



UNIVERSIDADE FEDERAL DO PIAUÍ
CENTRO DE CIÊNCIAS DA NATUREZA
PÓS-GRADUAÇÃO EM MATEMÁTICA
MESTRADO PROFISSIONAL EM MATEMÁTICA - PROFMAT

Um Estudo Rigoroso do Conjunto dos Números Reais

Gideône Barros Mendes

Teresina - 2016

Gideône Barros Mendes

Dissertação de Mestrado:

Um Estudo Rigoroso do Conjunto dos Números Reais

Dissertação submetida à Coordenação do Programa de Pós-Graduação em Matemática, da Universidade Federal do Piauí, como requisito parcial para obtenção do grau de Mestre em Matemática.

Orientador:

Prof. Dr. Roger Peres de Moura

Teresina - 2016



UNIVERSIDADE FEDERAL DO PIAUÍ - UFPI
CENTRO DE CIÊNCIAS DA NATUREZA
CENTRO DE EDUCAÇÃO ABERTA E À DISTÂNCIA
MESTRADO PROFISSIONAL EM MATEMÁTICA EM REDE NACIONAL - PROFMAT

Dissertação de Mestrado submetida à coordenação Acadêmica institucional, na Universidade Federal do Piauí, do Programa de Mestrado Profissional em Matemática em Rede Nacional para a obtenção do grau de **mestre em Matemática** intitulada: **Um estudo Rigoroso do Conjunto dos Números Reais**, defendida por *Gideône Barros Mendes* em 05/08/2016 e aprovada pela banca constituída pelos professores:

Prof. Dr. Roger Peres de Moura
Presidente da Banca Examinadora

Prof. Dr. João Benício de Melo Neto
Examinador

Prof. Dr. Gleison do Nascimento Santos
Examinador Externo

FICHA CATALOGRÁFICA

Serviço de Processamento Técnico da Universidade Federal do Piauí

Biblioteca Setorial do CCN

M538e Mendes, Gideône Barros.

Um estudo rigoroso do conjunto dos números reais / Gideône Barros Mendes. - Teresina, 2016. 66f.: il.

Dissertação (Mestrado Profissional) - Universidade Federal do Piauí, Centro de Ciências da Naturaza, Pós-Graduação em Matemática, 2016.

Orientador: Prof. Dr. Roger Peres de Moura.

1. Números Reais. 2. Teoria dos Números. 3. Relações de Equivalência. I. Título

CDD 512.7

Dedico esta dissertação a:

Vitória Fernanda minha amada esposa, ao meu pai Francisco Mendes, ao meu irmão Otoniel Mendes; e aos meus avós *Maria de Jesus e Carivaldo Mendes (in memoriam)*.

Agradecimentos

Agradeço primeiramente a Deus por me conceder a oportunidade de poder concluir mais uma etapa em meus estudos, a Ele seja toda honra e toda glória. Quero agradecer também ao meu pai, Francisco Mendes, por sempre ter me apoiado, ao meu irmão que sempre acreditou em meu potencial, o meu sincero agradecimento. Não posso esquecer dos meus colegas de graduação, Alexson, Raimundo Nonato, Eder, José Carlos, Milena, Flávio, Franciane, João Luis, Roberto, entre outros, obrigado por todos os momentos de aprendizado e descontração juntos.

Agradeço aos meus amigos do PROFMAT, Fernando, Gilson Amorim, Delano Moura, Pedro, Rubens, Gerson, Samuel, Reneé, Bruno, Huerlen, Vivian, Leonardo, Raimundinho, Kelson, Itaércio, Egilberto, Josemar, Felipe, Aline pela ajuda e os valorosos dias de estudo durante todo o curso.

Agradeço a todos os professores do PROFMAT por todo o conhecimento a nós transmitido no período no curso.

Agradeço a todos os colegas de trabalho que sempre torceram por mim, entre os quais destaco, Joaquim Giovanni, Francisco Dias e Sandra Caminha, obrigado pela ajuda.

O meu muito obrigado a minha amada esposa Vitória Fernanda que durante esse curso sempre esteve ao meu lado, me ajudando sempre que possível, me incentivando naqueles momentos mais difíceis e sempre acreditando que eu era capaz de concluir mesmo perante as imensas dificuldades, muito obrigado, Te amo!

Agradeço também a meu orientador professor Dr. Roger Peres de Moura, que muito me ajudou nesta dissertação, com dicas e sugestões imprescindíveis para a conclusão deste trabalho.

Agradeço também ao professor Dr. João Benício de Melo Neto e ao professor Dr. Gleison do Nascimento Santos por terem aceitado participar da banca.

“Quem é sábio, que entenda estas coisas;
quem é prudente, que as saiba, porque os
caminhos do SENHOR são retos, e os jus-
tos andarão neles, mas os transgressores
neles cairão.”

Oséias 14.9

Resumo

O presente trabalho tem por objetivo ser uma ferramenta para professores de nível básico e estudante de graduação para a compreensão e estudo mais rigoroso dos números reais. Para tanto efetuamos a construção dos números reais via Cortes de Dedekind, mas usando o conceito de ínfimo em vez de empregar o de supremo, como é de praxe. Inicialmente faremos um apanhado dos conteúdos indispensáveis para o desenvolvimento do tema principal da dissertação. No segundo capítulo abordamos a construção do conjunto dos números racionais e suas principais propriedades, por exemplo, sua enumerabilidade. No terceiro capítulo, para motivar a construção dos números reais, começamos falando sobre segmentos comensuráveis, segmentos incomensuráveis e a existência de grandezas que não são racionais. No mesmo capítulo fazemos a construção dos números reais empregando a ideia cortes de Dedekind. Finalizamos o trabalho com algumas aplicações, a saber, o estudo do valor absoluto e a representação decimal de um número real.

Palavras-chave: Números Reais, Cortes de Dedekind, Relação de equivalência.

Abstract

This present work has as aim to be a tool for entry-level teachers and undergraduate students for understanding and more rigorous study of real numbers. Therefore we have made the construction of the real numbers through Dedekind cuts, but using the concept of infinitesimal instead of employing the supreme, as usual. Initially we will make an overview of the essential subject to the development of the main theme of the dissertation. In the second chapter we discuss the construction of the set of rational numbers and their main properties, for example, your enumerable. In the third chapter, to motivate the construction of real numbers, we started talking about commensurable segments, incommensurable segments and the existence of quantities that are not rational. In the same chapter we make the construction of the real numbers using the idea of cuts Dedekind. We will finished the work with some applications, namely the study of the absolute value and the decimal representation of a real number.

Keywords: Real Numbers, Dedekind Cuts, equivalence Relation.

Sumário

Resumo	iv
Abstract	v
1 Relações Binárias e Funções	4
1.1 Definições Básicas	4
1.2 Relações de equivalência	8
1.3 Relações de Ordem	12
1.4 Funções ou Aplicações	16
2 O Conjunto \mathbb{Q} dos Números Racionais	18
2.1 Construção dos Números Racionais	18
2.2 Operações em \mathbb{Q}	19
2.2.1 Adição em \mathbb{Q}	19
2.2.2 Multiplicação em \mathbb{Q}	21
2.3 Relação de ordem e enumerabilidade de \mathbb{Q}	22
3 O Conjunto dos Números Reais	25
3.1 Algumas limitações de \mathbb{Q}	25
3.1.1 Segmentos Comensuráveis e Segmentos Incomensuráveis	26
3.2 A História do número π	27
3.3 Cortes de Dedekind	29
4 Aplicações	40
4.1 Função maior inteiro	40
4.2 Intervalos e Valor absoluto	41
4.3 Representação decimal dos números reais	46

Sumário	vii
4.3.1 Dízimas Periódicas	50
4.4 Considerações Finais	51
Referências Bibliográficas	52

Introdução

Você em algum momento já se perguntou como se deu a criação dos números? Ou como os usamos a quase todo instante no nosso dia a dia? O homem criou os números devido a sua necessidade e nós já estamos tão acostumados com eles que às vezes parece que sempre existiram. Eles são tão comuns, presentes e necessários que não imaginamos nossa vida sem eles. O conceito de Número Real no estudo de Matemática é de fundamental importância, nos mais diversos níveis que se possa ocorrer este estudo.

A compreensão de tal conceito é essencial para que se possa discutir com segurança aspectos como determinação correta do conjunto Domínio e do conjunto Imagem de uma dada função, na delimitação correta de um conjunto solução de uma dada inequação, enfim, entre outras inúmeras situações, reconhecer com segurança a racionalidade ou a não racionalidade de um dado número.

O presente trabalho tem como principal objetivo a construção dos números reais. Para atingí-lo, o primeiro capítulo, Relações Binária e Funções, introduz a terminologia de conjuntos e funções que será utilizada no restante do trabalho. Já no segundo capítulo, O Conjunto dos Números Racionais \mathbb{Q} , mostraremos a construção de \mathbb{Q} a partir das relações de equivalência, apresentaremos as principais propriedades deste conjunto e ainda mostraremos que o mesmo é arquimediano. No terceiro capítulo faremos a construção do conjunto dos números reais via cortes de Dedekind, entretanto definimos um corte de maneira diferente da original, para isso consideramos cortes racionais limitados inferiormente. Um trabalho árduo entretanto prazeroso que nos propocionará uma melhor compreensão sobre o que é um número real.

O quarto capítulo é apenas uma pequena abordagem sobre intervalos, valor absoluto de um número real (algumas de suas principais propriedades), e ainda falamos um pouco sobre a representação decimal de um número real. A abordagem mesmo sutil é de fundamental importância pois visa dar um esclarecimento para o leitor de tópicos usados de

maneira bastante intensa na educação básica. O uso de expressões decimais e de inequações modulares na 1ª série do Ensino Médio muitas vezes causa nos alunos uma certa dificuldade, e este capítulo busca amenizar tais dificuldades.

Para finalizar esta parte apresentamos a seguir um pouco da história da teoria dos números reais. Tudo começou com o surgimento dos números naturais, tais números surgirão devido a necessidade do homem expressar o resultado de uma contagem. Os números inteiros surgiram na época do Renascimento, quando os matemáticos começaram a sentir a necessidade de contar com números específicos para garantir a boa resolução de equações simples. Eram necessários números e símbolos que pudessem representar temperaturas acima e abaixo de 0°C e tantas outras necessidades das ciências.

Diante disso, os cientistas, físicos, astrônomos e matemáticos começaram a buscar uma nova linguagem matemática capaz de expressar diversos fenômenos. Dessa forma, foi criado o conjunto dos números inteiros, que reúne os números naturais, os números opostos dos números naturais e o zero, [7].

Os Números racionais surgiram da necessidade de representar partes de um inteiro. No Egito Antigo, durante inundações do Rio Nilo, muitas terras ficavam submersas, e isso fazia com que elas recebessem nutrientes. Essas terras tornavam-se muito férteis para a agricultura. Dessa forma, quando as águas baixavam, era necessário remarcar os limites entre os terrenos de cada proprietário. No entanto, por mais eficientes que tentassem ser, não encontravam um número inteiro para representar tais medidas, o que os levou à utilização de frações, [11].

A origem histórica da necessidade de criação dos números não racionais está intimamente ligada com fatos de natureza geométrica e de natureza aritmética. Os de natureza geométrica podem ser ilustrados com o problema da medida da diagonal do quadrado quando a comparamos com o seu lado, [17].

A atenção de Dedekind se voltara para o problema dos números não racionais desde 1858, quando dava aulas de Cálculo. Segundo ele o conceito de limite deveria ser desenvolvido através da aritmética apenas, sem usar a geometria como guia. Em vez de simplesmente procurar uma saída do círculo vicioso de Cauchy, Dedekind se perguntou o que existia na grandeza geométrica que a diferenciava dos números racionais. Galileu e Leibniz tinham julgado que a “continuidade” de pontos sobre a reta era consequência de sua densidade, isto é, do fato de que entre dois pontos quaisquer sempre existe um

terceiro. Porém os números racionais têm essa propriedade, no entanto não formam um *continuum*. Ao refletir sobre a questão, Dedekind chegou a conclusão de que a essência da continuidade de um segmento de reta não se deve a uma vaga propriedade de ligação mútua, mas a propriedade exatamente oposta, a natureza da divisão do segmento em duas partes por um ponto sobre o segmento.



Figura 1: Richard Dedekind.

Dedekind viu que o domínio dos números racionais podia ser estendido de modo a formar um *continuum* de números reais se supusermos o que agora se chama o axioma Cantor-Dedekind, que os pontos da reta podem ser posto em correspondência biunívoca com os números reais. Isto significa que para toda divisão dos números racionais em duas classes A e B de modo que todo número da primeira classe, A, é menor que todo número da segunda classe, B, existe um e só um número real que produz esse corte de Dedekind. Se A tem um maior elemento ou B tem um menor elemento, o corte define um número racional, caso contrário o corte define um número não racional. Em outras palavras a ideia de Dedekind era representar cada número real como um corte nos números racionais.

No começo do século XX uma modificação do corte de Dedekind foi proposta por Bertrand Russell (1872-1970). Ele notou que como qualquer das duas classes A, B de Dedekind é univocamente determinada pela outra, uma só basta para a determinação de um número real. Assim por exemplo $\sqrt{2}$ pode ser definido simplesmente como o segmento ou subclasse do conjunto dos números racionais formando todos os números racionais positivos cujos quadrados são menores que dois e também todos os números racionais negativos; semelhantemente, todo número real nada mais é que um segmento do sistema dos números racionais, [1] páginas 390 e 391.

Uma das maiores contribuições de Dedekind foi talvez a de possibilitar o nascimento

de um novo estilo de Matemática. O seu brilhantismo consistia não apenas na criação de teoremas e conceitos, mas na sua habilidade ímpar em formular e expressar idéias de modo tão claro. Ele representou um marco neste novo estilo que seria dali em diante de enorme influência e inspiração para as novas gerações de matemáticos, [18].

Capítulo 1

Relações Binárias e Funções

Neste capítulo temos como objetivo apresentar os principais pré-requisitos dos assuntos a serem desenvolvidos no decorrer da dissertação. Apresentaremos inicialmente a definição de relações e relações binárias, para em seguida apresentarmos os importantes conceitos de relação de equivalência, relação de ordem e por último, o de função.

1.1 Definições Básicas

Definição 1. *Sejam A e B conjuntos não-vazios arbitrários.*

(a) *O par de elementos (\mathbf{a}, \mathbf{b}) , onde $\mathbf{a} \in A$ e $\mathbf{b} \in B$, escolhidos sempre nessa ordem é chamado de **par ordenado**. Dizemos que dois pares ordenados (\mathbf{a}, \mathbf{b}) e (\mathbf{c}, \mathbf{d}) são iguais se, e somente se, $\mathbf{a} = \mathbf{c}$ e $\mathbf{b} = \mathbf{d}$. Neste caso escreveremos $(\mathbf{a}, \mathbf{b}) = (\mathbf{c}, \mathbf{d})$.*

(b) *O **produto cartesiano** de A por B , indicado por $A \times B$, é o conjunto de todos os pares ordenados (\mathbf{a}, \mathbf{b}) , com $\mathbf{a} \in A$ e $\mathbf{b} \in B$. Na notação de conjuntos,*

$$A \times B = \{(\mathbf{a}, \mathbf{b}) \mid \mathbf{a} \in A \text{ e } \mathbf{b} \in B\}.$$

Analogamente, define-se o produto cartesiano de três conjuntos $A_1 \times A_2 \times A_3$, de quatro conjuntos, etc. Dado um conjunto A , indicaremos por A^n o produto de cartesiano de n conjuntos A , ou seja,

$$A^n = \underbrace{A \times A \times \dots \times A}_{n \text{ vezes}}.$$

Exemplo 1. *O produto cartesiano de $A = \{1, 2, 3\}$ por $B = \{2, 3\}$ é o conjunto $A \times B = \{(1, 2), (1, 3), (2, 2), (2, 3), (3, 2), (3, 3)\}$.*

Observação 1. Em geral $A \times B \neq B \times A$, ocorrendo a igualdade se, e somente se, $A = B$.

