Universidade Federal da Paraíba
Centro de Ciências Exatas e da Natureza
Departamento de Matemática
Mestrado Profissional em Matemática
em Rede Nacional PROFMAT

# Existência e Unicidade dos Números Reais via Cortes de Dedekind. [†]

**por**

Kerly Monroe Pontes

**sob orientação de**

Prof.Dr Napoleón Caro Tuesta

Dissertação apresentada ao Corpo Docente do Mestrado Profissional em Matemática em Rede Nacional PROFMAT-CCEN-UFPB, como requisito parcial para obtenção do título de Mestre em Matemática.

Agosto/2014
João Pessoa - PB

[†]O presente trabalho foi realizado com apoio da CAPES, Coordenação de Aperfeiçoamento de Pessoal de Nível Superior.

P814e Pontes, Kerly Monroe.
Existência e unicidade dos números reais via Corte de Dedekind / Kerly Monroe Pontes.-- João Pessoa, 2014.
75f.
Orientador: Napoleón Caro Tuesta
Dissertação (Mestrado) - UFPB/CCEN
1. Matemática. 2. Cortes de Dedekind. 3. Corpo ordenado completo. 4. Isomorfismo.

UFPB/BC CDU: 51(043)

# Existência e Unicidade dos Números Reais via Cortes de Dedekind.

por

**Kerly Monroe Pontes**

Dissertação apresentada ao Corpo Docente do Mestrado Profissional em Matemática em Rede Nacional PROFMAT-CCEN-UFPB, como requisito parcial para obtenção do título de Mestre em Matemática.

Área de Concentração: Análise.

Aprovada por:

---

**Prof.Dr Napoleón Caro Tuesta** - UFPB (Orientador)

---

**Prof.Dr Antonio de Andrade e Silva** - UFPB

---

**Prof.Dr Turíbio José Gomes dos Santos** - UFPB

**Agosto/2014**

# Agradecimentos

Ao meu orientador, professor Napoléon Caro Tuesta, pelas oportunas sugestões e luz quando fui acometido pela escuridão da dúvida, que foram sustentáculos para caminhada firme da minha investigação.

Aos professores, Antônio de Andrade e Silva e Turíbio Santos, pelo apoio e conselhos dados para realização desse trabalho.

À minha esposa Kézia Oliveira Cabral , a minha filha Letícia Monroe Cabral, e minha mãe Maria José criaturas mais importantes da minha vida, sem as quais eu não seria nada.

# Dedicatória

Dedico este trabalho aos professores e amigos que, direta ou indiretamente me ajudaram a concretizá-lo.

*"A matemática, vista corretamente, possui não apenas verdade, mas também suprema beleza - uma beleza fria e austera, como a da escultura."*
Bertrand Russell

# Resumo

Este trabalho tem como objetivo mostrar a Existência e a Unicidade do Corpo dos Números Reais, usando para isso, os Cortes de Dedekind e o teorema da definição por Recursão. Para cumprirmos tal objetivo, definimos a noção de Corte de Dedekind e apresentamos algumas de suas propriedades; em seguida, apresentamos as noções de Corpo, Corpo Ordenado e Arquimediano, Corpo Ordenado Completo e, finalmente, enunciamos e demonstramos o Teorema da Unicidade do Corpo dos Números Reais. .

Palavras-Chaves:
*Números Reais; Cortes de Dedekind; Corpo Ordenado Completo; Isomorfismo;*

# Abstract

This work aims to show the existence and Uniqueness of the field of Real Numbers, using for this, Dedekind' Cuts theorem and the Definition by Recursion.To fulfill his goal, we define the notion of Dedekind Cut and present some of its properties; then introduce the notions of Archimedean Ordered and Field, Complete Field Sorted and finally articulate and demonstrate the Uniqueness Theorem of Field Real Numbers.

.

Key Words:
*Real Numbers, Dedekind Cut, Complete Field Sorted,Isomorphism.*

# Sumário

# Introdução

O conceito de número real está associado desde a ideia de contagem de objetos, coisas e etc (noção de quantidade) à de localização de pontos da reta (noção geométrica) ou até mesmo de entes que satisfazem um corpo de propriedades (noção abstrata). Enquanto que a noção quantitativa de números reais e mesmo a geométrica resolve muito bem os problemas e demandas do mundo real; a noção abstrata resolve com muita precisão às questões fundamentais da própria matemática, estabelecendo uma visão mais profunda do conceito de número. No final do século IXX, Richard Dedekind sentiu a necessidade de uma investigação mais rigorosa dos números reais para justificar certos resultados do Cálculo Diferencial e Integral descobertos desde à sua criação por Isaac Newton e Leibniz.Assim, teve-se a ideia de fundamentar o conceito de números reais, graças aos trabalhos desenvolvidos por Richard Dedekind (1813-1916), Georg Cantor (1845-1918) e Giuseppe Peano (1858-1932). A partir dos trabalhos desses matemáticos, a noção de número real se tornou mais precisa.

Em geral, a ideia básica da Construção de Números Reais consiste em partir de um conjunto previamente estabelecido, por um corpo de axiomas,e em seguida, averiguar as propriedades de suas operações que dele suscitam (operações essas estabelecidas logo depois dos axiomas); se por algum motivo, surgir uma nova operação unária ou binária em que não é possível de ser executada por pelo menos um elemento ou par de elementos, então faz-se necessário contornar esse problema criando-se um novo elemento,e portanto, um novo conjunto, a partir dessa nova operação. Assim, todos os elementos do antigo e do novo conjunto passam a ser escritos em termos dessa nova operação. Os elementos desse novo conjunto possuem natureza diversa aos elementos do conjunto anterior, porém possuem as mesmas propriedades dele, além das novas operações e propriedades que dele possam surgir: esse é o verdadeiro sentido da Construção de Números.

Ao se construir Números Reais, podemos usar dois modos distintos de axiomatização: o primeiro modo é a trilogia $\mathbb{N} - \mathbb{Z} - \mathbb{Q}$, mais longo e completo, consiste em construir o conjunto dos Números Naturais partindo dos axiomas de Peano, definindo as operações de adição e multiplicação e estabelecendo a relação de ordem, deduzindo, a partir disso, várias propriedades relativas a elas, seguindo, logo depois, à construção do conjunto dos Números Inteiros, usando a noção de Classes de

Equivalência definindo sobre elas as operações binárias de adição, multiplicação; a operação unária de elemento oposto e estabelecendo a relação de ordem entre seus elementos e deduzindo suas consequências; caminho axiomático semelhante é usado, também, para construir o conjunto dos Números Racionais; o segundo, é a trilogia $\mathbb{Z} - \mathbb{N} - \mathbb{Q}$, relativamente ao anterior é mais curto, nele admite-se as propriedades dos números inteiros como axiomas caracterizando-o como um domínio de Integridade Ordenado, em seguida, são provados as principais propriedades dos Números Inteiros e números naturais algumas das quais consideradas, anteriormente, como axiomas de Peano; contudo, porém a construção dos Números Racionais continua sendo a mesma que a anterior.

Uma vez seguido um dos caminhos da trilogia, o passo seguinte consiste finalizar a construção dos números reais partindo do conjunto dos Números Racionais. Existe dois caminhos tradicionais: um deles consiste em usar os corte de Dedekind - esse método foi criado pelo matemático que leva seu nome; o outro, consiste em usar as sequências de Cauchy - método criado pelo matemático George Cantor. Vale à pena frisar, que ambos os métodos partem do conjunto dos Números Racionais. Além deles, existem outros, a saber: usando à noção de Quantidade, o conceito de Classes de Declives e a noção de Sucessão de Intervalos Encaixados e, ainda, a ideia de sucessão de Números Racionais Decimais. Dentre essas construções, optamos por descrever a construção via Cortes de Dedekind, isso é devido a um motivo básico: é que esse método depende apenas do conhecimento natural das propriedades dos Números Racionais dispensando as definições e propriedades demasiadamente longas de sequências numéricas vistas, por exemplo, no método de construção por sequências de Cauchy; isso torna o desenvolvimento mais didático e curto. Por fim, admitindo o conjunto dos números reais como um corpo ordenado completo, provaremos sua Unicidade e complementaremos a construção de números reais representando-os por meio da expansão decimal. Neste trabalho sobre construção (e portanto,sobre existência) dos números reais usando Cortes de Dedekind dispensaremos o caminho que leva começando pelo conjunto dos Números Naturais usando a Axiomática de Peano, e sua posterior construção dos Números Inteiros e Racionais. Admitimos que o leitor já tenha uma noção da trilha axiomática da trilogia $\mathbb{N} - \mathbb{Z} - \mathbb{Q}$ ou $\mathbb{Z} - \mathbb{N} - \mathbb{Q}$.

# Capítulo 1

# Cortes de Dedekind

Ao construirmos os números reais usando os Cortes de Dedekind, partirmos do pressuposto de que conhecemos e aceitamos todas as propriedades dos números racionais,herdadas direta ou indiretamente, dos axiomas dos números naturais e inteiros. A noção que adotaremos para o Corte de Dedekind ,neste trabalho,é aquela que coincide com a de Bertrand Russel.

**Definição 1.1** *Seja um subconjunto $A \subset \mathbb{Q}$. Dizemos que $A$ é um Corte de Dedekind se possui as seguintes propriedades:*

*I. $A \neq \emptyset$ e $A \neq \mathbb{Q}$, isto é, $A$ é um subconjunto não-vazio e próprio de $\mathbb{Q}$;*

*II. Dado que $x \in A$, se $y \in \mathbb{Q}$ e que $y \geq x$, então $y \in A$, isto é, todo elemento $y$ de $\mathbb{Q}$ maior do que ou a igual um elemento $x$ de $A$ é, também, elemento de $A$;*

*III. Dado que $x \in A$, existe um $y \in A$ tal que $y < x$, isto é, para qualquer elemento $x$ de $A$ sempre existe um elemento dele $y$ menor que $x$.*

O Lema seguinte prova a existência do Corte de Dedekind.

**Lema 1.1** *Seja $r \in \mathbb{Q}$. O conjunto $D = \{x \in \mathbb{Q} | x > r\}$ é um Corte de Dedekind.*

**Demonstração:** Provaremos que o conjunto acima satisfaz as três propriedades da definição de Corte de Dedekind.

I. Dado que $r \in \mathbb{Q}$ segue-se imediatamente que $r-1, r+1 \in \mathbb{Q}$ e que $r-1 < r < r+1$, do qual temos que $r+1 \in \mathbb{Q}$ e $r-1 \notin \mathbb{Q}$. Portanto, temos $\mathbb{Q} \neq \emptyset$ e $D \neq \mathbb{Q}$;

II. Dado que $x \in D$ e supondo dado um $y \in \mathbb{Q}$ tal que $y > x$ temos que $y > x > r$, pois, $x \in D$. Portanto, $y \in D$;

III. Dado que $x \in D$ temos que $r < x$. Tomando um $y = \frac{(r+x)}{2}$ temos $r < \frac{(r+x)}{2} < x$ e, portanto, $y \in D$.

■

**Definição 1.2** *Seja $r \in \mathbb{Q}$. Definimos um Corte Racional relativo a $r$, o qual denotamos por $D_r$, o Corte de Dedekind*

$$D_r = \{r \in \mathbb{Q} | x > r\}.$$

**Observação 1.2.1** *Embora tenhamos uma definição, a priori, de Corte Irracional como o conjunto dos números racionais maiores do que um número real que não é racional, o uso dela neste momento não permite uma prova que ele seja um Corte de Dedekind, pois, ainda não definimos o que significa número real. Por exemplo, o conjunto $D = \{x \in \mathbb{Q} | x > \sqrt{2}\}$ faz o uso de algo que ainda não foi definido, o número $\sqrt{2}$ . Teríamos que provar, primeiro, que esse número real existe e, ainda mais, provar que ele não é racional. Podemos sim, descrever o conjunto dado na definição de uma forma equivalente fazendo o uso de números racionais como, por exemplo, o conjunto $D = \{x \in \mathbb{Q} | x > 0 \quad e \quad x^2 > 2\}$: tal conjunto é equivalente a $D = \{x \in \mathbb{Q} | x > \sqrt{2}\}$. Até aqui faremos apenas, e nada mais, a prova de que esse conjunto na sua forma mais geral, $D = \{x \in \mathbb{Q} | x > 0$*
*e*
*$x^n > p\}$ onde $p \in \mathbb{Q}$, é um Corte de Dedekind, na proposição abaixo. Antes de demonstrá-lo, enunciaremos, sem demonstração, três lemas úteis que levarão a demonstração desta desta propriedade e de outra não menos importante.*

**Lema 1.2** *Dado $x \in \mathbb{Q}$ com $x > -1$ e $n \in \mathbb{N}$. Então vale a desigualdade de Bernoulli $(1 + x)^n \geq 1 + nx$.*

**Lema 1.3** *Seja um $r \in \mathbb{Q}$, $r > 0$, e $0<d<1$. Então para cada $r$ e $n \in \mathbb{N}$ existe um $A_n$, dependendo de $r$, tal que $(r + d)^n \leq r^n + A_n d$.*

**Lema 1.4** *Seja $r > 0$, um número racional. Se $r^n < p$, então existe um $k \in \mathbb{N}$ tal que se tem, ainda, $(r + \frac{1}{k})^n < p$.*

**Proposição 1.1** *O conjunto $M \subseteq \mathbb{Q}$ definido por $M = \{x \in \mathbb{Q} | x > 0 \quad e \quad x^n > p\}$, onde $p \in \mathbb{Q}$, $p > 0$, é um Corte de Dedekind.*

**Demonstração:** Temos dois casos possíveis:

(a) $0<p<1$;

(b) $p>1$;

Esses dois casos possíveis servirão apenas para demonstrarmos a primeira parte da definição de Corte. Vejamos:

I. *Parte (a)*: Se $0 < p < 1$, então $2 - p \in M$, pois, $2 - p > 1 > p > 0$ e que $(2-p)^n > 1 > p$. Logo, $M \neq \emptyset$.

*Parte (b)*: se $p > 1$ temos $p + 1 > p > 1$ o que implica $p + 1 > 0$ e $(p+1)^n > r$. Portanto, $p + 1 \in M$, isto é , $M \neq \emptyset$. Como $0 \notin M$, temos $M \neq \mathbb{Q}$.

II. Agora, provaremos a segunda parte da definição: supondo que $x \in M$ e que $y \geq x$ segue-se que $y \geq x > 0$ implica $y^n \geq x^n > p$ da qual se conclui $y \in M$.

III. Agora, vamos provar que existe um $y \in M$ tal que $y < x$. Temos dois casos possíveis:

(a) $x < \frac{x^n - p}{nx^{n-1}}$.

(b) $\frac{x^n - p}{nx^{n-1}} < x$.

(a) Se tomarmos um $y = \frac{x}{2}$ teremos pela hipótese y$< \frac{x^n - p}{nx^{n-1}}$. Assim, usando o Lema 1.2, temos $p < x^n - nyx^{n-1} = x^n(1 - n\frac{y}{x}) \leq x^n\left(1 - \frac{y}{x}\right)^n = (x-y)^n = \left(\frac{x}{2}\right)^n < x^n$ o que implica $y^n < x^n$ , logo, $y < x$. Pela desigualdade anterior , temos $y^n > p$, e pelo que definimos, $y > 0$. Portanto, provamos que existe um $y \in M$ tal que $y < x$.

(b) Pela hipótese, tomamos um s tal que $0 < s < \frac{x^n - p}{nx^{n-1}} < x$ e $0 < s < \frac{x}{n}$. Fazendo $y = x - s$, vemos que $y > 0$. Segue-se sucessivamente, que $p < x^n - nsx^{n-1} = x^n(1 - n\frac{s}{x}) \leq x^n(1 - \frac{s}{x})^n = (x - s)^n < x^n$ o que implica $y < x$ e $p < y^n$. Portanto, provamos que existe um $y \in M$ tal que $y < x$.

■

**Proposição 1.2** *Se $M = D_r$ para algum $r \in \mathbb{Q}$ então $r^n = p$.*

**Demonstração:** Suponha o contrário.Seja $r^n < p$. Se $r > 0$ existe um $k \in \mathbb{N}$ tal que $\left(r + \frac{1}{k}\right)^n < p$, Lema 1.4. Chamando $y = r + \frac{1}{k}$ temos $y > r$ e $y^n < p$.Segue-se que, existe um $y \in D_r$ tal que $y \notin M$. Portanto, temos $M \neq D_r$. Agora, se $r < 0$ devemos levar em consideração dois casos possíveis para $n$:

(a) $n$ é natural par.

(b) $n$ é natural ímpar.

(a) Note que $(-r)^n = r^n < p$, se $n$ é par.Como $-r > 0$,pelo Lema1.4, existe um $k \in \mathbb{N}$ tal que $\left(-r + \frac{1}{k}\right)^n < p$. Chamando $y = -r + \frac{1}{k}$ temos $y > r$ e $y^n < p$. Assim, temos a implicação de que existe um $y \in D_r$ tal que $y \notin M$. Portanto, temos $M \neq D$.

(b)Note que, neste caso, $r^n < p$ para todo $r < 0$ e $n$ ímpar. Chamando $y = \frac{r}{2}$ temos $y > r$ e $y^n < p$, pois, $y < 0$. Portanto, temos que $y \in D_r$ implica $y \notin M$. Assim, em ambos os casos verificamos que $M \neq D_r$ para todo $r \in \mathbb{Q}$.

Agora, suponha $r^n > r$. Temos dois casos:

(a) Se $r > 0$ temos que existe um $k \in N$ tal que $\left(r - \frac{1}{k}\right)^n > p$. Caso tenhamos $r - \frac{1}{k} > 0$ podemos tomar $y = r - \frac{1}{k}$ . Assim, temos $y > 0$ e $y^n > p$, com $y < r$. Portanto, provamos que existe $y \in M$ tal que $y \notin D_r$. Agora, se tivermos $y = r - \frac{1}{k} < 0$, tomamos um $y = r - \frac{1}{s}$, com $s > k$ e $rs > 1$. Isso atende nosso requisito, pois, de $s > k$ temos $y^n > p$ e de $rs > 1$ temos $y > 0$. Como $y < r$ concluímos que existe um $y \in M$ tal que $y \notin D_r$. Portanto, $M \neq D_r$.

(b) Se $r < 0$ tomamos um $y > r$, pórem, $y < 0$. Assim, existe um $y \in D_r$ tal que $y \notin M$. Portanto, $M \neq D_r$.

■

Doravante, provaremos algumas propriedades dos Cortes de Dedekind, começando pela prova de um lema que usaremos com muita frequência na demonstração de alguns resultados.

**Lema 1.5** *Seja $A \subset \mathbb{Q}$ um Corte de Dedekind.*

*I.* $\mathbb{Q} - A = \{x \in Q | x < a, \forall a \in A\}$;

*II. Seja $x \in \mathbb{Q} - A$. Se $y \in \mathbb{Q}$ e $y \leq x$, então $y \in \mathbb{Q} - A$.*

**Demonstração:** (I) Se $x \in \mathbb{Q} - A$ e $a \in A$ então temos pela lei da tricotomia dos números racionais que ou $x > a$ ou $x = a$ ou $x < a$. Provaremos que somente ocorre a possibilidade $x < a$. Com efeito, se $x = a \in A$, por definição, o que é um absurdo; se $x > a$ e como $a \in A$ e $x \in \mathbb{Q}$ temos, pela propriedade *II* da definição de corte, que $x \in A$, o que também é um absurdo. Assim, somente ocorre $x < a$. Portanto, $\mathbb{Q} - A \subset \{x \in \mathbb{Q} | x < a, \forall a \in A\}$. Agora, suponha que $y \in \{x \in \mathbb{Q} | x < a, \forall a \in A\}$ e $y \in A$, assim, teríamos $y < y$, o que é um absurdo. Isso implica que $y \in \mathbb{Q} - A$. Daí concluímos $\{x \in \mathbb{Q} | x < a, \forall a \in A\} \subset \mathbb{Q} - A$. Portanto, segue o resultado.
(II) Pela hipótese, temos que $y \in \mathbb{Q}$, $y \leq x < a$, pois, $x \in A$, segue-se imediatamente que $y \in \mathbb{Q} - A$. ■

O próximo lema prova a lei da tricotomia para os Cortes de Dedekind.

**Lema 1.6** *Sejam $A, B \in \mathbb{Q}$ Cortes de Dedekind. Então ocorre exatamente uma das possibilidades: $A \subsetneq B$ ou $A = B$ ou $B \subsetneq A$.*

**Demonstração:** Se $A = B$, não há nada o que provar, suponha que $A \neq B$. Dado $a \in A$, então temos dois casos:

1. Existe um $a \in A$ tal que $a \notin B$; ou
2. Existe um $b \in B$ tal que $b \notin A$.

Caso 1. Então temos $a \in A$ e $a \in \mathbb{Q} - B$. Pelo Lema 1.5 temos $a < b, \forall b \in B$, como $a \in A$ e $a < b, \forall b \in B$, temos, pela parte II da definição de Corte, que $b \in A, \forall b \in B$, ou seja , $B \subseteq A$. Como supomos $A \neq B$, temos , portanto, que $B \subsetneq A$. O caso 2, é semelhante ao caso 1, portanto, temos $A \subsetneq B$. ■

**Lema 1.7** *Seja $\mathcal{A}$ uma família de subconjuntos não-vazios de $\mathbb{Q}$. Suponha que todo $X \in \mathcal{A}$ é um Corte de Dedekind. Se $\bigcup_{X \in \mathcal{A}} X \neq \mathbb{Q}$, então $\bigcup_{X \in \mathcal{A}} X$ é um Corte de Dedekind.*

**Demonstração:** Vamos chamar $B = \bigcup_{X \in \mathcal{A}} X$. Mostraremos que $B$ satisfaz as três partes da definição de Cortes de Dedekind.

(I) Como $X \neq \emptyset$, para todo $X \in \mathcal{A}$ segue-se que $B = \bigcup_{X \in \mathcal{A}} X \neq \emptyset$ e, pela hipótese, $B = \bigcup_{X \in \mathcal{A}} X \neq \mathbb{Q}$. Com isso, provamos que $B$ satisfaz a parte (I) da definição;

(II) Seja $x \in B$. Suponhamos um $y \in \mathbb{Q}$ tal que $y \geq x$. Logo, $x \in X$, para algum $X \in \mathcal{A}$. Ora, $X$ é um Corte de Dedekind, segue-se então pela parte (II) da definição que $y \in X$, o que implica $y \in B$. Portanto, provamos a parte (II) da definição;

(III) Se $x \in B$, então $x \in X$ para algum $X \in \mathcal{A}$. Pela parte (III) da definição, existe $y \in X$, que consequentemente, $y \in B$, tal que $y < x$. Portanto, provamos a parte (III) da definição de Corte.

■

**Lema 1.8** *Sejam $A, B \subseteq \mathbb{Q}$ Cortes de Dedekind. Então são válidas as seguintes afirmações:*

*(i) O conjunto definido por $M = \{r \in \mathbb{Q} | r = a + b,$ para algum $a \in A$ e $b \in B\}$ é um Corte de Dedekind;*

*(ii)* *O conjunto definido por* $M = \{r \in \mathbb{Q} | -r < c \ \ para \ \ algum \ \ c \in \mathbb{Q} - A\}$ *é um Corte de Dedekind;*

*(iii)* *Suponha que* $0 \in \mathbb{Q} - A$ *e* $0 \in \mathbb{Q} - B$. *O conjunto definido por* $M = \{r \in \mathbb{Q} | r = ab, \ \ para \ \ algum \ \ a \in A \ \ e \ \ b \in B\}$ *é um Corte de Dedekind;*

*(iv)* *Suponha que exista um* $q \in \mathbb{Q} - A$ *tal que* $q > 0$. *O conjunto definido por* $M = \{r \in \mathbb{Q} | r > 0 \ \ e \ \ \frac{1}{r} < c, \ \ para \ \ algum \ \ c \in \mathbb{Q} - A\}$ *é um Corte de Dedekind.*

**Demonstração:** Vamos provar a parte $(i)$:

*(I)* Com efeito, como $A$ e $B$ são não-vazios existem $a \in A$ e $b \in B$. Logo, existe $r = a + b \in M$. Daí, temos $M \neq \emptyset$. Agora, pela hipótese de Corte, temos que $A \neq \mathbb{Q}$ e $B \neq \mathbb{Q}$. Assim, existem $p \in \mathbb{Q} - A$ e $q \in \mathbb{Q} - B$ que, pelo Lema 1.5, são tais que $p < a, \forall a \in A$ e $q < b, \forall b \in B$; somando as duas desigualdades anteriores, teremos $p+q < a+b, \forall a+b \in M$. Daí, temos que $p+q \in \mathbb{Q}-M$,isto é, $M \neq \mathbb{Q}$. Portanto, provamos que $M \neq \emptyset$ e $M \neq \mathbb{Q}$.

*(II)* Suponha um $r \in M$ e um $s \in \mathbb{Q}$ tais que $s \geq r$. Como $r \in M$ temos $r = a + b$, para algum $a \in A$ e $b \in B$. Usando a lei da desigualdade aditiva para os racionais temos $a + (s - r) \geq a$, assim, pela $2^{a}$ parte da definição, $a + (s - r) \in A$. Daí, segue-se que $s = [a + (s - r)] + b \in M$.

*(III)* Se $r \in M$, então existem $a \in A$ e $b \in B$ tais que $r = a + b$. Como $A$ é um Corte de Dedekind existe um $c \in A$ tal que $c < a$. Daí, segue-se que $s = c + b < a + b = r$, onde $c \in A$ e $b \in B$. Assim, $s < r$ e, portanto, $s \in M$.

Parte $(ii)$:

*(I)* Sabemos que $A \neq \mathbb{Q}$, logo, existe um $b \in \mathbb{Q} - A$. Pela segunda parte do Lema 1.5, temos que $b - 1 \in \mathbb{Q} - A$. Note que $-[-(b - 1)] < b$, isto é, $-(b - 1) \in M$. Assim, fica provado que $M \neq \emptyset$. Vamos provar que $-a \notin M$, isto é, $-a \in \mathbb{Q} - M$. Resultando disso, o fato de que $M \neq \mathbb{Q}$. Com efeito, note que $-(-a) \in A$, isto é, $-(-a) \notin \mathbb{Q} - A$. Ora, pela parte 2 do Lema 1.5 vemos que existe um $b \in \mathbb{Q} - A$ tal que $-(-a) > b$. Isso implica $-a \notin M$. Portanto, segue-se o resultado.

*(II)* Suponha que $x \in M$ e para $y \in \mathbb{Q}$ temos $y \geq x$. Assim, para algum $c \in \mathbb{Q} - A$ temos $-x < c$, o que implica $-y \geq -x < c$. Portanto, $y \in M$.

*(III)* Se $x \in M$, então existe um $c \in \mathbb{Q} - A$ tal que $-x < c$ o que implica $x > -c$. Chamando de $y = \frac{x+(-c)}{2}$, temos que, usando a propriedade dos números racionais, $-c < \frac{x+(-c)}{2} < x$. Dessa desigualdade, obtemos $y < x$ e $-x < \frac{-(x+(-c))}{2} < c$, o que nos leva a concluir que $y \in M$.

Parte (*iii*)

*(I)* Como $A \neq \emptyset$ e $B \neq \emptyset$, existem $a \in A$ e $b \in B$. Assim, existe $r$ tal que $r = ab$. Ora, $r \in M$, isto é, $M \neq \emptyset$. Claramente, $0 \notin M$, pois, podemos escrever $0 = a \cdot 0$ com $a \in A$ e $0 \notin B$, por hipótese. Assim, $M \neq \mathbb{Q}$. Portanto, provamos que $M \neq \emptyset$ e $M \neq \mathbb{Q}$.

