, $sup(C) = x \in \mathbb{K}$ e $\phi(x) = C$.

1. Seja $y \in C_x$, isto é, $y < x$. Supondo que y não seja elemento do corte C, temos que

$$y \geq sup(C) \Rightarrow y \geq x \Rightarrow y \in (\mathbb{Q} - C_x).$$

Portanto y não pertencer ao corte C implica que ele não pertence ao corte C_x. Pela contrapositiva, temos que se $y \in C_x$ então $y \in C$. Assim, é válida a inclusão $C_x \subset C$.

2. Seja $y \in C$. Temos que $y \leq sup(C)$, logo $y \leq x$. A igualdade não pode ocorrer, pois teríamos $y = sup(C)$ e resultaria em $y = max(C)$. Mas C é corte, isto é, não possui elemento máximo. Portanto $y \in C \Rightarrow y \in C_x$ e assim é válida a inclusão $C \subset C_x$.

Logo $C = C_x$ e a aplicação ϕ é sobrejetiva.

Concluímos então que ϕ é bijetiva. Mostraremos agora a correspondência das operações entre os corpos ordenados completos. Dados $x, y \in \mathbb{K}$ temos:

1. $\phi(x + y) = \phi(x) + \phi(y)$. Pela definição de ϕ, temos que

$$\phi(x + y) = C_{x+y} = \{r \in \mathbb{Q};\ r < x + y\}.$$

Em contrapartida,

$$\phi(x) + \phi(y) = C_x + C_y = \{r \in \mathbb{Q};\ r = a + b,\ a \in C_x,\ b \in C_y\},$$

pela definição de soma de cortes de Dedekind. Então, se $s \in \phi(x+y)$, então $s < x+y$. Tomando $a < x$ e definindo $b = s - a$, basta provarmos que $b < y$. Suponhamos que $b \geq y$. Neste caso teríamos:

$$b \geq y \Rightarrow a + b \geq a + y \Rightarrow s \geq a + y \Rightarrow x + y \geq a + y \Rightarrow x \geq a,$$

contrariando a hipótese inicial que $a < x$. Portanto $a \in C_x, b \in C_y$ e $s = a + b$, logo $s \in \phi(x) + \phi(y)$. Concluímos a inclusão $\phi(x + y) \subset \phi(x) + \phi(y)$. Por outro lado, se $s \in \phi(x) + \phi(y) \Rightarrow s = a + b$, onde $a \in C_x$ e $b \in C_y$. Portanto,

$$s = a + b < x + b < x + y \Rightarrow s \in C_{x+y} \Rightarrow s \in \phi(x + y)$$

Logo, é válida a inclusão de $\phi(x) + \phi(y) \subset \phi(x + y)$. Portanto, $\phi(x + y) = \phi(x) + \phi(y),\ \forall\ x, y \in \mathbb{K}$.

2. $\phi(x \cdot y){=}\phi(x) \cdot \phi(y)$. Provaremos somente o caso em que $C_x, C_y \in \mathbb{D}^+$. os demais casos são análogos. Observemos que nesse caso $x > 0$ e $y > 0$. Pela definição da função ϕ temos que

$$\phi(x \cdot y) = \{r \in \mathbb{Q}; r < x \cdot y\}.$$

Por outro lado, da definição de produto de cortes, sabemos que

$$\phi(x) \cdot \phi(y) = \{r \in \mathbb{Q};\ r < 0 \text{ ou } r = a \cdot b,\ a \in C_x,\ b \in C_y,\ a, b > 0\}.$$

Então, se $\phi(x \cdot y)$ temos que $r < x \cdot y$. Agora, temos dois casos a considerar: se $r < 0$, então por definição $r \in \phi(x) \cdot \phi(y)$. Se $r > 0$, tomando $a \in C_x$ tal que $a > 0$, definamos $b = \dfrac{r}{a}$. Assim, basta provar que $b \in C_y$. Suponha que $b \notin C_y$. Temos:

$$b \geq y \Rightarrow a \cdot b \geq a \cdot y \Rightarrow r \geq a \cdot y \Rightarrow x \cdot y \geq a \cdot y \Rightarrow x \geq a,$$

contrariando a hipótese de que $a \in C_x$. Portanto $s \in \phi(x) \cdot \phi(y)$ e $\phi(x \cdot y) \subset \phi(x) \cdot \phi(y)$. Seja agora $s \in \phi(x) \cdot \phi(y)$. Isso implica que $r < 0$, ou $r = a \cdot b$ com $0 < a \in C_x,\ 0 < b \in C_y$. Como x, y são positivos, no primeiro caso temos claramente $r < 0 < x \cdot y$, e, portanto $r \in C_{x \cdot y}$. No segundo caso temos:

$$r = a \cdot b < x \cdot b < x \cdot y \Rightarrow r \in C_{x \cdot y} \Rightarrow r \in \phi(x \cdot y)$$

e concluímos que $\phi(x) \cdot \phi(y) \subset \phi(x \cdot y)$. Portanto, $\phi(x \cdot y) = \phi(x) \cdot \phi(y), \forall\ x, y \in \mathbb{K}$.