Definição 2. Sejam A e B conjuntos não-vazios quaisquer. Chamamos de relação binária de A em B a qualquer subconjunto R de $A \times B$. Se R é uma relação de A em A , diremos simplesmente que R é uma relação sobre A .

Geralmente indicaremos que $(a, b) \in R$ através da notação aRb . Quando $(a,b) \notin R$, indicaremos por $a \not R b$. Tal notação é mais conveniente, pois coincide por exemplo com o modo usual de expressar que dois números são iguais, ou que um certo número é menor que outro, pois usualmente escreve-se $a = b$ em vez de $(a, b) \in \{ (x, y) \in A^2 \mid x \text{ é igual a } y \}$, $a < b$ em vez de $(a, b) \in \{ (x, y) \in A^2 \mid x \text{ é menor que } y \}$.

Podemos escrever uma relação sobre um conjunto A por extenso ou (quando conveniente, se possível) por uma lei de formação, como ilustrado nos exemplos a seguir.

Exemplo 2. Considere em $A = \{1, 2, 3, 4, 5, 6\}$ as seguintes relações:

$$R_1 = \{(1, 1), (2, 2), (3, 3), (4, 4), (5, 5), (6, 6)\};$$

$$R_2 = \{(1, 3), (1, 4), (1, 5), (1, 6), (2, 5), (2, 6)\};$$

$$R_3 = \{(1, 1), (1, 2), (1, 3), (1, 4), (1, 5), (1, 6)\}.$$

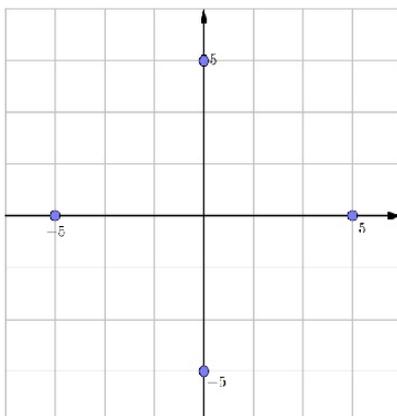
Podemos escrever essas relações da seguinte maneira:

$$R_1 = \{(x, y) \in A^2 \mid x = y\};$$

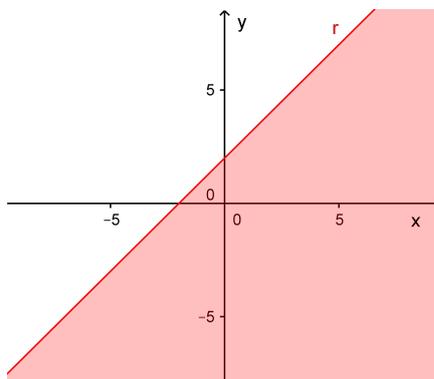
$$R_2 = \{(x, y) \in A^2 \mid 2x < y\};$$

$$R_3 = \{(x, y) \in A^2 \mid 2x < y \text{ ou } x + 2y < 6\}.$$

Exemplo 3. Em \mathbb{Z} considere a relação $R = \{(x, y) \in \mathbb{Z}^2 \mid x^2 + y^2 = 25\}$, cuja representação no plano cartesiano é:



Exemplo 4. Sobre \mathbb{R} , considere a relação $R = \{(x, y) \in \mathbb{R}^2 \mid y \leq x+2\}$. Abaixo exibiremos a representação gráfica de R .



Definição 3. Seja R uma relação sobre um conjunto A e $B \subset A, B \neq \emptyset$. A relação $R_B = R \cap (B \times B)$ é chamada de relação induzida por R sobre B . Neste caso, R é dito ser um prolongamento de R_B .

Um modo equivalente e mais prático de se definir R_B é o seguinte:

$$\text{Dados } a, b \in B, \quad aR_B b \Leftrightarrow aRb. \tag{1.1}$$

Exemplo 5. $R = \{(x, y) \in \mathbb{Z}^2 \mid x^2 + y^2 = 25\}$ é uma relação induzida pela relação $C = \{(x, y) \in \mathbb{R}^2 \mid x^2 + y^2 = 25\}$.

Definição 4. Seja um conjunto $A \neq \emptyset$. Chamamos de relação de igualdade ou relação diagonal de A à relação $\Delta_A = \{(a, a) \mid a \in A\}$. A relação de igualdade é comumente descrita na forma $\Delta_A = \{(x, y) \in A^2 \mid x = y\}$.

Obviamente a todo conjunto não vazio está associada uma e somente uma relação diagonal. E o número de pares ordenados da relação diagonal é o mesmo que o número de elementos dos conjunto.

Exemplo 6. A relação $R_1 = \{(1, 1), (2, 2), (3, 3), (4, 4), (5, 5), (6, 6)\}$ do Exemplo 2 é a relação diagonal de $A = \{1, 2, 3, 4, 5, 6\}$.

Definição 5. Seja R uma relação sobre A (i.e., $R \subset A \times A$). Defina a relação R^{-1} como:

$$aR^{-1}b \text{ se e somente se } bRa.$$

Ou seja, $(a, b) \in R^{-1}$ se, e somente se $(b, a) \in R$. R^{-1} é denominada relação inversa (ou relação oposta) a R .

Exemplo 7. A relação inversa de $R_2 = \{(1, 3), (1, 4), (1, 5), (1, 6), (2, 5), (2, 6)\}$ é a relação $R_2^{-1} = \{(3, 1), (4, 1), (5, 1), (6, 1), (5, 2), (6, 2)\}$.

Observação 2. Cuidado para não confundir relação inversa com complementar de uma relação.

Definição 6. Seja R uma relação sobre um conjunto $A \neq \emptyset$. Dizemos que R é:

1. reflexiva se, e somente se, $\forall a \in A, aRa$, ou seja, $\Delta_A \subseteq R$;
2. simétrica se, e somente se, $R = R^{-1}$, ou seja, dados $a, b \in A, aRb \Leftrightarrow bRa$;
3. antissimétrica se, e somente se, $R \cap R^{-1} \subseteq \Delta_A$, ou seja, dados $a, b \in A, aRb, bRa \Rightarrow a = b$;
4. transitiva se, e somente se, dados $a, b, c \in A$, se aRb e bRc então aRc .

Observação 3. Seja R uma relação sobre um conjunto $A \neq \emptyset$. Segue por contraposição que:

1. R não é reflexiva se, e somente se, existe $a \in A$ tal que $a \not R a$; ou seja, $\Delta_A \not\subseteq R$;
2. R não é simétrica se, e somente se, existem $a, b \in A$ tais que, aRb mas $b \not R a$; ou seja, $R \neq R^{-1}$;
3. R não é antissimétrica se, e somente se, existem $a, b \in A$, tais que aRb, bRa mas $a \neq b$;
4. R não é transitiva se, e somente se, existem $a, b, c \in A$ tais que aRb, bRc , mas $a \not R c$.

Exemplo 8. Defina sobre $A = \{a, b, c\}$ as seguintes relações:

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

Temos que R é reflexiva (pois, $aRa, bRb, e cRc$), enquanto que S não o é, pois por exemplo $b \not S b$ (i.e., $(b, b) \notin S$).

Exemplo 9. Sobre \mathbb{R} defina as seguintes relações : $R = \{(x, y) \in \mathbb{R} \times \mathbb{R} \mid x \leq y\}$ e $S = \{(x, y) \in \mathbb{R} \times \mathbb{R} \mid x^2 = y\}$. R é reflexiva, mas S não é reflexiva, pois por exemplo, $(2, 2) \notin S$.

Exemplo 10. Defina sobre \mathbb{R} as seguintes relações:

$$R = \{(x, y) \in \mathbb{R} \times \mathbb{R} \mid x^2 = y^2\} \quad e \quad S = \{(x, y) \in \mathbb{R} \times \mathbb{R} \mid x \geq y\}.$$

R é simétrica, porém S não é simétrica, pois $(2, 1) \in S$, mas $(1, 2) \notin S$, ou seja, $2S1$ mas $1 \not\geq 2$.

Exemplo 11. Considere sobre $A = \{1, 2, 3\}$ as relações

$$R = \{(1, 1), (1, 3)\} \quad e \quad S = \{(1, 1), (1, 3), (3, 1)\}.$$

Temos que R é antissimétrica e S não é antissimétrica, pois $(1, 3) \in S$ e $(3, 1) \in S$, mas $1 \neq 3$. Observe que S é simétrica e R não o é.

Observação 4. Uma relação ser antissimétrica não significa que ela não seja simétrica e vice-versa, isto é, antissimétrica não implica em não simétrica e vice-versa; em outras palavras, existem relações que são antissimétricas e simétricas simultaneamente. Por exemplo a relação $R = \{(1, 1), (2, 2)\}$ sobre o conjunto $A = \{1, 2, 3\}$ é simétrica e antissimétrica.

1.2 Relações de equivalência

Definição 7. Dizemos que uma relação binária R sobre um conjunto A é uma **relação de equivalência** sobre A se, e somente se, R é **reflexiva, simétrica e transitiva**.

Exemplo 12. Seja $A = \{a, b, c\}$ e seja $R = \{(a, a), (b, b), (c, c), (b, a), (a, b)\}$. R é uma relação de equivalência sobre A .

Exemplo 13. A relação diagonal (ou seja, a relação de igualdade) é uma relação de equivalência sobre qualquer conjunto $A \neq \emptyset$, pois:

- (a) $\forall x \in A, x = x$;
- (b) $\forall x, y \in A, x = y \Rightarrow y = x$;
- (c) $\forall x, y, z \in A, x = y$ e $y = z \Rightarrow x = z$.

Exibiremos a seguir um exemplo muito importante de relação de equivalência, a relação de congruência módulo m .

Definição 8. Dados $a, b \in \mathbb{Z}$, dizemos que a é um divisor de b (ou que a divide b) se, e somente se, existe $c \in \mathbb{Z}$ tal que $b = a \cdot c$. Para indicar que a é divisor de b usaremos a notação $a|b$.

Definição 9. Seja $m \in \mathbb{Z}^* = \mathbb{Z} - \{0\}$ fixado. Definamos sobre \mathbb{Z} a seguinte relação:

aRb se, e somente se, $\exists k \in \mathbb{Z}$ tal que, $a - b = k \cdot m$ (i.e., $m|(a - b)$).

R é denominada congruência módulo m (i.e., determinado por m).

Notação: usaremos $a \equiv b \pmod{m}$ para indicar que a é congruente a b módulo m , e, $a \not\equiv b \pmod{m}$ indicará que a não é congruente a b módulo m .

Exemplo 14. Consideremos $m = 3$. temos que $12 \equiv 9 \pmod{3}$, $-1 \equiv 2 \pmod{3}$, etc.

Teorema 1. Dado $m \in \mathbb{Z}^*$ fixado, a relação de congruência módulo m é uma relação de equivalência.

Demonstração. Dado $a \in \mathbb{Z}$, temos que $a - a = 0m$. Logo, $a \equiv a \pmod{m}$. Portanto, $\equiv \pmod{m}$ é reflexiva. Observe também que $\equiv \pmod{m}$ é simétrica, pois dados $a, b \in \mathbb{Z}$, se $a \equiv b \pmod{m}$, então existe um $k \in \mathbb{Z}$ tal que, $a - b = km$. Logo, $b - a = (-k)m$ e portanto, $b \equiv a \pmod{m}$. Para terminarmos vamos mostrar a transitividade. Dados $a, b, c \in \mathbb{Z}$ tais que, $a \equiv b \pmod{m}$ e $b \equiv c \pmod{m}$, existem $k_1, k_2 \in \mathbb{Z}$ tais que, $a - b = k_1m$ e $b - c = k_2m$ e daí, $a - c = (a - b) + (b - c) = (k_1 + k_2)m$; portanto, $a \equiv c \pmod{m}$. □

Seja R uma relação de equivalência sobre $A \neq \emptyset$. Se $a, b \in A$ são tais que aRb , dizemos que a é equivalente a b segundo R . Motivados pela notação de congruência, indicaremos que aRb por meio da notação $a \equiv b \pmod{R}$ e $a \not\equiv b \pmod{R}$ caso contrário. Quando não houver dúvida sobre a relação de equivalência considerada, usaremos simplesmente $a \equiv b$ ou $a \not\equiv b$ para indicar que $a \equiv b \pmod{R}$ ou $a \not\equiv b \pmod{R}$, respectivamente.

Definição 10. Seja R uma relação de equivalência sobre $A \neq \emptyset$. Dado $a \in A$, o conjunto

$$\bar{a} = \{x \in A \mid a \equiv x \pmod{R}\}$$

é chamado **classe de equivalência módulo R** determinada por a , e a , por sua vez, é chamado representante da classe de equivalência \bar{a} .

Observação 5. \bar{a} é subconjunto de A , e $\bar{a} \neq \emptyset$, pois pelo menos $a \in \bar{a}$. Por $\equiv \pmod{R}$ ser simétrica, vale que $\bar{a} = \{x \in A \mid x \equiv a \pmod{R}\}$.

Lema 1. $x \in \bar{a}$ se, e somente se, $\bar{x} = \bar{a}$. Ou seja, todo elemento de uma classe de equivalência pode ser considerado como representante dessa classe.

Demonstração. (\Rightarrow) Se $x \in \bar{a}$, então dado $y \in \bar{x}$ temos que $y \equiv x$ e $x \equiv a$, daí pela transitividade, $y \equiv a$. Logo, $\bar{x} \subseteq \bar{a}$. Por outro lado, se $y \in \bar{a}$, então como $x \equiv a$ e $a \equiv y$, segue que $x \equiv y$ e portanto $y \in \bar{x}$; daí $\bar{a} \subseteq \bar{x}$. Concluímos assim que $\bar{a} = \bar{x}$. (\Leftarrow) Segue imediatamente da observação 5. \square

O conjunto das classes de equivalência de A módulo R é chamado de **conjunto quociente** de A por R e será denotado por A/R . Em notação de conjunto, $A/R = \{\bar{a} \mid a \in A\}$.

Exemplo 15. Seja $A = \{a, b, c\}$ e seja $R = \{(a, a), (b, b), (c, c), (a, b), (b, a)\}$. sabemos que R é uma relação de equivalência sobre A . As classes de equivalência são

$$\bar{a} = \{x \in A \mid a \equiv x\} = \{a, b\},$$

$$\bar{b} = \{x \in A \mid b \equiv x\} = \{a, b\};$$

$$\bar{c} = \{x \in A \mid x \equiv c\} = \{c\};$$

logo, $A/R = \{\{a, b\}, \{c\}\}$.

Definição 11. Seja $A \neq \emptyset$ e seja \mathcal{P} um subconjunto não vazio do conjunto das partes de A . Dizemos que \mathcal{P} é uma **partição** de A se, e somente se:

(i) dados $X, Y \in \mathcal{P}$, ou $X = Y$ ou $X \cap Y = \emptyset$;

(ii) $\bigcup_{X \in \mathcal{P}} X = A$.