*(II)* Suponha $x \in M$ e $y \in \mathbb{Q}$ tais que $y \geq x$. Se $x \in M$, então existem $a \in A$ e $b \in B$ tais que $x = ab$. Pela hipótese, vemos que $a > 0$ e $b > 0$ . Fazendo $y = a \cdot \frac{y}{a}$, concluímos que $a \in A$ e $\frac{y}{a} \in B$. Assim, vemos que $y \in M$. Portanto, temos que se $y \geq x$, então $y \in M$.

*(III)* Se $x \in M$ temos que existem $a \in A$ e $b \in B$ tais que $x = ab$. Pela hipótese, deduzimos que $a > 0$ e $b > 0$ . Pela definição de Corte de Dedekind(III), existem $c \in A$ e $d \in B$ tais que $c < a$ e $d < b$. Isso implica em $y = cd < ab$ e $y \in M$. Portanto, existe um $y \in M$ tal que $y < x$.

Parte *(iv)*

*(I)* Pela hipótese, $q > 0$ e $q \in \mathbb{Q} - A$, isto é, $0 < q < a$, para todo $a \in A$. Se $r \in \mathbb{Q}$ é tal que $r \leq 0$, então $r \notin M$ o que leva a concluir que $M \neq \mathbb{Q}$. Sabemos que $0 < \frac{q}{2} < q$. Assim se tomarmos $r = \left(\frac{2}{q}\right)^{-1}$ teremos $r \in M$ do qual resulta $M \neq \emptyset$. Portanto, provamos que $M \neq \emptyset$ e $M \neq \mathbb{Q}$.

*(II)* Se $x \in M$ e $y \in \mathbb{Q}$ são tais que $y \geq x$. De $x \in M$ e da desigualdade, obtemos $\frac{1}{y} < \frac{1}{x} < c$ para algum $c \in \mathbb{Q} - A$. Portanto, $y \in M$.

*(III)* Se $x \in M$, então $x > 0$ e para algum $c \in \mathbb{Q} - A$ temos $0 < \frac{1}{x} < c$ cuja desigualdade resulta em $\frac{1}{c} < x$. Podemos tomar um $y = \frac{x + \frac{1}{c}}{2}$ . Assim, podemos concluir que $y \in \mathbb{Q}$ e $\frac{1}{c} < y < x$. Dessa última desigualdade resulta $0 < \frac{1}{y} < c$, isto é, $y \in M$. Portanto, se $x \in M$ existe um $y \in M$ tal que $y < x$.

■

O resultado da segunda parte do lema a seguir será usado na prova do Teorema 2.3, mais precisamente em sua parte (5), que mostra algumas propriedades relativas aos números reais; a sua primeira parte, servirá de base para prova da sua segunda parte, e também, da parte (4) do Teorema 2.1. Para provarmos o lema a seguir, enunciaremos duas proposições sobre números racionais, sem demonstrá-las, que serão usadas na prova do lema que se segue.

**Proposição 1.3** *Sejam $r, s \in \mathbb{Q}$ racionais tais $r > 0$ e $s > 0$. Então existe um natural $n \in \mathbb{N}$ tal que se tenha $s < nr$.*

**Teorema 1.1 (Princípio da Boa Ordenação)** *Seja $A \subseteq \mathbb{N}$ um subconjunto não-vazio. Então existe um $m \in A$ tal que $m \leq x$, para todo $x \in A$.*

**Lema 1.9** *Seja $A$ um Corte de Dedekind e $y \in \mathbb{Q}$.*

*(I) Supondo que $y > 0$. Então existem $u \in A$ e $v \in \mathbb{Q} - A$ tais que $y = u - v$, e $v < e$, para algum $e \in \mathbb{Q} - A$ ;*

*(II) Suponha que $y > 1$ e que exista um $q \in \mathbb{Q} - A$ tal que $q > 0$. Então existem $r \in A$ e $s \in \mathbb{Q} - A$ tais que $s > 0$ e $y > \frac{r}{s}$ , com $s < g$, para algum $g \in \mathbb{Q} - A$ .*

**Demonstração:**

(I) Como $A$ é um Corte temos, $A \neq \emptyset$ e $A \neq \mathbb{Q}$. Isso implica que existem $z \in A$ e $w \in \mathbb{Q} - A$. Sabemos, pelo Lema 1.5, que $w < z$ o que leva$z - w > 0$. Como $z - w$ e $y$ são racionais positivos existe um $n \in \mathbb{N}$ tal que $z - w < ny$. Da qual tiramos e reescrevemos $z + n(-y) < w$. Do Lema 1.5 tiramos $z + n(-y) \in \mathbb{Q} - A$. Vamos definir o conjunto $M$ tal que:

$$M = \{p \in \mathbb{N} | z + p(-y) \in \mathbb{Q} - A\}.$$

Anteriormente, como existe $n \in \mathbb{N}$ tal que $z + n(-y) \in \mathbb{Q} - A$ segue-se que $M \neq \emptyset$. Ora, pelo Princípio da Boa Ordenação,existe um $m \in \mathbb{N}$ tal que $z + m(-y) \in \mathbb{Q} - A$ e $z + (m-1)(-y) \in A$ . Disso resulta pelo Lema 1.5 (II) que, existe um $e \in \mathbb{Q} - A$ tal que $z + m(-y) < e$. Façamos $u = z + (m-1)(-y)$ e $v = z + m(-y)$. Do qual tiramos $y = u - v$, com $v < e$, para algum $e \in \mathbb{Q} - A$.

(II) A demonstração dessa 2ª parte do Lema exige um artifício engenhoso. Vamos mostrar a construção do raciocínio em duas etapas. Primeira Etapa do Raciocínio: É natural que tenhamos inclinação em usar a 1ª parte desse mesmo lema para aparecer as ditas letras u e v que aparecem como forma de quociente com $y > \frac{u}{v}$,onde $u \in A$, e $v \in \mathbb{Q} - A$, com $v > 0$ e $v < g$, para algum $g \in \mathbb{Q} - A$. A ideia que se tem é construir uma desigualdade $(y-1)v > u - v$ (cuja implicação nos dá $y > \frac{u}{v}$). Para que isso ocorra, é necessário que ela advenha da desigualdade $(y-1)v > (y-1)\frac{q}{2} = u - v$. Agora, para que essa desigualdade, junto com essa igualdade, tenha sentido de ser, impomos na hipótese do lema $y > 1$ e exista um $q > 0$,onde $q \in \mathbb{Q} - A$ para que faça sentido o uso da parte (I) do lema. Outro impasse que devemos resolver é a relação entre $v$ e $\frac{q}{2}$. Se durante a prova impomos $v > \frac{q}{2} > 0$, essa etapa da demonstração fica resolvida. Vejamos: Como $y > 1$ e $q > 0$ temos $(y-1)\frac{q}{2} > 0$. Logo, pela parte (I) desse lema temos que existem $u \in A$ e $v \in \mathbb{Q} - A$ tais que $(y-1)\frac{q}{2} = u - v$

com $v < g$, para algum $g \in \mathbb{Q} - A$. Se este $v$ for tal que $v > \frac{q}{2}$, então teremos $(y-1)v > (y-1)\ \frac{q}{2} = u - v$, ou seja, $(y-1)v > u - v$ o que implica sucessivamente em $yv - v > u - v$ e $y > \frac{u}{v}$, pois, $v > 0$. Chamando $r = u$ e $s = v$ temos $y > \frac{r}{s}$, com $s > 0$ e $s < g \in \mathbb{Q} - A$. Portanto, provamos que existem $r \in A$ e $s \in \mathbb{Q} - A$ tais que $y > \frac{r}{s}$ com $s > 0$ e $s < g$,para algum $g \in \mathbb{Q} - A$ .

Agora, vamos construir o raciocínio quando $v \leq \frac{q}{2}$ . A ideia consiste em construir outros elementos $r \in A$ e $s \in \mathbb{Q} - A$ tais que ainda tenhamos $(y-1)\frac{q}{2} = u - v = r - s$ devemos fazer que ocorra $(y-1)s > (y-1)\frac{q}{2} = r - s$ e que $s = \frac{3}{4}q$. Agora, basta mostrarmos com isso que $r \in A$ e $s \in \mathbb{Q} - A$ . Com efeito, é imediato que por $s = \frac{3}{4}\ q < \frac{1}{2}q < q$ resulta $s \in \mathbb{Q} - A$, e que por $r = u + (s - v) > u$ (pois, $s > \frac{q}{2} \geq v$) resulta $r \in A$. Assim, a segunda parte do lema fica provado. Vejamos: Façamos $r = u + (s - v)$ e seja $s = \frac{3}{4}q$. A partir disso temos $r - s = u - v = (y-1)\frac{q}{2} < (y-1)s$ e, portanto, $r < sy$ o que implica $y > \frac{r}{s}$. Agora, como $s = \frac{3}{4}q < q$ e $q \in \mathbb{Q} - A$ concluímos que $s \in \mathbb{Q} - A$ e que, por transitividade, $s < q = g \in \mathbb{Q} - A$. Ora, vemos que $r = u + (s - v) > u$, pois, $s - v > 0$. Logo, $r \in A$. Portanto, provamos que existem $r \in A$ e $s \in Q - A$ tais que $y > \frac{r}{s}$ com $s < g$, para algum $g \in \mathbb{Q} - A$ .

■

# Capítulo 2

# Construção dos Números Reais

No capítulo anterior, tivemos o duro trabalho de assimilar a definição de Corte de Dedekind e a tarefa árdua de provar os lemas que serão utilizados neste capítulo. Este capítulo mostra, de fato, a construção dos números reais usando os Corte de Dedekind. Vamos verificar que, com a definição seguinte, os Corte de Dedekind é identificado com os Números Reais e, mais adiante, se comportam da mesma maneira que os números reais em relação as suas operações de adição, multiplicação, inverso aditivo e multiplicativo, e a relação de ordem.

**Definição 2.1** *O conjunto dos números reais, denotado por $\Re$, é definido por:*

$$\Re = \{A \subseteq \mathbb{Q} | A \ \ seja \ \ um \ \ corte \ \ de \ \ Dedekind\}.$$

Sabemos que os Corte de Dedekind são subconjuntos de números racionais, definiremos a relação de Ordem sobre os Números reais em termos da relação de "está contido"sobre conjunto de números racionais.

**Definição 2.2** *Dados $A, B \in \Re$, dizemos que "A é menor do que B", denotado por $A < B$ se, $B \subseteq A$ e $A \neq B$ ($B \subsetneq A$), isto é, quando $A$ é um subconjunto próprio de $B$. Definimos $A \leq B$, isto é, "A é menor do que ou igual a B"se, $B \subset A$ ou $A = B (B \subseteq A)$.*

Usaremos os itens $(i)$ e $(ii)$ do Lema 1.8 para definirmos a adição e elemento oposto de números reais. É fácil ver, pelo mesmo lema, que as operações de adição e elemento oposto são fechadas sobre conjunto dos números reais.

**Definição 2.3** *Dados $A, B \in \Re$, definimos a soma de $A$ com $B$, denotada por $A+B$ o número real*

$$A + B = \{r \in \mathbb{Q} | r = a + b \ \ para \ \ algum \ \ a \in A \ \ e \ \ b \in B\}.$$

**Definição 2.4** *Dado $A \in \Re$ , definimos oposto de $A$, denotado por $-A$ o número real*

$$-A = \{r \in \mathbb{Q} | -r < c \ \ para \ \ algum \ \ c \in \mathbb{Q} - A\}.$$

A definição de multiplicação e inverso multiplicativo para os números reais é um pouco mais complicada de que a definição de adição e elemento oposto, pois, nele vamos precisar de alguns requisitos. Começaremos com o seguinte lema.

**Lema 2.1** *Seja $A \in \Re$, e $r \in \mathbb{Q}$. Então são válidas as seguintes afirmações:*

*(i)* $A > D_r$ *se e somente se existe* $q \in \mathbb{Q} - A$ *tal que* $q > r$.

*(ii)* $A \geq D_r$ *se e somente se* $r \in \mathbb{Q} - A$ *se e somente se* $a > r$, *para todo* $a \in A$.

*(iii) Se* $A < D_0$ *então* $-A \geq D_0$ .

**Demonstração:**

$(i)$ Por hipótese, temos $A \in D_r$ e $A \neq D_r$, isto quer dizer que $r < a, \forall a \in A$ e que existe um $q \in D_r$ tal que $q \notin A$ ou, equivalentemente, existe um $q \in \mathbb{Q} - A$ tal que $r < q$. Reciprocamente, se existe $q \in \mathbb{Q} - A$ tal que $r < q$, temos pelo lema 1.7, que $r < q \leq a, \forall a \in A$. Assim vemos que $A \subseteq D_r$. Se tomarmos um $y = \frac{r+q}{2}$ vemos de $r < y < q$ que $y \in D_r$ e $y \in \mathbb{Q} - A$ .Logo, existe um $y \in D_r$ tal que $y \notin A$. Portanto, $A \neq D_r$.

$(ii)$ $A \subseteq D_r$ ou $A = D_r$ é equivalente, pela definição de subconjunto ou da igualdade de conjuntos, a $r < a, \forall a \in A$, e que, por sua vez, pela parte (I) do lema 1.5, é equivalente a $r \in \mathbb{Q} - A$ .

$(iii)$ Suponha que $A < D_0$. Disso resulta que existe um $q \in A$ tal que $q \leq 0$. Pela parte (II) da definição de corte de Dedekind, concluímos que $0 \in A$. Assim, $0 \notin \mathbb{Q} - A$, e portanto $-0 \notin \mathbb{Q} - A$, o que implica $0 \notin -A$. Pela parte (II) deste lema concluímos que $-A \geq D_0$ o que é um absurdo.

■

Agora, as definições a seguir sobre multiplicação e elemento inverso (inverso multiplicativo) sobre números reais fazem sentido devido aos Lemas 1.8 e 2.1.

**Definição 2.5** *Sejam $A, B \in \Re$. Definimos multiplicação de $A$ por $B$, o qual denotamos por $A \cdot B$, o Corte de Dedekind:*

*(I)* $A \cdot B = \{r \in \mathbb{Q} | r = ab \ \ para \ \ algum \ \ a \in A \ \ e \ \ b \in B\}$ , *se* $A \geq D_0$ *e* $B \geq D_0$.

*(II)* $A \cdot B = -[(-A) \cdot B]$, *se* $A < D_0$ *e* $B \geq D_0$ .

*(III)* $A \cdot B = -[A \cdot (-B)]$, *se* $A \geq D_0$ *e* $B < D_0$.

*(IV)* $A \cdot B = (-A) \cdot (-B)$, *se* $A < D_0$ *e* $B < D_0$ .

**Definição 2.6** *Dado* $A \in \Re$. *Definimos o elemento inverso de* $A$, *denotado por* $A^{-1}$, *o Corte de Dedekind:*

*(I)* $A^{-1} = \{r \in \mathbb{Q} | r > 0 \ \ e \ \ \frac{1}{r} < c \ \ para \ \ algum \ \ c \in \mathbb{Q} - A\}$, *se* $A < D_0$.

*(II)* $A^{-1} = -(-A)^{-1}$, *se* $A > D_0$.

Com as definições das operações básicas em mãos, esboçaremos e provaremos, a seguir, as propriedades algébricas fundamentais dos Corte de Dedekind. Frisemos que, as propriedades estão enumeradas e organizadas numa sequência lógica de forma que a prova de uma propriedade depende da aceitação da propriedade anterior já demonstrada.

**Teorema 2.1** *Sejam* $A, B, C \in \Re$. *Então são válidas as seguintes propriedades Aditivas:*

1. $A + (B + C) = (A + B) + C$ *(Lei Associativa para Adição)*
2. $A + B = B + A$ *(Lei Comutativa)*
3. $A + D_0 = A$ *(Lei da Identidade Aditiva)*
4. $A + (-A) = D_0$ *(Lei do Inverso Aditivo)*

**Demonstração:**

1. Usando a definição de soma de Corte de Dedekind temos:

   $A + (B + C) = \{r \in \mathbb{Q} | r = a + (b + c), \ \ para \ \ algum \ \ a \in A, b \in B, e \ \ c \in C\}$

   $= \{r \in \mathbb{Q} | r = (a+b)+c, \ \ para \ \ algum \ \ a \in A, b \in B, \ \ e \ \ c \in C\} = (A+B)+C.$

2. Usando a definição de soma vemos que $A+B = \{r \in \mathbb{Q} | r = a+b \ \ para \ \ algum \ \ a \in A \ \ e \ \ b \in B\} = \{r \in \mathbb{Q} | r = b + a \ \ para \ \ algum \ \ b \in B \ \ e \ \ a \in A\} = B + A.$

3. Usando a definição de soma vemos que $A+D_0 = \{r \in \mathbb{Q} | r = a+b, \ \ para \ \ algum \ \ a \in A \ \ e \ \ b \in D_0\}$. Seja $a \in A$. Então pela parte (III) da definição de Corte de Dedekind existe um $c \in A$ tal que $c < a$. Portanto, $a = c + (a - c) \in A + D_0$. Isso resulta que $A \subset A + D_0$. Agora, se $d \in A + D_0$, então temos $d = p + q$ onde $p \in A$ e $q \in D_0$. Pela definição de $D_0$ vemos que $q > 0$ o que implica $p + q > p$. Pela parte (II) da definição de Corte de Dedekind concluímos que $d = p + q \in A$ . Isso resulta que $A + D_0 \subset A$ e assim temos $A + D_0 = A$.

4. Usando a definição de soma de Corte de Dedekind vemos que

$$A + (-A) = \{r \in \mathbb{Q} | r = a + b, \ \ para \ \ algum \ \ a \in A \ \ e \ \ b \in -A\}$$

Seja $x \in A+(-A)$. Então $x = p+q$,onde $p \in A$ e $q \in -A$. Usando a definição de $-A$ temos que $-q < c$ para algum $c \in \mathbb{Q} - A$. Pela parte (II) do lema 1.5 concluímos que $-q \in \mathbb{Q} - A$. Isso resulta que $-q < a, \forall a \in A$, em particular para $p \in A$. Assim, temos $-q < p$, ou seja, $x = p + q > 0$. Portanto, $x \in D_0$. Deduzimos que $A + (-A) \in D_0$. Agora, se $y \in D_0$ temos $y > 0$. Isso resulta pela parte (I) do lema 1.9 que existem $u \in A$ e $v \in \mathbb{Q} - A$ tais que $y = u - v$ com $v < e$ para algum $e \in \mathbb{Q} - A$. Note que $-(-v) < e$ implica $-v \in -A$. Assim, $y = u - v \in A + (-A)$ o que implica $D_0 \in A + (-A)$. Portanto, temos $A + (-A) = D_0$.

■

**Teorema 2.2** *Sejam $A, B \in \Re$. Então são válidas as seguintes propriedades:*

1. *Se $A + B = A + C$,então $B = C$. (Lei do Cancelamento)*
2. *$A = -(-A)$ para todo $A \in \Re$.*
3. *$-(A + B) = (-A) + (-B)$ para todo $A, B \in \Re$.*

**Demonstração:**

1. $B = B + D_0 = B + [A + (-A)] = (B + A) + (-A) = (A + B) + (-A) = (A+C)+(-A) = (C+A)+(-A) = C+[A+(-A)] = C+D_0 = C$. Portanto, $B = C$.
2. $A + (-A) = (-A) + A = D_0 = (-A) + [-(-A)] = [-(-A)] + (-A)$. Isso resulta de (1), que $A = -(-A)$.
3. $(A + B) + [-(A + B)] = D_0 = D_0 + D_0 = [A + (-A)] + [B + (-B)] = A+[(-A)+B+(-B)] = A+[B+(-A)+(-B)] = (A+B)+[(-A)+(-B)]$. Isso resulta de (1), que $-(A + B) = (-A) + (-B)$.

■

**Teorema 2.3** *Sejam $A, B, C \in \Re$. Então são válidas as seguintes propriedades:*

1. *Ocorre uma das situações ou $A = B$ ou $A > B$ ou $A < B$ (Lei daTricotomia)*
2. *$AB = BA$ (Lei Comutativa)*

3. $A(BC) = (AB)C$ *(Lei Associativa para a Multiplicação)*

4. $AD_1 = A$ *(Lei da Identidade Multiplicativa)*

5. *Se* $A \neq D_0$, *então* $AA^{-1} = D_1$ *(Lei do Inverso Multiplicativo)*

6. $A(B + C) = AB + AC$ *(Lei da Distributiva)*

**Demonstração:**

1. Essa parte segue-se imediatamente do Lema 1.6 e da definição sobre a relação de ordem.

2. Pela parte (1) deste teorema, sabemos que ou $A \geq D_0$ ou $A < D_0$ o mesmo ocorrendo com $B$. Isso resulta quatro casos:

   - Primeiro, suponha que $A \geq D_0$ e $B \geq D_0$. Então

   $$AB = \{r \in \mathbb{Q} | r = ab, \ \ para \ \ algum \ \ a \in A \ \ e \ \ b \in B\}$$

   $$= \{r \in \mathbb{Q} | r = ba, \ \ para \ \ algum \ \ a \in A \ \ e \ \ b \in B\} = BA.$$

   - Segundo, supondo $A \geq D_0$ e $B < D_0$ vemos pela parte (Ill) do Lema 2.1 que $-B \geq D_0$ . Usando a definição de multiplicação de reais temos $AB = -[A \cdot (-B)] = -[(-B) \cdot A] = -(-B) \cdot A = BA$, pois, $-(-A) = A$.
   - Terceiro, o caso $A < D_0$ e $B \geq D_0$ é análogo ao segundo caso.
   - Quarto, supondo $A < D_0$ e $B < D_0$ vemos pela parte (III) do Lema 2.1 que $-A \geq D_0$ e $-B \geq D_0$. Usando a definição teremos $AB = (-A)(-B) = (-B)(-A) = BA$.

3. Temos oito casos.

   - Primeiro, suponha $A \geq D_0$, $B \geq D_0$, e $C \geq D_0$. Se $A \geq D_0$, $B \geq D_0$ e $C \geq D_0$ então é fácil concluir, pela definição de multiplicação, que $AB \geq D_0$ e $BC \geq D_0$. Usando a definição de multiplicação vemos que $A(BC) = \{r \in \mathbb{Q} | r = ad \ \ para \ \ algum \ \ a \in A \ \ e \ \ d \in BC \ \ e \ \ se, \ \ e \ \ somente \ \ se, \ \ para \ \ algum \ b \in B \ \ e \ \ c \in C \ \ tais \ \ que \ d = bc\} = \{r \in \mathbb{Q} | r = a(bc) \ \ para \ \ algum \ \ a \in A, b \in B \ \ e \ \ c \in C\} = \{r \in \mathbb{Q} | r = (ab)c \ \ para \ \ algum \ \ a \in A, b \in B \ \ e \ \ c \in C\} = \{r \in \mathbb{Q} | r = (ab)c \ \ para \ \ algum \ \ (ab) \in AB \ \ e \ \ c \in C\} = (AB)C$.
   - Segundo, suponha que $A \geq D_0$, $B < D_0$, e $C \geq D_0$ . Então é fácil, também, concluir que $-B \geq D_0$, $AB < D_0$ e $BC < D_0$. Usando a definição de multiplicação vemos que $A(BC) = -[A(-BC)] = -\{A[(-B)C]\} = -\{[A(-B)]C\} = -[A(-B)]C = (AB)C$.

- O terceiro caso ($A \geq D_0$, $B < D_0$, e $C \geq D_0$ ) e o quarto ($A < D_0$, $B \geq D_0$, e $C \geq D_0$) são análogos ao segundo caso , por isso, omitiremos suas demonstrações.
- Quinto, suponha $A \geq D_0$, $B < D_0$, e $C < D_0$. Então, temos $-B \geq D_0$,$-C \geq D_0$,$AB < D_0$ e $BC \geq D_0$. Usando a definição de multiplicação vemos que $A(BC) = A[(-B)(-C)] = [A(-B)](-C) = \{-[A(-B)]\}C = (AB)C$.
- O sexto caso ($A < D_0$, $B \geq D_0$, e $C < D_0$) e o sétimo ($A < D_0$, $B < D_0$, e $C \geq D_0$) são análogos ao quinto caso, por essa razão, omitiremos suas demonstrações.
- Oitavo, suponha $A < D_0$, $B < D_0$, e $C < D_0$. Então, temos $AB \geq D_0$ e $BC \geq D_0$. Usando a definição vemos que $A(BC) = -[(-A)(BC)] = -\{(-A)[(-B)(-C)]\} = -\{[(-A)(-B)](-C)\} = -\{(AB)(-C)\} = (AB)C$.

4. Temos dois casos.
   - Primeiro, suponha $A \geq D_0$. Seja $x \in AD_1$. Como $D_1 \geq D_0$, usando a definição de multiplicação temos que $x = rs$ para algum $r \in A$ e $s \in D_1$. Disso resulta que, $s > 1$ e $r > 0$ o que implica $rs \geq r$. Ora, $A$ é um Corte de Dedekind. Logo, $x = rs \in A$. Portanto, provamos $AD_1 \subseteq A$. Agora, seja $z \in A$. Pela definição de Corte (III), existe um $y \in A$ tal que $y < z$. Disso resulta que, $\frac{z}{y} > 1$,pois, $y > 0$. Assim, $z = y \cdot \frac{z}{y} \in AD_1$. Assim, temos $A \subseteq AD_1$, e portanto $AD_1 = A$.
   - Segundo, suponha $A < D_0$. Então temos $-A \geq D_0$ e $D_1 \geq D_0$. Usando a definição de multiplicação vemos que $AD_1 = -[(-A)D_1] = -[(-A)] = -(-A) = A$.

5. Suponha $A \neq D_0$. Pela parte (1) deste teorema temos ou $A > D_0$ ou $A < D_0$. Primeiro, suponha $A > D_0$. Disto resulta que, $A^{-1} > D_0$. Usando a definição de multiplicação de Cortes de Dedekind temos $AA^{-1} = \{r \in \mathbb{Q} | r = ab, \ \ com \ \ a \in A, b \in A^{-1}\}$. Seja $x \in AA^{-1}$. Então $x = uv$ para algum $u \in A$ e $v \in A^{-1}$. Como $A > D_0$ e $A^{-1} > D_0$ concluímos que $u > 0$ e $v > 0$. Assim, $\frac{1}{v} < h$ para algum $h \in \mathbb{Q} - A$. Disso resulta pela parte (II) do lema 1.5 que $\frac{1}{y} \in \mathbb{Q} - A$. Assim, temos que pela parte (I) do Lema 1.5 que $\frac{1}{v} < u$. Logo, $x = uv > 1$. Portanto, $x \in D_1$. Assim, provamos que $AA^{-1} \subseteq D_0$. Agora, seja $y \in D_1$. Então $y > 1$. Por causa de $A > D_0$ sabemos pela parte (I) do Lema 2.1 que existe um $q \in \mathbb{Q} - A$ tal que $q > 0$. Disso resulta pela parte (II) do Lema 1.9 que existem $r \in A$ e $s \in \mathbb{Q} - A$ tais que $s > 0$, e $y > \frac{r}{s}$ com $s < e$ para algum $e \in \mathbb{Q} - A$. Sabemos que $\frac{1}{s} > 0$ e que $s = \dfrac{1}{\frac{1}{s}} < e$ para algum $e \in \mathbb{Q} - A$ o que implica $\frac{1}{s} \in A^{-1}$. Assim, $\frac{r}{s} = r \cdot \frac{1}{s} \in AA^{-1}$. Como $y > \frac{r}{s}$,

então pela parte (II) da definição de Corte de Dedekind temos que $y \in AA^{-1}$ . Assim, $D_1 \subseteq AA^{-1}$ , e portanto $AA^{-1} = D_1$. Vamos supor agora, que $A < D_0$. Então pela definição do elemento inverso vemos que $A^{-1} = -(-A)^{-1}$. Assim, $-A^{-1} = -[-(-A)^{-1}]$ o que implica $-A^{-1} = -(-A)^{-1}$ (Note que usamos $A = -(-A)$). Sabemos que $A < D_0$ se e somente se $-A > D_0$ o que implica $(-A)^{-1} > D_0$ ou, equivalentemente, $-A^{-1} > D_0$. Disso resulta $A^{-1} < D_0$. Usando, agora, a definição de multiplicação de Cortes de Dedekind para o caso $A < D_0$ e $A^{-1} < D_0$ teremos $AA^{-1} = (-A)(-A^{-1}) = (-A)(-A)^{-1} = D_1$.