3. $x < y \Rightarrow \phi(x) < \phi(y)$. Suponha $x < y$. então:

$$s \in \phi(x) \Rightarrow s \in C_x \rightarrow s < x \Rightarrow s < y \Rightarrow s \in C_y \Rightarrow s \in \phi(y).$$

Logo, $\phi(x) \subset \phi(y)$, o que é equivalente em $\mathbb{D}$ a $\phi(x) < \phi(y)$.

Finalmente, concluimos que a função ϕ é um isomorfismo entre o corpo ordenado completo $\mathbb{K}$ e o corpo de Dedekind $\mathbb{D}$, o qual na construção de Dedekind chamamos de $\mathbb{R}$. Fazendo $\mathbb{K} = \mathbb{S}$, este sendo o corpo ordenado de Cauchy, obtemos um isomorfismo entre $\mathbb{S}$ e o corpo ordenado completo de Dedekind (isto é, $\mathbb{R}$). Dessa forma, existe apenas um corpo ordenado completo, a menos de isomorfismos.

6 Considerações finais

Neste trabalho apresentamos a construção dos conjuntos numéricos $\mathbb{Z}, \mathbb{Q}$ e $\mathbb{R}$, a partir da axiomatização do conjunto $\mathbb{N}$ dos números naturais. Vimos através dos Axiomas de Peano como é possível definir as operações e obter as propriedades básicas de $\mathbb{N}$, sendo a formalização das demonstrações dadas na maioria das vezes pelo Axioma de Indução. O princípio de indução é visto geralmente no início dos cursos de matemática. Apesar disso, os resultados aqui apresentados requerem um pouco mais de maturidade para o desenvolvimento das demonstrações. De fato, podemos observar a partir das construções realizadas, o rigor necessário para chegarmos nos conjuntos numéricos aqui discutidos.

Dentre as construções discutidas, destacamos a do conjunto dos números reais. Esta foi feita de duas formas, através dos métodos de Dedekind e de Cantor. Após a discussão dos dois métodos foi mostrado que existe apenas um corpo ordenado completo, donde concluiu-se que os dois corpos construídos de maneiras distintas são, de fato, o mesmo corpo, chamado de conjunto dos números reais.

Por fim, com base nas construções aqui discutidas, pode-se pensar, como trabalhos futuros, em continuar a construção de outros conjuntos como por exemplo, o Conjunto dos Números complexos e dos Números Hiperreais.

Referências

1 SALES, R. B. *AS CONTRIBUIÇÕES DA ESCOLA PITAGÓRICA PARA A MATEMÁTICA*. Tese (Dissertação de Mestrado) — Universidade Federal do Piauí, 2015. Citado na página 1.

2 CALEFE, M. *Construção de conjuntos numéricos : dos números inteiros aos hiperreais*. Tese (Dissertação de Mestrado) — Universidade Estadual de Campinas, 2016. Citado na página 1.

3 MILLIES C. P.; COELHO, S. P. *Números: uma introdução à matemática*. 3. ed. São Paulo: edUSP, 2001. Citado 5 vezes nas páginas 3, 5, 12, 25 e 56.

4 HRBACEK JECH, T. *Introduction to Set Theory*. 3. ed. New York: Marcel Dekker, 1999. Citado na página 3.

5 LIMA, E. L. *Curso de Análise. Vol. I*. Rio de Janeiro: IMPA, 2017. Citado 3 vezes nas páginas 21, 31 e 58.

6 SILVA, P. B. *Construção dos Números Reais por Sequências de Cauchy e Cortes de Dedekind*. Tese (Dissertação de Mestrado) — Universidade Federal da Paraíba, 2018. Citado 3 vezes nas páginas 31, 33 e 34.

7 GONÇALVES, A. *Introdução à Álgebra*. Rio de Janeiro: IMPA, 2017. Citado na página 31.

8 FERREIRA, J. *A Construção dos Números*. 2. ed. Rio de Janeiro: SBM, 2001. Citado na página 54.