Exemplo 16. Seja $A = \{0, 1, 2, 3\}$. O conjunto $\mathcal{P} = \{\{0\}, \{1\}, \{2, 3\}\}$ é uma partição de A . Considerando $R = \{(0, 0), (1, 1), (2, 2), (3, 3), (2, 3), (3, 2)\}$, temos que R é uma relação de equivalência sobre A . É fácil ver que $A/R = \mathcal{P}$.

Observe que o conjunto A/R do exemplo 15 é uma partição de A . Surge então uma pergunta: Será que todo conjunto quociente de um conjunto A por uma relação de equivalência R é uma partição de A ? Outra pergunta: É possível associar a qualquer partição de um conjunto uma relação de equivalência de modo que o conjunto quociente módulo essa relação coincida com aquela partição? As respostas estão nos dois teoremas a seguir.

Teorema 2. Se R é uma relação de equivalência sobre um conjunto $A \neq \emptyset$, então A/R é uma partição de A .

Demonstração. Vamos provar que A/R satisfaz (i) e (ii) da Definição 11.

(i) Dadas duas classes $\bar{a}, \bar{b} \in A/R$, se $\bar{a} \cap \bar{b} \neq \emptyset$, então considerando $c \in \bar{a} \cap \bar{b}$. Daí temos que $a \equiv c$ e $c \equiv b$, e conseqüentemente, pela transitividade de R , $a \equiv b$. Logo, pelo Lema 1, $\bar{a} = \bar{b}$. Portanto, (i) está provada.

(ii) $\bigcup_{a \in A} \bar{a} \subseteq A$, pois $\bar{a} \subset A, \forall a \in A$. Por outro lado, dado $x \in A$, como $x \in \bar{x}$ (vide observação 5) segue que $x \in \bigcup_{a \in A} \bar{a}$, portanto $A \subset \bigcup_{a \in A} \bar{a}$. Logo, $\bigcup_{a \in A} \bar{a} = A$. \square

Teorema 3. *Se \mathcal{P} é uma partição de A , então existe uma única relação de equivalência R sobre A tal que, $A/R = \mathcal{P}$.*

Demonstração. Existência: Seja \mathcal{P} uma partição de A . Definimos sobre A a seguinte relação:

$$xRy \text{ se, e somente se, existe } X \in \mathcal{P} \text{ tal que } x, y \in X.$$

Na notação de conjunto,

$$R = \{(x, y) \in A \times A \mid \exists X \in \mathcal{P}, \text{ onde } x, y \in X\}. \quad (1.2)$$

(a) $\forall a \in A, aRa$, pois como $A = \bigcup_{X \in \mathcal{P}} X$ e $a \in A$; segue que existe $X \in \mathcal{P}$ tal que $a \in X$. Logo, R é reflexiva.

(b) Obviamente R é simétrica.

(c) Sejam $a, b, c \in A$ tais que, aRb e bRc . Então existem $X, Y \in \mathcal{P}$ tal que $a, b \in X$ e $b, c \in Y$. Como $b \in X \cap Y$ temos $X \cup Y \neq \emptyset$, logo $X = Y$. Assim $a, c \in X$. Concluimos que aRc .

De (a), (b) e (c) temos que R é uma relação de equivalência.

Unicidade: Suponhamos que existam $R_1 \neq R_2$ relações de equivalência sobre $A \neq \emptyset$ tais que $A/R_1 = A/R_2 = \mathcal{P}$. Já que $R_1 \neq R_2$, podemos afirmar sem perda de generalidade que existem $a, b \in A$ tais que, $(a, b) \in R_1$ mas $(a, b) \notin R_2$. Assim

$$\{x \in A \mid x \equiv a \text{ mod } R_1\} = \{x \in A \mid x \equiv b \text{ mod } R_1\}$$

e

$$\{x \in A \mid x \equiv a \text{ mod } R_1\} \neq \{x \in A \mid x \equiv b \text{ mod } R_2\}.$$

Temos que para algum $c \in A$,

$$\{x \in A \mid x \equiv a \text{ mod } R_1\} = \{x \in A \mid x \equiv c \text{ mod } R_2\}$$

logo $a \equiv c \pmod{R_2}$ para algum $c \in A$.

Ainda, como $b \in \{x \in A \mid x \equiv b \pmod{R_1}\} = \{x \in A \mid x \equiv a \pmod{R_1}\}$ segue que $b \equiv c \pmod{R_2}$.

Daí, $a \equiv b \pmod{R_2}$ ou seja $(a, b) \in R_2$. Um absurdo. \square

Bom, a partir de agora sabemos que a cada partição de um conjunto A está associada univocamente uma relação de equivalência sobre A .

Exemplo 17. *Seja $A = \{a, e, i, o, u\}$ e seja $\mathcal{P} = \{\{a, u\}, \{e, o\}, \{i\}\}$. É claro que \mathcal{P} é uma partição de A . Determinemos R tal que $A/R = \mathcal{P}$. Segue imediatamente de (1.2) e da definição de relação de equivalência que*

$$R = \{(a, a), (e, e), (i, i), (o, o), (u, u), (a, u), (u, a), (e, o), (o, e)\}.$$

Exemplo 18. *Consideremos \mathbb{Z} a seguinte partição:*

$$\mathcal{P} = \{\{0, \pm 3, \pm 6, \pm 9, \dots\}, \{\dots, -8, -5, -2, 1, 4, 7, \dots\}, \{\dots, -4, -1, 2, 5, 8, 11, \dots\}\}.$$

A demonstração do Teorema 3 nos mostra como determinar uma relação de equivalência associada à partição \mathcal{P} . Devemos exibir uma relação de equivalência R tal que $A/R = \mathcal{P}$. Temos então três classe de equivalência:

$$\bar{0} = \{0, \pm 3, \pm 6, \pm 9, \dots\} = \{x \in \mathbb{Z} \mid x = 3k, k \in \mathbb{Z}\},$$

$$\bar{1} = \{\dots, -8, -5, -2, 1, 4, 7, \dots\} = \{x \in \mathbb{Z} \mid x = 3k + 1, k \in \mathbb{Z}\} \text{ e}$$

$$\bar{2} = \{\dots, -4, -1, 2, 5, 8, 11, \dots\} = \{x \in \mathbb{Z} \mid x = 3k + 2, k \in \mathbb{Z}\}.$$

Encontraremos uma lei que identifique a que classe pertence um elemento arbitrário $x \in \mathbb{Z}$. Observemos que, $x \in \bar{0} \Leftrightarrow x = 3k$, para algum $k \in \mathbb{Z}$, ou seja, x é múltiplo de 3; $x \in \bar{1} \Leftrightarrow x = 3k + 1$, para algum $k \in \mathbb{Z}$, ou seja, quando dividimos x por 3 temos 1 como resto; $x \in \bar{2} \Leftrightarrow x = 3k + 2$, para algum $k \in \mathbb{Z}$, o que significa que quando dividimos x por 3 temos 2 de resto. Portanto, dados $x, y \in \mathbb{Z}$

$$xRy \text{ se, e somente se, } \exists k \in \mathbb{Z} \text{ tal que } x - y = 3k,$$

ou seja, R é a relação de congruência módulo 3.

1.3 Relações de Ordem

Definição 12. *Dizemos que uma relação binária R sobre um conjunto A é **uma relação de ordem** (sobre A) se, e somente se, R é:*

- a) reflexiva.
- b) antissimétrica
- c) transitiva.

Costuma-se dizer simplesmente que R é uma ordem sobre A , e que A é um conjunto ordenado (ou parcialmente ordenado) por R . Se a ordem R está subentendida, dizemos simplesmente que A é ordenado (i.e., não se faz necessário mencionar a relação). Geralmente indicaremos um conjunto A ordenado por uma ordem R através da notação (A, R) .

O exemplo abaixo mostra que nem toda relação de ordem é relação de equivalência.

Exemplo 19. Sobre $A = \{1, 2, 3, 4, 5\}$ definimos a seguinte relação:

$$R = \{(1, 1), (2, 2), (3, 3), (4, 4), (4, 2), (1, 2), (1, 4)\}.$$

Então R é uma relação de ordem sobre A . No entanto R não é uma relação de equivalência, pois $1R2$ e $2 \not R1$ por exemplo.

Definição 13. Se uma ordem R sobre A verifica a condição

$$\forall x, y \in A, xRy \text{ ou } yRx, \tag{1.3}$$

dizemos que R é uma **relação de ordem total** sobre A , ou que **A é um conjunto totalmente ordenado por R** .

Exemplo 20. Os conjuntos (\mathbb{N}, \leq) , (\mathbb{Z}, \leq) , (\mathbb{Q}, \leq) , (\mathbb{R}, \leq) , onde \leq é a conhecida relação menor que ou igual, são exemplos clássicos de conjuntos totalmente ordenados.

Exemplo 21. A relação de divisibilidade (veja a definição 8) sobre conjunto dos números naturais \mathbb{N} é uma relação de ordem. De fato,

- (a) $\forall a \in \mathbb{N}, a|a$ (reflexibilidade);
- (b) $\forall a, b \in \mathbb{N}$, se $a|b$ e $b|a$, então $a = b$ (antissimétrica);
- (c) $\forall a, b, c \in \mathbb{N}$, se $a|b$ e $b|c$, então $a|c$, pois $a|b$ e $b|c \Rightarrow \exists m, n \in \mathbb{N}$ tal que $b = ma$ e $c = nb \Rightarrow c = (mn)a$. Portanto, vale a transitividade.

Mas $(\mathbb{N}, |)$ não é totalmente ordenado, porque $2, 3 \in \mathbb{N}$ mas $2 \not|3$ e $3 \not|2$. É importante observar que a relação de divisibilidade não é uma relação de ordem sobre \mathbb{Z} . De fato, $|$ não é antissimétrica, porque $2|-2$ e $-2|2$, mas $-2 \neq 2$.

A seguir provamos que a relação inversa de uma relação de ordem é também uma relação de ordem.

Proposição 1. *Seja R uma relação sobre um conjunto $A \neq \emptyset$. Então:*

- (a) R é uma relação de ordem se, e somente se, R^{-1} é ordem.
- (b) R é ordem total se, e somente se R^{-1} é ordem total.

Demonstração. (a)(\Rightarrow) Seja R uma ordem sobre A . Então segue da definição de R^{-1} que:

(i) $\forall a \in A \ aR^{-1}a$, pois aRa .

(ii) Dados $a, b \in A$, se $aR^{-1}b$ e $bR^{-1}a$, então bRa e aRb . Como R é antissimétrica, segue que $a = b$. Portanto, R^{-1} é antissimétrica.

(iii) Dados $a, b, c \in A$, se $aR^{-1}b$ e $bR^{-1}c$, então cRb e bRa . Segue da transitividade de R que cRa , e conseqüentemente, $aR^{-1}c$. Logo, R^{-1} é transitiva.

(a)(\Leftarrow) i) $\forall a \in A \ aRa$, pois $aR^{-1}a$.

ii) Dados $a, b \in A$. Se $aR^{-1}b$ e $bR^{-1}a$ então bRa e aRb , portanto R é antissimétrica.

iii) Dados $a, b, c \in A$. Se aRb e $bRc \Rightarrow cR^{-1}b$ e $bR^{-1}a \Rightarrow cR^{-1}a \Rightarrow aRc$. Logo, R é transitiva.

(b) \Rightarrow) R é ordem total $\Leftrightarrow \forall a, b \in A, aRb$ ou $bRa \Rightarrow aR^{-1}b$ ou $bR^{-1}a \Rightarrow R^{-1}$ é ordem total.

De maneira análoga prova-se a volta. □

Exemplo 22. *A ordem oposta à relação de divisibilidade em \mathbb{N} é a relação de multiplicidade, ou seja, dados $a, b \in \mathbb{N}$, $a|b$ se e somente se, b é múltiplo de a .*

Notação: A partir de agora, nos casos genéricos, usaremos os símbolos \leq e \geq para ordem e ordem oposta, respectivamente.

Definição 14. *Seja (A, \leq) um conjunto ordenado. Chamaremos de **ordem estrita** sobre A associada à ordem \leq , e indicada pelo símbolo $<$, à relação definida por:*

$$\forall a, b \in A, a < b \Leftrightarrow a \leq b \text{ e } a \neq b.$$

Exibiremos na proposição abaixo uma outra caracterização de ordem estrita.

Proposição 2. *$<$ é ordem estrita sobre A associada a \leq se, e somente se, $<$ satisfaz as seguintes afirmações:*

- (a') $\forall a \in A, a \not< a$;
- (b') $\forall a, b \in A$ se $a < b$ então $b \not< a$;
- (c') $<$ é transitiva.

Demonstração. (\Rightarrow) (a') é imediata, pois $a = a$.

(b') Dados $a, b \in A$, se $a < b$, então pela definição 15, $a \leq b$ e $a \neq b$. Como \leq é ordem, segue da antissimetria que $b \not\leq a$ e portanto, $b \not< a$.

(c') Dados $a, b, c \in A$, $a < b$ e $b < c \Leftrightarrow (a \leq b \text{ e } a \neq b)$ e $(b \leq c \text{ e } b \neq c) \Leftrightarrow (a \leq b \text{ e } b \leq c)$ e $(a \neq b \text{ e } b \neq c)$. Como \leq é ordem, segue então da transitividade de \leq que $a \leq c$.

Falta somente provar que $a \neq c$. De $a \neq b$ e $b \neq c$ inferimos que $a \neq c$, pois $a = c$, seguiria de $b \leq c$ e $a \leq b$, que $a = b$, o que é um absurdo (pois contradiz a hipótese de $a \neq b$). Logo $a < c$. Portanto $<$ é transitiva.

(\Leftarrow) Suponhamos que $<$ satisfaz (a') , (b') e (c') . Definamos a seguinte relação R :

$$aRb \text{ se, e somente se, } a = b \text{ ou } a < b. \quad (1.4)$$

É tarefa simples verificar que R é uma ordem sobre A .

Denotemos por \prec a ordem estrita associada à ordem R . Afirmamos que \prec coincide com $<$. De fato, dados $(a, b) \in \prec$ (ou seja, $a < b$), segue da definição de ordem estrita e de (1.4) que $a \prec b$, ou seja, $(a, b) \in \prec$; logo $\prec \subseteq <$. Agora, dado $(a, b) \in <$, temos que aRb e $a \neq b$. Daí por (1.4) $a < b$ e conseqüentemente, $(a, b) \in \prec$; logo $< \subseteq \prec$. Portanto, $<$ e \prec coincidem, e a proposição está demonstrada. \square

Proposição 3. *Seja (A, \leq) um conjunto ordenado e seja $B \subset A$. Então, a relação \leq_B , induzida por \leq sobre B , é uma ordem. Além disso, se \leq é uma relação de ordem total, então \leq_B também o é.*

Demonstração. Sugestão: veja (1.1) e a definição de relação de ordem e ordem total. \square

Definição 15. *Seja (A, \leq) um conjunto ordenado. Dizemos que:*

(i) *um subconjunto B de A é limitado inferiormente quando existe $a \in A$ tal que, para todo $x \in B$, $a \leq x$. a é comumente chamado de limite (ou cota) inferior de B ;*

(ii) *B é limitado superiormente quando existe $c \in A$ tal que, para todo $x \in B$, $x \leq c$. c é comumente chamado de limite (ou cota) superior de B ;*

(iii) *Se B é limitado inferior e superiormente, dizemos simplesmente que B é um conjunto limitado;*

(iv) *Dizemos que um elemento $m \in A$ é mínimo de B quando m é limite inferior B e $m \in B$.*

(v) Um elemento $n \in A$ é máximo de B quando é limite superior de B e $n \in B$.