6. Temos oito casos.

   - Primeiro, suponha $A \geq D_0$, $B \geq D_0$, e $C \geq D_0$. Pelo Lema 2.1 $(ii)$, todos os elementos de cada conjunto $A, B$,e $C$ é maior do que 0. Pela definição de soma de $B + C$, resulta que todos os seus elementos são maiores que 0. Além disso, usando a definição de $AB$ para $A \geq D_0$ e $B \geq D_0$ verificamos, também, que todos os elementos de $AB$ são maiores do que 0. Usando o mesmo argumento, concluímos que os elementos dos conjuntos $AC, A(B + C)$, e $AB + AC$ são maiores do que 0. Seja $x \in A(B + C)$. Como mencionamos, $x > 0$. Pela definição, sabemos que $x = aq$ para algum $a \in A$ e $q \in B + C$, e que $q = b + c$ para algum $b \in B$ e $c \in C$. Assim, $x = a(b + c) = ab + ac$ com $ab \in AB$ e $ac \in AC$ o que implica $x \in AB + AC$. Portanto, $A(B + C) \subseteq AB + AC$. Agora, tomamos $y \in AB + AC$. Então, $y = u + v$ para algum $u \in AB$ e $v \in AC$. Assim, $u = a_1b$ e $v = a_2c$ com $a_1, a_2 \in A, b \in B$, e $c \in C$. Se $a_1 = a_2$, então $y = a_1(b + c)$, logo $y \in A(B + C)$. Supondo, $a_1 \neq a_2$ . Sem perda de generalidade, suponha $a_1 > a_2$. Note que $\frac{a_1b}{a_2} > b$, e assim pela parte (II) de Corte de Dedekind vemos que $\frac{a_1b}{a_2} \in B$.Como $y = a_2\left(\frac{a_1b}{a_2} + c\right)$, concluímos que $y \in A(B + C)$.Portanto, temos $AB + AC \subseteq A(B + C)$, e assim $A(B + C) = AB + AC$.
   - Segundo, suponha $A \geq D_0$, $B \geq D_0$, e $C < D_0$. Pelo Lema 2.1(iii), obtemos $-C \geq D_0$. Temos dois casos a considerar : $B + C \geq D_0$ ou $B + C < D_0$. Primeiro, suponha que $B + C \geq D_0$. Usando a propriedade distributiva já demonstrada (nesta primeira parte) obtemos $A(-C) = -AC$ [veja o Teorema 2.5 $(II)$]. Logo, vemos que $AB + AC = A[(-C) + (B + C)] + AC = A(-C) + A(B + C) + AC = -AC + A(B + C) + AC = A(B + C)$. Segundo, suponha que se $B + C < D_0$, então $-(B + C) \geq D_0$. Usando o teorema 2.2 (3) e a definição de multiplicação, vemos que $AB + AC = AB + \{-[A(-C)]\} = AB + \{-[A[B + [-(B + C)]]]\} = AB + \{-[AB + A[-(B + C)]]\} = AB + \{-[AB]\} + \{-[A[-(B + C)]]\} = -[A[-(B + C)]] = A(B + C)$.

- O terceiro caso ($A \geq D_0$, $B < D_0$, e $C \geq D_0$) e o quarto ($A < D_0$, $B \geq D_0$, e $C \geq D_0$) são análogos ao segundo caso , por isso, omitiremos suas demonstrações.
- Quinto, $A \geq D_0$, $B < D_0$, e $C < D_0$. Então, $B+C < D_0$,$-B \geq D_0$,$-C \geq D_0$ e $-(B+C) \geq D_0$. Então, usando a definição de multiplicação vemos que $A(B+C) = -[A[-(B+C)]] = -[A[(-B)+(-C)]] = -[A(-B)+A(-C)] = -[A(-B)] + [-[A(-C)]] = AB + AC$.
- O sexto caso ($A < D_0, B \geq D_0$, e $C < D_0$) e o sétimo ($A < D_0, B < D_0$, e $C \geq D_0$) são análogos ao quinto caso, por essa razão, omitiremos suas demonstrações.
- Oitavo, suponha $A < D_0$, $B < D_0$, e $C < D_0$. Então, $-A \geq D_0$, $-B \geq D_0$, e $-C \geq D_0$. Usando a definição de multiplicação temos $A(B+C) = \{(-A)[-(B+C)]\} = \{(-A)[(-B)+(-C)]\} = (-A)(-B)+(-A)(-C) = AB + AC$.

■

**Teorema 2.4** *Sejam $A, B \in \Re$. Então são válidas as seguintes propriedades.*

1. $AD_0 = D_0$
2. $A(-B) = (-A)B = -AB$

**Demonstração:**

1. $AD_0 + AD_0 = A(D_0 + D_0) = AD_0 = AD_0 + D_0$ . Disso resulta que, $AD_0 = D_0$.
2. De $AD_0 = A[B + (-B)] = AB + A(-B)$ e $D_0 = AB + (-AB)$ vemos, por (1), que $AB + A(-B) = AB + (-AB)$ . Disso resulta pela Lei do Cancelamento que, $A(-B) = -AB$. De maneira análoga , prova-se que $(-A)B = -AB$. Portanto, segue-se o resultado.

■

**Teorema 2.5** *Sejam $A, B, C \in \Re$. Então são válidas as seguintes propriedades.*

1. *Se $A < B$ e $B < C$ então $A < C$ (Lei da Transitividade)*
2. *Se $A < B$ então $A + C < B + C$ (Lei Aditiva para Ordem)*
3. *Se $A < B$ e $C > D_0$ então $AC < BC$ (Lei Multiplicativa para Ordem)*
4. *$D_0 < D_1$*

**Demonstração:**

1. Pela definição temos $B \subsetneq A$ e $C \subsetneq B$. Disso resulta, pela propriedade transitiva de conjuntos, que $C \subsetneq A$. Portanto, temos A<C.

2. Supondo que $A < B$. Pela definição de relação, $B \subsetneq A$. Seja $x \in B + C$. Isso resulta que $x = u + v$ para algum $u \in B$ e $v \in C$. Por hipótese, $u \in A$, e assim $x = u + v \in A + C$. Logo, $B + C \subseteq A + C$. Novamente da hipótese, existe um $p \in A$ tal que $p \notin B$. Assim, embora se tenha $x = p + v \in A + C$, porém, $x = p + v \notin B + C$. Logo, temos $A + C \neq B + C$. Assim, vemos que $B + C \subsetneq A + C$. Portanto, temos $A + C < B + C$.

3. Suponha $A < B$ e $C > D_0$. Pela parte (2) deste teorema vemos que $D_0 = A + (-A) < B + (-A)$. Logo, $B + (-A) > D_0$. De $C > D_0$ e $B + (-A) > D_0$ obtemos $[B + (-A)]C > D_0$. Usando a parte (2) deste teorema vemos que $AC + [B + (-A)]C > D_0 + AC = AC$. Usando os Teorema 2.3 (6) e 2.1 (4) deduzimos que $BC > AC$.

4. É imediato que $D_1 \subseteq D_0$. Sabemos que $0 < 1$. Se tomarmos $y = \frac{1}{2}$ vemos que $y > 0$, porém $y < 1$. Isso implica que existe um $y \in D_0$ tal que $y \notin D_1$. Assim, concluímos que $D_0 \neq D_1$. Disso resulta que $D_1 \subsetneq D_0$. Portanto, temos $D_0 < D_1$.

■

**Definição 2.7** *Um isomorfismo é uma função $f : A \longrightarrow B$ bijetora que satisfaz as seguintes condições:*

*(1)* $f(x + y) = f(x) + f(y)$, *para todo* $x, y \in A$;

*(2)* $f(xy) = f(x)f(y)$, *para todo* $x, y \in A$.

Se $f : A \longrightarrow B$ é um isomorfismo, então dizemos que $A$ e $B$ são isomorfos ou $A$ é isomorfo a $B$, e indicamos por $A \approx B$.

Os teoremas 2.1, 2.3 e 2.5 formam um conjunto de propriedades chamado de Corpo de números reais. Essas propriedades são gozadas, também, pelos números racionais e, por isso, eles são caracterizados como um Corpo. O que vai diferenciar ambos, porém, é a existência de uma propriedade peculiar apenas ao conjunto de números reais não racionais. Ela é que vai dar ao conjunto de números reais uma característica de Completude, para isso, vamos precisar de alguns conceitos que serão tratados em capítulos posteriores. No entanto, o que vamos fazer agora, é formalizar a ideia de que o conjunto dos números racionais "está contido" no conjunto dos números reais. Acontece que os números racionais são objetos que possuem natureza distinta dos números reais, pois, enquanto os primeiros são classes de equivalência

o segundo são subconjuntos de números racionais. Parece estranho, o uso das aspas na frase "está contido" , pois, a ideia que subjaz essa frase, normalmente, é que o conjunto de números reais, somente contém, literalmente, o conjunto de números racionais se esses tiverem a mesma natureza dos reais, isto é, eles também são subconjuntos de números racionais, mas isso, pelo menos acontece, no ponto de vista intuitivo; no ponto de vista da construção de números reais, porém, esses elementos (números racionais e números reais) são distintos. A pergunta natural que surge é "Como fazer para que o conjunto dos números racionais sejam vistos como subconjuntos de números reais ?" A resposta para essa pergunta é encontrar uma cópia do conjunto de números racionais de modo ela possua elementos de mesma natureza que os números reais. Mais precisamente, a solução consiste em encontrar um isomorfismo entre o conjunto dos números racionais $\mathbb{Q}$ e um conjunto $\overline{\mathbb{Q}}$ chamado **conjunto cópia de** $\mathbb{Q}$ que preservem $0, 1 \in \mathbb{Q}$, as operações binárias de adição e multiplicação, e a relação de ordem. Raciocínio similar é estendido quando queremos formalizar que os naturais está contido nos inteiros e que , por sua vez, está contido nos racionais. Vamos mostrar isso através do seguinte teorema.

**Teorema 2.6** *Seja* $f : \mathbb{Q} \to \overline{\mathbb{Q}} = \{D_r \in \Re | r \in \mathbb{Q}\}$, *definida por* $f(r) = D_r$ *para todo* $r \in Q$. *Então a função satisfaz os seguintes requisitos:*

*(i)* $f$ *é injetiva;*

*(ii)* $f$ *é sobrejetiva;*

*(iii)* $f(0) = D_0$ *e* $f(1) = D_1$*;*

*(iv) Seja* $r, s \in \mathbb{Q}$. *Então:*

- *(a)* $f(r + s) = f(r) + f(s)$*;*
- *(b)* $f(-r) = -f(r)$*;*
- *(c)* $f(rs) = f(r)f(s)$*;*
- *(d) Se* $r \neq 0$ *então* $f(r^{-1}) = [f(r)]^{-1}$*;*
- *(e)* $r < s$ *se e somente se* $f(r) < f(s)$.

**Demonstração:**

$(i)$ Para provarmos a injetividade, devemos provar a afirmação : Se $D_r = D_s$, então temos necessariamente $r = s$. Suponha por absurdo, que $r \neq s$. Então pela lei da tricotomia temos $r > s$ ou $r < s$. Suponha $r > s$. Então vemos que $s < \frac{r+s}{2} < r$. Fazendo $y = \frac{r+s}{2}$ .Disso resulta, pela definição do conjunto $D_t, t \in \mathbb{Q}$, que existe um $y \in D_s$ tal que $y \notin D_r$. Portanto, $D_r \neq D_s$. O mesmo raciocínio leva ao mesmo resultado se supormos, agora, que $r < s$. Assim, $f(r) = f(s)$ implica $D_r = D_s$ , e portanto, $r = s$. Logo, $f$ é injetiva.

(*ii*) Pela definição de $\overline{\mathbb{Q}}$ é imediato que $f$ é sobrejetiva.

(*iii*) É trivial, pela definição de $f$.

(a) Devemos provar a afirmação: $D_{r+s} = D_r + D_s$. Com efeito, seja $x \in D_r + D_s$. Então, pela definição de soma de Cortes, existem $u \in D_r ev \in D_s$ tais que $x = u + v$. Assim, vemos que $u > r$ e $v > s$. Disso resulta, $x = u + v > r + s$. Isso implica que $x \in D_{r+s}$. Portanto, $D_r + D_s \subseteq D_{r+s}$.

Seja $z \in D_{r+s}$. Então $z > r + s$. Escrevendo $z = \frac{z+r-s}{2} + \frac{z+s-r}{2}$ vemos que $\frac{z+r-s}{2} = \frac{z}{2} + \frac{r-s}{2} > r$ e que $\frac{z+s-r}{2} = \frac{z}{2} + \frac{s-r}{2} > s$. Pela definição de Corte de Dedekind (II), resulta $\frac{z+r-s}{2} \in D_r$ e $\frac{z+s-r}{2} \in D_s$. Assim, pela definição de soma temos $z \in D_r + D_s$. Portanto, $D_{r+s} \subseteq D_r + D_s$ , e assim concluímos que $D_{r+s} = D_r + D_s$. Pela definição de $f$, segue-se imediatamente que $f(r + s) = f(r) + f(s)$.

(b) Devemos provar a afirmação: $D_{-r} = -D_r$. Com efeito, $x \in -D_r$ se e somente se $-x < c$ para algum $c \in \mathbb{Q} - D_r$ se e somente se $-x < c \leq r$ se e somente $-x > r$ se e somente se $x \in D_{-r}$. Usando esse fato, concluímos, pela definição de $f$, que $f(-r) = -f(r)$.

(c) Vamos provar a afirmação: $D_{rs} = D_r D_s$. Temos quatro casos.

- Primeiro, suponha $D_r \geq D_0$ e $D_s \geq D_0$. Seja $x \in D_{rs}$. Então $x > rs > 0$, pois, $r > 0$ e $s > 0$. Escrevendo $x = \frac{rs+x}{2s} \cdot \frac{2sx}{rs+x}$, verificamos que $\frac{rs+x}{2s} > r$ e $\frac{2sx}{rs+x} > s$. Disso resulta, $\frac{rs+x}{2s} \in D_r$ e $\frac{2sx}{rs+x} \in D_s$. Assim, vemos que $x \in D_r D_s$, e portanto $D_{rs} \subseteq D_r D_s$. Seja $y \in D_r D_s$. Pela hipótese, temos que $y = uv$ para algum $u \in D_r, v \in D_s$. Isso resulta em $u > r$ e $v > s$ e, portanto em $y = uv > rs$. Assim, vemos que $y \in D_{rs}$. Logo, temos $D_{rs} \subseteq D_r D_s$, e assim concluímos que $D_{rs} = D_r D_s$.
- Segundo, suponha $D_r \geq D_0$ e $D_s < D_0$. Então temos $-D_s \geq D_0$. Disso resulta que $D_{-s} = -D_s \geq D_0$. Usando a definição de multiplicação e o resultado anterior, vemos que $D_r D_s = -[D_r \cdot (-D_s)] = -[D_r D_{-s}] = -D_{-rs} = D_{-(-rs)} = D_{rs}$.
- Terceiro, $D_r < D_0$ e $D_s \geq D_0$. É análogo ao segundo caso, e por isso iremos omitir sua demonstração.
- Quarto, $D_r < D_0$ e $D_s < D_0$. Então $-D_r \geq D_0$ e $-D_s \geq D_0$. Isso resulta em $D_{-r} = -D_r \geq D_0$ e $D_{-s} = -D_s \geq D_0$ . Agora, usando a definição de multiplicação de Corte de Dedekind e o resultado anterior vemos que $D_r D_s = (-D_r) \cdot (-D_s) = D_{-r} D_{-s} = D_{(-r)(-s)} = D_{rs}$. Portanto, usando a definição de $f$ vemos imediatamente que $f(rs) = f(r)f(s)$.

(d) Vamos provar a afirmação: $D_{r^{-1}} = [D_r]^{-1}$. Temos dois casos.

- Primeiro, suponha $D_r > D_0$. Então, neste caso, $\frac{1}{r} > 0$, pois, $r > 0$. Seja $x \in D_{r^{-1}}$. Resulta da definição que $x > \frac{1}{r}$ , o que implica $x > 0$ e $\frac{1}{x} < r \in \mathbb{Q} - D_r$. Assim, pela Definição 2.6 $(II)$ concluímos que $x \in [D_r]^{-1}$. Portanto, $D_{r^{-1}}[D_r]^{-1}$. Agora, seja $y \in [D_r]^{-1}$. Então, pela Definição 2.6 $(I)$ resulta que $y > 0$ e $\frac{1}{y} < c$ para algum $c \in \mathbb{Q} - D_r$. Disso resulta que $c \leq r$, pois, $c \notin D_r$. Assim, vemos que $\frac{1}{y} < r$ e, portanto $y > r$. Logo, $y \in D_r$, e assim $[D_r]^{-1} \subseteq D_r$. Portanto, $D_{r^{-1}} = [D_r]^{-1}$.
- Segundo, suponha $D_r < D_0$. Então $-D_r \geq D_0$. Isso resulta em $D_{-r} = -D_r > D_0$. Agora, usando a Definição 2.6 $(II)$ e o resultado anterior vemos $[D_r]^{-1} = -(-D_r)^{-1} = -(D_{-r})^{-1} = -(D_{(-r)^{-1}}) = D_{-(-r)^{-1}} = D_{r^{-1}}$. Portanto, em qualquer um dos casos, temos $D_{r^{-1}} = [D_r]^{-1}$. Podemos ter usado um caminho mais curto para afirmar esse resultado. Veja. Usando o resultado anterior vemos que $D_r D_{r^{-1}} = D_{rr^{-1}} = D_1$. Assim, concluímos que $D_{r^{-1}} = [D_r]^{-1}$.

(e) Pela parte $(i)$ vemos que, se $r \neq s$ então temos $D_r < D_s$ ou $D_r > D_s$. Suponha que $D_r > D_s$. Por definição, temos $D_r \subset D_s$,ou equivalentemente, todo $x > r$ implica em $x > s$. Agora, vamos provar o seguinte argumento: "Se todo $x > r$ implica em $x > s$ então temos, necessariamente, que $r > s$". Suponha o contrário, $r < s$. Fazendo $y = \frac{r+s}{2}$. Concluímos, com isso que, embora se tenha $y > r$ vemos, no entanto, que $y < s$, mostrando uma contradição na hipótese. Para não contrariar a hipótese, então devemos ter necessariamente $r > s$. Assim, provamos que se $D_r > D_s$ temos necessariamente $r > s$. Portanto, provamos a afirmação de que se $r < s$,então temos $D_r < D_s$. Usando a definição de $f$ concluímos que se $r < s$ então $f(r) < f(s)$.

■

É importante salientar, que o subconjunto $\overline{\mathbb{Q}}$, obviamente, herda todas as propriedade do corpo $\Re$ dos reais e que o Teorema 2.6 nos diz que todos os números racionais são copiados para o conjunto $\overline{\mathbb{Q}}$ e, além disso, preserva todas as operações binárias e a relação de ordem dos números racionais. Então operar com os números reais (Corte de Dedekind) é o mesmo que operar com os números racionais (classes de Equivalência), por isso, usaremos, sem distinção, os símbolos $0, 1, \bar{0}, \bar{1}$ e os demais que não foram mencionados. De um modo intuitivo, podemos pensar que $0, 1 \in \mathbb{Q}$, ou que $0, 1 \in \Re$.

# Capítulo 3

# Propriedades Algébricas dos Números reais

As propriedades que vamos mencionar neste capítulo, são meras consequências e repetições dos teoremas 2.1, 2.3, 2.2, 2.4. Antes de descrevê-las e demonstrá-las, vamos definir algumas operações binárias de subtração e divisão combinadas com as operações de adição, multiplicação, e operações unárias de inverso aditivo e multiplicativo; outra coisa que vamos fazer é associar os números reais por letras minúsculas do nosso alfabeto, já que as maiúsculas lembram os Cortes de Dedekind.

**Definição 3.1** *Sejam* $\mathbf{a}, \mathbf{b} \in \Re$. *Definimos a diferença de* $\mathbf{a}$ *com* $\mathbf{b}$, *denotado por* $\mathbf{a} - \mathbf{b}$, *o número real tal que* $\mathbf{a} - \mathbf{b} = \mathbf{a} + (-\mathbf{b})$.

**Definição 3.2** *Sejam* $\mathbf{a}, \mathbf{b} \in \Re$, *com* $\mathbf{b} \neq 0$. *Definimos a divisão de* $\mathbf{a}$ *por* $\mathbf{b}$, *denotado por* $\mathbf{a} \div \mathbf{b}$, *o número real tal que* $\mathbf{a} \div \mathbf{b} = \mathbf{a}\mathbf{b}^{-1}$. *Podemos denotar a divisão de* $\mathbf{a}$ *por* $\mathbf{b}$, *também, por* $\frac{\mathbf{a}}{\mathbf{b}}$.

**Definição 3.3** *Seja* $\mathbf{a} \in \Re$ . *Definimos o quadrado de* $\mathbf{a}$, *denotado por* $\mathbf{a}^2$, *o número real tal que* $\mathbf{a}^2 = \mathbf{a} \cdot \mathbf{a}$

**Definição 3.4** *Sejam* $\mathbf{a}, \mathbf{b} \in \Re$. *Dizemos que* $\mathbf{a}$ *é menor do que ou igual a* $\mathbf{b}$, *denotado por* $\mathbf{a} \leq \mathbf{a}$, *se* $\mathbf{a} < \mathbf{b}$ *ou* $\mathbf{a} = \mathbf{b}$.

**Definição 3.5** *Dado* $1 \in \Re$. *Definimos o número real dois, pelo símbolo* 2, *tal que* $2 = 1 + 1$.

***Observação 3.5.1*** *Usando a definição de diferença e divisão sobre* $\Re$, *é óbvio que* $0 - b = -b$, $\frac{1}{b} = b^{-1}$ *e que* $\frac{0}{b} = 0$.

***Observação 3.5.2*** *As definições 3.3, 3.4 e 3.5, bem como as definições de adição e multiplicação, são repetidamente usadas ao se construir os números naturais, inteiros e racionais.*

**Teorema 3.1** *Sejam $a, b, c \in \Re$ números reais quaisquer. Então são válidas as seguintes propriedades:*

*(I)* $Se\ a + c = b + c\ então\ a = b;$

*(II)* $Se\ a + b = a\ então\ b = 0;$

*(III)* $Se\ a + b = 0\ então\ b = -a$

*(IV)* $-(a + b) = (-a) + (-b);$

*(V)* $-0 = 0;$

*(VI)* $a \cdot 0 = 0 \cdot a = 0;$

*(VII)* $a \cdot 1 = 1 \cdot a = a;$

*(VIII)* $Se\ ac = bc\ e\ c \neq 0,\ então\ a = b;$

*(IX)* $Se\ ab = a\ e\ a \neq 0\ então\ b = 1;$

*(X)* $Se\ ab = 1\ então\ b = a^{-1};$

*(XI)* $Se\ a \neq 0\ e\ b \neq 0,\ então\ (ab)^{-1} = a^{-1}b^{-1};$

*(XII)* $(-a)b = a(-b) = -ab;$

*(XIII)* $(-1)a = -a;$

*(XIV)* $-(-a) = a;$

*(XV)* $(-1)^2 = 1\ e\ 1^{-1} = 1;$

*(XVI)* $Se\ ab = 0\ então\ a = 0\ ou\ b = 0;$

*(XVII)* $Se\ a \neq 0\ então\ (a^{-1})^{-1} = a;$

*(XVIII)* $Se\ a \neq 0\ então\ (-a)^{-1} = -a^{-1};$

**Demonstração:** Omitiremos as provas das propriedades $(I)$,$(IV)$, $(VI)$, $(VII)$, $(XII)$ e $(XIII)$ pois, já a demonstramos nos teoremas 2.2, 2.3 e 2.4 do capítulo anterior com a diferença de que foram usadas letras maiúsculas, e as notações $D_0$ e $D_1$ , em vez de, letras minúsculas, do zero(0) e um(1), respectivamente. O leitor interessado em rever as demonstrações, basta trocar as letras maiúsculas, por minúsculas, e a notação de $D_0$ e $D_1$, por zero (0) e um (1), nos teoremas mencionados.

Parte $(II)$: Veja que $a + b = a = a + 0$. Pela parte $(I)$, deduzimos que $b = 0$.

Parte $(III)$: Veja que $a + b = 0 = a + (-a)$. Pela parte $(I)$, deduzimos que $b = -a$.

Parte $(V)$: Usando a parte $(IV)$ deste teorema e o teorema 2.1 (3) e (4), vemos que $-0 + (-0) = -0 = -0 + 0$. Pela parte $(I)$, deduzimos que $-0 = 0$.

Parte $(VIII)$: Usando a parte $(VII)$, o teorema 2.3 (3) e (5), vemos que $a = a \cdot 1 = a(c \cdot c^{-1}) = (ac)c^{-1} = (bc)c^{-1} = b(c \cdot c^{-1}) = b \cdot 1 = b$. Assim, $a = b$.

Parte $(IX)$: Veja que $ab = a = a.1$. Pela parte $(VIII)$, deduzimos que $b = 1$.

Parte $(X)$: Veja que $ab = 1 = aa^{-1}$. Pela parte $(VIII)$, deduzimos que $b = a^{-1}$.

Parte $(XI)$: Veja que $(ab)(ab)^{-1} = 1 = 1 \cdot 1 = (aa^{-1})(bb^{-1})$ . Usando o teorema 2.3 (2) e (3), vemos que $(ab)(ab)^{-1} = (aa^{-1})(bb^{-1}) = (ab)(a^{-1}b^{-1})$. Assim, $(ab)(ab)^{-1} = (ab)(a^{-1}b^{-1})$. Pela parte $(VIII)$, deduzimos que $(ab)^{-1} = a^{-1}b^{-1}$.

Parte $(XIII)$: Fazendo, na parte $(XII)$, $a = 1$ e $b = a$, vemos que $(-1)a = -a$.

Parte $(XV)$: Fazendo $a = -1$ na parte $(XIII)$, usando a definição 3.3 e a parte $(XIV)$, vemos que $(-1)^2 = (-1)(-1) = -(-1) = 1$. Agora, usando o teorema 2.3 (5) e parte $(VII)$ deste teorema, segue-se que $1 = 1.1^{-1} = 1^{-1}$. Portanto, temos $1^{-1} = 1$.

$(XVI)$: Suponha $a \neq 0$. Se $ab = 0$, então $b = b \cdot 1 = b \cdot (aa^{-1}) = (ba) \cdot a^{-1} = (ab)a^{-1} = 0 \cdot a^{-1} = 0$. Assim, $b = 0$. Usando o mesmo raciocínio para $b \neq 0$, concluímos que $a = 0$. Portanto, temos $a = 0$ ou $b = 0$.

Parte $(XVII)$: Suponha $a \neq 0$. Assim, vemos que $a^{-1}(a^{-1})^{-1} = 1 = a^{-1}a$. Pela parte $(VIII)$, deduzimos que $(a^{-1})^{-1} = a$.

Parte $(XVIII)$ Note que:

$(-a)(-a)^{-1} = 1 = (-1)(-1) \cdot 1 = (-1)(-1)(a \cdot a^{-1}) = [(-1)a] \cdot [(-1)a^{-1}] = (-a)(-a^{-1})$. Usando a parte $(VIII)$, deduzimos que $(-a)^{-1} = -a^{-1}$.

É interessante notar que podemos usar as propriedades acima para provar a unicidade dos elementos zero (0), um (1) e dos inversos aditivos e multiplicativos.

■

**Teorema 3.2** *Sejam $a, b, c, d \in \Re$ números reais quaisquer. Então são válidas as seguinte propriedades:*

*(I)* *Se* $a \leq b$ *e* $b \leq a$ *então* $a = b$.

*(II)* *Se* $a \leq b$ *e* $b \leq c$,*então* $a \leq c$.*Se* $a \leq b$ *e* $b < c$ *então* $a < c$. *Se* $a < b$ *e* $b \leq c$ *então* $a < c$.

*(III)* *Se* $a \leq b$ *então* $a + c \leq b + c$,*para todo* $c \in \Re$.

*(IV)* *Se* $a < b$ *e* $c < d$ *então* $a + c < b + d$. *Se* $a \leq b$ *e* $c \leq d$ *então* $a + c \leq b + d$.

*(V)* $a > 0$,*se somente se*,$-a < 0; a < 0$,*se e somente se*,$-a > 0; a \geq 0$,*se somente se*,$-a \geq 0; a \geq 0$,*se e somente se*,$-a \geq 0$;

*(VI)* $a < b$ *se e somente se* $b - a > 0$ *se e somente se* $-b < -a; a \leq b$ *se e somente se* $b - a \geq 0$ *se e somente se* $-b \leq -a$;

*(VII)* *Se* $a \neq 0$ *então* $a^2 \neq 0$.

*(VIII)* $-1 < 0 < 1$

*(IX)* $a < a + 1$

*(X)* *Se* $a \leq b$ *e* $c > 0$ *então* $ac \leq bc$.

*(XI)* *Se* $0 \leq a < b$ *e* $0 \leq c < d$ *então* $ac < bd$; *Se* $0 \leq a \leq b$ *e* $0 \leq c \leq d$ *então* $ac \leq bd$.

*(XII)* *Se* $a < b$ *e* $c < 0$ *então* $ac > bc$.

*(XIII)* *Se* $a > 0$ *então* $a^{-1} > 0$.

*(XIV)* *Se* $a > 0$ *e* $b > 0$ *então* $a < b$ *se e somente se* $b^{-1} < a^{-1}$ *se e somente se* $a^2 < b^2$.

**Demonstração:**

*(I)* Suponha que $a \leq b$ e $b \leq a$. Sabemos que $a < b$ ou $a = b$, e $b < a$ ou $b = a$. Primeiro, suponha $a < b$. Pela lei da tricotomia, não pode ocorrer o caso $a > b$ e $a = b$. Isso contradiz, que $a \geq b$. Suponha, agora, $a > b$. Pela lei da tricotomia, não pode ocorrer $a = b$ ou $a < b$. Isso contradiz, que $a \leq b$. Somente uma possibilidade ocorre $a = b$.

*(II)* Se $a \leq b$ e $b \leq c$. Então, pela definição de relação temos $a = b$ ou $a < b$,e $b = c$ ou $b < c$. Existem quatro casos. Primeiro, suponha que $a = b$ e $b = c$. Isso resulta, pela transitividade da igualdade, que $a = c$, Assim, $a \leq c$. Segundo, suponha $a = b$ e $b < c$. Disso resulta, que $a < c$ e, portanto, $a \leq c$. Terceiro, suponha $a < b$ e $b = c$. Disso resulta, que $a < c$, assim $a \leq c$. Quarto, suponha

$a < b$ e $b < c$. Usando a lei da transitividade (teorema 2.5 (1)), temos $a < c$. Assim, $a \leq c$. Portanto, em qualquer um dos casos temos sempre $a \leq c$. Se $a \leq b$ e $b \leq c$. Temos dois casos. Suponha $a = b$ e $b < c$. Disso resulta, que $a < c$, e assim temos $a < c$. Suponha, agora, $a < b$ e $b < c$. Pela lei da transitividade, temos que $a < c$. Portanto, em qualquer um dos casos temos sempre $a < c$.

$(III)$ Se $a \leq b$, então $a = b$ ou $a < b$. De $a = b$ resulta que $a + c = b + c$, e assim $a + c \leq b + c$. De $a < b$ resulta pelo teorema 2.5 (II), que $a + c < b + c$, e assim $a + c \leq b + c$. Portanto, vemos que em qualquer um dos casos que $a + c \leq b + c$.

$(IV)$ Se $a < b$, então pela parte $(III)$ temos $a + c < b + c$, e que se $c < d$ temos analogamente, $b + c < b + d$. Pela lei da transitividade, temos $a + c < b + d$. Agora, se $a \leq b$ e $c \leq d$. Temos quatro casos. Primeiro, se $a = b$ e $c = d$, então $a + c = b + c$ e $b + c = b + d$. Pela lei da transitividade, temos $a + c = b + d$. Assim, $a + c \leq b + d$. Segundo, se $a < b$ e $c = d$, então $a + c < b + c$ e $b + c = b + d$. Disso resulta, que $a + c < b + d$. Assim, temos $a + c \leq b + d$. O terceiro e o quarto casos são análogos aos primeiro e segundo casos.

$(V)$ Usando a lei comutativa, da identidade, do inverso aditivo e da adição para ordem, vemos que $a > 0$ se e somente se $a + (-a) > 0 + (-a)$ se e somente se $0 > -a$, e que $a < 0$ se e somente se $a + (-a) < 0 + (-a)$ se e somente se $0 < -a$. Usando a parte (III) deste teorema, provamos as outras duas partes de maneira semelhante, por isso, vamos omiti-las.

$(VI)$ Usando a definição 3.1, a lei da identidade, a lei aditiva para ordem, e a do inverso aditivo vemos que $a < b$ se e somente se $a + (-a) < b + (-a)$ se e somente se $0 < b - a$ se e somente se $0 < b + (-a)$ se e somente se $(-b) + 0 < (-b) + b + (-a)$ se e somente se $-b < -a$. A prova para a desigualdade $\leq$ é feita de maneira análoga, e por isso, vamos omiti-la.

$(VII)$ Suponha $a \neq 0$. Pela lei da tricotomia temos dois casos: $a > 0$ ou $a < 0$. Primeiro, se $a > 0$, então usando a lei multiplicativa para ordem e a definição 3.3, vemos que $a \cdot a > 0 \cdot a$ e, portanto, $a^2 > 0$. Segundo, se $a < 0$, então pela parte $(VI)$, deduzimos que $-a > 0$ o que implica $(-a)(-a) > 0$, ou seja, $(-a)^2 > 0$. Assim, resulta que $(-a)^2 = -[a(-a)] = -(-a^2) = a^2 > 0$. Portanto, se $a \neq 0$ temos $a^2 > 0$.

$(VIII)$ Pelo teorema 2.5 (IV), concluímos que $1 \neq 0$.Então, usando a parte $(VII)$, vemos que $1^2 > 0$. Disso resulta, pela lei da identidade multiplicativa que $1 > 0$. Agora, usando $(VI)$ vemos que $-1 < 0$. Juntando, as duas últimas desigualdades, obtemos $-1 < 0 < 1$.

$(IX)$ Sabemos que $0 < 1$. Usando a lei aditiva para ordem, obtemos $0 + a < 1 + a$. Então, usando a lei da identidade aditiva e a lei comutativa, obtemos $a < a+1$.

$(X)$ Temos dois casos. Primeiro, suponha $a < b$. Então, se $c > 0$ resulta, pela lei multiplicativa, que $ac < bc$. Segundo, suponha $a = b$. Segue-se imediatamente, que $ac = bc$. Portanto, por esses dois últimos resultados, concluímos que $ac \leq bc$.

$(XI)$ Temos quatro casos. Primeiro, suponha $0 < a < b$ e $0 < c < d$. Aplicando a lei multiplicativa para cada uma dessas desigualdades temos $ac < bc$ e $bc < bd$. Disso resulta, pela lei da transitividade, que $ac < bd$. Segundo, suponha $a = 0 < b$ e $0 < c < d$. Segue-se que $ac = 0 \cdot c < bc$ e que $bc < bd$. Pela lei da transitividade, temos $ac < bd$. Terceiro, suponha $0 < a < b$ e $c = 0 < d$. Esse caso é semelhante, ao segundo caso, por isso, vamos omitir seu desenvolvimento. Quarto, suponha $a = 0 < b$ e $c = 0 < d$. Então, temos $b0 < bd$ o que implica $ac = b0 = 0 < bd$. O raciocínio é similar se $0 \leq a \leq b$ e $0 \leq c \leq d$ e, por isso, omitiremos o seu desenvolvimento.

$(XII)$ Suponha $a < b$ e $c < 0$. Então, por $(VI)$ vemos que $-c > 0$. Resulta da lei multiplicativa que $a(-c) < b(-c)$, ou seja, $-ac < -bc$ o que implica, por $(VI)$, que $-(-bc) < -(-ac)$, isto é, $bc < ac$.

$(XIII)$ Suponha que $a^{-1} \leq 0$. Se $a^{-1} = 0$,então $aa^{-1} = a \cdot 0$ implica em $1 = 0$,o que é um absurdo,pois,$1 \neq 0$. Agora, se $a^{-1} < 0$ vemos que $a \cdot a^{-1} < a.0$, ou seja, $1 < 0$, o que é uma contradição. Portanto, devemos ter $a^{-1} > 0$.

$(XIV)$ Sabemos, por $(XIII)$, que $a^{-1} > 0$ e $b^{-1} > 0$,então pela parte $(XI)$, temos que $a^{-1}b^{-1} > 0$. Assim, vemos que $a < b$ se e somente se $a(a^{-1}b^{-1}) < b(a^{-1}b^{-1})$ se e somente se, pela lei comutativa, associativa e do inverso multiplicativo, $b^{-1} < a^{-1}$ se somente se $a < b$ se e somente se,por $(XI)$, $a \cdot a < b \cdot b$, isto é, $a^2 < b^2$, pois, $a > 0$ e $b > 0$.

■

**Corolário 3.2.1** *Sejam* $a, b, c, d \in \Re$.

*(I)* *Se* $a > 0$ *e* $b > 0$,*então* $a + b > 0$. *Se* $a > 0$ *e* $b \geq 0$,*então* $a + b > 0$.*Se* $a \geq 0$ *e* $b \geq 0$,*então* $a + b \geq 0$.

*(II)* *Se* $a < 0$ *e* $b < 0$,*então* $a + b < 0$. *Se* $a < 0$ *e* $b \leq 0$,*então* $a + b < 0$. *Se* $a \leq 0$ *e* $b \leq 0$,*então* $a + b \leq 0$.

*(III)* *Se* $a > 0$ *e* $b > 0$,*então* $ab > 0$. *Se* $a > 0$ *e* $b \geq 0$,*então* $ab \geq 0$. *Se* $a \geq 0$ *e* $b \geq 0$,*então* $ab \geq 0$.

*(IV)* *Se* $a < 0$ *e* $b < 0$, *então* $ab > 0$. *Se* $a < 0$ *e* $b \leq 0$, *então* $ab \geq 0$. *Se* $a \leq 0$ *e* $b \leq 0$, *então* $ab \geq 0$.

*(V)* *Se* $a < 0$ *e* $b > 0$, *então* $ab < 0$. *Se* $a < 0$ *e* $b \geq 0$, *então* $ab \leq 0$. *Se* $a \leq 0$ *e* $b > 0$, *então* $ab \leq 0$. *Se* $a \leq 0$ *e* $b \geq 0$, *então* $ab \leq 0$.

*(VI)* *Sejam* $a \geq 0$ *e* $b \geq 0$. *Se* $a + b = 0$, *então* $a = b = 0$.

*(VII)* *Sejam* $a > 0$ *e* $b > 0$. *Se* $a^2 \leq b^2$, *então* $a \leq b$.

Não demonstraremos esse corolário, pois, os argumentos usados em sua prova, são similares aos que foram utilizados no teorema anterior.

**Observação 3.2.1** *O corpo dos números reais, junto com o corolário 3.2.1, forma o corpo ordenado de números reais. Esse fato, é verdadeiro, também, para o conjunto dos números racionais e portanto, é um corpo ordenado, mas relativamente ao números reais ele visto como um subcorpo ordenado. Uma questão interessante que se levanta é "Existe outros corpos (ou subcorpos de* $\mathbb{R}$*) ordenados?" A resposta é sim se definirmos, de uma forma geral, o conceito de corpo ordenado.*

# Capítulo 4

# Corpo Ordenado

**Definição 4.1** *Dado um conjunto $F$, não vazio, munido com as operações de adição e multiplicação, fechadas em $F$. Sejam $a, b, c \in F$, dizemos que $F$ é um Corpo se os seus elementos satisfazem as seguintes propriedades:*

*(1)* $a + (b + c) = (a + b) + c$;

*(2)* $a + b = b + a$;

*(3)* $a + 0 = a$;

*(4)* $a + (-a) = 0$;

*(5)* $ab = ba$;

*(6)* $a.1 = a$;

*(7)* $a(b + c) = ab + ac$;

*(8) Se* $a \neq 0$, *então existe* $b = a^{-1}$ *tal que* $aa^{-1} = 1$;

Agora, temos condição de definir Corpo Ordenado.

**Definição 4.2** *Seja $F$ um corpo. Dizemos que $F$ é um corpo ordenado se existem dois subconjuntos disjuntos $P$ e $-P$ tais que:*

*(I) Se* $a, b \in P$, *então* $a + b, ab \in P$;

*(II)* $F = P \bigcup -P \bigcup \{0\}$ *onde $P$ e $-P$ são chamados de conjunto dos números positivos e negativos, respectivamente.*

**Observação 4.2.1** $-P = \{-a | a \in P\}$, *isto é,* $x \in P$ *se, e somente se,* $-x \in -P$.

**Observação 4.2.2** *A primeira condição diz que a soma e o produto de números positivos são positivos; a segunda diz que o corpo $F$ é a união dos conjuntos disjuntos $P, -P$ e $\{0\}$. Em outras palavras,$a \in F$ se, e somente se, $a = 0$ ou $a \in P$ ou $-a \in P$.*

**Observação 4.2.3** *Num corpo ordenado $F$, dizemos que $a < b$ ($a$ é menor do que $b$) se $b - a \in P$ e que $a \leq b$ se $b - a \in P \bigcup \{0\}$ ou, equivalentemente, $b - a \in P$ ou $a = b$.*

**Observação 4.2.4** *Podemos concluir pela Observação 4.2.3, que $a \in P$ se, e somente se, $a > 0$, e que $a \in -P$ se, e somente se, $a < 0$.*

**Propriedade 4.2.1** *Tendo em mente a Definição 4.2 e suas observações,vemos que um corpo ordenado $F$ possui as seguintes propriedades:*

*(a) Se $a < b$ e $b < c$, então $a < c$.*

*(b) Dados $a, b \in F$. Ocorre exatamente umas das alternativas: $a = b$, ou $a < b$, ou $a > b$.*

*(c) Se $a < b$, então $a + c < b + c$ para todo $c \in F$.*

*(d) Se $a < b$ e $c > 0$, então $ac < bc$; e se $c < 0$, então $ac > bc$.*

*(e) Se $a \neq 0$,então $a^2 \in P$.*

*(f) Se $a^2 = b^2$, então $a = b$ ou $a = -b$.*

**Demonstração:**

(a) Se $a < b$ e $b < c$, vemos, pela Observação 4.2.3, que $b - a \in P$ e que $c - b \in P$. Disso resulta da Definição 4.2 (I) que $(b - a) + (c - b) = b + (-a) + c + (-b) = c - a \in P$. Portanto, temos que $a < c$.

(b) Se $a, b \in F$,
então $b - a \in F$, pois $F$ é um corpo. Então,da Definição 4.2 (II), temos $b - a \in P$, ou $-(b - a) \in P$, ou $b - a \in \{0\}$. Portanto, de uma forma equivalente temos que $b > a$ ou $a > b$ ou $a = b$.

(c) Se $a < b$, vemos, pela Observação 4.2.3, que $b - a \in P$ o que implica $(b + c) - (a + c) = b - a \in P$. Logo, temos imediatamente que $a + c < b + c$.

(d) Se $a < b$ e $c > 0$, então segue-se que $b - a, c \in P$. Usando a Definição 4.2 (I), temos que $(b - a)c \in P$, ou seja, $bc - ac \in P$ e, portanto, $ac < bc$. Agora, se $c < 0$ vemos que $-c \in P$. Assim, temos que $(b - a)(-c) \in P$ o que implica em $ac - bc = -bc + ac = (b - a)(-c) \in P$ e, portanto, $ac > bc$.

(e) Se $a \neq 0$, então $a > 0$ ou $a < 0$. Supondo $a > 0$, temos $a \in P$. Logo, $a^2 = a \cdot a \in P$, isto é, $a^2 \in P$. Agora, supondo que $a < 0$, temos $-a \in P$. Disso resulta, que $a^2 = (-a)(-a) \in P$, ou seja, $a^2 \in P$.

(f) Com efeito, se $a^2 = b^2$, então $a^2 - b^2 = (a-b)(a+b) = 0$ o que implica em $a - b = 0$ ou $a + b = 0$. Assim, vemos que $a = b$ ou $a = -b$.

■

**Observação 4.2.5** *Esses fatos reforçam que o corpo $\mathbb{R}$ dos números reais é ordenado. Vamos mostrar que existe um subcorpo ordenado de $F$ que contém $\mathbb{Q}$. Considere o conjunto*

$$Q(t) = \left\{ \frac{p(t)}{q(t)} | p(t), q(t) \quad \textit{são polinômios de coeficientes racionais, com } q(t) \neq 0 \right\}.$$

*É fácil verificar que, $Q(t)$ é um corpo; agora, se definirmos que um elemento de $Q(t)$ é positivo, quando no produto $p(t)q(t)$, o coeficiente do termo de maior grau for positivo ( caso contrário, o elemento de $Q(t)$ é negativo) podemos provar que $Q(t)$ é um corpo ordenado. Com efeito, sejam $\frac{p(t)}{q(t)}, \frac{u(t)}{v(t)} \in P$, e os respectivos coeficientes dos termos de maior grau de cada polinômio $p(t)q(t)$ e $u(t)v(t)$ são tais que $pq > 0$ e $uv > 0$. Então, vemos que $\frac{p(t)}{q(t)} + \frac{u(t)}{v(t)} = \frac{p(t)v(t)+u(t)q(t)}{q(t)v(t)}$ . Assim, temos que o coeficiente do termo de maior grau de $p(t)q(t)[v(t)]^2 + u(t)v(t)[q(t)]^2$ pode ser $pqv^2$ ou $uvq^2$,ou ainda, $pqv^2 + uvq^2$. Vemos que qualquer um desses termos é positivo. Logo, temos $\frac{p(t)}{q(t)} + \frac{u(t)}{v(t)} \in P$. Agora, se $\frac{p(t)}{q(t)}, \frac{u(t)}{v(t)} \in P$, segue-se que $\frac{p(t)}{q(t)} \cdot \frac{u(t)}{v(t)}$ o coeficiente do termo de maior grau de $p(t)q(t)u(t)v(t)$ é $pquv = (pq)(uv) > 0$. Portanto, temos $\frac{p(t)}{q(t)} \cdot \frac{u(t)}{v(t)} \in P$. Note que o coeficiente do termo de maior grau, $pq \in \mathbb{Q}$ de $\frac{p(t)}{q(t)}$ pode ser $pq > 0$ ou $pq = 0$ ou $pq < 0$. Ocorrendo $pq > 0$, temos $\frac{p(t)}{q(t)} \in P$; ocorrendo $pq < 0$, temos $(-p)q > 0$ o que implica em $-\frac{p(t)}{q(t)} \in P$; se ocorrer $pq = 0$,temos $q \neq 0$, pois, $q(t)$ é um polinômio não-nulo e, portanto, $p = 0$. Como $p$ é o coeficiente do termo de maior grau de $p(t)$, segue-se que $p(t) \in 0$. Portanto, $\frac{p(t)}{q(t)} = 0$. Agora, note que se $p(t)$ e $q(t)$ são polinômio constantes, então $\frac{p(t)}{q(t)} = \frac{p}{q} \in \mathbb{Q}(t)$. Disso concluímos que, $\mathbb{Q} \in \mathbb{Q}(t)$. Portanto, inferimos que $\mathbb{Q}(t)$ é um subcorpo ordenado de $F$ que contém $\mathbb{Q}$.*

**Observação 4.2.6** *Outra questão que se levanta, é saber qual é o menor subcorpo de $F$ que contém $\mathbb{Q}$ . Essa indagação pode ser respondida olhando-se para o corpo $F$. Todo corpo $F$ contém pelo menos dois elementos $0'$ e $1'$, e que em todo corpo ordenado $F$ temos que $0' < 1'$ do qual se segue a sucessão $0' < 1' < 1' + 1' < 1' + 1' + 1' < \cdots < 1' + 1' + 1' + \cdots$ em que definimos $2' = 1' + 1', 3' = 1' + 1' + 1'$, e assim por diante. O subconjunto $\mathbb{N}' \subset F$ formado por esses elementos é, portanto,*

***infinito*** [1] *e a identificamos com* $\mathbb{N}$ *(conjunto da forma que conhecemos) através do isomorfismo a seguir: Seja* $f : \mathbb{N} \to \mathbb{N}', \mathbb{N}' \subset F$ *definida por* $f(n) = n'$ [2]*. É fácil ver, que temos* $f(n+m) = f(n) + f(m)$ *e que* $f(nm) = f(n)f(m)$*. Além disso,* $f$ *é bijetiva, pois, evidentemente,* $f$ *é sobrejetiva pela definição de* $f$*, e que* $f$ *é injetiva, pois, vemos que de* $m < n$ *implica* $f(m) < f(n)$*, pois, os valores de* $f$ *são positivos. Assim, podemos considerar* $\mathbb{N} \subset F$*. Agora, como* $\mathbb{N}'$ *é um subconjunto de números positivos de* $P$*, então* $-n'$ *é um elemento de um subconjunto de números negativos do corpo ordenado* $F$*, chamando de* $-\mathbb{N}'$ *esse subconjunto, e definindo* $-2' = (-1') + (-1'), -3' = (-1') + (-1') + (-1')$*, e etc, para cada elemento* $-n' - \mathbb{N}'$*, vemos que* $\cdots < -3' < -2' < -1' < 0'$*, pois,* $\cdots < (-1') + (-1') + (-1') < (-1') + (-1') < -1' < 0'$ *. Disso resulta que,* $-\mathbb{N}'$ *é infinito. Reunindo todos esses elementos, incluindo o zero* $(0')$ *teremos o subconjunto* $\mathbb{Z}' = \mathbb{N}' \bigcup -\mathbb{N}' \bigcup \{0'\} \subset F$ *que identificamos com* $\mathbb{Z}$ *(conjunto da forma que conhecemos) através do isomorfismo a seguir : Seja* $f : \mathbb{Z} \to \mathbb{Z}', \mathbb{Z}' \subset F$*, definida por* $f(n) = n'$ *para todo* $n \in \mathbb{Z}$*. Vê-se, facilmente, que* $f$ *é um isomorfismo. Portanto, podemos fazer* $\mathbb{Z} \subset F$*. Definindo* $\mathbb{Q}' = \{m' \cdot n'^{-1} | m', n' \in \mathbb{Z}', n' \neq 0\}$ *verificamos, facilmente, que é um subcorpo de* $F$ *e que* $\mathbb{Z}' \subset \mathbb{Q}'$*, portanto,* $\mathbb{Z}' \subset \mathbb{Q}' \subset F$*. Verificamos imediatamente, que podemos identificar* $\mathbb{Q}'$ *com* $\mathbb{Q}$ *(conjunto da forma que conhecemos) através do isomorfismo* $f : \mathbb{Q} \to \mathbb{Q}'$ *definido por* $f\left(\frac{m}{n}\right) = m'n'^{-1}$*.Trata-se, do menor subcorpo de* $F$*, pois, todo subcorpo deve conter pelo menos* $0'$ *e* $1'$*; por adições sucessivas de* $1'$ *, todo subcorpo de* $F$ *deve conter* $\mathbb{N}'$*; por tomadas de simétricos, dever conter,* $\mathbb{Z}'$ *e, por divisões em* $\mathbb{Z}'$*, deve conter o conjunto* $\mathbb{Q}'$ *das frações* $m'n'^{-1} = \frac{m'}{n'}$*, com* $m', n' \in \mathbb{Z}', n' \neq 0'$*. Dessa forma, podemos considerar que* $\mathbb{N}' \subset \mathbb{Z}' \subset \mathbb{Q}' \subset F$*, ou por isomorfismo,* $\mathbb{N} \subset \mathbb{Z} \subset \mathbb{Q} \subset F$*.*

## 4.1 Intervalos

Vimos anteriormente, que um dado subconjunto de um corpo pode caracterizá-lo como ordenado devido as propriedades que eles mesmos guardam. Em um corpo ordenado F existe, particularmente, um subconjunto não menos importante que, também, possuem propriedades interessantes para análise matemática. Esses subconjuntos, de um dado corpo ordenado, são chamados de intervalos; se o corpo ordenado for o conjunto dos números reais, e fizermos uma correspondência geométrica com os pontos da reta, esses intervalos são "pedaços" da reta, ou até mesmo, a reta inteira, se tomarmos todos os números reais. Existem vários tipos de intervalos, a serem definidos a seguir.

[1] O termo **infinito**, neste texto, é usado de forma intuitiva, e por isso, vamos dispensar uma definição precisa.

[2] Estamos afirmando, de um modo intuitivo, que a função $f$ da forma que definimos, existe. No entanto, existe um teorema que anunciaremos, mais adiante, que garante a existência dessa função. Ele é conhecido como teorema da definição por recursão.