O mínimo e o máximo de um conjunto B , caso existam, seram indicados por, $\min B$ e $\max B$, respectivamente.

Proposição 4. O máximo e o mínimo de B , caso existam, são únicos.

Demonstração. Sejam m_1 e m_2 mínimos de B . Então, $m_1 \leq m_2$ e $m_2 \leq m_1$; daí, pela antissimétrica, segue que $m_1 = m_2$. De modo análogo mostra-se que o máximo, quando existe, é único. \square

Exemplo 23. O conjunto dos números naturais com ordem usual, (\mathbb{N}, \leq) , tem mínimo, mas não possui máximo.

Exemplo 24. Os conjuntos numéricos \mathbb{Z} , \mathbb{Q} e \mathbb{R} munidos da ordem usual \leq , não têm máximo nem mínimo.

Exemplo 25. Considere $2\mathbb{N} := \{a \in \mathbb{N} \mid a \text{ é par}\}$ e $B = \{x \in 2\mathbb{N} \mid 2 \leq x \leq 30\} \subset \mathbb{N}$, onde \leq é a ordem usual de \mathbb{N} . Sabemos que a relação de divisibilidade é uma ordem sobre B . vejamos que se b tem máximo e / ou mínimo em relação à divisibilidade:

Conforme a definição 15 (iv), $m = \min B \Leftrightarrow m|a \forall a \in B$ e $m \in B$. Portanto, $2 = \min B$. Do mesmo modo, $n = \max B \Leftrightarrow a|n \forall a \in B$ e $n \in B$, daí é fácil ver que, apesar de ser limitado superiormente, B não possui máximo.

1.4 Funções ou Aplicações

A noção de função é uma das mais básicas e importantes da Matemática. Função (ou aplicação) é o nome dado a uma relação entre dois conjuntos não vazios, que a cada elemento do primeiro associa um e somente um elemento do segundo conjunto, de modo que todos os elementos do primeiro conjunto fazem parte da relação.

Definição 16. Sejam A e B conjuntos. Dizemos que uma relação f de A em B é uma função se, e somente se, para todo $x \in A$ existe um único $y \in B$ tal que $(x, y) \in f$. Ou equivalentemente,

- (i) para todo $x \in A$ existe um $y \in B$ tal que $(x, y) \in f$ (ou seja, $x f y$);
- (ii) se $(x, y) \in f$ e $(x, y') \in f$ então $y = y'$.

Dado $x \in A$, o (único) elemento $y \in B$ tal que $(x, y) \in f$ será representado pela notação $f(x)$ e é chamado o valor de f em x , ou a imagem de x por f ou simplesmente f de x . A função f é a relação

$$f = \{(x, f(x)) \mid x \in A\}. \quad (1.5)$$

Sejam A e B conjuntos e sejam $X \subseteq A$ e $Y \subseteq B$.

(i) Uma função f de A em B será designada por uma das seguintes notações: $f : A \rightarrow B$, ou $x \mapsto f(x)$ onde x é um elemento arbitrário de A .

(ii) A é chamado de o domínio e B é o contradomínio de f . O conjunto $f(A) = \{f(x) \mid x \in A\}$ é a imagem de f .

(iii) Os conjuntos $f(X) = \{f(x) \mid x \in A\}$ e $f^{-1}(Y) = \{x \mid f(x) \in Y\}$ são, respectivamente, a imagem de X por f e a imagem inversa de Y por f .

(iv) Quando $f(A) = B$ dizemos que f é uma função sobrejetora. E dizemos que f é injetora (ou biunívoca) se, e somente se, dados $x_1, x_2 \in A$, $x_1 \neq x_2$ implicar que $f(x_1) \neq f(x_2)$, ou equivalentemente, $f(x_1) = f(x_2)$ implicar que $x_1 = x_2$.

(v) Uma função injetora e sobrejetora é dita bijetora.

A representação (1.5) de uma função f é comumente chamada de gráfico de f .

Exemplo 26. Sejam $f = \{(0, 1), (1, 1), (2, 1), (2, 2)\}$ um subconjunto de $A \times B$, onde $A = \{0, 1, 2\}$ em $B = \{1, 2\}$. A relação de f não é função, pois $(2, 1), (2, 2) \in f$, mas $1 \neq 2$. Já a relação $g = \{(0, 1), (1, 1), (2, 2)\}$ de A em B é uma função e sua imagem é B ; assim, g é sobrejetora $g(\{0, 1\}) = \{1\}$. $g^{-1}\{1\} = \{0, 1\}$.

Exemplo 27. Determinaremos todas as funções de $A = \{1, 2\}$ em $B = \{a, b\}$, com $a \neq b$. Seja $f : A \rightarrow B$ uma função arbitrária. Então existem y_1 e $y_2 \in B$ tais que $(1, y_1), (2, y_2) \in f$ e portanto, $f = \{y_1, y_2\}$. Como $y_1, y_2 \in B$ são arbitrários, as possíveis funções de A em B são as seguintes:

$$f_1 = \{(1, a), (2, b)\}, f_2 = \{(1, a), (2, a)\}, f_3 = \{(1, b), (2, a)\}, f_4 = \{(1, b), (2, b)\}.$$

As funções f_1 e f_3 são bijetoras, enquanto que as funções f_2 e f_4 são sobrejetoras de A sobre $\{a\}$ e $\{b\}$, respectivamente.

Definição 17. Seja $f : X \rightarrow Y$ uma função injetora. Definimos a função inversa de f , denotada por f^{-1} , pela seguinte relação: $(y, x) \in f^{-1}$ se, e somente se, $(x, y) \in f$, ou seja, $f^{-1} = \{(y, x) \mid (x, y) \in f\}$. O domínio de f^{-1} é o conjunto $f(X)$. Neste caso, f é bijetora se, e somente se, $f(X) = Y$.

Definição 18. *Sejam $f : X \rightarrow Y$ e $g : Y \rightarrow Z$ funções. Definimos a composta de g e f denotada por $g \circ f : X \rightarrow Z$, pela regra: $(g \circ f)(x) = g(f(x))$.*

Exemplo 28. *Sejam $f, g : \mathbb{R} \rightarrow \mathbb{R}$ as funções definidas por $f(x) = 2x + 1$ e $g(x) = x^2 - 1$, $x \in \mathbb{R}$. Então as compostas $g \circ f$ e $f \circ g$ são dadas respectivamente por $(g \circ f)(x) = g(2x + 1) = (2x + 1)^2 - 1$ e $(f \circ g)(x) = 2(x^2 - 1) + 1$. Portanto, $g \circ f \neq f \circ g$. Em geral isso é verdadeiro.*

Capítulo 2

O Conjunto \mathbb{Q} dos Números Racionais

Aprendemos no ensino fundamental que um número racional é a “razão” entre dois números inteiros. O estudo de **Números Racionais**¹ nos ajuda a compreender desde a numeração decimal, as frações, as dízimas periódicas, as porcentagens, proporções, além de proporcionar ao aluno uma melhor compreensão e atuação no dia-a-dia. Ao resolver problemas que envolvam números racionais, o aluno consegue, conseqüentemente analisar situações que estão relacionadas no seu cotidiano, pois os mesmos se encontram em grande parte da nossa vida, seja ela dentro ou fora da escola. Por exemplo, o troco em centavos rebido por uma pessoa ao fazer compras.

Neste capítulo faremos a construção axiomática de \mathbb{Q} , mostrando algumas de suas principais características.

2.1 Construção dos Números Racionais

Dados $(a, b), (c, d) \in \mathbb{Z} \times \mathbb{Z}^*$, diremos que a relação $(a, b) \sim (c, d)$ quando e somente quando $a \cdot d = b \cdot c$.

Teorema 4. *A relação acima é de equivalência.*

Demonstração. \sim tem as propriedades reflexiva, simétrica e transitiva. De fato, da definição de \sim , $(a, b) \sim (a, b)$. Por outro lado se $(a, b) \sim (c, d) \Rightarrow a \cdot d = b \cdot c \Leftrightarrow c \cdot b = a \cdot d$

¹O conjunto dos números racionais será denotado por \mathbb{Q} .

$\Rightarrow (c, d) \sim (a, b)$. Para finalizar, se $(a, b) \sim (c, d)$ e $(c, d) \sim (e, f) \Rightarrow a \cdot d = b \cdot c$ e $c \cdot f = d \cdot e \Rightarrow a \cdot d \cdot f = b \cdot c \cdot f$ e $b \cdot c \cdot f = b \cdot d \cdot e \Rightarrow a \cdot d \cdot f = b \cdot d \cdot e$ cancelando o d ($d \neq 0$) temos, $a \cdot f = b \cdot e \Rightarrow (a, b) \sim (e, f)$. \square

Exemplo 29. *Observe:*

i) $(1, 2) \sim (2, 4)$; ii) $(3, 4) \sim (9, 12)$

Definição 19. *Dado $(a, b) \in \mathbb{Z} \times \mathbb{Z}^*$, denotamos por $\frac{a}{b}$ (que lê-se “a sobre b”) a classe de equivalência do par (a, b) pela relação \sim acima. Assim,*

$$\frac{a}{b} = \{(x, y) \in \mathbb{Z} \times \mathbb{Z}^* \mid (x, y) \sim (a, b)\}. \quad (2.1)$$

O símbolo $\frac{a}{b}$, denominado **fração**, não passa de uma maneira convencional de se escrever o par ordenado $(a, b) \in \mathbb{Z} \times \mathbb{Z}^*$, que responde à pergunta: “Qual o número que devemos multiplicar por b para obter a ?” ou que constitui a solução em \mathbb{Z} da equação $bx = a$.

Exemplo 30. $\frac{1}{2} = \{(x, y) \in \mathbb{Z} \times \mathbb{Z}^* \mid 2x = y\}$.

Observação 6. : *A propriedade “ $\frac{a}{b} = \frac{c}{d} \Leftrightarrow a \cdot d = b \cdot c$ ” é a propriedade fundamental das frações.*

Definição 20. *O conjunto quociente de $\mathbb{Z} \times \mathbb{Z}^*$ por \sim , ou seja, o conjunto de todas as classes de equivalência determinadas por \sim sobre $\mathbb{Z} \times \mathbb{Z}^*$, será designado por \mathbb{Q} . Portanto,*

$$\mathbb{Q} = \left\{ \frac{a}{b} \mid a \in \mathbb{Z} \text{ e } b \in \mathbb{Z}^* \right\}. \quad (2.2)$$

A definição tal como está em (2.2) é a mesma que é ensinada no ensino fundamental.

2.2 Operações em \mathbb{Q}

Iremos definir duas operações no conjunto dos números racionais \mathbb{Q} , munindo-o, de uma estrutura que estudaremos logo adiante.

2.2.1 Adição em \mathbb{Q}

Definição 21. *Sejam $m = \frac{a}{b}$ e $n = \frac{c}{d}$ elementos de \mathbb{Q} . Chama-se soma de m com n e indica-se por $m + n$ o elemento de \mathbb{Q} definido da seguinte maneira:*

$$m + n = \frac{a}{b} + \frac{c}{d} = \frac{a \cdot d + b \cdot c}{b \cdot d}.$$

A soma independe dos pares utilizados para definir m e n . De fato, tomando

$$m = \frac{a}{b} = \frac{a'}{b'} \text{ e } n = \frac{c}{d} = \frac{c'}{d'},$$

então $a \cdot b' = b \cdot a'$ e $c \cdot d' = d \cdot c'$.

Multiplicando a primeira dessas igualdades por $d \cdot d'$ e a segunda por $b \cdot b'$ e, em seguida, somando membro a membro as igualdades obtidas, têm-se

$$\begin{aligned} a \cdot d \cdot b' \cdot d' + b \cdot c \cdot d' \cdot b' &= b \cdot d \cdot a' \cdot d' + b \cdot d \cdot c' \cdot b' \\ \Leftrightarrow (a \cdot d + c \cdot b) \cdot b' \cdot d' &= b \cdot d \cdot (a' \cdot d' + c' \cdot b'), \end{aligned}$$

o que garante,

$$\frac{a \cdot d + c \cdot b}{b \cdot d} = \frac{a' \cdot d' + c' \cdot b'}{b' \cdot d'}.$$

Portanto, a correspondência

$$(m, n) \rightarrow m + n,$$

quaisquer que sejam $m, n \in \mathbb{Q}$, é uma operação sobre \mathbb{Q} .

Exemplo 31. *Temos:*

$$1) \frac{1}{2} + \frac{5}{3} = \frac{1 \cdot 3 + 2 \cdot 5}{2 \cdot 3} = \frac{13}{6};$$

$$2) \frac{2}{3} + \frac{7}{2} = \frac{2 \cdot 2 + 3 \cdot 7}{3 \cdot 2} = \frac{26}{6}.$$

Para essa operação, valem as seguintes propriedades:

Proposição 5. *Para quaisquer $a, b, c \in \mathbb{Q}$ valem:*

α_1) $(a + b) + c = a + (b + c)$ (*Associatividade*);

α_2) $a + b = b + a$ (*comutatividade*);

α_3) *Existe elemento neutro (único): que é a classe de equivalência $\frac{0}{1} = \{\frac{0}{b} \mid b \in \mathbb{Z}^*\}$.*

α_4) *Para todo $m = \frac{a}{b} \in \mathbb{Q}$, existe um elemento n tal que $m + n = 0$.*

Demonstração. De fato, $n = \frac{-a}{b} \in \mathbb{Q}$, pois

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

□

Observação 7. *O elemento $\frac{-a}{b}$ é chamado simétrico aditivo ou oposto de $\frac{a}{b}$.*

Usaremos a seguinte notação $\mathbb{Q}^* = \{a \in \mathbb{Q} \mid a \neq 0\}$.

2.2.2 Multiplicação em \mathbb{Q}

Definição 22. Definimos o produto de dois números racionais $\frac{a}{b}$ e $\frac{c}{d}$ da seguinte maneira:

$$\frac{a}{b} \cdot \frac{c}{d} = \frac{a \cdot c}{b \cdot d}.$$

O produto é necessariamente um número racional, pois sendo b e d diferentes de 0, o produto $b \cdot d$ será não-nulo.

Para a multiplicação em \mathbb{Q} , valem as seguintes propriedades:

Proposição 6. Para quaisquer $a, b, c \in \mathbb{Q}$ valem:

m_1) $(a \cdot b) \cdot c = a \cdot (b \cdot c)$ (propriedade associativa;)

m_2) $a \cdot b = b \cdot a$ (propriedade comutativa;)

m_3) Existe elemento neutro: é a classe de equivalência $\frac{1}{1} = \{\frac{a}{a} \mid a \in \mathbb{Z}^*\}$.

Demonstração. De fato, uma vez que

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

qualquer que seja $\frac{a}{b} \in \mathbb{Q}$. □

Observação 8. A classe de equivalência

$$\frac{1}{1} = \{\frac{a}{a} \mid a \in \mathbb{Z}^*\}$$

será denotada simplesmente por 1.

m_4) Para todo $m = \frac{a}{b} \in \mathbb{Q}^*$, existe um único elemento n tal que $m \cdot n = 1$.

Demonstração. Trata-se de $n = \frac{b}{a}$ que é um elemento de \mathbb{Q} , pois $a \neq 0$, e

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

□

Observação 9. O elemento $\frac{b}{a}$ é chamado simétrico multiplicativo ou inverso de $\frac{a}{b}$ e é denotado por $\frac{b}{a} = \left(\frac{a}{b}\right)^{-1}$. Ou seja, todo $m \in \mathbb{Q}^*$ tem simétrico multiplicativo ou inverso.