**Definição 4.3** *Seja $a, b \in F$ de um corpo ordenado tais que $a < b$.Definimos os seguintes intervalos:*

1. *Um intervalo aberto é o subconjunto de $F$ da forma $(a, b) = \{x \in F | a < x < b\}$;*
2. *Um intervalo fechado é o subconjunto de $F$ da forma $[a, b] = \{x \in F | a \leq x \leq b\}$;*
3. *Um intervalo semiaberto à direita ( à esquerda) é o subconjunto de $F$ da forma $[a, b) = \{x \in F | a \leq x < b\}((a, b] = \{x \in F | a < x \leq b\})$ . Podemos dizer, também, que o intervalo $[a, b)((a, b])$ é semifechado à esquerda ( semifechado à direita);*
4. *Um intervalo semiaberto ilimitado à direita (à esquerda) é o subconjunto de $F$ da forma $(a, +\infty) = \{x \in F | x > a\}((-\infty, a) = \{x \in F | a < x\})$;*
5. *Um intervalo semifechado ilimitado à direita ( à esquerda) é o subconjunto de $F$ da forma $[a, +\infty) = \{x \in F | x \geq a\}$ $((-\infty, a] = \{x \in F | a \leq x\}))$.*
6. *Um intervalo aberto ou fechado é o corpo $F$ inteiro da forma $F = (-\infty, +\infty)$.*

**Observação 4.3.1** *Quando considerarmos um intervalo de extremos $a$ e $b$, suporemos sempre $a < b$, exceto se o intervalo for da forma $[a, b]$, pois, podemos ter $a = b$. Esse é caso do intervalo degenerado $[a, a] = \{a\}$.*

**Observação 4.3.2** *Todo intervalo não-degenerado é um conjunto infinito.*

**Propriedade 4.3.1** *Seja $I \subseteq F$ um intervalo.*

*(I) Se $x, y \in I$ e $x \leq y$, então $[x, y] \subseteq I$.*

*(II) Se $I$ é um intervalo aberto, e se $x \in I$, então existe um $\delta > 0$ tal que $[x - \delta, x + \delta] \subseteq I$.*

**Demonstração:**

(I) Sendo $I$ um intervalo, teremos que considerar 9 casos; no entanto, porém vamos considerar alguns casos, já que eles servem como argumentos análogos aos casos não demonstrados. Primeiro, suponha o intervalo fechado $I$ de extremos $a$ e $b$, com $a < b$ ( os casos de intervalos semiabertos, semifechados à esquerda e à direita possuem argumentos similares). Seja $z \in [x, y]$. Então, por definição de intervalos temos que $x \leq z \leq y$. Disso, e usando a hipótese vemos que $a \leq x \leq z \leq y \leq b$. Assim, temos $a \leq z \leq b$, ou seja, $z \in I$. Portanto, temos $[x, y] \subseteq I$.

Segundo, suponha que $I$ seja um intervalo semifechado ilimitado à direita de extremo finito $a$, isto é, $I = [a, +\infty)$ (os casos de intervalos semifechados ilimitado à esquerda e semiaberto ilimitados à esquerda e à direita possuem argumentos similares). Seja $z \in [x, y]$. Disso, e usando a hipótese vemos que $a \leq x \leq z \leq y$. Assim, temos que $a \leq z$,ou seja, $z \in I$. Portanto, temos $[x, y] \subseteq I$.

(II) Vamos considerar apenas dois casos de intervalos abertos, pois, os demais possuem raciocínio semelhante. Primeiro, suponha que $I$ seja um intervalo aberto de extremos $a$ e $b$. Pela hipótese, se $x \in I$, então $a < x < b$. Seja $\epsilon = \min\{x - a, b - x\}$. Tomando um $\delta = \frac{\epsilon}{2}$, supondo que $\epsilon = x - a$, e notando que $\delta < \epsilon \leq b - x$, vemos que $a < x - \delta < x + \delta < b$. Assim, temos $x - \delta, x + \delta \in I$. Então, pela parte (I) desta propriedade inferimos que $[x - \delta, x + \delta] \subseteq I$. Segundo, suponha $I$ um intervalo semiaberto ilimitado à direita de extremo finito $a$. Então, pela hipótese, se $x \in I$ temos $a < x$. Seja $\epsilon = x - a > 0$. Tomando um $\delta = \frac{\epsilon}{2}$, notando que $\delta < \epsilon$ e que $x - \delta < x + \delta$ vemos que $a < x - \delta < x + \delta$. Assim, temos $x - \delta, x + \delta \in I$. Portanto, pela parte (I) temos que $[x - \delta, x + \delta] \in I$.

■

Vamos definir o conceito de módulo de um número num corpo ordenado F , muito útil em análise.

**Definição 4.4** *Dado $x \in F$ de um corpo ordenado. Definimos módulo de $x$, denotado por $|x|$,o número tal que*

$$|x| = \max\{x, -x\}.$$

**Propriedade 4.4.1** *Dado que $x \in F$,então $|x|$ possui as seguintes características:*

$$|x| = \begin{cases} x & ,se \quad x > 0 \\ 0 & ,se \quad x = 0 \\ -x & ,se \quad x < 0 \end{cases}$$

**Demonstração:** Dado que $x \in F$ vemos, pela definição (II) de um corpo ordenado $F$, que $x \in P$,ou $-x \in P$, ou $x = 0$. Se $x \in P$ segue-se imediatamente, que $-x \in -P$ . Pela observação 4.2.4 vemos que $x > 0$ e $-x < 0$, ou seja, $-x < x$. Portanto, se $x > 0$ temos $|x| = \max\{x, -x\} = x$. Agora, se $-x \in P$ temos $-x > 0$, ou seja, $x < 0$. Assim, vemos que $x < -x$. Portanto, se $x < 0$ temos $|x| = \max\{x, -x\} = -x$. Sabemos que num corpo $-0 = 0$. Disso resulta que, se $x = 0$, então $|0| = \max\{0, -0\} = \max\{0, 0\} = 0$. Reunindo os três casos, inferimos as características. ■

**Propriedade 4.4.2** *Sejam quaisquer $a, b \in F$. Então são válidas as seguintes situações:*

1. $|a| \geq 0$ *e* $|a| = 0$ *se e somente se* $a = 0$.
2. $-|a| \leq a \leq |a|$.
3. $|a| = |b|$ *se e somente se* $a = b$ *ou* $a = -b$.
4. $|a| < b$ *se e somente* $-b < a < b$, *e* $|a| \leq b$ *se e somente se* $-b \leq a \leq b$.
5. $|a|^2 = a^2$.
6. $|ab| = |a||b|$.
7. $|a + b| \leq |a| + |b|$.*(desigualdade triangular)*
8. $|a| - |b| \leq |a + b|$ *e* $|a| - |b| \leq |a - b|$.
9. $|a| - |b| \leq |(|a| - |b|)| \leq |a - b|$
10. $a \leq 0$ *se e somente se* $a < \epsilon$ *para todo* $\epsilon > 0$.
11. $a \geq 0$ *se e somente se* $a > -\epsilon$ *para todo* $\epsilon > 0$.
12. $a = 0$ *se e somente se* $|a| < \epsilon$ *para todo* $\epsilon > 0$.

**Demonstração:**

1. Pela propriedade 4.4.1 segue-se que $|a| \geq 0$. Veja que se $a = 0$, então pela propriedade 4.4.1 temos $|a| = 0$. Se $a \neq 0$ implica em $|a| > 0$ o que é um absurdo. Portanto, temos $|a| = 0$ se e somente se $a = 0$.

2. Pela definição de módulo, vemos que $|a| \geq a$ e $|a| \geq -a$. Dessa última desigualdade, resulta $-|a| \leq a$. Portanto, temos $-|a| \leq a \leq |a|$.

3. Temos cinco casos, pois, não ocorre os casos $a = 0$ e $b > 0$, e $a > 0$ e $b = 0$. Primeiro, suponha $a > 0, b > 0$. Então pela propriedade 4.3.1 temos $a = |a| = |b| = b$, ou seja, $a = b$. Segundo, se $a = 0$ e $b = 0$ temos, imediatamente, $a = b$. Terceiro, suponha $a > 0$ e $b < 0$. Disso resulta pela definição que $a = |a| = |b| = -b$. Portanto, temos $a = -b$. O quarto ($a < 0$ e $b > 0$) é semelhante ao terceiro. Quinto, suponha $a < 0$ e $b < 0$. Disso resulta, pela definição de módulo que, $-a = |a| = |b| = -b$, ou seja, $-a = -b$ e, portanto, $a = b$. Logo, temos em qualquer caso $a = b$ ou $a = -b$.

4. Suponha $|a| < b$. Assim, $|a| < b$ se e somente se $a \leq |a| < b$ e $-a \leq |a| < b$, ou seja, $a < b$ e $-a < b$. Da última desigualdade, tiramos $a > -b$. Portanto, temos que $-b < a < b$. Agora, suponha a condição $-b < a < b$, ela implica em $b > 0$. Se $a = 0$, vemos que $|a| = 0 < b$, ou seja, $|a| < b$. Se $a > 0$, então $|a| = a < b$, ou seja, $|a| < b$. Se $a < 0$, então $-a > 0$, e portanto de $-b < a$ tiramos $b > -a = |a|$, isto é, $|a| < b$. Logo, temos $|a| < b$ se e somente se $-b < a < b$. Suponha $|a| = b$. Então, temos $a \leq |a| = b$ e $-a \leq |a| = b$. Dessa última desigualdade, tiramos $-a \leq b$, ou seja, $a \geq -b$. Portanto, temos $-b \leq a \leq b$. Agora, suponha $-b \leq a \leq b$. Temos três casos. Se $-b = a < b$, vemos que $b > 0$ e, portanto, $|a| = |-b| = b$, ou seja, $|a| = b$. Suponha que $-b < a = b$. Note que, $b > 0$. Portanto, $|a| = |b| = b$, ou seja, $|a| = b$. Suponha que $-b = a = b$. Segue-se imediatamente, $b = 0$ e $a = 0$, isto é, $a = b = 0$ implica em $|a| = b$. Logo, em qualquer um dos casos temos que $|a| = b$ se e somente se $-b \leq a \leq b$.

5. Se $a > 0$, então $|a|^2 = |a||a| = a \cdot a = a^2$; se $x < 0$, então $|a|^2 = |a||a| = (-a)(-a) = a^2$; agora, se $a = 0$, teremos $|0|^2 = |0||0| = 0.0 = 0 = 0^2$, ou seja, $|0|^2 = 0^2$. Portanto, em qualquer caso temos $|a|^2 = a^2$.

6. Usando a propriedade 4.4.2 (5) e a lei comutativa multiplicativa, temos sucessivamente

$$|ab|^2 = (ab)^2 = (ab)(ab) = a^2b^2 = |a|^2|b|^2 = (|a||b|)(|a||b|) = (|a||b|)^2,$$

isto é, $|ab|^2 = (|a||b|)^2$. Disso resulta, pela propriedade 4.2.1 (f), que $|ab| = |a||b|$ ou $|ab| = -|a||b|$. Na segunda igualdade, tiramos $|ab| + |a||b| = 0$. Como $|ab| \geq 0$ e $|a||b| \geq 0$, resulta do corolário 3.2.1 (VI) que $|ab| = |a||b| = 0$ e, portanto, $|a| = 0$ ou $|b| = 0$, isso implica que podemos ter $a = 0$ ou $b = 0$. Portanto, em qualquer um desses casos vemos que $|ab| = |a||b|$.

7. Se $a = b = 0$, então vale a igualdade $|a + b| = |a| + |b|$. Portanto, $|a + b| \leq |a| + |b|$. Suponha que $a \neq 0$ ou $b \neq 0$. Usando a lei distributiva e comutativa, junto com as partes (2) e (5) desta propriedade, vemos que

$$|a + b|^2 = (a + b)^2 = (a + b)(a + b) = a^2 + 2ab + b^2$$

$$= |a|^2 + 2ab + |b|^2 \leq |a|^2 + 2|ab| + |b|^2 = (|a| + |b|)^2.$$

Assim, temos $|a + b|^2 \leq (|a| + |b|)^2$. Como |a+b|>0 e |a+b|>0, pois, $a \neq 0$ ou $b \neq 0$. Resulta, pelo corolário 3.2.1 (VII), que $|a + b| \leq |a| + |b|$.

8. Note que, $|a| = |a + b + (-b)| \leq |a + b| + |-b| = |a + b| + |b|$, ou seja, $|a| \leq |a+b|+|b|$, e portanto, $|a|-|b| \leq |a+b|$. Agora, veja que $|a| = |a-b+b| \leq |a - b| + |b|$, ou seja, $|a| \leq |a - b| + |b|$, e portanto, $|a| - |b| \leq |a - b|$.

9. Vamos dividir a demonstração em duas partes:

   Primeira, sabemos, pela parte (2), que $x - y \leq |x - y|, \forall x, y \in F$. Fazendo $x = |a|$ e $y = |b|$ vemos que $|a| - |b| \leq |(|a| - |b|)|$.

   Segunda, agora, veja que se $a = b = 0$, então temos a igualdade $|(|a| - |b|)| = |a - b|$, ou seja, $|(|a| - |b|)| \leq |a - b|$. Suponha $a \neq 0$ ou $b \neq 0$. Então, $|(|a| - |b|)| > 0$ e $|a - b| > 0$. Segue-se que $|(|a| - |b|)|^2 = (|a| - |b|)^2 = |a|^2 - 2|a||b| + |b|^2 \leq |a|^2 - 2ab + |b|^2 = a^2 + 2ab + b^2 = (a - b)^2 = |a - b|^2$. Assim, temos $|(|a| - |b|)|^2 \leq |a - b|^2$. Disso resulta, pelo corolário 3.2.1 (VII), que $|(|a| - |b|)| \leq |a - b|$. Portanto, juntando a primeira e a segunda parte, temos $|a| - |b| \leq |(|a| - |b|)| \leq |a - b|$.

10. Com efeito, suponha $a \leq 0$.Então tomando qualquer $\epsilon > 0$ vemos que $a \leq 0 < \epsilon$, ou seja, $a < \epsilon$ para todo $\epsilon > 0$. Agora, suponha que $a < \epsilon$ para todo $\epsilon > 0$. Devemos provar que com essa hipótese, teremos necessariamente $a \leq 0$. Suponha o contrário, $a > 0$. Tomando $\epsilon = \frac{a}{2}$, verificamos que existe um $\epsilon > 0$ tal que $\epsilon < a$, o que é um absurdo. Assim, devemos ter $a \leq 0$. Portanto, provamos $a \leq 0$ se somente se $a < \epsilon$ para todo $\epsilon > 0$.

11. Com efeito, se $a \geq 0$ então para todo $\epsilon > 0$ temos $-\epsilon < 0 \leq a$,ou seja, $-\epsilon < a$, para todo $\epsilon > 0$. Suponha, agora, que $a > -\epsilon$, para todo $\epsilon > 0$. Devemos provar que com essa hipótese, teremos necessariamente $a \geq 0$. Suponha o contrário, $a < 0$. Tomando $\epsilon = -\frac{a}{2}$, vemos que existe um $\epsilon > 0$ tal que $a < \frac{a}{2} = -\epsilon$, ou seja, $a < -\epsilon$, o que é um absurdo. Assim, devemos ter $a \geq 0$. Portanto, provamos $a \geq 0$ se e somente se $a > -\epsilon$ para todo $\epsilon > 0$.

12. É óbvio que se $a = 0$ então $|a| = 0 < \epsilon$, para qualquer $\epsilon > 0$. Agora, pela parte (4), veja que $|a| < \epsilon, \forall \epsilon > 0$ se e somente se $-\epsilon < a < \epsilon, \forall \epsilon > 0$. Ora, se $a > -\epsilon, \forall \epsilon > 0$, então, pela parte (11), concluímos que $a \geq 0$. No entanto, se $a < \epsilon, \forall \epsilon > 0$, então,pela parte (10), concluímos $a \leq 0$. Assim, temos $a \geq 0$ e $a \leq 0$, portanto,segue-se pelo teorema 3.2 (I),que $a = 0$.

■

# Capítulo 5

# Corpo Ordenado Completo

Neste capítulo, apresentaremos uma propriedade fundamental que alguns corpos ordenados possuem. Essa propriedade, é caracterizada pela existência de um conceito chamado de supremo, o qual permite dizer se um dado corpo ordenado é ou não completo. Em outras palavras, um corpo ordenado é completo se, o tal corpo ordenado, inclui outros números, além dos números racionais. Para chegarmos a essa conclusão iremos definir os conceitos de supremo e de ínfimo. A definição a seguir, permite mostrar que o conjunto dos números racionais $\mathbb{Q}$ não é completo. Isso acontece, devido a inexistência de supremo em $\mathbb{Q}$.

**Definição 5.1** *Seja $X \subseteq F$ um subconjunto de um corpo ordenado. Dizemos que $X$ é limitado superiormente, se existe um $a \in F$ tal que $x \leq a, \forall x \in X$. O elemento $a$ é chamado de cota superior.*

**Definição 5.2** *Seja $X \subseteq F$ um subconjunto de um corpo ordenado. Dizemos que $a \in F$ é o supremo de $X$ em $F$, denotado por $\sup X$, se $a$ é uma cota superior que possui a seguinte propriedade: Dado $b \in F$, se $b < a$, então existe um $x \in X$ tal que $b < x < a$, ou equivalentemente: Dado $b \in F$, se $x \leq b, \forall x \in X$, então $a \leq b$. Neste caso, dizemos que o conjunto $X$ possui supremo em $F$, ou seja , $\sup X \in F$.*

**Definição 5.3** *Seja $X \subseteq F$ um subconjunto de um corpo ordenado. Dizemos que $X$ é limitado inferiormente, se existe um $a \in F$ tal que $a \leq x, \forall x \in X$. O elemento $a$ é chamado de cota inferior.*

**Definição 5.4** *Seja $X \in F$ um subconjunto de um corpo ordenado. Dizemos que $a \in F$ é o ínfimo de $X$ em $F$, denotado por $\inf X$, se $a$ é uma cota inferior que possui a seguinte propriedade: Dado $b \in F$, se $a < b$, então existe um $x \in X$ tal que $a < x < b$, ou equivalentemente: Dado $b \in F$,se $x \leq b, \forall x \in X$, então $a \leq b$. Neste caso, dizemos que o conjunto $X$ possui ínfimo em $F$, ou seja, $\inf X \in F$.*

**Definição 5.5** *Um conjunto $X \subseteq F$ é limitado, quando existem as cotas inferior e superior.*

**Observação 5.1** *A definição 5.2 quer dizer que não existe cota superior menor que o supremo, isto é, o supremo é a menor das cotas superiores. Agora, um conjunto $X \subseteq F$* ***não possui supremo em*** $\mathbf{F}$ *significa dizer que $X$ não possui cota superior ou que para cada cota superior $a \in F$ existe um $b \in F$ tal que para $b < a, x \leq b, \forall x \in X$.*

**Observação 5.2** *A definição 5.4 quer dizer que não existe cota inferior menor que o ínfimo, isto é, o ínfimo é a maior das cotas inferiores. Agora, um conjunto $X \subseteq F$* ***não possui ínfimo em*** $\mathbf{F}$ *significa dizer que $X$ não possui cota inferior ou que para cada cota inferior $a \in F$ existe um $b \in F$ tal que para $a < b, b \leq x, \forall x \in X$.*

**Observação 5.3** *Se o conjunto $X \subseteq F$ for vazio, então todo $a \in F$ é cota superior e inferior de $X$ , ou seja, $X$ não possui supremo e nem ínfimo em $F$.*

**Observação 5.4** *Note que* $\sup X \in X$*, se e somente se,* $\sup X$ *é o máximo de $X$, e que* $\inf X \in X$*, se somente se, $infX$ é o mínimo de $X$.*

O que é interessante notar, nas observações 5.1 e 5.3, que determinados subconjuntos $X \subseteq F$, pode não possuir supremo (ínfimo) em $F$, embora tenham cota superior (cota inferior). Agora, temos condições de definir o conceito de corpo ordenado completo.

**Definição 5.6** *Dizemos que um corpo ordenado $F$ é completo se todo subconjunto,não-vazio $X \subseteq F$, limitado superiormente, possui supremo. Agora, vamos enunciar o axioma da Completude.*

**Axioma 5.1** *Existe um corpo ordenado completo, $\Re$, chamado conjunto dos números reais.*

**Observação 5.1.1** *$\Re$ é um corpo ordenado, então devemos ter $\mathbb{N} \subseteq \mathbb{Z} \subseteq \mathbb{Q} \subseteq \Re$.*

**Observação 5.1.2** *O axioma acima, embora declare a existência dos números reais, contudo, não afirma que ele é único.*

**Lema 5.1** *Sejam os conjunto $X, Y \in F$, não-vazios, de um corpo ordenado completo $F$. Definimos os seguintes conjuntos:*

$$-X = \{-x | x \in X\}, X + Y = \{x + y | x \in X, y \in Y\} \quad e \quad XY = \{xy | x \in X, y \in Y\}.$$

*São válidas as seguintes afirmações:*

1. *Se $X$ é limitado superiormente(inferiormente), então o supremo (ínfimo) existe e é único.*

2. *$X$ admite supremo se e somente se $-X$ possui ínfimo e são tais que* $\inf(-X) = -\sup X$.

3. *Se $X$ possui supremo,então para todo $\epsilon > 0$, existe um $x \in X$ tal que* $\sup X - \epsilon < x < \sup X$.

4. *Se $X$ possui ínfimo,então para todo $\epsilon > 0$, existe um $x \in X$ tal que* $\inf X < x < \inf X + \epsilon$.

5. *Sejam $X, Y \in F$ conjuntos não-vazios ,limitados superiormente que possuem supremo. Se $X + Y = \{x + y | x \in X, y \in Y\}$, então $X + Y$, definido acima, é limitado superiormente,e vale a relação* $\sup(X + Y) = \sup X + \sup Y$.

6. *Se $X, Y$ são subconjuntos de números positivos de $F$, limitados superiormente. Então $XY$, definido acima, é limitado superiormente,e portanto,vale a relação* $\sup(XY) = \sup X \sup Y$.

7. *Dados dois conjuntos $X$ e $Y$ tais que $X \subseteq Y$. Se $Y$ é limitada superiormente, então* $\sup X \leq \sup Y$.

**Demonstração:**

1. Como $X$ é limitado superiormente, então pelo axioma acima, $X$ possui supremo. Suponha que o conjunto $X \subseteq F$ admita dois supremos $a$ e $b$. Pela definição sobre supremo vemos que $x \leq a, \forall x \in X$, e que $x \leq b, \forall x \in X$. Ora, $b$ é cota superior de $X$, logo $a \leq b$. Da mesma forma, $a$ é também cota superior de $X$, logo $b \leq a$. Usando o teorema 2.3 (I), temos, portanto, que $a = b$.

2. Veja que $X$ admite supremo se e somente se $x \leq \sup X \leq b, \forall x \in X$ e qualquer cota superior $b$ de $X$, se e somente se $-b \leq -\sup X \leq -x, \forall(-x) \in -X$ e qualquer cota inferior-b de $-X$, isto é, $\inf(-X) = -\sup X$.

3. Para cada $b < \sup X$ façamos corresponder um $\epsilon = \sup X - b > 0$. Então pela definição de Supremo resulta que, existe um $x \in X$ tal que $b < x < \sup X$ para todo $b < \sup X$, ou equivalentemente, existe um $x \in X$ tal que $\sup X - \epsilon < x < \sup X$ para todo $\epsilon > 0$.

4. Para cada $b > \inf X$ façamos corresponder um $\epsilon = b - \inf X > 0$. Então usando a definição de Ínfimo resulta que, existe um $x \in X$ tal que $\inf X < x < b$ para todo $b > \inf X$, ou equivalentemente, existe um $x \in X$ tal que $\inf X < x < \inf X + \epsilon$ para todo $\epsilon > 0$.

5. Como $X$ e $Y$ são limitados superiormente, então $X$ e $Y$ possuem supremo, e portanto, $x \leq \sup X, \forall x \in X$, e que $y \leq \sup Y, \forall y \in Y$. Disso resulta que, $x + y \leq \sup X + \sup Y$, para todo $x \in X$ e $y \in Y$, ou seja, $\sup X + \sup Y$ é uma cota superior de $X+Y$. Como $X$ e $Y$ são não-vazios, segue-se que $X+Y$ é não-vazio, e portanto possui supremo. Assim, temos que $\sup(X + Y) \leq \sup X + \sup Y$. Suponha que $\sup(X + Y) < \sup X + \sup Y$. Tomando um $\epsilon = \sup X + \sup Y - \sup(X + Y) > 0$, vemos que, por (3), que existem $x \in X, y \in Y$ tais que $\sup X - \frac{\epsilon}{2} < x$ e $\sup Y - \frac{\epsilon}{2} < y$, o que implica em $\sup X + \sup Y - \epsilon < x + y$, isto é, $\sup(X + Y) < x + y$, o que é uma contradição. Portanto, devemos ter $\sup(X + Y) = \sup X + \sup Y$.

6. Como $X$ e $Y$ são subconjuntos de números positivos,temos que $x > 0$ e $y > 0$. Além disso, $X$ e $Y$ são limitados superiormente, e portanto, admitem supremo. Assim, $0 < x \leq \sup X$ e que $0 < y \leq \sup Y$ para todo $x \in X$ e $y \in Y$.Disso resulta que, $xy < \sup X \sup Y$, para todo $x \in X$ e $y \in Y$, o que implica dizer que $\sup X \sup Y$ é uma cota superior de $XY$. Segue-se que $XY$ admite supremo. Assim, vemos que $0 < xy \leq \sup(XY) \leq \sup X \sup Y$, para todo $x \in X$ e $y \in Y$. Suponha que $\sup(XY) < \sup X \sup Y$. Tomando um $\epsilon = \sup X \sup Y - \sup X \sup Y > 0$, vemos que para todo $x \in X$ e $y \in Y$ temos $xy < \sup X \sup Y < \sup X \sup Y + 2\sup(XY) = \sup XY - \epsilon$, ou seja, $xy \leq \sup XY - \epsilon$, o que é uma contradição ao fato de que $\sup(XY)$ ser o supremo de $XY$. Portanto, devemos ter $\sup(XY) = \sup X \sup Y$.

7. Se Y é limitada superiormente,então $Y$ admite supremo. Assim, $y \leq \sup Y, \forall y \in Y$. Em particular, para todo $x \in X$ temos $x \leq \sup Y$ pois, $X \subseteq Y$. Isso mostra que, $\sup Y$ é uma cota superior para $X$. Disso resulta, que $X$ admite supremo, e portanto,temos $\sup X \leq \sup Y$.

■

Sabemos que o conjunto dos números naturais $\mathbb{N}$ é ilimitado superiormente e limitado inferiormente quando olhamos, propriamente, para o conjunto $\mathbb{N}$ e quando o olhamos como subconjunto de $\mathbb{Z}$; já o conjunto dos números inteiros $\mathbb{Z}$ é ilimitado superiormente e inferiormente, quando o olhamos propriamente. No entanto, quando o olhamos como subconjuntos de corpos ordenados isso pode não ser verdade. De

outra forma, podemos verificar que existem corpos ordenados $F$ que contêm $\mathbb{N}$ e $\mathbb{Z}$, onde, eles são ilimitados superiormente ( esse é o caso mais comum) em $F$; e que existem corpos ordenados $F$ que contêm $\mathbb{N}$ e $\mathbb{Z}$, onde, eles limitados superiormente em F. Antes de mostrá-los, vamos definir o conceito de conjunto ilimitado.