Logo, é imediato que $\left(\left(\frac{a}{b}\right)^{-1}\right)^{-1} = \frac{a}{b}$.

m_5) $a \cdot (b + c) = a \cdot b + a \cdot c$ distributiva.

Proposição 7. *Seja Ω o subconjunto de \mathbb{Q} constituído por todas as classes $\frac{a}{1}$ ou $\frac{a}{b}$ sendo $b \neq 0$.*

A cada elemento b de \mathbb{Z} associemos $\frac{b}{1}$ em Ω . Chamemos de f essa aplicação de \mathbb{Z} em Ω , ou seja, $f: \mathbb{Z} \rightarrow \Omega$, é tal que $f(b) = \frac{b}{1}$.

É evidente que f é uma bijeção.

Por outro lado,

$$f(a + b) = \frac{a + b}{1} = \frac{a}{1} + \frac{b}{1} = f(a) + f(b) \quad (*)$$

e

$$f(a \cdot b) = \frac{a \cdot b}{1} = \frac{a}{1} \cdot \frac{b}{1} = f(a) \cdot f(b). \quad (**)$$

A bijeção que acabamos de definir nos permite identificar qualquer inteiro b com o número racional $\frac{b}{1}$. A aplicação f é o que se chama uma “imersão” de \mathbb{Z} em \mathbb{Q} . As propriedades () e (**) dizem que f preserva as operações $+$ e \cdot . Sendo assim, por meio da identificação de \mathbb{Z} com Ω podemos dizer que \mathbb{Z} é um subconjunto de \mathbb{Q} .*

2.3 Relação de ordem e enumerabilidade de \mathbb{Q}

Definição 23. *Sejam $\frac{a}{b}$ e $\frac{c}{d}$ são números racionais com $b, d > 0$. Diremos que $\frac{a}{b} \leq \frac{c}{d}$ se, e somente se, $a \cdot d \leq b \cdot c$.*

Teorema 5. *A relação \leq , introduzida acima, é uma relação de ordem.*

Demonstração. Dados $\frac{a}{b}$, $\frac{c}{d}$ e $\frac{e}{f} \in \mathbb{Q}$, com b, d e $f > 0$ temos que:

(i) (Reflexiva) obviamente $\frac{a}{b} \leq \frac{a}{b}$, pois $a \cdot b \leq a \cdot b$.

(ii) (Antissimétrica) Se $\frac{a}{b} \leq \frac{c}{d}$ e $\frac{c}{d} \leq \frac{a}{b} \Rightarrow a \cdot d \leq b \cdot c$ e $b \cdot c \leq a \cdot d$. Daí $a \cdot d = b \cdot c$.

Logo, $\frac{a}{b} = \frac{c}{d}$.

(iii) (Transitiva) Se $\frac{a}{b} \leq \frac{c}{d}$ e $\frac{c}{d} \leq \frac{e}{f} \Rightarrow a \cdot d \leq b \cdot c$ e $c \cdot f \leq d \cdot e$ respectivamente.

Multiplicando a primeira desigualdade por f e a segunda por b temos:

$$a \cdot d \cdot f \leq b \cdot c \cdot f \text{ e } c \cdot f \cdot b \leq d \cdot e \cdot b \Rightarrow a \cdot d \cdot f \leq d \cdot e \cdot b$$

dividindo ambos os lados da desigualdade por b teremos:

$$a \cdot f \leq b \cdot e \Rightarrow \frac{a}{b} \leq \frac{e}{f}.$$

□

Observação 10. Para quaisquer que sejam os números racionais $\frac{a}{b}$ e $\frac{c}{d}$ temos que:

$$\frac{a}{b} < \frac{c}{d} \text{ ou } \frac{c}{d} < \frac{a}{b} \text{ ou } \frac{a}{b} = \frac{c}{d} \quad (2.3)$$

A propriedade (2.3) é chamada de tricotomia.

Proposição 8. Se a e b são números racionais tais que $0 < a < b$, então existe um inteiro positivo n tal que $n \cdot a > b$.

Demonstração. De fato, seja $a = \frac{x}{y}$ e $b = \frac{r}{s}$, sendo x, y, r e s inteiros positivos. Vamos tomar $n = 2 \cdot y \cdot r$, que $2 \cdot y \cdot r \cdot \left(\frac{x}{y}\right) > \left(\frac{r}{s}\right)$.

É fácil ver que a desigualdade anterior decorre de ser $2 \cdot y \cdot r \cdot x \cdot s > y \cdot r$ pois, $2 \cdot x \cdot s > 1$, por serem $x > 0$ e $s > 0$. □

Por causa da Proposição 8 dizemos que \mathbb{Q} é **arquimediano**.

Definição 24. Um conjunto X diz-se enumerável quando é finito ou quando existe uma bijeção $f : \mathbb{N} \rightarrow X$. No segundo caso, X diz-se infinito enumerável e, pondo-se $x_1 = f(1), x_2 = f(2), \dots, x_n = f(n), \dots$, tem-se $X = \{x_1, x_2, \dots, x_n, \dots\}$. Cada bijeção $f : \mathbb{N} \rightarrow X$ chama-se enumeração (dos elementos) de X .

A seguir usaremos o seguinte fato: Todo subconjunto de \mathbb{N} possui um menor elemento.

Lema 2. Todo subconjunto infinito de \mathbb{N} é enumerável.

Demonstração. Considere $\{x_1, x_2, x_3, \dots, x_{n+1}, \dots\} = X \subset \mathbb{N}$ e X é infinito, então existe

$x_1 = \min X$ (menor elemento de X) daí teremos:

$$x_2 = \min\{X - \{x_1\}\}$$

$$x_3 = \min\{X - \{x_1, x_2\}\}$$

$$x_4 = \min\{X - \{x_1, x_2, x_3\}\}$$

⋮

$$x_{i+1} = \min\{X - \{x_1, x_2, x_3, \dots, x_i\}\}$$

Definia $\varphi : \mathbb{N} \rightarrow X$ tal que $\varphi(i) = x_i$. A função φ definida desta forma é bijetora.

Portanto, segue que qualquer subconjunto infinito de \mathbb{N} é enumerável. □

Lema 3. Seja X um conjunto enumerável. Se $f : X \rightarrow Y$ é sobrejetiva, então, Y é enumerável.

Demonstração. A demonstração deste Lema pode ser encontrada em [8], página 50. \square

Lema 4. *Todo número racional positivo $\frac{a}{b}$, ($a, b > 0$), pode ser escrito, de modo único, como uma fração irredutível, isto é, na forma $\frac{m}{n}$, onde $m \nmid n$.*

Demonstração. Vamos considerar as decomposições em fatores primos de a e de b , dadas pelo Teorema Fundamental da Aritmética. Seja k o produto de todos os fatores primos comuns a a e a b , de modo que $\frac{a}{b} = \frac{k \cdot a'}{k \cdot b'}$. Pela propriedade fundamental das frações obtemos que $\frac{a}{b} = \frac{a'}{b'}$, em que a' e b' são primos entre si. Se existisse uma fração irredutível $\frac{c}{d}$ igual a $\frac{a'}{b'}$, teríamos pela propriedade fundamental das frações que $a' \cdot d = b' \cdot c$, daí, pela decomposição em fatores primos, d conteria os fatores primos de b' e vice-versa, ocorrendo o mesmo para a' e c , ou seja, $a' = c$ e $b' = d$. \square

Observação 11. *O conjunto dos números inteiros \mathbb{Z} é enumerável. Basta definir uma função $f: \mathbb{N} \rightarrow \mathbb{Z}$ bijetora da seguinte forma.*

$$f(x) = \begin{cases} \frac{n}{2}, & \text{se } n \text{ é par} \\ \frac{-(n-1)}{2}, & \text{se } n \text{ é ímpar.} \end{cases}$$

Teorema 6. *O conjunto \mathbb{Q} dos números racionais é enumerável.*

Demonstração. Defina $f: \mathbb{Z} \times \mathbb{Z}^* \rightarrow \mathbb{Q}$ tal que $f(a, b) = \frac{a}{b}$ e observe que f é sobrejetiva (Pelo Lema 3) e como $\mathbb{Z} \times \mathbb{Z}$ é enumerável temos \mathbb{Q} também enumerável. \square

Capítulo 3

O Conjunto dos Números Reais

Veremos primeiramente, neste capítulo que o conjunto dos números racionais possui algumas “lacunas”, no sentido que existem muitos números diretamente ligados a situações cotidianas que não são números racionais. No sentido geométrico, os racionais não preenchem toda a reta, ou seja, não é completo. Logo em seguida, faremos o complemento de \mathbb{Q} utilizando um método devido ao matemático alemão Richard Dedekind¹ (1831 - 1916). Tal método consiste em utilizar o conjunto dos números racionais com suas propriedades, Relação de Ordem e a noção de Corte para construir o conjunto dos números reais.

3.1 Algumas limitações de \mathbb{Q}

Embora bastante rica, a estrutura algébrica do conjunto dos números racionais é insuficiente para efeitos da Análise Matemática e também para o uso prático, a exemplo, a construção de um quarto de formato quadrado e área igual a 17m^2 . O fato de alguns conjuntos limitados de números racionais não possuírem máximo (ou mínimo) é o mais grave deles. Este fato está ligado à inexistência de raízes racionais para alguns números inteiros. Um exemplo clássico é a diagonal de um quadrado de lado 1. Provaremos logo abaixo que tal número não é racional. Em seguida provaremos que nem todos os conjuntos de números racionais limitados superiormente ou inferiormente, possui máximo ou mínimo respectivamente. Este problema gerou alguns paradoxos famosos, como o

¹Julius Wilhelm Richar Dedekind foi um dos quatro filhos de uma família luterana de Braunschweig, Alemanha. Entrou em Göttingen aos dezenove anos e aos vinte e dois obteve seu doutoramento com uma tese sobre Cálculo, elogiada até por Gauss. Foi aluno de Dirichlet e dedicou-se ao ensino secundário em Brunswick até os últimos anos de sua vida.

paradoxo de Zenão, que diz:

Se um segmento de reta pode ser subdividido indefinidamente então, o movimento é impossível pois, para percorrê-lo, será preciso andar metade do segmento, logo em seguida andar metade do que resta e assim sucessivamente. Segue-se daí que o movimento é impossível.

Antes de provarmos que a diagonal de um quadrado de lado igual a 1 não é racional, falaremos um pouco sobre segmentos comensuráveis e segmentos incomensuráveis.

3.1.1 Segmentos Comensuráveis e Segmentos Incomensuráveis

Definição 25. *A medida de um segmento AB , representada por \overline{AB} , é um número que deve exprimir quantas vezes o segmento AB contém o segmento unitário u tomado como segmento de medida.*

Dado um ponto inteiro positivo n , se for possível obter $n - 1$ pontos intermediários A_1, A_2, \dots, A_{n-1} do segmento AB tal que os segmentos $AA_1, A_1A_2, \dots, A_{n-1}B$ sejam todos iguais ao segmento unitário, então a medida AB será n .

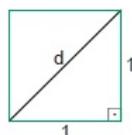
Pergunta: E se por acaso o segmento AB não contém o segmento u um número inteiro de vezes?

Daí procederemos da seguinte maneira: Tome um segmento w que esteja contido n vezes em u e m vezes em AB com $m, n \in \mathbb{Z}_+^*$. Então,

$$\overline{AB} = m\overline{w}, \quad \overline{u} = n\overline{w} \Rightarrow \frac{\overline{AB}}{\overline{u}} = \frac{m\overline{w}}{n\overline{w}} = \frac{m}{n} \Rightarrow \overline{AB} = \frac{m}{n}.$$

Dizemos que w é um submúltiplo comum de AB e u e com isso, AB e u são comensuráveis. Portanto, AB é comensurável com u quando sua medida AB for um número inteiro ou fracionário. Caso contrário chama-se incomensurável. Segue abaixo o exemplo clássico de incomensurabilidade, em que a diagonal do quadrado de lado igual a 1 é incomensurável em relação ao seu lado.

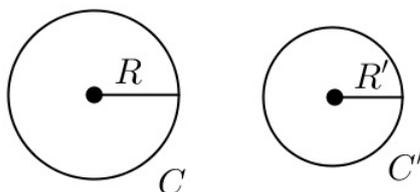
Lema 5. *Não existe número racional cujo quadrado seja igual a 2.*



Demonstração. Suponhamos por absurdo que exista $x = \frac{p}{q} \in \mathbb{Q}$ com $p, q \in \mathbb{Z}$ primos entre si, tal que $x^2 = 2$. Daí, $\frac{p^2}{q^2} = 2$ ou seja, $p^2 = 2q^2$. Neste caso temos que p é par (pois p^2 é par). Logo podemos escrever $p = 2k$ com $k \in \mathbb{Z}$. Portanto $(2k)^2 = 2q^2$ implica que $2k^2 = q^2$. Portanto q também é par, o que contradiz a hipótese de p e q serem primos entre si. \square

3.2 A História do número π

O número π , que é encontrado pela razão entre o perímetro do círculo e seu diâmetro, tem uma história fascinante, que começou há cerca de 4000 anos atrás. No antigo testamento (II Crônicas 4:2) lê-se: “E ele (Salomão) também mandou fazer um tanque redondo de bronze, com dois metros e vinte e cinco de profundidade, quatro metros e meio de diâmetro e treze metros e meio de circunferência (NTLH) ²”. Esta passagem ocorre em uma lista de especificações para o grande templo de Salomão, construído cerca de 950 a.C. A circunferência era, pois, três vezes o diâmetro. Isto significa que os antigos Hebreus se contentavam em atribuir a π o valor 3. Este valor foi muito possivelmente encontrado por medição.



Sejam duas circunferências de comprimento C e C' e raios R e R' , respectivamente, e considere polígonos regulares de mesmo número de lados inscritos e circunscritos nessas circunferências. Denote por p_n e P_n o perímetro do polígono inscrito e circunscrito ao círculo C , e p'_n e P'_n o perímetro do polígono inscrito e circunscrito ao círculo C' . Por semelhança entre polígonos temos:

$$\frac{p_n}{p'_n} = \frac{R}{R'} \text{ e } \frac{P_n}{P'_n} = \frac{R}{R'}.$$

Daí temos:

$$p_n < C < P_n \text{ e } p'_n < C' < P'_n \Rightarrow \frac{p_n}{2R} < \frac{C}{2R} < \frac{P_n}{2R} \text{ e } \frac{p'_n}{2R'} < \frac{C'}{2R'} < \frac{P'_n}{2R'}.$$

²NTLH - Nova Tradução na Linguagem de Hoje.

Portanto,

$$\frac{C}{2R} = \frac{C'}{2R'} = \pi.$$

Concluimos assim que a razão entre o comprimento do círculo e o seu diâmetro é um número constante representado por π .

Exemplo 32. (Unicamp 92) *Considere duas circunferências, uma delas tendo o raio com medida racional e a outra com medida não-racional. Suponha que essas circunferências têm centros fixos e estão se tocando de modo que a rotação de uma delas produz uma rotação na outra, sem deslizamento. Mostre que os dois pontos (um de cada circunferência) que coincidem no início da rotação, nunca mais voltarão a se encontrar.*

Demonstração. Sejam as circunferências C e C' e seus pontos de encontro A e B respectivamente. Sejam R e R' os raios de C e C' respectivamente. Logo, R é racional e R' não é racional. Se o ponto A andar um comprimento x o ponto B também vai andar um comprimento x pois não há deslizamento. Suponhamos por absurdo que após n voltas completadas por A e m voltas completadas por B temos:

$$n2\pi R' = m2\pi R \Rightarrow R' = \frac{m}{n}R. \text{ Absurdo, pois } m, n \text{ e } R \text{ são racionais.}$$

□

A prova de que o número π é irracional pode ser encontrada em [13], nas páginas 152 e 153.