**Definição 5.7** *Seja $X \subseteq F$ ,onde $F$ é um corpo ordenado. $X$ é ilimitado superiormente em $F$, se para todo $a \in F$ existe $b \in X$ tal que $b > a$; $X$ é ilimitado inferiormente em $F$, se para todo $a \in F$ existe $b \in X$ tal que $b < a$.*

**Teorema 5.1** *O conjunto dos números naturais $\mathbb{N}$ é ilimitado superiormente no conjunto dos números racionais $\mathbb{Q}$.*

**Demonstração:** Seja $\frac{x}{y} \in \mathbb{Q}$. Então, temos $|x| + 1 \in \mathbb{N}$ e que $|x| + 1 > \frac{x}{y}, \forall x, y \in \mathbb{Z}, comy \neq 0$. ■

**Teorema 5.2** *O conjunto dos números naturais $\mathbb{N}$ é limitado superiormente no conjunto das frações racionais $\mathbb{Q}(t)$.*

**Demonstração:** Seja o corpo ordenado $\mathbb{Q}(t)$,cuja ordem foi introduzida no capítulo IV. Sabemos que $r(t) = t \in \mathbb{Q}(t)$ e $s(t) = t - n = \frac{t-n}{1} \in \mathbb{Q}(t)$ para todo $n \in \mathbb{N}$, e que o produto dos coeficientes dos polinômios de $s(t)$(numerador e denominador) é positivo. Assim, temos $t - n > 0$, ou seja, $t > n, \forall n \in \mathbb{N}$. Deduzimos que, $p(t)$ é cota superior de qualquer que seja $n \in \mathbb{N}$,e portanto $\mathbb{N}$ é limitado em $\mathbb{Q}(t)$. ■

**Teorema 5.3** *Num corpo ordenado $F$, as seguintes afirmações são equivalentes:*

*(I)* $\mathbb{N} \subseteq F$ *é ilimitado superiormente;*

*(II) Dados $a, b \in F$,com $a > 0$, existe $n \in \mathbb{N}$ tal que $na > b$;*

*(III) Dado qualquer $a > 0$ em $F$, existe $n \in \mathbb{N}$ tal que $0 < \frac{1}{n} < a$.*

**Demonstração:**

(I) implica em (II). Dados $a, b \in F$,vemos que sendo $F$ um corpo temos que $ba^{-1} = \frac{b}{a} \in F$, com $a > 0$. Se $\mathbb{N}$ é ilimitado em $F$, então existe um $n \in \mathbb{N}$ tal que $n > \frac{b}{a}$, isto é, $na > b$.

(II) implica em (III). Pela hipótese feita em (II), se tomarmos qualquer $a > 0$ e um $b = 1$, temos que existe um $n \in \mathbb{N}$ tal que $na > 1$, isto é, $0 < \frac{1}{n} < a$.

(III) implica (I). Se F é um corpo ordenado, então temos dois casos. Primeiro, se $a \leq 0$. Então vemos que $n > 0 \geq a, \forall n \in \mathbb{N}$, isto é, $n > a, \forall n \in \mathbb{N}$. Segundo, se $a > 0$ então $\frac{b1}{a} > 0$. Assim,pela hipótese, temos que existe um $n \in \mathbb{N}$ tal que $0 < \frac{1}{n} < \frac{1}{a}$, ou seja, $n > a$. Portanto, deduzimos, pelos dois casos, que $\mathbb{N}$ é ilimitado em $F$.

■

**Definição 5.8** *Um corpo ordenado $F$ é arquimediano se ocorrer qualquer umas das condições do teorema 5.3.*

**Observação 5.8.1** *O teorema 5.1 afirma que o corpo dos números racionais $\mathbb{Q}$ é arquimediano. No entanto, o teorema 5.2 afirma que o corpo ordenado $\mathbb{Q}(t)$ não é arquimediano. E mais, o axioma acima afirma que o conjunto dos números reais $\Re$ é arquimediano por ser um corpo ordenado completo. Esse atributo, garante, por si só, a segunda afirmação do teorema 5.3. As demais afirmações seguem-se, por equivalência. Vejamos isso no teorema a seguir.*

**Teorema 5.4** *Num corpo ordenado completo $F$ vale a propriedade: Se $a, b \in F$, com $a > 0$, então existe um $n \in \mathbb{N}$ tal que $b < na$.*

**Demonstração:** Primeiro suponha que $b \leq 0$. Seja $n = 1$. Então, vemos que $b \leq 0 < a = 1 \cdot a = na$. Segundo, suponha $b > 0$. Vamos usar a prova por contradição. Suponha que tenhamos $na \leq b$, para todo $n$ natural. Seja o conjunto $A = \{ka | k \in \mathbb{N}\}$. Note que $A \subseteq F$ e que $a = 1 \cdot a \in A$. Logo, vemos que $A \neq \emptyset$. Por hipótese, temos $ka \leq b, \forall k \in \mathbb{N}$. Assim, o conjunto A de um corpo ordenado completo $F$ é não-vazio e limitado superiormente, e portanto, admite supremo. Ora, se $m + 1 \in \mathbb{N}$, então $(m + 1)a \in A$, e portanto temos $(m + 1)a \leq \sup A$, ou seja, $ma \leq \sup A - a$, para $a > 0$. Esse resultado mostra uma contradição do fato de $\sup A$ ser supremo de $A$. Portanto, devemos ter $na > b$. ■
O teorema 5.4 mostra que todo corpo ordenado completo é arquimediano. Em particular, para $F = \Re$, o teorema 5.4 é chamado de lei (axioma) de arquimedes.

**Corolário 5.4.1** *Seja $F$ um corpo ordenado completo. Sejam $C_x = \{y \in \mathbb{Q} | y < x\}$ para cada $x \in F$ e $\overline{C_x} = \{y \in \mathbb{Q} | 0 < y < x\}$ para cada $x \in F$, $x>0$. Então temos:*

1. $\sup C_x = x$, *para todo* $x \in F$.
2. $\sup \overline{C_x} = x$, *se* $x > 0$.
3. $\sup C_x = \sup \overline{C_x} = x$, *se* $x > 0$.
4. *Dado $x \in F$. Então existe um $m \in \mathbb{Z}$ tal que $m - 1 \leq x < m$. Se $x \geq 0$, então $m \in \mathbb{N}$.*

**Demonstração:**

1. Pela definição de $C_x$, vemos que $x$ é uma cota superior de $C_x$. Como $F$ é um corpo ordenado, então temos três casos. Primeiro, $x > 0$. Pelo teorema 5.4, sabemos que $F$ é um corpo arquimediano, portanto, pelo teorema 5.3, existe um natural $n \in \mathbb{N}$ tal que $x < n$, o que implica em $-n < -x < x$, o que implica $-n < x$, ou seja,$-n \in C_x$. Segundo, $x < 0$. Então, $-x > 0$. Analogamente, temos que existe um $n$ natural tal que $-x < n$, o que implica $-n < x$, ou seja, $-n \in C_x$. Terceiro, suponha $x = 0$. Então, segue-se que $-n < 0$ para todo natural $n$. Logo, temos novamente,$-n \in C_x$. Assim, em qualquer caso temos $C_x \neq \emptyset$. Portanto, $C_x$ admite supremo. Logo, temos $\sup C_x \leq x$. Suponha que $\sup C_x < x$. Tomando um $\epsilon = x - C_x > 0$, vemos que para todo $y \in C_x$, tem-se $y < x = \sup C_x - \epsilon$ o que é uma contradição ao fato de que $\sup C_x$ ser o supremo de $C_x$. Assim, devemos ter $\sup C_x = x$.

2. É óbvio que,todo $x > 0$ é cota superior de $\overline{C_x}$. Pelo teorema 5.4, existe um natural $n \in \mathbb{N}$ tal que $x < n$ o que implica em $n < x$. Logo, $\overline{C_x} \neq \emptyset$. Portanto, $\overline{C_x}$ admite supremo. Disso resulta que, $\sup \overline{C_x} \leq x$. Suponha que $\overline{C_x} < x$. Tomando um $\epsilon = x - \overline{C_x} > 0$, vemos que para todo $y \in \overline{C_x}$, tem-se $y < x = \overline{C_x} - \epsilon$ o que é uma contradição. Assim, devemos ter $\sup \overline{C_x} = x$.

3. Por (1) e (2), quando $x > 0$, segue-se, imediatamente, que $\sup C_x = \sup \overline{C_x} = x$.

4. **Unicidade**. Suponha que existam $m, n \in \mathbb{Z}$ distintos tais que $n - 1 \leq x < n$ e $m - 1 \leq x < m$. Sem perda de generalidade suponha, $n < m$. Segue-se que, $n + 1 \leq m$. Assim, $n \leq m - 1$, e portanto, $x < n \leq m - 1 \leq x$, o que é uma contradição. Logo, $m = n$.

   **Existência**. Primeiro, suponha que $x = 0$. Então podemos tomar $m = 1 \in \mathbb{Z}$. Segundo, suponha que $x > 0$. Vamos considerar o conjunto $B = \{n \in \mathbb{N} | x < n\}$. Note que, $B \subseteq \mathbb{N}$. Como $x > 0$, vemos, pelo teorema 5.4, que existe um $n \in \mathbb{N}$ tal que $x < n$. Isso implica que $B \neq \emptyset$. Assim, existe um $m \in B$ tal que $m \leq n, \forall n \in B$. Como $m \in B$, temos que $x < m$. Pela minimalidade de $m$, vemos que $m - 1 \notin B$. Assim, podemos ter $m - 1 > 0$ ou $m - 1 = 0$: se $m - 1 > 0$, então $m - 1 \in \mathbb{N}$ e, portanto, $m - 1 \leq x$; se $m - 1 \leq 0$, então $m = 1$, ou seja, $m - 1 < x$. Portanto, nos dois casos temos $m - 1 \leq x < m$. Terceiro, supondo $x < 0$, temos imediatamente que $-x > 0$. Como anteriormente, existe $n \in \mathbb{N}$ tal que $n - 1 \leq -x < n$. Disso resulta que, $-n < x \leq -n + 1$.

Temos dois casos. Supondo, $x = -n + 1$ e tomando $m = -n + 2$, vemos que $x = m - 1$ e que $m \in \mathbb{Z}$,pois, $n \in \mathbb{N}$. Assim, temos que existe $m \in \mathbb{Z}$ tal que $m - 1 \leq x < m$. Agora, supondo $-n < x < -n + 1$ tomamos $m = -n + 1$, vemos que $m \in \mathbb{Z}$ e que $m - 1 \leq x < m$.

■

**Lema 5.2** *Seja $p \in (0, +\infty)$.Então existe um único $x \in (0, +\infty)$ tal que $x^n = p$.*

**Demonstração:**

Seja $S = \{w \in \Re | w > 0 \ \ e \ \ w^n < p\}$. Vamos considerar dois possíveis valores de $p$. Primeiro, suponha $p > 1$. Então $p^n \geq p$ para todo $n \in \mathbb{N}$. Note que $1 \in S$, pois, $1 > 0$ e $1^n = 1 < p$. Assim, $S \neq \emptyset$. Agora, tomando qualquer real $w > p$, segue-se que $w^n > p^n \geq p$, e portanto $w \notin S$. Disso resulta que, se $w \in S$,então $w \leq p$. Logo, $p$ é uma cota superior de $S$. Os resultados anteriores permitem deduzir que existe um único $x = \sup S$. Como $1 \in S$,vemos que $x \geq 1$. Vamos mostrar que $x^n = p$. Suponha $x^n > p$. Tomando um $t = x - \epsilon$ tal que $0 < \epsilon < x$ e $0 < \epsilon < \frac{x^n - p}{nx^{n-1}}$, segue-se que $t < x$, e que da última desigualdade envolvendo $\epsilon$ temos, sucessivamente, $p < x^n - nx^{n-1}\epsilon = x^n(1 - n\frac{\epsilon}{x}) \leq x^n(1 - \frac{\epsilon}{x})^n = (x - \epsilon)^n = t^n$, ou seja, $t^n > p$. Por outro lado, se $w \in S$,então $w^n < p < t^n$, ou seja, $w^n < t^n$ o que implica $w < t$, pois, $w$ e $t$ são positivos. Logo, $t$ é uma cota superior de $S$ menor do que $x$, o que é uma contradição ao fato de que $x$ é o supremo de $S$ ( a menor das cotas superiores de $S$).

Antes de considerar a segunda hipótese, mostraremos a seguinte afirmação: Se $0 < \epsilon < 1$ e $x > 0$, então existe um $k \in \Re$, positivo, tal que $(x + \epsilon)^n \leq x^n + k\epsilon$. Com efeito, vemos que $(x + \epsilon)^n = x^n + A(x, \epsilon)\epsilon$, onde $A(x, \epsilon)$ é um número real positivo expresso como soma de termos positivos de $x$ e $\epsilon$. Como $A(x, \epsilon) > 0$, segue-se que o real positivo $nA(x, \epsilon) \geq A(x, \epsilon)$, para todo natural $n$. Tomando $k = nA(x, \epsilon)$, temos que $(x + \epsilon)^n = x^n + A(x, \epsilon)\epsilon \leq x^n + k\epsilon$.

Agora, suponha $x^n < p$. Tomando um $t = x + \epsilon$ tal que $0 < \epsilon < 1$ e $\epsilon < \frac{p - x^n}{k}$ para algum $k > 0$, segue-se que $x < t$, e que da última desigualdade envolvendo $\epsilon$ temos, sucessivamente, $p > x^n + k\epsilon \geq (x + \epsilon)^n = t^n$, ou seja, $t^n < p$. Isso implica que $t \in S$ é maior do que o seu supremo, o que é uma contradição. Portanto, devemos ter $x^n = p$. Segundo, suponha $p \leq 1$. Então, $p^n \leq p \leq 1$, para todo $n \in \mathbb{N}$. Note que, $\frac{p}{2} \in S$, pois, $\frac{p}{2} > 0$ e $\left(\frac{p}{2}\right)^n = \frac{p^n}{2^n} < p^n \leq p$, ou seja, $\left(\frac{p}{2}\right)^n < p$. Assim, $S \neq \emptyset$. Agora, tomando qualquer real $w > 1$, segue-se que $w^n > 1$, e portanto, $w \notin S$. Assim, se $w \in S$, então $w \leq 1$. Esse fato mostra que 1 é cota superior de $S$. Logo, existe um único $x = \sup S$. Disso resulta que $x \leq 1$. Para mostrar que $x^n = p$, usamos o mesmo raciocínio desenvolvido anteriormente. Portanto, devemos ter, também, $x^n = p$.

■

**Definição 5.9** *O número real $x \in (0, +\infty)$ tal que $x^n = p$ é chamado de raiz quadrada de p, denotado por $\sqrt[n]{p}$.*

**Lema 5.3** *Seja $p \in \mathbb{N}$. Se não existe um $x \in \mathbb{Z}$ tal que $x^n = p$.Então $\sqrt[n]{p} \notin \mathbb{Q}$.*

**Demonstração:** Pela hipótese, vemos que $x \notin \mathbb{Z}$. Logo, devemos ter ou $x \in \mathbb{Q}$ ou $x \in \Re - \mathbb{Q}$. Suponha, $x \in \mathbb{Q}$ . Então existem inteiros $u$ e $v$ ($v \neq 0$) tais que $x = \frac{u}{v}$ e $(u, v) = 1$, onde $(u, v)$ é o máximo divisor comum entre $u$ e $v$. Devemos ter $v \neq 1$, pois, se $v = 1$ teremos $x \in \mathbb{Z}$, o que é um absurdo. Pela definição, temos $\left(\frac{u}{v}\right)^n = p$. Isso implica em $u^n = v^n p$. Assim, $v^n$ divide $u^n$. Isso resulta em $(u, v) \neq 1$, o que é um absurdo. Portanto, devemos ter necessariamente, que $\sqrt[n]{p} \notin \mathbb{Q}$. ■

**Observação 5.3.1** *Ao demonstrarmos o lema 5.3, usamos um resultado da teoria dos números inteiros: Se u e v são inteiros não nulos tai que $(u, v) = 1$, então $(u^n, v^n) = 1$, para todo natural n.*

**Observação 5.3.2** *Em particular, se $p = 2$ sabemos que não existe um inteiro x tal que $x^2 = 2$. Pelo lema 5.3, concluímos que $\sqrt{2} \notin \mathbb{Q}$.*

**Teorema 5.5 (Existência dos Números Irracionais)** *O corpo ordenado dos racionais $\mathbb{Q}$ não é completo.*

**Demonstração:** Suponha $\mathbb{Q}$ completo. Devemos exibir um subconjunto $S \subseteq \mathbb{Q}$ onde o supremo $\sup S \notin \mathbb{Q}$. Vamos considerar o conjunto $S$ do lema 5.2 para $p = 2$. Portanto, seja $S = w \in \mathbb{Q} | w > 0 \ \ e \ \ w^2 < 2$. Ora, $1 \in S$, pois, $1 > 0$ e $1^2 < 2$. Assim, $S \neq \emptyset$. Sabemos do lema 5.2, que $p = 2$ é cota superior de $S$. Pelo axioma da completude, S existe um único $x = \sup S$. Ora, pelo lema 5.2, vemos que $x^2 = 2$. Como $\mathbb{Q}$ é completo devemos ter $x = \sup S = \sqrt{2} \in \mathbb{Q}$, o que contradiz o lema 5.3. Portanto, deduzimos que $\mathbb{Q}$ não é completo. ■

Sabemos que no conjunto $\mathbb{Z}$, nem sempre existe um número inteiro $x$ entre um par de números inteiros $a$ e $b$. No entanto, quando estendemos para o conjunto dos números racionais $\mathbb{Q}$ esse fato se torna verdade, pois, sabemos que para quaisquer $a, b \in \mathbb{Q}$ se tomarmos $x = \frac{a+b}{2} \in \mathbb{Q}$, vemos que $a < x < b$. Em outras palavras, entre dois números racionais quaisquer existe sempre um número racional, podemos estender essa propriedade para os números reais . Isso mostra, intuitivamente, que os números reais está espalhado por toda a reta, ou seja, dizemos que o conjunto dos números reais é denso. Vamos formalizar essa noção através da seguinte definição.

**Teorema 5.6** *O conjunto $\mathbb{Q}$ dos números racionais e o conjunto $\Re - \mathbb{Q}$ dos irracionais são ambos densos em $\Re$.*

**Demonstração:** Vamos dividir a demonstração em duas partes.

- Primeira: $\mathbb{Q}$ é denso. Com efeito, dados $a, b \in \Re$, com $a < b$, vemos que $b - a > 0$. Como $\Re$ é um corpo arquimediano, pelo teorema 5.3 (III), existe um $n \in \mathbb{N}$,tal que $\frac{1}{n} < b - a$. Disso resulta que $an + 1 < bn$. Pelo corolário 5.4.1 (4), existe um inteiro $m$ tal que $m - 1 \leq an < m$ o que implica em $m \leq an + 1 < bn$. Assim, $m < an < bn$, e portanto, $a < \frac{m}{n} < b$. Pelo que conhecemos sobre $\mathbb{Q}$,vemos que $\frac{m}{n} \in \mathbb{Q}$. Portanto, segue-se o resultado.

- Segundo: $\Re - \mathbb{Q}$ é denso. Com efeito, como $\sqrt{2} > 0$, então $\frac{1}{\sqrt{2}} > 0$. Disso resulta que $\frac{a}{\sqrt{2}} < \frac{b}{\sqrt{2}}$. Pela primeira parte, sabemos que existe um $q \in \mathbb{Q}$ tal que $\frac{a}{\sqrt{2}} < q < \frac{b}{\sqrt{2}}$. Se $q = 0$ teremos $\frac{a}{\sqrt{2}} < 0 < \frac{b}{\sqrt{2}}$ . Assim, escolheremos um racional $q' \neq 0$ tal que $\frac{a}{\sqrt{2}} < q' < 0 < \frac{b}{\sqrt{2}}$ ou $\frac{a}{\sqrt{2}} < 0 < q' < \frac{b}{\sqrt{2}}$ . De qualquer forma, devemos escolher um $q \neq 0$ entre $\frac{a}{\sqrt{2}}$ e $\frac{b}{\sqrt{2}}$ . Segue-se que $\frac{a}{\sqrt{2}} < q < \frac{b}{\sqrt{2}}$. Como $q \neq 0$, vemos que $q\sqrt{2} \in \Re - \mathbb{Q}$ .

■

**Corolário 5.6.1** *Sejam $C_x$ e $\overline{C_x}$ dois conjuntos dados no corolário 5.4.1. Então, temos:*

1. $C_{a+b} = C_a + C_b$, *para cada* $a, b \in \Re$.
2. $\overline{C_{ab}} = \overline{C_a} \cdot \overline{C_b}$, *para todo* $a, b \in \Re$, *com* $a, b > 0$.

**Demonstração:**

1. Seja $w \in C_a + C_b$. Então, existem $x \in C_a$ e $y \in C_b$ tais que $w = x + y$. Segue-se que, $x < a$ e $y < b$, implica em $w = x + y \in \mathbb{Q}$ e $w = x + y < a + b$. Assim, vemos que $w \in C_(a + b)$, e portanto, $C_a + C_b \subseteq C_(a + b)$. Agora, seja dado $x \in C_(a + b)$. Então, temos $x \in Q$ e $x < a + b$, ou seja, $x - b < a$. Então, pelo teorema 5.6, existe um número racional $u$ tal que $x - b < u < a$. Fazendo, $x = u + (x - u)$, vemos que $u, x - u \in \mathbb{Q}$, e que $u < a$ e $x - u < b$. Assim, deduzimos que $x \in C_a + C_b$, ou seja, $C_(a + b) \subseteq C_a + C_b$. Portanto, temos $C_(a + b) = C_a + C_b$.

2. Seja $w \in \overline{C_a} \cdot \overline{C_b}$. Então, existem $x \in \overline{C_a}$ e $y \in \overline{C_b}$ tais que $w = xy$. Note que $xy \in \mathbb{Q}$, pois, $x$ e $y$ são racionais. Segue-se que, $0 < x < a$ e $0 \leq y < b$ implica em $0 < xy < ab$, ou seja, $0 < w < ab$. Logo, vemos que $w \in \overline{C_{ab}}$ e, portanto, $\overline{C_a} \cdot \overline{C_b} \subseteq \overline{C_{ab}}$. Seja dado $w \in \overline{C_{ab}}$. Disso resulta que, $w \in \mathbb{Q}$, com $0 < w < ab$, ou seja, $\frac{w}{a} < b$, pois, $a, b > 0$. Usando o teorema 5.6, temos que existe um

$x \in \mathbb{Q}$ tal que $\frac{w}{a} < x < b$. Fazendo, $w = \frac{w}{x} \cdot x$, vemos que $\frac{w}{x}, x \in \mathbb{Q}$ e são tais que $0 < \frac{w}{x} < a$ e $0 < x < b$, ou seja, $\frac{w}{x} \in \overline{C_a}$ e $x \in \overline{C_b}$. Assim, deduzimos que $w \in \overline{C_a} \cdot \overline{C_b}$ , isto é, $\overline{C_{ab}} \subseteq \overline{C_a} \cdot \overline{C_b}$. Portanto, provamos que $\overline{C_{ab}} = \overline{C_a} \cdot \overline{C_b}$.

■

Doravante, usaremos o lema a seguir na demonstração da unicidade dos números reais.

**Lema 5.4** *Sejam $A, B \subseteq X$, não vazios, e a função $f : X \to Y$. São válidas as seguintes afirmações:*

*(I) Se $f(x+y) = f(x)+f(y)$, para todo $x, y \in X$, então $f(A+B) = f(A)+f(B)$.*

*(II) Se $f(xy) = f(x)f(y)$, para todo $x, y \in X$, então $f(AB) = f(A)f(B)$.*

**Demonstração:** Sejam $A, B \subseteq X$, não vazios, e a função $f : X \to Y$. São válidas as seguintes afirmações:

(I) Note que, $w \in f(A+B)$ se, e somente se, existe $t \in A+B$, tal que $w = f(t)$ se, e somente se, existem $p \in A, q \in B$ tais que $t = p+q$ e $w = f(p+q) = f(p)+f(q)$ se, e somente se, existem $p \in A$, $q \in B$ tais que $t = p + q$ e $w = f(p) + f(q)$, onde $f(p) \in A$, $f(q) \in B$ se, e somente se, $w \in f(A) + f(B)$. Portanto, $f(A + B) = f(A) + f(B)$.

(II) Note que, $w \in f(AB)$ se, e somente se, existe $t \in AB$, tal que $w = f(t)$ se, e somente se, existem $p \in A, q \in B$ tais que $t = pq$ e $w = f(pq) = f(p)f(q)$ se, e somente se, existem $p \in A, q \in B$ tais que $t = pq$ e $w = f(p)f(q)$, onde $f(p) \in A, f(q) \in B$ se, e somente se, $w \in f(A)f(B)$. Portanto, $f(AB) = f(A)f(B)$.

■

# Capítulo 6

# Unicidade dos Números Reais

O processo de construção de números reais, seja por meio de cortes de Dedekind ou por meio de Classes de sequências de Cauchy - idealizada por Cantor, assegura o fato de que o conjunto dos números reais existe. Seja qual for o processo pelo qual levou a construção de números reais, existe sempre um sistema de propriedades comuns de um corpo ordenado, oriundo de qualquer processo de construção que parte dos números racionais. Podemos dizer de uma maneira mais geral, que qualquer corpo ordenado completo de números que advém de um certo tipo de construção e que parte dos números racionais é chamado de conjunto de números reais. Uma outra questão que não devemos negligenciar, é saber se existe outro conjunto de números reais que possua o mesmo elenco de propriedades. Podemos responder esse questionamento sob dois pontos de vistas: a primeira resposta é sim, de um ponto de vista da natureza de seus elementos. Com efeito, se usarmos os cortes de Dedekind, os números reais são vistos como seções ou corte; se usarmos as classes de equivalências, sugerida por Cantor, os números reais são vistos como limite de sequências de Cauchy de números racionais. A segunda resposta é não, de um ponto de vista de estrutura, ou seja, no que diz respeito às propriedades relativas as operações de adição, multiplicação, relação de ordem, e de ser um corpo ordenado completo. Não obstante, o questionamento deve fornecer apenas uma resposta. A segunda é a mais acertada, pois, retiramos o problema da distinção dos elementos intrínsecos, postura usada ao fazermos as inclusões $\mathbb{N} \subset \mathbb{Z} \subset \mathbb{Q} \subset \Re$. Definitivamente, vamos demonstrar de uma maneira mais rigorosa, a unicidade do conjunto dos números reais através da existência de uma função (isomorfismo) bijetiva que possua certas propriedades. Essa função é que mostra a unicidade, de um ponto de vista da preservação das estruturas algébricas e da completude do conjunto dos números reais. Antes de enunciar a unicidade dos números reais, vamos demonstrar um resultado, extremamente importante, usada na prova, chamado de teorema da definição por recorrência, o qual, por sua vez, depende das informações contidas nos Axiomas de Peano. Vamos enunciá-los.

Axiomas de Peano:
Seja $s : \mathbb{N} \to \mathbb{N}$ uma função que satisfaz as seguintes condições:

(I) $s$ é injetiva.

(II) $\mathbb{N} - s(\mathbb{N}) = \{1\}$ é um conjunto unitário,ou seja, $s(n) \neq 1, \forall n \in \mathbb{N}$.

(III) Seja o subconjunto $S \subset \mathbb{N}$ que satisfaz as seguintes condições:

(a) $1 \in \mathbb{N}$

(b) Se para todo $n \in \mathbb{N}$ implica em $s(n) \in \mathbb{N}$.

Então $S = \mathbb{N}$.

Observação: A função $s$ associa cada $n \in \mathbb{N}$ o elemento $s(n)$ chamado de sucessor de $n$, o qual definimos por $s(n) = n + 1$, por essa razão, chamamos função sucessão $s : \mathbb{N} \to \mathbb{N}$.

## 6.1 Definição por Recorrência

Sabemos que uma sequência de elementos de H é uma função $f : \mathbb{N} \to H$ que associa a cada número $n \in \mathbb{N}$ o elemento $f(n) \in H$, a qual denotamos tradicionalmente por $(a_n)_{n\in\mathbb{N}}$, ou simplesmente, $(a_n)$. Podemos escrever uma sequência, seja arbitrando cada elemento de $H$ na sucessão, seja por meio de uma lei de formação ou de construção de seus elementos. Se a sequência possuir uma lei de formação, os seus elementos podem ser construídos em função, exclusiva, da ordem dos elementos da sequência ou em função do(s) termo(s) precedente(s) da sequência, a qual é chamada **lei de definição por recorrência**, ou ainda, pela combinação explícita de ambas as leis. Ilustramos, a seguir, algumas sequências construídas por lei de formação.

**Exemplo 6.1.1** *A sequência dada por* $(a_n) = (2, 5, 10, \cdots)$ *é descrita pela lei* $a_n = n^2 + 1$.

**Exemplo 6.1.2** *A sequência dada por* $(a_n) = (2, 5, 10, )$ *é descrita pela lei* $a_n = n^2 + 1$.

**Exemplo 6.1.3** *O fatorial do número natural n denotado por* $(n!)$ *pode ser visto como uma sequência descrita pela lei de recorrência*

$$a_n = n! = \begin{cases} 1, & se, \quad n = 1 \\ na_{n-1} & se, \quad n \geq 2 \end{cases}$$

**Exemplo 6.1.4** *O produto dos n primeiros números reais $a_1 \cdots a_n$ da sequência $(a_n)$ pode ser visto como uma sequência descrita pela lei de recorrência*

$$b_n = \begin{cases} a_1, & se, \quad n = 1 \\ b_{n-1}a_n, & se, \quad n \geq 3 \end{cases}$$

**Exemplo 6.1.5** *A sequência $(a_n) = (1, 2, 5, \cdots)$ é descrita pela lei de recorrência $a_n = (a_{n-1})^2 + 1$.*

**Exemplo 6.1.6** *A sequência $(a_n) = (1, 3, 12, \cdots)$ é descrita pela lei de recorrência $a_n = n + (a_{n-1})^2$.*

Podemos reescrever as leis de recorrência dos exemplos 6.1.2, 6.1.3 e 6.1.5 como $f(s(n)) = k(f(n))$ para todo $n$ natural e $f(1) = r$, onde $k$ é a função $k : H \to H, r \in H, f$ é a função $f : N \to H$, e $s$ é função sucessão $s : \mathbb{N} \to \mathbb{N}$; a lei do exemplo 6.1.6 pode ser reescrita como $f(s(n)) = t(f(n), n)$, para todo natural $n$, onde $f$ é a função $f : \mathbb{N} \to H$ tal que $f(1) = r$, $t$ é a função $t : H \times \mathbb{N} \to H$, e $s$ é a função sucessão $s : \mathbb{N} \to \mathbb{N}$; no entanto, a lei de recorrência do exemplo 6.1.4 é reescrita da seguinte forma: $f(s(n)) = p(k(n))$, onde $r \in H, f$ é a função $f : \mathbb{N} \to H$ tal que $f(1) = r, k$ é a função $k : \mathbb{N} \to X = \{\varphi_n : H^n \to H | n \in \mathbb{N}\}$ definida por $k(n) = \varphi_n$, e $p : X \to H$ é a função produto de $n$ elementos de $H$ definida por $p(\varphi_n) = \varphi_n(x)$, onde $x$ é uma $n$-upla de elementos de $H$. O teorema seguinte, garante a existência da definição $f$ por recorrência caracterizada pelos exemplos 6.1.2, 6.1.3 e 6.1.5.

**Teorema 6.1 (Definição por Recursão)** *Sejam um conjunto $H$ tal que $r \in H$ e uma função $k : H \to H$. Então existe uma única função $f : \mathbb{N} \to H$ tal que $f(1) = r$, e que $f(s(n)) = k(f(n)), \forall n \in \mathbb{N}$.*

**Demonstração:**

Vamos dividir a prova em duas partes.

- Existência. Podemos pensar em todas as funções de $\mathbb{N} \to H$ como subconjuntos de $\mathbb{N} \times H$ satisfazendo certas condições. Seja o conjunto

$$C = \{W \subseteq \mathbb{N} \times H | (1, r) \in W, \quad se \quad (n, y) \in W, \quad então \quad (s(n), k(y)) \in W\}.$$

  Note que $C \neq \emptyset$, pois, $\mathbb{N} \times H \in C$. Tomando $f = \bigcap_{W \in C} W$, vemos que $f \subseteq \mathbb{N} \times H$. Como $(1, r) \in W$, para todo $W \in C$, resulta que $(1, r) \in f$. Suponha que $(n, y) \in f$. Então $(n, y) \in W$ para todo $W \in C$, o que resulta em $(s(n), k(y)) \in W$ para todo $W \in C$. Assim, vemos que $(s(n), k(y)) \in f$. Logo, $f \in C$. É claro que $f \subseteq W$ para todo $W \in C$.

Vamos mostrar a seguinte afirmação: Dado $(n, y) \in f$ tal que $(n, y) \neq (1, r)$, então existe algum $(m, u) \in f$ tal que $(n, y) = (s(m), k(u))$. Com efeito, suponha o contrário, dado um $(n, y) \neq (1, r)$, então temos $(n, y) \neq (s(m), k(u))$ para todo $(m, u) \in f$. Seja $\bar{f} = f - \{(n, y)\}$. É óbvio que $\bar{f} \subseteq \mathbb{N} \times H$ e que $(1, r) \in \bar{f}$. Se $(p, q) \in \bar{f}$, então $(p, q) \in f$, segue-se que $(s(p), k(q)) \in f$. Pela hipótese, sabemos que $(s(p), k(q)) \neq (n, y)$ para todo $(p, q) \in f$. Logo, $(s(p), k(q)) \in \bar{f}$. Assim, $\bar{f} \in C$. Ora, por construção de $\bar{f}$ vemos que $\bar{f} \subseteq f$, o que é uma contradição ao fato de que $f \subseteq W$, para todo $W \in C$. Mostraremos que $f$ é de fato a função $f : \mathbb{N} \to H$. Para isso, devemos certificar que para todo $n \in \mathbb{N}$ existe um único $y$ tal que $(n, y) \in f$. Considere o conjunto $G = \{m \in \mathbb{N} |\ \textit{existe um único } z \in H \textit{ tal que } (m, z) \in f\}$.

Afirmação: $G = N$. Com efeito, $1 \in G$, pois, caso contrário, existiria um $s \in H$, distinto de $r$, tal que $(1, s) \in f$. Disso resulta, que $(1, s) \neq (1, r)$. Assim, existe um $(u, v) \in f$ tal que $(s(u), k(v)) = (1, s)$, o que implica em $s(u) = 1$. Absurdo, pois, isso contraria o axioma (II) de Peano. Agora, seja $n \in G$. Então, existe um único $y \in H$ tal que $(n, y) \in f$. Assim, pelo que definimos sobre $f$, vemos que $(s(n), k(y)) \in f$. Para mostrarmos que $s(n) \in f$, devemos provar que $k(y) \in H$ é único. Com efeito, suponha $(s(n), z) \in f$. Como $(s(n), z) \neq (1, r)$, existe um $(m, u) \in f$ tal que $(s(m), k(u)) = (s(n), z)$. Pela injetividade de $s$, temos $m = n$, pela hipótese $n \in G$, portanto, $u = y$. Disso resulta que $z = k(u) = k(y)$. Logo, toda vez que $(s(n), z) \in f$ resulta sempre em $z = k(y)$. Assim, vemos que $s(n) \in G$. Portanto, pelo axioma (III) de Peano, concluímos que $G = \mathbb{N}$. Pelo o que mostramos acima, vemos que existe um f tal que $f(1) = r$, pois, $(1, r) \in f$, e que a implicação de que $(n, y) \in f$ resulta em $(s(n), k(y)) \in f$, é equivalente a, $f(s(n)) = k(f(n))$, para todo $n$ natural.

- Unicidade. Suponha que exista duas funções $f, g : \mathbb{N} \to H$ tais que $f(1) = r$ e $g(1) = r$, e que $f \circ s = k \circ f$ e $g \circ s = k \circ g$. Seja $V = \{m \in \mathbb{N} | f(m) = g(m)\}$. Afirmação: $V = \mathbb{N}$. Com efeito, $1 \in V$, pois, $f(1) = r = g(1)$. Suponha $n \in V$. Então, $f(n) = g(n)$. Disso resulta, sucessivamente, em $f(s(n)) = k(f(n)) = k(g(n)) = g(s(n))$, ou seja, $f(s(n)) = g(s(n))$. Assim, $s(n) \in V$, e portanto, pelo axioma (III) de Peano, $V = \mathbb{N}$.

■

**Teorema 6.2 (Unicidade dos Números Reais)** *Sejam dois corpos ordenados completos $\Re_1$ e $\Re_2$. Então existe uma função bijetiva $f : \Re_1 \to \Re_1$ que satisfaz as seguintes condições:*

*(I)* $f(x + y) = f(x) + f(y), \forall x, y \in \Re_1$.

*(II)* $f(xy) = f(x)f(y), \forall x, y \in \Re_1$

*(III) Se $x < y$, então $f(x) < f(y)$.*

**Observação 6.2.1** *É importante salientar que os símbolos de adição $(+)$, multiplicação $(\cdot)$ e da relação de ordem $(<)$ são usados em dois contextos distintos, por exemplo, a adição em $\Re_1$ é diferente da adição em $\Re_2$, a multiplicação em $\Re_1$ é diferente da multiplicação em $\Re_2$, e assim por diante, bem como os respectivos elementos neutros da adição e multiplicação. A atitude em usar os mesmos símbolos em ambos os contextos, é para que o leitor tenha melhor entendimento da demonstração, além de não carregar o texto com muitos símbolos, evitando uma leitura cansativa.*

**Demonstração:** A ideia da prova consiste, primeiro, em considerar todas as propriedades do conjunto dos números reais $\Re$, igualmente válidas, para os conjuntos $\Re_1$ e $\Re_2$; fazer uma analogia dos conjuntos $\mathbb{N}, \mathbb{Z}$ e $\mathbb{Q}$ com os subconjuntos $\mathbb{N}_1, \mathbb{Z}_1$ e $\mathbb{Q}_1$ de $\Re_1$, e os subconjuntos $\mathbb{N}_2, \mathbb{Z}_2$ e $\mathbb{Q}_2$ de $\Re_2$, bem como considerar todas as propriedades de $\mathbb{N}, \mathbb{Z}$ e $\mathbb{Q}$, também, igualmente válidas, para os respectivos análogos subconjuntos de $\Re_1$ e $\Re_2$; mostrar a existência da função $g : \mathbb{N}_1 \to \mathbb{N}_2$ e sua unicidade, primeiramente, sobre o domínio de $\mathbb{N}_1$, mostrando a bijetividade bem como as condições típicas de um isomorfismo; em seguida, estenderemos o domínio de $g$ para $\mathbb{Z}_1$,definindo a função $h : \mathbb{Z}_1 \to \mathbb{Z}_2$ e mostrando novamente a bijetividade e as condições típicas de um isomorfismo neste domínio; posteriormente, estenderemos o domínio de $h$ para $\mathbb{Q}_1$, definindo a função $r : \mathbb{Q}_1 \to \mathbb{Q}_2$, e finalmente estenderemos a função $r$ para $\Re_1$, definindo a função $f : \Re_1 \to \Re_2$, mostrando, claro, as condições fundamentais de um isomorfismo, seguidas pelas extensões anteriores. Portanto, vamos dividir a demonstração em quatro partes.

**1ª Parte**: Fazendo $H = \mathbb{N}_2$, $\mathbb{N} = \mathbb{N}_1$, $k = s : \mathbb{N}_2 \to \mathbb{N}_2$ (função sucessão) e tomando $r = 1 \in \mathbb{N}_2$, vemos pelo teorema da Definição por Recursão (teorema 6.1), que existe uma única função $g : \mathbb{N}_1 \to \mathbb{N}_2$ tal que $g(1) = 1$ e $g(s(n)) = s(g(n))$, para todo $n \in \mathbb{N}_1$, ou equivalentemente, $g(n+1) = g(n) + 1$, para todo $n \in \mathbb{N}_1$. Agora, vamos mostrar que $g$ é bijetiva. Com efeito, fazendo $H = \mathbb{N}_1$, $\mathbb{N} = \mathbb{N}_2$, $k = s : \mathbb{N}_1 \to \mathbb{N}_1$ (função sucessão) e tomando um $r = 1 \in \mathbb{N}_1$, vemos pelo teorema 6.1 que existe uma única função $p : \mathbb{N}_2 \to \mathbb{N}_1$ tal que $p(1) = 1$ e $p(s(n)) = s(p(n))$, para todo $n \in \mathbb{N}_2$, ou equivalentemente, $p(n+1) = p(n) + 1$, para todo $n \in \mathbb{N}_2$. Note que, a composta $g \circ p : \mathbb{N}_2 \to \mathbb{N}_2$ é tal que $g \circ p(1) = g(p(1)) = g(1) = 1$ e $g \circ p(n+1) = g(p(n+1)) = g(p(n)+1) = g(p(n)) + 1 = gop(n) + 1$, para todo $n \in \mathbb{N}_2$. Observe que função identidade $I : \mathbb{N}_2 \in \mathbb{N}_2$ temos $I(1) = 1$ e $I(n+1) = n + 1 = I(n) + 1$, para todo $n \in \mathbb{N}_2$. Disso resulta, pela unicidade dom teorema 6.1, que $g \circ p = I$. Assim, $g : \mathbb{N}_1 \to \mathbb{N}_2$ e $p : \mathbb{N}_2 \to \mathbb{N}_1$ são inversas uma da outra e bijetivas. Mostraremos agora, que $g(m+n) = g(m) + g(n)$, para todo $m, n \in \mathbb{N}_1$. Considere o conjunto

$$S = \{a \in \mathbb{N} | g(m+a) = g(m) + g(a), \forall m \in \mathbb{N}_1\}$$

Afirmação: $S = \mathbb{N}$. Com efeito, $1 \in S$, pois, sabemos que $g(m+1) = g(m)+1$, para todo $m \in \mathbb{N}_1$. Suponha $n \in G$. Ora, $g[m+(n+1)] = g[(m+n)+1] = g(m+n)+1 = g(m) + g(n) + 1 = g(m) + g(n+1)$. Assim, $n+1 \in G$. Portanto, deduzimos que $S = \mathbb{N}$, ou seja, $g(m+n) = g(m)+g(n)$, para todo $m, n \in \mathbb{N}_1$. Agora, vamos deduzir que $g(mn) = g(m)g(n)$, para todo $m, n \in \mathbb{N}_1$. Considere o conjunto

$$P = \{a \in \mathbb{N} | g(ma) = g(m)g(a), \forall m \in \mathbb{N}_1\}$$

Afirmação: P=N. Com efeito, $1 \in P$, pois, $g(m \cdot 1) = g(m) = g(m) \cdot 1 = g(m)g(1)$. Suponha $n \in P$. Ora, $g[m(n+1)] = g(mn+m) = g(mn) + g(m) = g(m)g(n) + g(m) = g(m)[g(n)+1] = g(m) \cdot g(n+1)$, ou seja, $g[m(n+1)] = g(m) \cdot g(n+1)$. Assim, $n+1 \in P$. Portanto, temos $P = \mathbb{N}$, isto é, $g(mn) = g(m)g(n)$, para todo $m, n \in \mathbb{N}_1$. Suponha $m < n$. Então existe um $k \in \mathbb{N}_1$ tal que $n = m + k$. Disso resulta, imediatamente, que $g(n) = g(m) + g(k)$. Como $g(k) \in \mathbb{N}_2$, concluímos que g(m)<g(n).

**2ª Parte**: Seja a função $h : \mathbb{Z}_1 \to \mathbb{Z}_2$ definida por $h(n) = \begin{cases} g(n), & \text{se}, \quad n \in \mathbb{N}_1 \\ 0, & \text{se}, \quad n = 0 \\ -g(-n), & \text{se}, \quad n \in -\mathbb{N}_1 \end{cases}$.

Pela definição de $h$ vemos que ele é uma extensão de g para $\mathbb{Z}_1$, e que dado $n \in \mathbb{Z}_1$, $h(n) \in \mathbb{N}_2$ se e somente se $n \in \mathbb{N}_1$; $h(n) = 0$ se e somente se $n = 0$; e $h(n) \in -\mathbb{N}_2$ se e somente se $n \in -\mathbb{N}_1$. Vamos provar que $h(m+n) = h(m)+h(n)$ para todo $m, n \in \mathbb{Z}_1$. Com efeito, temos quatro casos a considerar. Primeiro, $n, m \in \mathbb{N}_1$. Pela 1ª parte desta demonstração vemos que $h(m+n) = h(m) + h(n)$, para todo $m, n \in \mathbb{N}_1$. Segundo, $n \in \mathbb{N}_1$ e $m \in -\mathbb{N}_1$. Com isso, temos dois subcasos: $m+n \in \mathbb{N}_1$ ou $m+n \in -\mathbb{N}_1$. Suponha, $m+n \in \mathbb{N}_1$. Ora, $h(m)+h(n) = -g(-m)+g(n)$. Fazendo, $n = -m$, segue-se da última igualdade que $h(-m) = -h(m)$. Assim, pelo primeiro caso, vemos que $h(n-m) = h[n+(-m)] = h(n) + h(-m) = h(n) - h(m)$, isto é, $h(n-m) = h(n) - h(m)$, para todo, $n \in \mathbb{N}_1$ e $m \in -\mathbb{N}_1$. Usando esse resultado, vemos que $h(m) = h[(m+n)-n] = h(m+n)-h(n)$, ou seja, $h(m) = h(m+n)-h(n)$, o que implica em $h(m+n) = h(m) + h(n)$, para todo $n \in \mathbb{N}_1$ e $m \in -\mathbb{N}_1$. Seja $m+n \in -\mathbb{N}_1$ . Sabemos que $h(a-b) = h(a) - h(b)$, para todo, $a \in \mathbb{N}_1$ e $b \in -\mathbb{N}_1$. Tendo em vista essa última igualdade e fazendo $a = n$ e $b = m+n$, vemos que $h[n-(m+n)] = h(n) - h(m+n)$, ou seja, $h(-m) = h(n) - h(m+n)$, o que implica $h(m+n) = h(m) + h(n)$, para todo $n \in \mathbb{N}_1$ e $m \in -\mathbb{N}_1$. O terceiro caso é análogo ao segundo, por isso, omitiremos a demonstração deste caso. Quarto, suponha $n, m \in -\mathbb{N}_1$. Então, $-n, -m \in \mathbb{N}_1$ e $m+n \in -\mathbb{N}_1$. Usando a definição de $h$, temos $h(m+n) = -g[-(m+n)] = -g[(-m)+(-n)] = -g[(-m)+(-n)] = -g(-m) + g(-n) = -g(-m) + [-g(-n)] = h(m) + h(n)$. Vamos mostrar que $h(mn) = h(m)h(n)$, para todo $m, n \in \mathbb{Z}_1$. Com efeito, temos quatro casos a considerar. Primeiro, suponha $m, n \in \mathbb{N}_1$. Então, $mn \in \mathbb{N}_1$. Pela definição de $h$, temos $h(mn) = g(mn) = g(m)g(n)$, para todo $m, n \in \mathbb{N}_1$. Segundo caso, $m \in -\mathbb{N}_1$ e $n \in \mathbb{N}_1$. Então, $-m \in \mathbb{N}_1$ e $mn \in -\mathbb{N}_1$. Usando a definição de $h$, vemos

que $h(mn) = -g(-mn) = -\{g[(-m)n]\} = -\{g(-m)g(n)\} = -g(-m)g(n) = h(m)h(n)$, para todo $m \in -\mathbb{N}_1$ e $n \in \mathbb{N}_1$. O terceiro caso é semelhante ao segundo, por isso, vamos omitir o seu desenvolvimento. Quarto, seja $m, n \in -\mathbb{N}_1$. Então, $-m, -n \in \mathbb{N}_1$ e $mn \in \mathbb{N}_1$. Usando a definição de $h$, temos $h(mn) = g(mn) = g[(-m)(-n)] = g(-m)g(-n) = h(-m)h(-n) = [-h(m)][-h(n)] = h(m)h(n)$, para todo $m, n \in \mathbb{N}_1$. Suponha $m < n$. Então. $n - m \in \mathbb{N}_1$, o que implica, pela observação feita no início da 2ª parte, que $h(n-m) \in \mathbb{N}_2$,isto é, $h(n-m) > 0$. É óbvio, que $h(n-m) = h(n) - h(m)$, para todo $m, n \in \mathbb{Z}_1$. Observando a última desigualdade e igualdade, concluímos facilmente que $h(m) < h(n)$. Vamos provar que $h : \mathbb{Z}_1 \to \mathbb{Z}_2$. Como acabamos de mostrar que se ocorrer $m < n$, então $h(m) < h(n)$. Essa condição mostra que $h$ é injetiva. Com efeito, suponha $h(m) = h(n)$. Assim, $h(m) \leq h(n)$, o que implica pela condição acima que $m \leq n$. Se $m > n$, então temos $h(m) > h(n)$, o que contradiz o fato de ser $h(m) = h(n)$. Portanto, devemos ter necessariamente, $m = n$. Agora, vamos mostrar que $h$ é sobrejetiva. Com efeito, temos três casos possíveis. Primeiro, seja um dado $p \in \mathbb{N}_2$. Como $g : \mathbb{N}_1 \to \mathbb{N}_2$ é bijetiva, existe um $p_0 \in \mathbb{N}_1$, isto é, $p_0 \in \mathbb{Z}_1$ tal que $g(p_0) = p$. Ora, $h(p_0) = g(p_0) = p$, se $p_0 \in \mathbb{N}_1$. Segundo, se $p = 0$, vemos que existe um $x \in \mathbb{Z}_1$ tal que h(x)=0. De fato, neste caso pela definição de $h$, sabemos que o valor para $x = 0$, satisfaz $h(x) = 0$. Terceiro, dado $w \in \mathbb{N}_2$, segue-se que $-w \in \mathbb{N}_2$. Pela bijetividade de $g : \mathbb{N}_1 \to \mathbb{N}_2$, sabemos que existe um $w_0 \in \mathbb{N}_1$. Assim, temos $-w = g(w_0)$, o que implica $w = -g(w_0) = -g[-(-w_0)] = h(-w_0)$, pois, $-w_0 \in \mathbb{N}_1$. De uma forma mais sucinta, existe $-w_0 \in \mathbb{N}_1$, ou seja, $-w_0 \in \mathbb{Z}_1$ tal que $h(-w_0) = w$.

**3ª Parte**: Construiremos uma função $k$, cuja restrição deve ser $k_{|Z_1} = h$. Seja $k : \mathbb{Q}_1 \to \mathbb{Q}_2$ definida por $k\left(\frac{a}{b}\right) = \frac{h(a)}{h(b)}$ ,onde $a, b \in \mathbb{Z}_1$, com $b \neq 0$. Como $a, b \in \mathbb{Z}_1$, com $b \neq 0$, segue-se pela definição de $h$, que $h(a), h(b) \in \mathbb{Z}_2$ e $h(b) \neq 0$. Assim, temos $\frac{h(a)}{h(b)} \in \mathbb{Q}_2$. Note que, se $\frac{a}{b} \in \mathbb{Z}_1$, então $b = 1$, logo, pela definição de $h$ teremos $k(a) = h(a)$, para todo $a \in \mathbb{Z}_1$. Portanto, concluímos que $k : \mathbb{Q}_1 \to \mathbb{Q}_2$ é uma extensão de $h : \mathbb{Z}_1 \to \mathbb{Z}_2$. Vamos mostrar que $k$ está bem definida. Sejam $a, b, c, d \in \mathbb{Z}_1$ com $b \neq 0$ e $d \neq 0$ tais que $\frac{a}{b} = \frac{c}{d}$. Então, $ad = bc$, portanto, $h(ad) = h(bc)$. Disso resulta que, $h(a)h(d) = h(b)h(c)$ o que implica $\frac{h(a)}{h(b)} = \frac{h(c)}{h(d)}$, ou seja, $k\left(\frac{a}{b}\right) = k\left(\frac{c}{d}\right)$. Esse resultado mostra que $k : \mathbb{Q}_1 \to \mathbb{Q}_2$ está bem definida. Sejam $x, y \in \mathbb{Q}_1$. Então, existem $a, b, c, d \in \mathbb{Z}_1$, com $b \neq 0$, $d \neq 0$ tais que $x = \frac{a}{b}$ e $y = \frac{c}{d}$. Sabemos que no conjunto dos racionais temos $x + y = \frac{ad+bc}{bd}$ , e que $xy = \frac{ac}{bd}$. Então, podemos mostrar que:

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

$$k(xy) = k\left(\frac{ac}{bd}\right) = \frac{h(ac)}{h(bd)} = \frac{h(a)h(c)}{h(b)h(d)} = \frac{h(a)}{h(b)} \cdot \frac{h(c)}{h(d)} = k(x)k(y).$$

Agora, suponha $x < y$, ou seja, $\frac{a}{b} < \frac{c}{d}$. Temos dois casos. Primeiro, se $bd > 0$, então temos $bc - ad > 0$. Assim, pela 2ª parte desta demonstração, temos que $h(bc - ad) > h(0)$ e $h(bd) > h(0)$. Disso resulta que, $h(b)h(c) - h(a)h(d) > 0$ e $h(b)h(d) > 0$, o que implica

$$0 < \frac{h(b)h(c) - h(a)h(d)}{h(b)h(d)} = \frac{h(c)}{h(d)} - \frac{h(a)}{h(b)}.$$

Logo, temos $\frac{h(a)}{h(b)} < \frac{h(c)}{h(d)}$ . Segundo, se $bd < 0$, então $bc - ad < 0$. Assim, pela 2ª parte desta demonstração, temos que $h(bc - ad) < h(0)$ e $h(bd) < h(0)$. Disso resulta que, $h(b)h(c) - h(a)h(d) < 0$ e $h(b)h(d) < 0$, o que implica

$$0 < \frac{h(b)h(c) - h(a)h(d)}{h(b)h(d)} = \frac{h(c)}{h(d)} - \frac{h(a)}{h(b)}.$$

Logo, temos novamente, $\frac{h(a)}{h(b)} < \frac{h(c)}{h(d)}$ . Portanto, em ambos os casos temos $k(x) < k(y)$, sempre que $x < y$. Com essa condição, inferimos que $k$ é injetiva. Dado $z \in \mathbb{Q}_2$, segue-se que existem $p, q \in \mathbb{Z}_2$, com $q \neq 0$, tais que $z = \frac{p}{q}$. Como $h : \mathbb{Z}_1 \to \mathbb{Z}_2$ é bijetiva, vemos que existem $u, v \in \mathbb{Z}_1$ tais que $h(u) = p$, $h(v) = q$. Como $q \neq 0$, resulta da definição de $h$ que $v \neq 0$. Assim, $z = \frac{p}{q} = \frac{h(u)}{h(v)} = k\left(\frac{u}{v}\right)$. Portanto, dado $z \in \mathbb{Q}_2$ existe $\frac{u}{v} \in \mathbb{Q}_1$, para algum $u, v \in \mathbb{Z}_1$, com $v \neq 0$, tal que $k\left(\frac{u}{v}\right) = z$.