Através do teorema seguinte mostraremos que alguns subconjuntos dos números racionais não possuem máximo e nem mínimo.

Teorema 7. *Sejam $A = \{p \in \mathbb{Q} \mid p \geq 0 \text{ e } p^2 < 2\}$ e $B = \{p \in \mathbb{Q} \mid p > 0 \text{ e } p^2 > 2\}$. Os conjuntos A e B não possuem $\max A$ e nem o $\min B$ em \mathbb{Q} .*

Demonstração. i) O conjunto A não possui um maior elemento. Com efeito, dado $p \in A$ tomamos um número racional $r < 1$ tal que $0 < r < \frac{(2 - p^2)}{2 \cdot p + 1}$. Afirmamos que $p + r$ ainda pertence a A . De fato, de $r < 1$ temos $r^2 < r$. Da outra desigualdade que r satisfaz ganhamos que $r \cdot (2 \cdot p + 1) < 2 - p^2$. Por outro lado $(p + r)^2 = p^2 + 2 \cdot p \cdot r + r^2 < p^2 + r \cdot (2 \cdot p + 1) < p^2 + 2 - p^2 = 2$. Portanto, dado qualquer $p \in A$, existe um número maior, $p + r \in A$.

ii) O conjunto B não possui elemento mínimo. Com efeito, dado qualquer $p \in B$, temos $p > 0$ e $p^2 > 2$. Logo podemos obter um número racional r tal que $0 < r < \frac{p^2 - 2}{2 \cdot p}$. Então $2 \cdot r \cdot p < p^2 - 2$ e daí $(p - r)^2 = p^2 - 2 \cdot p \cdot r + r^2 > p^2 - 2 \cdot p \cdot r > 2$. Veja também que $r < \frac{p}{2} - \frac{1}{p}$, donde $r < p$, isto é, $p - r$ é positivo. Assim dado $p \in B$ arbitrário, podemos obter $p - r \in B, p - r < p$. \square

Usaremos o método de Dedekind para fazer o complemento do conjunto \mathbb{Q} .

3.3 Cortes de Dedekind

Definição 26. Dizemos que um subconjunto $\alpha \subset \mathbb{Q}$ é um corte quando satisfaz as propriedades:

- i) $\alpha \neq \emptyset$ e $\alpha \neq \mathbb{Q}$;
- ii) Se $p, q \in \mathbb{Q}$ são tais que, $p \in \alpha$ e $p < q$, então $q \in \alpha$;
- iii) Em α não existe racional mínimo.

Em outras palavras, um **Corte de Dedekind** é um par ordenado (K, α) onde K e α são subconjuntos disjuntos não-vazios de números racionais, tais que α não possui elemento mínimo, $K \cup \alpha = \mathbb{Q}$ e, dados $x \in K$ e $y \in \alpha$ quaisquer tem-se $x < y$.

Designaremos por R o conjunto de todos os cortes, ou seja, $R = \{\alpha \subset \mathbb{Q} \mid \alpha \text{ é corte}\}$.

Exemplo 33. Mostremos que $\mathbb{Q}_+^* \cap B$ é um corte, onde $\mathbb{Q}_+^* = \{p \in \mathbb{Q} \mid p > 0\}$ e B é o conjunto definido no teorema 7.

Demonstração. De fato, observe que $B \subset \mathbb{Q}_+^*$, então $\mathbb{Q}_+^* \cap B = B$. Daí temos:

- i) $B \neq \emptyset$ e $B \neq \mathbb{Q}$. (4 por exemplo pertence ao conjunto B .)
- ii) Sejam p e $q \in \mathbb{Q}$ tais que $p \in B$ e $p < q \Rightarrow 2 < p^2 < q^2 \Rightarrow q^2 > 2$. Portanto $q \in B$.

iii) O conjunto B não possui elemento mínimo. Com efeito, dado qualquer $p \in B$, temos $p > 0$ e $p^2 > 2$. Logo podemos obter um número racional q tal que $0 < q < \frac{p^2 - 2}{2 \cdot p}$. Então $2 \cdot p \cdot q < p^2 - 2$ e daí $(p - q)^2 = p^2 - 2 \cdot p \cdot q + q^2 > p^2 - 2 \cdot p \cdot q > 2$. Veja também que $q < \frac{p}{2} - \frac{1}{p}$, donde $q < p$, isto é, $p - q$ é positivo. Assim dado $p \in B$ arbitrário, podemos obter $p - q \in B, p - q < p$. \square

Proposição 9. Sejam $\alpha \in R$ e $q \in \mathbb{Q}$. Se $q \notin \alpha$, então $q < p$, para todo $p \in \alpha$.

Demonstração. A prova é imediata pelo item ii) da Definição 26. \square

Proposição 10. *Seja $r \in \mathbb{Q}$ e seja $\alpha = \{p \in \mathbb{Q} \mid r < p\}$ então $\alpha \in \mathbb{R}$ e r é cota inferior máxima de α .*

Demonstração. α é um corte.

De fato,

i) $\alpha \neq \emptyset$ e $\alpha \neq \mathbb{Q}$ pois dado $p \in \mathbb{Q}$ com $p > r$ tem-se:

$$\frac{p+r}{2} \in \alpha \text{ e } \frac{2 \cdot r - 1}{2} \in \mathbb{Q} \text{ e } \frac{2 \cdot r - 1}{2} \notin \alpha.$$

ii) Sejam p e $q \in \mathbb{Q}$, com $p \in \alpha$ e $p < q$. Daí temos: $r < p$ e $p < q \Rightarrow r < q \Rightarrow q \in \alpha$.

iii) Dado $p \in \alpha$, observe que $r < \frac{p+r}{2} < p$. Portanto qualquer que seja o $p \in \alpha$ sempre é possível encontrar um elemento de α menor. Concluimos assim que α não tem elemento mínimo. \square

Definição 27. *Dado $r \in \mathbb{Q}$, o conjunto $\{p \in \mathbb{Q} \mid r < p\}$ será denotado por r^* , ou seja, $r^* = \{p \in \mathbb{Q} \mid r < p\}$, o qual será chamado de **corte racional**.*

O conjunto de todos os cortes racionais será indicado por \mathbb{Q}^ , ou seja, $\mathbb{Q}^* = \{r^* \mid r \in \mathbb{Q}\}$.*

Definição 28. *Dados $\alpha, \beta \in \mathbb{R}$, definimos $\alpha + \beta = \{p + q \mid p \in \alpha \text{ e } q \in \beta\}$.*

Teorema 8. *Sejam $\alpha, \beta \in \mathbb{R}$. Então $\alpha + \beta \in \mathbb{R}$.*

Demonstração. i) $\alpha + \beta \neq \emptyset$, pois $\alpha \neq \emptyset$ e $\beta \neq \emptyset$. Como $\alpha \neq \mathbb{Q}$ e $\beta \neq \mathbb{Q}$ temos que existem $a, b \in \mathbb{Q}$ tais que $a \notin \alpha$ e $b \notin \beta$, ou seja, $a < p$ para todo $p \in \alpha$ e $b < q$ para todo $q \in \beta$. Daí,

$$a + b < p + q \quad \forall p \in \alpha, q \in \beta.$$

Isso implica que $a + b \notin \alpha + \beta$. Portanto $\alpha + \beta \neq \mathbb{Q}$.

ii) Sejam $a, b \in \mathbb{Q}$ tais que $a < b$ e $a \in \alpha + \beta$. Daí existem $p \in \alpha$ e $q \in \beta$ tais que $a = p + q$. Seja $t \in \mathbb{Q}$ de forma que $b = t + q$. Então,

$$a < b \Rightarrow p + q < t + q \Rightarrow p < t \Rightarrow t \in \alpha.$$

Portanto $b \in \alpha + \beta$.

iii) Dado $p \in \alpha + \beta$ então existem $a \in \alpha$ e $b \in \beta$ tal que $a + b = p$. Além disso existem $r \in \alpha$ com $r < a$ e $s \in \beta$ com $s < b$. Daí,

$$q = r + s < a + b = p \Rightarrow q < p \text{ e que } q \in \alpha + \beta.$$

Portanto, $\alpha + \beta$ não tem elemento mínimo. □

Corolário 1. *Sejam $p^*, q^* \in \mathbb{Q}^*$. Então $p^* + q^* \in \mathbb{Q}^*$.*

Demonstração. Sabemos que $(p + q)^* \in \mathbb{Q}^*$. Basta então mostrar que $(p + q)^* = p^* + q^*$.

1) Seja $c \in p^* + q^*$. Por definição temos que $c = a + b$ tal que $a \in p^*$ e $b \in q^*$. Além disso pela definição de corte temos que:

$$a > p \text{ e } b > q \Rightarrow a + b > b + p \text{ e } b + p > p + q$$

Por transitividade temos que $a + b > p + q$. Portanto $a + b \in (p + q)^*$. Logo, $p^* + q^* \subseteq (p + q)^*$.

2) Seja $x \in (p + q)^*$, então $x - (p + q) > 0$. Sejam $h = x - (p + q)$, $y = \frac{h}{2} + p$ e $z = \frac{h}{2} + q$. Então $y \in p^*, z \in q^*$ e $x = y + z$. Portanto $x \in p^* + q^*$. Logo, $(p + q)^* \subseteq p^* + q^*$. □

Lema 6. *Seja $\alpha \in R$ e seja $r \in \mathbb{Q}$, $r > 0$. Então existem $p, q \in \mathbb{Q}$ com $p \in \alpha, q \notin \alpha$, onde q não é cota inferior máxima de α e $r = p - q$.*

Demonstração. Seja $x \in \alpha$ e considere a seguinte sequência:

$$x, x - r, x - 2 \cdot r, \dots, x - m \cdot r, \dots$$

com,

$$x > x - r > x - 2 \cdot r > \dots > x - m \cdot r > \dots$$

Como a sequência é ilimitada inferiormente, α é limitada inferiormente e $x \in \alpha$, então existe um único inteiro $m \geq 0$ tal que $x - m \cdot r \in \alpha$ e $x - (m + 1) \cdot r \notin \alpha$. Se $x - (m + 1) \cdot r$ não for cota inferior máxima de α , então devemos tomar $p = x - m \cdot r$ e $q = x - (m + 1) \cdot r$. Caso $x - (m + 1) \cdot r$ for cota inferior máxima tome $p = x - m \cdot r - \frac{r}{2}$ e $q = x - (m + 1) \cdot r - \frac{r}{2}$. □

Teorema 9. *$(R, +)$ satisfaz as seguintes propriedades:*

Dados $\alpha, \beta, \mu \in R$, valem:

a) $(\alpha + \beta) + \mu = \alpha + (\beta + \mu)$ (*Associatividade*);

b) $\alpha + \beta = \beta + \alpha$ (*Comutatividade*);

c) $\alpha + 0^* = \alpha = 0^* + \alpha$ (*Elemento Neutro da Adição*);

d) *Para cada $\alpha \in R$, existe um único $\beta \in R$ tal que $\alpha + \beta = 0^*$. Esse corte β é o oposto de α e é denotado por $-\alpha$.*

Demonstração. a) $(\alpha + \beta) + \mu = \{(p + q) + r \mid p + q \in \alpha + \beta \text{ e } r \in \mu\} = \{p + (q + r) \mid p \in \alpha \text{ e } q + r \in \beta + \mu\} = \alpha + (\beta + \mu)$.

b) $\alpha + \beta = \{p + q \mid p \in \alpha \text{ e } q \in \beta\} = \{q + p \mid q \in \beta \text{ e } p \in \alpha\} = \beta + \alpha$.

c) Seja $r = p + q \in \alpha + 0^*$ com $p \in \alpha$ e $q > 0$. Assim, $r > p$, $r \in \alpha$. Logo $\alpha + 0^* \subset \alpha$. Tomemos agora $r \in \alpha$ e $s \in \alpha$ tal que $s < r$. Observemos que podemos expressar $r = s + (r - s)$, em que $r - s > 0$ e, portanto $s - r \in 0^*$. Logo, $r \in \alpha + 0^*$, e assim, $\alpha \subset \alpha + 0^*$.

d) Existência: Dado, $\beta = \{p \in \mathbb{Q} \mid -p \text{ é cota inferior de } \alpha, \text{ mas não máxima}\}$. Então $\beta \in \mathbb{R}$. De fato,

i) Do fato de $\alpha \neq \emptyset$ e $\alpha \neq \mathbb{Q}$ segue que $\beta \neq \emptyset$ e $\beta \neq \mathbb{Q}$.

ii) Se $p \in \beta$, então $-p \in \alpha$. Como $-p$ é cota inferior de α , mas não máxima, existe $-q \in \alpha$ tal que $-q < -p \Rightarrow q > p$. Portanto, $q \in \beta$.

iii) Dado $p \in \beta$, temos que $-p$ é cota inferior de α mas não máxima, ou seja, existe $q \in \mathbb{Q}$ tal que $q < p$ ($-q > -p$) e $-q \in \alpha$.

Seja $r = \frac{p + q}{2}$; então $-p < -r < -q$, de modo que $-r$ é cota inferior de α mas não máxima. Isso mostra que $p > r$ e $r \in \beta$ e assim, não existe elemento mínimo em β .

Provaremos agora que $\alpha + \beta = 0^*$. Seja $\alpha + \beta = \{r = p + q \mid p \in \alpha \text{ e } q \in \beta\}$.

Tome $r \in \alpha + \beta$. Então $r = p + q$, com $p \in \alpha$ e $q \in \beta$. Como $-q \notin \alpha$ então $-q < p$, de modo que $0 < p + q = r$ ou seja, $r \in 0^*$.

Reciprocamente, suponhamos $t \in 0^*$, isto é, $t > 0$. Pelo lema 6 existem $p \in \alpha$ e $p' \notin \alpha$ (p' não sendo cota inferior máxima de α), tais que $p - p' = t$ (lema 6). Segue que $t = p + (-p')$, com $p \in \alpha$ e $-p' \in \beta$, ou seja, $r \in \alpha + \beta$.

Unicidade: Suponhamos que $\alpha + \beta_1 = \alpha + \beta_2 = 0^*$ para todo $\alpha \in \mathbb{R}$. Então,

$$\beta_1 = \beta_1 + 0^* = \beta_1 + (\alpha + \beta_2) = (\beta_1 + \alpha) + \beta_2 = 0^* + \beta_2 = \beta_2.$$

□

Corolário 2. Dados $\alpha, \beta \in \mathbb{R}$, existe um único $\mu \in \mathbb{R}$ tal que $\alpha + \mu = \beta$.

Definição 29. O corte μ encontrado no corolário anterior é chamado de diferença entre β e α e é denotado por $\beta - \alpha$.

Definição 30. Dados $\alpha, \beta \in \mathbb{R}$, dizemos que:

- 1) $\alpha \leq \beta$ se, e somente se, $\alpha \supseteq \beta$.
- 2) $\alpha < \beta$ se, e somente se, $\alpha \supseteq \beta$ e $\alpha - \beta \neq \emptyset$.