**4ª Parte**: É importante salientar, duas observações que precisamos ter em mente para que façam sentido algumas conclusões . Primeiro, sejam $x, y \in \Re_2$, tais que $x < y$. Pelo teorema 5.6, existe um racional $p \in \mathbb{Q}_2$ tal que $x < p < y$. Pela parte 3 desta demonstração, sabemos que $k : \mathbb{Q}_1 \to \mathbb{Q}_2$ é bijetiva. Logo, existe um $q \in \mathbb{Q}_1$ tal que $k(q) = p$. Assim, $x < k(q) < y$. Resumidamente, para quaisquer reais $x < y$ existe um $q$ racional tal que $x < k(q) < y$. Segundo, é verdadeira a recíproca da afirmação: se $x < y$, então $k(x) < k(y)$. Com efeito, se $k(x) < k(y)$, pela observação anterior, vemos que existe um racional q tal que $k(x) < k(q) < k(y)$. Dessa condição, temos necessariamente, $x < q < y$. Caso contrário, se $q < x$, então $k(q) < k(x)$, o que é um absurdo; se $y < q$, então $k(y) < k(q)$, o que, também, é um absurdo. Assim, devemos ter $x < q < y$. Portanto, deduzimos $x < y$. Agora, considerando o conjunto $C_x = \{w \in \mathbb{Q}_1 | w < x\}$ e as observações anteriores somos inspirados a definir a função $f : \Re_1 \to \Re_2$, por $f(x) = \sup k(C_x)$. Mostraremos que $f$ é a função pretendida. Vamos seguir sete passos.

1. $f$ é uma função. Com efeito, sabemos pelo Corolário 5.4.1, que para cada $x \in \Re_1$ associamos o conjunto $C_x$, o qual possui o supremo $x = \sup C_x$. Como

$C_x \neq \emptyset$, segue-se que $k(C_x) \neq \emptyset$. Assim, podemos associar para cada $x \in \Re_1$, o conjunto, não vazio, $k(C_x) \in \Re_2$. Vamos mostrar que ele admite supremo. Dado $z \in k(C_x)$, temos que existe um $v \in C_x$ tal que $z = k(v)$. Ora, $v < x$, e como $\Re_1$ é arquimediano existe um natural $n$ tal que $x < n$. Disso resulta que, $v < x < n$, o que implica em $k(v) < k(x) < k(n)$, ou seja, $z < k(n)$. Portanto, concluímos que $k(n)$ é uma cota superior de $k(C_x)$. Pelo axioma da completude, $k(C_x)$ possui supremo $\sup k(C_x)$. Portanto, $f$ é uma função que associa $x \in \Re_1$ ao supremo $\sup k(C_x)$.

2. $f$ é uma extensão de $k : \mathbb{Q}_1 \to \mathbb{Q}_2$ . Vamos mostrar que $f(x) = k(x)$, para todo $x \in \mathbb{Q}_1$. Com efeito, dado $z \in k(C_x)$, sabemos que existe um $v \in C_x$ tal que $z = k(v)$. Ora, $v < x$, o que implica $k(v) < k(x)$, isto é, $z < k(x)$. Assim, vemos que $k(x)$ é uma cota superior de $k(C_x)$. Logo, $\sup k(C_x) \leq k(x)$. Suponha, $\sup k(C_x) < k(x)$. Pela observação acima, existe um $q \in \mathbb{Q}_1$ tal que $\sup k(C_x) < k(q) < k(x)$. Resulta da observação acima que $q < x$, ou seja, $q \in C_x$. Assim, vemos que $k(q) \in k(C_x)$, o que é uma contradição de $k(q) < \sup k(C_x)$. Portanto, devemos ter $\sup k(C_x) = k(x)$.

3. $f(x+y) = f(x) + f(y)$, para quaisquer $x, y \in \Re_1$. Usando a definição de $f$, os lemas 5.1 (5) e 5.4 (I) e o Corolário 5.6.1 (1), temos

$$f(x+y) = \sup k(C_{x+y}) = \sup k(C_x + C_y) = \sup[k(C_x)+k(C_y)] = \sup k(C_x)+\sup k(C_y)$$

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

4. $f(xy) = f(x)f(y)$, para quaisquer $x, y \in \Re_1$. Vamos considerar cinco casos.

   4.1 Suponha, $x > 0$ e $y > 0$. Então, $xy > 0$. Usando a definição $f$, o lema 5.4 (II), e os Corolários 5.4.1 (3) e 5.6.1 (2) vemos que

   $$f(xy) = \sup k(\overline{C_{xy}}) = \sup k(\overline{C_x} \cdot \overline{C_y}) = \sup[k(\overline{C_x}) \cdot k(\overline{C_y})] = \sup[k(\overline{C_x})] \cdot \sup[k(\overline{C_y})]$$

   $$= f(x)f(y).$$

   4.2 Suponha, $x = 0$ ou $y = 0$. Então, $f(0) = k(0) = 0$. Sem perda de generalidade, considere $y = 0$. Portanto, vemos que $f(x \cdot 0) = f(0) = 0 = f(x) \cdot 0 = f(x)f(0)$.

   4.3 Suponha, $x > 0$ e $y < 0$. Então, $-y > 0$. Note que, $f(-x) = -f(x)$(verifique!). Assim, temos

   $$f(xy) = f(-(-x)y) = -f((-x)y) = -[f(-x)f(y)] = -[-f(x)f(y)] = f(x)f(y).$$

4.4 Suponha, $x > 0$ e $y < 0$. Esse passo é análogo ao passo (4.3), portanto, omitiremos o seu desenvolvimento.

4.5 Suponha, $x < 0 e y < 0$. Então, $-x > 0 e - y > 0$. Assim, temos sucessivamente,

$$f(xy) = f((-x)(-y)) = f(-x)f(-y) = [-f(x)][-f(y)] = f(x)f(y).$$

5. Suponha, $x < y$. Então, $C_x \subseteq C_y$, o que implica $k(C_x) \subseteq k(C_y)$. Segue-se do Lema 5.1 (7), que $\sup k(C_x) \leq \sup k(C_y)$, isto é, $f(x) < f(y)$.

6. $f$ é injetiva. Com efeito, o quinto passo, garante que $f$ é injetiva.

7. $f$ é sobrejetiva. A demonstração desse passo é mais elaborada. Para melhor entendimento, descrevemos as ideias fundamentais que devemos ter em mente. A sobrejetividade de $f$ é provada, desde que para todo $b \in \Re_2$, tenhamos, sempre, um $a \in \Re_1$, tal que $f(a) = b$. Ora, sabemos que $b = \sup C_b = \sup\{w \in \mathbb{Q}_2 | w < b\}$,para todo $b \in \Re_2$. Assim, devemos ter $\sup k(C_a) = b$. Para que isso aconteça, devemos mostrar que $C_a = k^(-1)(C_b)$, ou seja, devemos mostrar que $W = k^{-1}(C_b)$ é não vazio e limitado superiormente, cujo supremo é $\sup W = a$ e tal que $C_a = W$.

**Demonstração**: Suponha, $b \in \mathbb{Q}_2$. Como $k : \mathbb{Q}_1 \to \mathbb{Q}_2$ é bijetiva, existe um $a \in \mathbb{Q}_1$ tal que $b = k(a) = f(a)$. Agora, suponha $b \notin \mathbb{Q}_2$. Baseando-se na ideia acima, seja $W = k^{-1}(C_b)$. Levando em consideração que $(C_b) \neq \emptyset$ e $k$ é bijetiva, vemos que $W = k^{-1}(C_b) \neq \emptyset$. Ora, sabemos que $C_b \subseteq \mathbb{Q}_2$. Então existe um natural $n$ tal que $b < n$. Como $n \in \mathbb{Q}_2$, existe um $p \in \mathbb{Q}_1$ tal que $k(p) = n$. Assim, se $x \in W$, então $k(x) < b$, e portanto, $k(x) < k(p)$. Disso resulta que, $x < p$. Deduzimos que $p$ é uma cota superior de $W$. Seja $a = \sup W$. Vamos mostrar que $a \notin Q_1$. Suponha o contrário, $a \in \mathbb{Q}_1$. Então, $f(a) = k(a)$. Sabemos que podemos ter $k(a) = b$, ou $k(a) < b$, ou $k(a) > b$. A primeira possibilidade não pode ocorrer, pois, teríamos $b = k(a) \in \mathbb{Q}_2$. Mas isso, contradiz a suposição inicial de que $b \notin \mathbb{Q}_2$. Suponha, $k(a) < b$. Então, existe um racional $q$ tal que $k(a) < k(q) < b$. Disso resulta que, $a < q$. Segue-se que, $q \in W$, o que contraria a suposição de que $a = \sup W$. Suponha, $k(a) > b$. Logo, existe um racional $q$ tal que $b < k(q) < k(a)$. Disso resulta que, $q < a$. Como $a = \sup W$, existe um $r \in W$ tal que $q < r < a$. Assim, temos $k(q) < k(r)$, ou seja, $k(r) > b$, o que é um absurdo (pois, sendo $r \in W$ deveríamos ter $k(r) < b$). Portanto, devemos ter $a \notin \mathbb{Q}_1$.

Agora, vamos mostrar que $W = C_a$, onde $a = \sup W$ . Com efeito, seja $u \in W$. Como $a = \sup W$ e $u \in \mathbb{Q}_1$, então de $u \leq a$, resulta $u < a$, pois, $a \notin \mathbb{Q}_1$. Assim, vemos que $u \in C_a$, e portanto, $W \subseteq C_a$. Agora, seja $w \in C_a$. Então, w é um racional tal que $w < a$. Como $a = supW$, resulta que existe um $q \in W$ tal que

$w < q < a$, o que implica $k(w) < k(q) < b$. Assim, $w \in W$, logo, $C_a \subseteq W$. Portanto, vemos que $W = C_a$.

■

# Capítulo 7

# Considerações históricas

Quando se comenta a história dos números no mundo antigo, é comum levar em conta a forma como eles eram escritos em diferentes civilizações, poderíamos tomar como exemplo, na civilização da antiga Roma, os algarismos romanos. Do ponto de vista da análise real, porém, pouco interessa a forma como eles eram escritos em diferentes períodos da história, mas como foi adquirido, ao longo da história, o conceito de número, ou seja, a forma como entendemos hoje como números reais. Na análise real, fazemos o uso extensivo das propriedades dos números reais, o que eles são e como se comportam, e não o uso da forma como eles são escritos.

Os números reais da forma como entendemos , agora, e da forma que usamos em análise real, inclui os números naturais (inteiros positivos), o zero, os inteiros negativos, os números racionais que não são inteiros, os números irracionais algébricos ( aqueles números irracionais que são raízes dos polinômios de coeficientes inteiros) e transcedentes (aqueles que não são algébricos). Vamos, resumidamente, relatar o desenvolvimento do conceito de números reais em cinco períodos da história: Mundo antigo, medieval, renascentista, século XVII e século XIX.

Nos primeiros relatos história da humanidade, o primeiro sistema de números conhecido pelo homem, embora conhecido de uma maneira empírica e rudimentar, era o sistema de números naturais. Eles eram usados, tão somente, para contagem de objetos. Cada civilização, de acordo com sua cultura, apresentavam formas simbólicas de representação e, também, de como elas as operavam ( adiciona e multiplica). Em algumas culturas, faziam-se o uso das razões (frações) desses números, constatando-se o aparecimento dos números racionais, sem, no entanto, saber que eles existiam. No antigo oriente médio e Europa, a palavra "número" significava os inteiros positivos e suas razões (frações). Na antiga China e Índia, até um certo ponto, os números negativos e o zero, foram entendidos como números e já tinham conhecimento sobre suas operações de adição e multiplicação. Os textos antigos em várias civilizações antigas, apresentavam o cálculo de $\sqrt{2}$ e do número $\pi$ em valores aproximados de números racionais. No entanto, apesar de ter sido conhecido

que tais aproximações não fossem o valor exato desses números, já se sabiam que na antiga China, Mesopotânia, Egito e Índia, que o tal valor exato não podia ser representado por meio de razões entre números inteiros. Na antiga Grécia, foi descoberto a ideia de relações de pares incomensuráveis de segmentos de retas. Essa relações representam de longe o que chamamos de números irracionais. Pitágoras e seus seguidores, sabiam que $\sqrt{2}$ é um número irracional, expresso geometricamente, em termos de pares de incomensuráveis (por exemplo, a diagonal e o lado do quadrado). Apesar dos Gregos terem conhecimento dos comprimentos incomensuráveis de segmentos, esta descoberta não levou à adoção de que os números irracionais (tal como $\sqrt{2}$ e outros, até então conhecidos naquela época) eram considerados números. Isto foi devido, talvez, à separação rígida que os gregos tinham entre Aritmética e Geometria. Essa separação, era reforçada pelo sábio Aristóteles (384-322 A.C), em seu livro VI sobre Física, no qual enfatizou a distinção entre as palavras "número" e "magnitude". A primeira, Aristóteles entende como quantidade discreta e indivisível; a segunda, como quantidade contínua e que não possuem indivisíveis, como por exemplo, os comprimentos de segmentos, áreas de regiões planas, tempo e outros objetos de significado físico (grandezas físicas). Essa distinção prevaleceu por vários séculos. No Livro VII dos Elementos de Euclides existe uma teoria sobre relações de números, que corresponde ao que chamamos de frações. No Livro V dos Elementos há uma teoria sobre proporções, ou seja, relações entre magnitudes. As duas magnitudes em uma proporção devem ter a mesma grandeza, embora se possa comparar grandezas de espécies diferentes. Nesta teoria, ainda, é estabelecida as definições de ordem, adição e multiplicação para razões(frações) de magnitudes e enunciado o princípio de Arquimedes. A teoria de proporções é muito importante para um certo número de teoremas dos Elementos de Euclides, por exemplo, quando é necessário indicar o fato de que as áreas de dois círculos possuem a mesma proporção como os quadrados dos seus diâmetros. Em alguns aspectos desta teoria prefigura a idéia de Cortes de Dedekind formuladas por Dedekind em 1858. A teoria das proporções é atribuído a Eudoxo de Cnidus (408-355 A.C).

Na idade medieval, os matemáticos da antiga Índia, estavam mais interessados em álgebra e cálculos numéricos do que os antigos gregos. Os indianos, ao contrário dos gregos, não tinha as restrições filosóficas no que diz respeito aos números. Esta liberdade para desenvolver os números, eventualmente, contribuiu para o desenvolvimento do cálculo. Na antiga Índia, os números inteiros negativos e o zero, eram reconhecidos, de fato, como números. Brahmagupta, em sua obra **Brahmasphutasiddhanta** (628 D.C ), considera o zero como o resultado a subtração entre dois números iguais, além disso, construiram regras para adição, subtração e multiplicação de números inteiros e o zero, embora não entendesse a divisão por zero. Com o desenvolvimento da Álgebra e da Geometria Analítica, passou-se a reconhecer os números reais como números. A álgebra de *Al-Khwarizmi* (780-850, D.C), em sua grande obra, datada em torno de 825, permitia que diferentes tipos de números,

racionais e irracionais fossem ser tratados de uma forma mais uniforme do que acontecia anteriormente. A indefinição da distinção entre diferentes tipos de números foi ainda mais reforçada por **Abu Kamil Shuja ibn Aslam** (850-930), cujo trabalho sobre álgebra era influenciado por **Leonardo de Pisa** (1170-1250), também conhecido como Fibonacci. Ele difundiu a Álgebra árabe, na Europa através de seu livro Liber ábacos de 1202. O matemático árabe **Al-Baghdadi** (980-1037) fez cair por terra a antiga tradição distinção grega entre número e magnitude e estabeleceu uma correspondência geométrica entre número e comprimento de segmento de reta onde consideramos números racionais aqueles segmentos de reta cujos comprimentos são múltiplos e submúltiplos de segmentos de comprimentos tomados como unidade fixa, e números irracionais aos segmentos de retas cujos comprimentos não podem ser tomados como múltiplos e submúltiplos de comprimento de segmentos tomados como unidade fixa. Além disso, ele demonstrou a densidade dos números irracionais. Outro matemático que contribui para o desenvolvimento da noção de número, neste período da história, foi Nicole Oresme (1323-1382). Ele foi o precursor da Geometria Analítica ao estabelecer a noção de coordenadas, por volta de 1350, e mais, a levantar o questionamento de saber o significado de um número escrito como uma potência de expoente irracional, problema esse resolvido, séculos mais tarde, com o rigor da matemática do século 19. Em paralelo com a disseminação da álgebra do mundo árabe para a Europa, foi a difusão do sistema de valor posicional decimal, ou simplesmente, sistema decimal. O sistemas de valor posicional para representar números (embora não tinha sido escrito na forma como a conhecemos) foram criados, separadamente, na antiga Mesopotâmia, Índia, China e América Central. O sistema Maya de números simbolizava o zero como marcador de posição e tinha base 20, ou seja, os números eram representados, por diferentes combinações, usando um dos 20 símbolos. Na Mesopotânia, o sistema de números era de base 60, embora nesse sistema não tivesse inicialmente o zero. Na índia e China, a base utilizada era 10 ( chamado decimal). O sistema indo-arábico que usamos para escrever os números de hoje, isto é, sistema de valor posicional decimal, tem três aspectos: o valor do símbolo em função da posição que ele ocupa no número, a base 10, e que possui 10 símbolos Hindo-Árabe, a saber: 0,1,..,9. O sistema de valor decimal para escrever números inteiros, incluindo o uso do zero tem sua origem na Índia, aparecendo, por volta do século 7, e totalmente desenvolvido por volta do século 8. O primeiro trabalho árabe que usou o sistema indiano para escrever números inteiros é a obra **Kitab al-jam wal-tafriq bi hisab al Hind** de **Al-Khwarizmi**, na qual apresenta algoritmos para adição, subtração, multiplicação, divisão. A tradução latina deste trabalho ajudou a disseminar o sistema de valor posicional decimal.

Voltando a questão sobre a irracionalidade de números, embora os matemáticos indianos e árabes considerassem os números irracionais como números, os antigos gregos e matemáticos da europa medieval não consideravam os irracionais como números, pelo menos até o século 16, quando a álgebra Hindu-arábica foi amplamente

adotada na Europa. Os números negativos que dois séculos antes não eram aceitos passaram a ser usados neste período, mas com o estigma de falsi numeri ou ficti numeri. Somente séculos depois, os números negativos foram aceitos, de fato, como números, sem estigma. Até o período da renascentista, o número 1 ainda não era considerado como número na Europa, em particular, na Grécia. Foi a partir do trabalho de Stevin, em sua obra L'arithmétique, é que número 1 foi amplamente aceito como tal. Embora, o zero ainda por Stevin não fosse considerado como número, não existia mais a distinção entre números e magnitude. A partir desse fato é que os números irracionais foram considerados, na Europa, como números.

No século 17, com o desenvolvimento da Geometria Analítica devido aos trabalhos simultâneos e independentes de Pierre de Fermat (1601-1665) e Rener Descarte (1596-1650) os números reais foram amplamente reconhecidos como números. Descartes retirou, em seu trabalhos sobre Geometria Analítica, a distinção números e comprimentos de segmentos de retas e estabeleceu uma correspondência geométrica entre o conjunto de comprimentos de segmentos de reta (associados a pontos da reta) e o conjunto de números reais. Neste século, foi deixado de lado a ideia unilateral de que os números representam quantidades de coisas numa coleção de objetos, e passam a representar ou associar entes abstratos, ou seja, os números foram aceitos como puros números, desvinculados da noção de quantidade de objetos ou comprimentos de segmentos. Por outro lado, os números reais ainda eram associados às ideias geométricas tais como comprimentos de segmentos de reta. Esta associação geometrica junto com a noção de continuidade da reta de números reais permitiu aos matemáticos a ter uma visão intuitiva de limites de sequência de números. No entanto, esta ligação geométrica levou a uma dependência intuitiva que impedia a necessidade de uma abordagem rigorosa para os números reais, por muito tempo. Gottfried von Leibniz (1646-1716) foi o primeiro matemático a distinguir duas categorias de números: números algébricos (como, por exemplo, é o caso do número $\sqrt{2}$) e os números transcedentes (como, por exemplo, é o caso do número $\pi$).

Em meados do século 19, Carl Friedrich Gauss (1777-1855) usou, informalmente, a ideia de supremo marcando assim, um passo a frente no desenvolvimento dos números reais, porém isso não proporcionou ainda uma construção de números reais. Gauss, tinha a antiga noção dos números reais como uma variação contínua, tomando isso como uma ideia intuitiva básica para análise real. Na primeira metade do século 19, o primeiro matemático a tentar a construir os números reais a partir dos números racionais foi Bernard Bolzano (1781-1848). Ele definiu números reais em termos de sequências de números racionais, sem, no entanto, fazer isso com detalhes e provou a propriedade do supremo supondo de antemão que as sequência de Cauchy são convergentes, a prova dessa suposição feita por ele, seria usada na tentativa de construção dos números reais, porém, não estava correta, levando a tenativa de construção dos números reais feita por Bolzano ao fracasso. Apesar das falhas encontradas em seu trabalho, ele tem mostrado muito perspicácia para essa

época. A não publicação dessas ideias não trouxe uma influência para os trabalhos posteriores de outros matemáticos. A tentativa por Augustin Louis Cauchy (1789-1857) de colocar o cálculo em uma base firme de fundamentação foi um grande avanço no desenvolvimento da análise real, mas sua visão dos números não escapava do paradigma da sua época e, portanto, não foi tão perspicaz como a abordagem de Bolzano. Num livro sobre um curso de análise em 1821, Cauchy usou o fato de que os números irracionais são limites de sequências de números racionais, porém numa perspectiva de Cauchy isso não era uma definição de números irracionais , mas uma observação sobre esses tais números, o que confirma simplesmente sua existência. Cauchy implicitamente, assumiu que as sequências que levam seu nome são convergentes, o que é verdade dentro de uma visão intuitiva que se tinha naquela época acerca dos números reais (vistos como "contínuos"). Na perspectiva atual, esse fato exige uma prova e essa prova requer uma construção dos números reais e uma axiomatização deles. William Rowan Hamilton (1805-1865), em um esforço para esclarecer o significado de números negativos e imaginários na década de 1830, deu uma definição de números negativos usando uma construção semelhante a que conhecemos sobre a construção dos inteiros a partir dos números naturais. Então, ele construi os números racionais a partir dos números inteiros, e tentou, embora sem êxito, a construção dos números reais a partir dos números racionais. Usando os números reais, no entanto construído, ele forneceu uma construção moderna dos números complexos a partir dos números reais. Neste mesmo período do século, o matemático Joseph Liouville (1809-1882), em 1844, apresentou a primeira prova da existência de números transcedentes. Charles Hermite (1822-1901) mostrou que o número e é transcedente em 1873, e Ferdinand von Linderman (1852-1939) provou que $\pi$ é transcedente em 1882. Apesar dos trabalhos anteriores de Bolzano e de Hamilton, foi somente na segunda metade do século 19 que houve um amplo esforço no sentido de abordar os números reais com o rigor num plano aritmético (aritmetização), em oposição a visão intuitivamente geométrica, ou seja, os números reais serem baseados apenas sobre os números racionais ( que por sua vez, é baseado nos números inteiros).

Antes do século 19, os números reais, de uma forma geral, eram associados à noção de quantidade objetos de uma coleção, à noção de comprimentos de segmentos geométricos (contínuos da reta), ou seja, grandezas geométricas, e grandezas físicas ( grandezas do mundo real), ou, no máximo vistos como abstrações de coisas que possuem significado. Até o final do século 19, a abordagem sobre números reais havia mudado, levando assim a uma visão mais moderna sobre eles. Esta transição contribui tanto para o desenvolvimento da noção de número por si só, e também para o desenvolvimento da teoria dos conjuntos como fundamentação da matemática (e em particular, como base para axiomatização dos números reais). A falta de um tratamento rigoroso dos números reais impede que o cálculo se apoie numa base sólida, sem uma boa compreensão dos números reais, não é possível dar provas

completas de alguns resultados importantes do cálculo. Um exemplo disso, seria a prova de Bolzano e Cauchy sobre o Teorema do Valor Intermediário que usa, de uma forma implícita, o teorema da convergência monótona, teorema este que, na época, não tinha sido provado, mais ainda, este teorema foi usado implicitamente por Cauchy e Riemann para provar que certos tipos de função era integrável. Portanto, para provar a Monotonicidade do teorema da convergência era necessário usar as propriedades fundamentais (e típicas) dos números reais.

Possivelmente, a primeira construção rigorosa dos números reais a partir do racional números deveu-se a Richard Dedekind (1831-1916), que trabalhou a sua construção em palestras em 1858, fazendo o uso de provas que não se baseassem em fatos geométricos, no intuito de fornecer uma base para um curso de análise real. Dedekind foi cauteloso em não publicar suas ideias até o ano de 1872, quando percebeu que Heine e Cantor estavam prestes a publicar suas versões sobre construção dos números reais. O método de Dedekind com base no que hoje chamamos de "cortes", relembra a abordagem de Eudoxus para teoria das proporções encontrada no livro V dos Elementos de Euclides. Vale frisar que o nome "Corte de Dedekind" não foi usado pelo próprio Dedekind em seu livro Stetigkeit irrationale und Zahlen, devendo-se o uso desse nome, atualmente, ao matemático e filósofo Bertrand Russell (1872-1970) . Outra matemático que construi os números reais a partir dos números racionais e que parece ter apresentado, pela primeira vez, suas ideias sobre números reais em palestras, em 1863, foi karl Weierstrass (1815-1897). Apesar de Weierstrass ter apresentado suas ideias em palestras, ele não as publicaram. Existia uma visão comum entre as ideias de Dedekind e Weierstrass, com o objetivo de fornecer uma base sólida para análise real, removendo todo raciocínio geométrico intuitivo da análise real, baseando a prova da construção dos números reais, por si só, na ideia aritmética de número. Weierstrass, deu uma definição, numa perspectiva puramente aritmética, de número irracional, dizendo que o mesmo é um "agregado" de números racionais que intuitivamente convergem para um número.

Charles Méray (1835-1911), inicialmente em 1869, e mais precisamente em 1872, definiu convergência de sequências de números racionais usando a condição de Cauchy, e em seguida, definia números irracionais como sequências de Cauchy que não convergem para limites racionais, porém a ideia apresentada por Méray não era inteiramente rigorosa. Independentemente de Méray, pelo menos aparentemente, George Cantor (1845-1918) teve a ideia de usar as sequências de Cauchy de números racionais para definir os números reais. Somente em 1872, é que essa ideia foi retomada por um colega de Cantor, chamado Eduard Heine (1821-1881) que forneceu um tratamento rigoroso desta abordagem via classes de equivalência. A busca do rigor em se construir os números reais levou os matemáticos do século 20, a pensar numa fundamentação axiomática na teoria dos conjuntos. Fundamentação esta que veio posteiormente, com os trabalhos de Cantor, Frankael e Skolen.

# Referências Bibliográficas


[1] A. A. E. Silva, *Uma introdução Axiomática dos Conjuntos*. Editora Universitária UFPB, 2011.Ed 1ª.

[2] A. Hefez, *Curso de Álgebra*, vol. 1. Coleção Matemática Universitária, IMPA/CNPq, Rio de Janeiro, 1993.

[3] D. G. Figueiredo, *Análise I*, 2ª edição. Livros Técnicos e Científicos. Editora, Rio de Janeiro, 1996.

[4] Elon.L. Lima, *Curso de análise*, Vol. 1, IMPA, Rio de Janeiro, 2004.

[5] Ethan D. Bloch, *The real numbers and Real Analysis*, Springer, New York, 2010.

[6] J.Ferreira, *A Construção dos Números*. Editora SBM, Rio de Janeiro, 2011. Ed 2ª.

[7] Manfred Stoll, *Introduction to Real Analysis*, 2nd ed., Addison-Wesley, Boston,2001.

[8] P. R. Halmos, *Teoria Ingênua dos Conjuntos*. Editora Universidade de São Paulo e Editora Polígono, São Paulo, 1970.

[9] William F. Trench, *Introduction to Real Analysis*, Prentice Hall, Upper Saddle River, NJ, 2003.