3) $\alpha \leq \beta$ se, e somente se, $\beta \geq \alpha$.

Proposição 11. Dados $\alpha, \beta \in R$, $\alpha < \beta$ se, e somente se existe $q \in \alpha$ tal que $q \notin \beta$.

Demonstração. Existência: Seja $\mu = \beta + (-\alpha)$; então pelo item d) do Teorema 9, pelo Teorema 8 $\mu \in R$ e $\alpha + \mu = \beta$. A unicidade é imediata. \square

Teorema 10. A relação \leq da Definição 30 é uma ordem total em R .

Demonstração. Mostraremos que vale as propriedades reflexiva, antissimétrica, transitiva e total.

1) \leq é reflexiva : Dado $\alpha \in R$, temos $\alpha \leq \alpha$, pois $\alpha \supseteq \alpha$.

2) \leq é antissimétrica : Dados $\alpha, \beta \in R$,

$$\alpha \leq \beta \text{ e } \beta \leq \alpha \Leftrightarrow \alpha \supseteq \beta \text{ e } \beta \supseteq \alpha \Leftrightarrow \alpha = \beta.$$

3) \leq é transitiva : Dados $\alpha, \beta, \mu \in R$, se $\alpha \leq \beta$ e $\beta \leq \mu$ então $\alpha \supseteq \beta$ e $\beta \supseteq \mu$. Pela transitividade de \supseteq temos que $\alpha \supseteq \mu$, e portanto, $\alpha \leq \mu$.

4) Sejam $\alpha, \beta \in R$. Vamos mostrar que $\alpha \leq \beta$ ou $\beta \leq \alpha$. Temos que $\alpha = \beta$ ou $\alpha \neq \beta$. Basta considerarmos o caso $\alpha \neq \beta$, pois se $\alpha = \beta$ não há nada o que fazer. Como α e β são subconjuntos de \mathbb{Q} , ocorre somente um dos casos:

a) Se $\alpha \neq \beta$ temos $\alpha \subset \beta$ e $\beta - \alpha \neq \emptyset$ ou $\beta \subset \alpha$ e $\alpha - \beta \neq \emptyset$.

b) $\alpha \not\subset \beta$ e $\beta \not\subset \alpha$.

Considerando o caso 2 temos que $\alpha \not\subset \beta$ e $\beta \not\subset \alpha$ se, e somente se existe $p \in \beta$ tal que $p \notin \alpha$ e exista $q \in \alpha$ tal que $q \notin \beta$. Daí, como $p \notin \alpha$ temos pela proposição 9 que, $p < q$ e assim, segue da definição de corte que $q \in \beta$, o que é uma contradição. Portanto, o caso 2 não pode ocorrer e isso significa que sempre ocorre o caso 1, o qual pela definição de ordem significa $\alpha < \beta$ ou $\beta < \alpha$. \square

Corolário 3. Em (R, \leq) vale a tricotomia, ou seja, para todo $\alpha, \beta \in R$, ou $\alpha < \beta$, ou $\beta < \alpha$, ou $\alpha = \beta$.

Teorema 11. Dados $\alpha, \beta, \mu \in R$, vale:

$$\alpha \leq \beta \text{ se, e somente se, } \alpha + \mu \leq \beta + \mu.$$

Demonstração. De fato, $\alpha = \beta \Leftrightarrow \alpha + 0^* = \beta + 0^* \Leftrightarrow \alpha + (\mu - \mu) = \beta + (\mu - \mu) \Leftrightarrow (\alpha + \mu) - \mu = (\beta + \mu) - \mu \Leftrightarrow \alpha + \mu = \beta + \mu$. Agora suponhamos sem perda de generalidade que $\alpha < \beta$. Escrevemos,

$$\alpha + \mu = \{r = p + q \mid p \in \alpha \text{ e } q \in \mu\}, \beta + \mu = \{s = t + z \mid t \in \beta \text{ e } z \in \mu\}.$$

Dizer que $\alpha < \beta$ significa que existe $p \in \alpha$ tal que $p \notin \beta$. Daí temos $p < t$ para todo $t \in \beta$. Disso, $p + q < t + q$ para todo $t \in \beta$ e $q \in \mu$, então $\alpha + \mu \supset \beta + \mu$. Além disso, $\alpha + \mu \neq \beta + \mu$. Logo, $\alpha + \mu < \beta + \mu$.

Suponhamos agora que $\alpha + \mu < \beta + \mu$. Segue que $(\alpha + \mu) + (-\mu) < (\beta + \mu) + (-\mu)$, pela associatividade,

$$(\alpha + \mu) + (-\mu) < (\beta + \mu) + (-\mu) \Leftrightarrow \alpha + (\mu + (-\mu)) < \beta + (\mu + (-\mu)), \text{ como } \mu + (-\mu) = 0^*,$$

temos $\alpha < \beta$. □

Corolário 4. *Se $\alpha \geq 0^*$ e $\beta \geq 0^*$, então $\alpha + \beta \geq 0^*$.*

Estamos prontos para definir a operação produto em R , a qual será uma extensão do produto usual em \mathbb{Q} .

Definição 31. *Seja $P = \{\alpha \in R \mid \alpha > 0^*\}$ o conjunto dos cortes estritamente positivos. Quando $\alpha \geq 0^*$ dizemos que α é positivo; α é negativo quando $\alpha \leq 0^*$. Quando $\alpha < 0^*$, dizemos que α é estritamente negativo.*

Definição 32. *Sejam $\alpha, \beta \in R$. Definimos*

$$1) \alpha \cdot \beta = \{r = p \cdot q \mid p \in \alpha, q \in \beta\}, \text{ se } \alpha \geq 0^* \text{ e } \beta \geq 0^*;$$

$$2) \alpha \cdot \beta = \begin{cases} (-\alpha) \cdot (-\beta), & \text{se } \alpha \leq 0^* \text{ e } \beta \leq 0^*; \\ -[(-\alpha) \cdot \beta], & \text{se } \alpha \leq 0^* \text{ e } \beta \geq 0^*; \\ -[\alpha \cdot (-\beta)], & \text{se } \alpha \geq 0^* \text{ e } \beta \leq 0^*. \end{cases}$$

Teorema 12. *Se $\alpha, \beta \in R$, então $\alpha \cdot \beta \in R$.*

Demonstração. Suponhamos $\alpha \geq 0^*$ e $\beta \geq 0^*$ e seja $\gamma = \alpha \cdot \beta$. Por R ser totalmente ordenado, podemos supor sem perda de generalidade que $\alpha \leq \beta$.

i) $\gamma \neq \emptyset$, pois $\alpha \neq \emptyset$ e $\beta \neq \emptyset$ e $\gamma = \{p \cdot q \mid p \in \alpha, q \in \beta\}$. $\gamma \neq \mathbb{Q}$, pois $-1 \in \mathbb{Q}$ e $-1 \notin \gamma$, pois $p \cdot q \geq 0$, para todo $p \in \alpha$ e para todo $q \in \beta$.

ii) Sejam $r, s \in \mathbb{Q}$, tais que, $r \in \gamma$ e $r < s$. Provaremos que $s \in \gamma$. De fato, por hipótese, $r < s$ e $r = p \cdot q$, com $p \in \alpha$ e $q \in \beta$. Como $p = \frac{r}{q}$, segue que $\frac{r}{q} \in \alpha$. Como $\alpha \in R$ e $\frac{r}{q} < \frac{s}{q}$, segue que $\frac{s}{q} \in \alpha$. Daí, $s = \frac{s}{q} \cdot q \in \gamma$, pois $\frac{s}{q} \in \alpha$ e $q \in \beta$.

iii) Seja $r \in \gamma$. Devemos mostrar que existe $s \in \gamma$ tal que $s < r$. Como $r = p \cdot q$, com $p \in \alpha$ e $q \in \beta$, existem $p_1 \in \alpha$ e $q_1 \in \beta$ tais que $p_1 < p$ e $q_1 < q$. Como p, q, p_1 e q_1 são positivos temos:

$$p_1 \cdot q_1 < p \cdot q_1 \text{ e } p \cdot q_1 < p \cdot q = r.$$

Segue da transitividade que $p_1 \cdot q_1 < r$. Como $p_1 \in \alpha$ e $q_1 \in \beta$ temos $s = p_1 \cdot q_1 \in \gamma$. Portanto, γ não possui elemento mínimo.

Os outros casos saem diretamente do item 2 da Definição 32. □

Corolário 5. *Sejam $p, q \in \mathbb{Q}$. Então vale $(p \cdot q)^* = p^* \cdot q^*$.*

Demonstração. Seja $r \in (p \cdot q)^*$. Então $r > p \cdot q$. Como $p, q \in \mathbb{Q}$, segue que $p \leq q$ ou $q \leq p$. Consideremos o caso $0 \leq p \leq q$. Então existe $n \in \mathbb{N}$ tal que $p \cdot q < (p + \frac{1}{n}) \cdot (q + \frac{1}{n}) < r$.

Considere $s = p + \frac{1}{n}$ e $t = \frac{r}{p + \frac{1}{n}}$. Então $r = s \cdot t$, com $s \in p^*$ e $t \in q^*$. Logo, $r \in p^* \cdot q^*$, e portanto, $(p \cdot q)^* \subset p^* \cdot q^*$.

Por outro lado, se $r \in p^* \cdot q^*$. Então $r = s \cdot t$, tal que $s \in p^*$ e $t \in q^*$. Como $0 < s$, $p \cdot q < s \cdot q$ e $s \cdot q < s \cdot t$, daí, $p \cdot q < r$. Logo, $r \in (p \cdot q)^*$.

Os demais casos saem de modo análogo. □

Teorema 13. *Dados quaisquer $\alpha, \beta, \gamma \in R$, valem:*

1. $(\alpha \cdot \beta) \cdot \gamma = \alpha \cdot (\beta \cdot \gamma)$ (*Associatividade*);
2. $\alpha \cdot \beta = \beta \cdot \alpha$ (*Comutatividade*);
3. $\alpha \cdot 1^* = \alpha$ (*Elemento Neutro*);
4. *existe um único $\alpha^{-1} \in R$ tal que $\alpha \cdot \alpha^{-1} = 1^*$ (*Elemento inverso*);*
5. $\alpha \cdot (\beta + \gamma) = \alpha \cdot \beta + \alpha \cdot \gamma$ (*Distributividade*).

Demonstração. Provaremos apenas para o caso que α, β, γ são cortes positivos. Os demais casos são feitos de modo análogo.

$$1. (\alpha \cdot \beta) \cdot \gamma = \{(p \cdot q) \cdot r \mid p \in \alpha, q \in \beta, r \in \gamma\} = \{p \cdot (q \cdot r) \mid p \in \alpha, q \in \beta, r \in \gamma\} = \alpha \cdot (\beta \cdot \gamma).$$

$$2. \alpha \cdot \beta = \{p \cdot q \mid p \in \alpha, q \in \beta\} = \{q \cdot p \mid q \in \beta, p \in \alpha\} = \beta \cdot \alpha.$$

3. $\alpha \cdot 1^* = \{p \cdot q \mid p \in \alpha, 1 < q\}$. Como $p \in \alpha$ e $q > 1$, segue que $p < p \cdot q$. Daí, $p \cdot q \in \alpha$. Logo, $\alpha \cdot 1^* \subset \alpha$.

Dado $p \in \alpha$, existe $q \in \alpha$ tal que $0 < q < p$, pois não existe elemento mínimo em α . Seja $r = \frac{p}{q}$ então $0 < 1 < r$ e portanto $r \in 1^*$. Daí, $p = q \cdot r$, $q \in \alpha$, $r \in 1^* \Rightarrow p \in \alpha \cdot 1^*$. Portanto $\alpha \subset \alpha \cdot 1^*$.

4. A unicidade de α^{-1} . Suponhamos que existam α_1^{-1} e α_2^{-1} tais que $\alpha \cdot \alpha_1^{-1} = 1^*$ e $\alpha \cdot \alpha_2^{-1} = 1^*$. Assim, $\alpha_1^{-1} = \alpha_1^{-1} \cdot 1^* = \alpha_1^{-1} \cdot (\alpha \cdot \alpha_2^{-1}) = (\alpha_1^{-1} \cdot \alpha) \cdot \alpha_2^{-1} = 1^* \cdot \alpha_2^{-1} = \alpha_2^{-1}$.

5. $\alpha \cdot (\beta + \gamma) = \{p \cdot q \mid p \in \alpha, q \in \beta + \gamma\} = \{p \cdot (r + s) \mid p \in \alpha, q = r + s \in \beta + \gamma\} = \{p \cdot r + p \cdot s \mid p \cdot r \in \alpha \cdot \beta, p \cdot s \in \alpha \cdot \gamma\} = \alpha \cdot \beta + \alpha \cdot \gamma$. \square

Teorema 14. *A relação \leq em R é compatível com a multiplicação em R . Ou seja, dados $\alpha, \beta, \gamma \in R$, se $\gamma \geq 0^*$, então: $\alpha \leq \beta \implies \alpha\gamma \leq \beta\gamma$.*

Demonstração. Dados α, β cortes positivos. Vamos provar que $\alpha \cdot \beta$ também é positivo. De fato, dado $r \in \alpha \cdot \beta$, tem-se que $r = p \cdot q$ onde $p \in \alpha$ e $q \in \beta$ o que implica que $r = p \cdot q$ é positivo. Portanto, $r \in 0^*$.

A relação \leq em R é compatível com a multiplicação em R . De fato, $\alpha \leq \beta \implies 0^* = \alpha + (-\alpha) \leq \beta + (-\alpha) \implies \beta + (-\alpha) \geq 0^*$. Como $\gamma \geq 0^*$, temos que:

$(\beta + (-\alpha)) \cdot \gamma \geq 0^* \implies \beta \cdot \gamma + (-\alpha) \cdot \gamma \geq 0^*$. Portanto, pelo teorema 11 tem-se que $\beta \cdot \gamma \geq \alpha \cdot \gamma$. \square

Proposição 12. *Sejam $\alpha, \beta \in R$ tais que $\alpha < \beta$. Então existe $r \in \mathbb{Q}$ tal que $\alpha < r^* < \beta$.*

Demonstração. Por hipótese temos que $\alpha < \beta$. Daí pela definição de corte existe $r \in \alpha$ tal que $r \notin \beta$.

1) $\alpha < r^*$. De fato, dado $p \in r^*$, $r < p$. Como $r \in \alpha$, segue que $p \in \alpha$. Logo, $\alpha \supset r^*$. Como $r \in \alpha$, segue do item (iii) da definição de corte que existe $s \in \alpha$ tal que $s < r$. Logo, $\alpha \neq r^*$. Daí, $\alpha < r$.

2) Analogamente prova-se que $r^* < \beta$. \square

Pelos Corolário 1, Teorema 10 e Corolário 5, podemos identificar cada elemento $p^* \in \mathbb{Q}^*$ com o seu correspondente $p \in \mathbb{Q}$. Consequentemente, podemos identificar \mathbb{Q}^* com o conjunto \mathbb{Q} dos números racionais. Vê-se que ambos têm as mesmas propriedades.

Teorema 15. *(do Complemento de Dedekind) Sejam A e B subconjuntos não vazios de R tais que:*

1. $R = A \cup B$ e $A \cap B = \emptyset$;
2. se $\alpha \in A$ e $\beta \in B$, então $\alpha < \beta$.

Então existe um único $\gamma \in R$, tal que, $\alpha \leq \gamma$ e $\gamma \leq \beta$, para todo $\alpha \in A$ e para todo $\beta \in B$. Em particular, ou $\gamma \in A$ ou $\gamma \in B$, ou seja, ou A tem máximo ou B tem mínimo.

Demonstração. Existência: Consideremos $\gamma = \{p \in \mathbb{Q} \mid p \in \beta, \text{ para algum } \beta \in B\}$. Então $\gamma \in \mathbb{R}$; de fato,

(i) $\gamma \neq \emptyset$, pois $B \neq \emptyset$. Se $\alpha \in A$, então $\alpha < \beta$ para todo $\beta \in B$; logo existe $q \in \alpha$ tal que $q \notin \beta \forall \beta \in B$ o que implica que $q \notin \gamma$. Portanto, $\gamma \neq \mathbb{Q}$.

(ii) Se $p \in \gamma$ e $p < q$, então $q \in \beta$, para algum $\beta \in B$, daí $q \in \gamma$.

(iii) Seja $p \in \gamma$. Então $p \in \beta$, para algum $\beta \in B$. Logo existe $q \in \beta$ tal que $q < p$ e portanto, $q \in \gamma$. Segue então que γ não possui elemento mínimo. Concluimos assim que $\gamma \in \mathbb{R}$.

Suponhamos por absurdo que existe um $\alpha \in A$ tal que $\gamma < \alpha$. Então existe $p \in \mathbb{Q}$ tal que $p \in \gamma$ e $p \notin \alpha$. Daí, pela definição de γ inferimos que $p \in \beta$, para algum $\beta \in B$. Mas isso implicaria que $\beta < \alpha$, o que é um absurdo, pois contradiz o item 2 da hipótese. Logo, $\alpha \leq \gamma, \forall \alpha \in A$.

Agora seja $\beta \in B$. Dado $p \in \beta$ segue da definição de γ segue que $p \in \gamma$; logo $\beta \subseteq \gamma$ e portanto $\gamma \leq \beta$.

Unicidade: Suponhamos que existem $\gamma_1, \gamma_2 \in \mathbb{R}$ que satisfazem a conclusão do teorema e $\gamma_1 < \gamma_2$. Pela proposição 12 existe um $\gamma_3 \in \mathbb{R}$ tal que $\gamma_1 < \gamma_3 < \gamma_2$. Daí segue que $\gamma_3 \in A \cap B$, o que é um absurdo, pois pelo item 1. da hipótese, $A \cap B = \emptyset$. \square

Definição 33. *Seja $A \subset \mathbb{R}$ um conjunto não vazio e limitado.*

a) Dizemos que $\omega \in \mathbb{R}$ é o **supremo** de A e escrevemos $\omega = \sup A$ se e somente se:

S₁. ω é cota superior de A , ou seja, $x \leq \omega \forall x \in A$.

S₂. dado $y \in \mathbb{R}$, $y \geq x \forall x \in A \Rightarrow y \geq \omega$.

b) Dizemos que $\alpha \in \mathbb{R}$ é o **ínfimo** de A e escrevemos $\alpha = \inf A$ se, e somente se:

I₁. α é cota inferior de A , ou seja, $\alpha \leq x \forall x \in A$;

I₂. Se $y \leq x \forall x \in A$, então $y \leq \alpha$.

O item S₂ diz, em outras palavras que ω é a menor das cotas superiores de A . e o ítem I₂ nos diz que α é a maior das cotas inferiores de A .

Proposição 13. *Dado $A \subset \mathbb{R}$, tanto o supremo como o ínfimo de A , se existem, são únicos.*

Demonstração. Suponhamos que A seja limitado inferiormente e que ω_1 e ω_2 são ínfimos de A . Então segue de I₁ e I₂ que $\omega_1 \leq \omega_2$ e $\omega_2 \leq \omega_1$ e portanto, $\omega_1 = \omega_2$, ou seja, $\inf A$ é único.

Analogamente prova-se a unicidade do supremo. □

Teorema 16. *Seja $A \subset \mathbb{R}$ um conjunto não vazio.*

a) *Se A é limitado superiormente, então existe o $\sup A$.*

b) *Se A é limitado inferiormente, então existe o $\inf A$.*

Demonstração. a) Seja $X = \{\alpha \in \mathbb{R} \mid \alpha < x, \text{ para algum } x \in A\}$ e seja $Y = X^c$. Se $\alpha \in X$, então α não é cota superior de A , e todo elemento de Y é cota superior de A . Basta provarmos que Y tem mínimo. X e Y satisfazem as condições do teorema 15. De fato, primeiro vejamos que $X \neq \emptyset$ e $Y \neq \emptyset$.

Como $A \neq \emptyset$, existe $x \in A$ e todo $\alpha \in \mathbb{R}$ tal que $\alpha < x$ pertence a X . Além disso, como A é ilimitado superiormente, segue que existe $y \in \mathbb{R}$ tal que $x \leq y \forall x \in A$, e conseqüentemente, $y \in Y$. Logo, $X \neq \emptyset$ e $Y \neq \emptyset$.

1. Segue imediatamente da definição de X e Y .

2. Dados $\alpha \in X$ e $\beta \in Y$, existe $x \in A$ tal que $\alpha < x$. Como $\beta \in B$, segue que $x \leq \beta$.

Logo, $\alpha < \beta$.

Assim, pelo teorema 15, ou X tem máximo ou Y tem mínimo. Provemos que X não tem máximo. Se $\alpha \in X$, então existe $x \in A$ tal que $\alpha < x$. Seja $\gamma \in \mathbb{R}$ tal que $\alpha < \gamma < x$. Então $\gamma \in X$; logo α não é máximo de X .

b) Dado A , seja $X = -A$, isto é, $X = \{-a \mid a \in A\}$. Então X é não-vazio e limitado superiormente; logo pelo item a) existe $\omega = \sup X$. Portanto tem-se $-\omega = \inf A$. □

Fica evidente que dado um $p \in \mathbb{Q}$, temos $p = \inf p^*$. Além disso, como todo corte α é limitado inferiormente, existe o $\inf \alpha$. Denominaremos por $\mathbb{R} = \{\inf \alpha \mid \alpha \in \mathbb{R}\}$. Então vale o seguinte resultado, que entre outras coisas nos mostra que aplicando-se o processo de construção da seção anterior ao conjunto \mathbb{R} , cada corte definido a partir de \mathbb{R} teria ínfimo e poderíamos indentificá-lo com esse ínfimo e nada de novo seria obtido.

Teorema 17. *Seja $f : \mathbb{R} \rightarrow \mathbb{R}$ definida por $f(\alpha) = \inf(\alpha)$. Vale:*

1. $f(\alpha + \beta) = f(\alpha) + f(\beta)$, ou seja, $\inf(\alpha + \beta) = \inf \alpha + \inf \beta$;

2. $f(\alpha \cdot \beta) = f(\alpha) \cdot f(\beta)$, ou seja, $\inf(\alpha \cdot \beta) = \inf \alpha \cdot \inf \beta$;

3. f é bijetora;

4. $\alpha \leq \beta$ se, e somente se, $\inf \alpha \leq \inf \beta$.

Demonstração. Item 3. $\alpha \neq \beta \Leftrightarrow \alpha < \beta$ ou $\beta < \alpha$, que pela definição de ordem em \mathbb{R} implica que $\inf \alpha < \inf \beta$ ou $\inf \beta < \inf \alpha$, ou seja, $\inf \alpha \neq \inf \beta$; portanto f é

injetora. Como todo corte é limitado inferiormente, segue do item b) do teorema 16 que f é sobrejetora. Logo, f é bijetora.

Item 1. Por definição α e β são limitadas inferiormente então:

$$p \geq \inf \alpha, \forall p \in \alpha \text{ e } q \geq \inf \beta, \forall q \in \beta.$$

Considerando o conjunto $\alpha + \beta = \{p + q \mid p \in \alpha, q \in \beta\}$ e usando as desigualdades acima obtemos:

$$p + q \geq \inf \alpha + \inf \beta, \forall p + q \in \alpha + \beta,$$

isto é, $\inf \alpha + \inf \beta$ é uma cota inferior de $\alpha + \beta$, e portanto, $\alpha + \beta$ é limitado inferiormente.

Mostraremos agora que esta cota inferior é ínfimo.

Tome $\epsilon > 0$. Logo, pela definição de corte sabemos que existe $p \in \alpha$ e $q \in \beta$ tal que:

$$p < \inf \alpha + \frac{\epsilon}{2} \text{ e } q < \inf \beta + \frac{\epsilon}{2} \Rightarrow p + q < \inf \alpha + \inf \beta + \epsilon.$$

Daí, para todo $\epsilon > 0$ existe $r = p + q \in \alpha + \beta$ tal que a última desigualdade ocorre, e portanto:

$$\inf(\alpha + \beta) = \inf \alpha + \inf \beta.$$

A demonstração dos demais itens podem ser feitas de maneira análoga. \square

Com o que fizemos, fica estabelecido que todos os cortes podem ser chamados de números e podemos apresentar cada corte α pelo seu ínfimo. Fica assim construído o conjunto dos números reais \mathbb{R} como conhecemos intuitivamente.

Capítulo 4

Aplicações

Faremos abaixo uma pequena abordagem sobre a importante noção de função maior inteiro, intervalo e valor absoluto, tentando entendê-lo do ponto de vista geométrico, além disso veremos suas propriedades. Logo em seguida falaremos sobre a representação decimal de um número real, finalizando assim essa dissertação.

4.1 Função maior inteiro

Definição 34. *Seja a um número real. Denota-se por $\lfloor a \rfloor$ o maior inteiro que não ultrapassa a , ou seja,*

$$\lfloor a \rfloor = \max\{m \in \mathbb{Z} \mid m \leq a\}.$$

Exemplo 34. 1) $\lfloor 3,2 \rfloor = 3$.

2) $\lfloor -4,11 \rfloor = -5$.

3) $\lfloor \sqrt{3} \rfloor = 1$.

A função de \mathbb{R} em \mathbb{Z} definida por $x \rightarrow \lfloor x \rfloor$, para todo número real x , chama-se **função maior inteiro** sobre \mathbb{R} .

Proposição 14. *Se a e b são números reais quaisquer, então:*

1) $\lfloor a \rfloor \leq a < \lfloor a \rfloor + 1$.

2) $a \leq b \Rightarrow \lfloor a \rfloor \leq \lfloor b \rfloor$.

3) $\lfloor a + m \rfloor = \lfloor a \rfloor + m$ para todo inteiro m .

4) $\lfloor a \rfloor + \lfloor b \rfloor \leq \lfloor a + b \rfloor \leq \lfloor a \rfloor + \lfloor b \rfloor + 1$.

Demonstração. 1) É consequência imediata da Definição 34.

2) Suponhamos por absurdo que possa ocorrer $\lfloor b \rfloor < \lfloor a \rfloor$, para algum par $a, b \in \mathbb{R}$, com $a \leq b$. Como $\lfloor a \rfloor, \lfloor b \rfloor$ são números inteiros, então $\lfloor b \rfloor + 1 \leq \lfloor a \rfloor$. Por outro lado $b < \lfloor b \rfloor + 1$ (por 1) e, daí, $b < \lfloor a \rfloor$. Como $\lfloor a \rfloor \leq a$, então $b < a$, o que é absurdo. Logo, segue-se que 2 é verdadeira.

3) Se $a_1 = a - \lfloor a \rfloor$, então $0 \leq a_1 < 1$ e $a = a_1 + \lfloor a \rfloor$. Então $\lfloor a + m \rfloor = \lfloor \lfloor a \rfloor + m + a_1 \rfloor = \lfloor a \rfloor + m$, pois $\lfloor a \rfloor + m \in \mathbb{Z}$.

4) Dados $a, b \in \mathbb{R}$ tem-se:

$$a = \lfloor a \rfloor + a_1, 0 \leq a_1 < 1.$$

$$b = \lfloor b \rfloor + b_1, 0 \leq b_1 < 1.$$

$$\text{Então, } a + b = \lfloor a \rfloor + \lfloor b \rfloor + a_1 + b_1, 0 \leq a_1 + b_1 < 2.$$

Pela propriedade 3 temos:

$$\lfloor a + b \rfloor = \lfloor \lfloor a \rfloor + \lfloor b \rfloor + a_1 + b_1 \rfloor = \lfloor a \rfloor + \lfloor b \rfloor + \lfloor a_1 + b_1 \rfloor \Rightarrow \lfloor a + b \rfloor \leq \lfloor a \rfloor + \lfloor b \rfloor + 1 \quad (\text{pois } \lfloor a_1 + b_1 \rfloor = 0 \text{ ou } \lfloor a_1 + b_1 \rfloor = 1).$$

Por outro lado, $\lfloor a + b \rfloor = \lfloor a \rfloor + \lfloor b \rfloor + \lfloor a_1 + b_1 \rfloor$ implica $\lfloor a \rfloor + \lfloor b \rfloor \leq \lfloor a + b \rfloor$, pois $\lfloor a_1 + b_1 \rfloor \geq 0$. Portanto, $\lfloor a \rfloor + \lfloor b \rfloor \leq \lfloor a + b \rfloor \leq \lfloor a \rfloor + \lfloor b \rfloor + 1$. \square

4.2 Intervalos e Valor absoluto

Já que \mathbb{R} é ordenado, vale a Definição 15 para subconjuntos de \mathbb{R} .

Definição 35. *Sejam $a, b \in \mathbb{R}$, com $a \leq b$. Os subconjuntos de \mathbb{R} abaixo definidos serão chamados de intervalos.*

- i) $[a, b] = \{x \in \mathbb{R} \mid a \leq x \leq b\}$ *intervalo fechado à esquerda e à direita;*
- ii) $(a, b] = \{x \in \mathbb{R} \mid a < x \leq b\}$ *intervalo aberto à esquerda e fechado à direita;*
- iii) $[a, b) = \{x \in \mathbb{R} \mid a \leq x < b\}$ *intervalo fechado à esquerda e aberto à direita;*
- iv) $(a, b) = \{x \in \mathbb{R} \mid a < x < b\}$ *intervalo aberto à esquerda e aberto à esquerda;*
- v) $(-\infty, b] = \{x \in \mathbb{R} \mid x \leq b\}$ *semi-reta esquerda, fechada, de origem b;*
- vi) $[a, +\infty) = \{x \in \mathbb{R} \mid x \geq a\}$ *semi-reta direita, fechada, de origem a;*
- vii) $(-\infty, b) = \{x \in \mathbb{R} \mid x < b\}$ *semi-reta esquerda, aberta, de origem b;*
- viii) $(a, +\infty) = \{x \in \mathbb{R} \mid x > a\}$ *semi-reta direita, aberta, de origem a;*
- ix) $(-\infty, +\infty) = \mathbb{R}$.

Notemos que os quatro primeiros são intervalos limitados e os cinco últimos são intervalos ilimitados. Além disso é importante ressaltar que $+\infty$ e $-\infty$ não são números reais, mas apenas símbolos para representar intervalos ilimitados.

Definição 36. *Seja $x \in \mathbb{R}$, definiremos valor absoluto de x como sendo x caso $x \geq 0$ e o oposto de x se $x < 0$. Denotaremos o valor absoluto de x por $|x|$. Assim,*

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

O valor absoluto de um número real $x \in \mathbb{R}$ é comumente chamado de módulo de x .

Dado um $x \in \mathbb{R}$, ou $x = 0$, ou $x > 0$, ou $x < 0$. Portanto poderíamos definir $|x| = \max\{-x, x\}$ ¹. Do ponto de vista geométrico, o módulo de um número real é igual a distância a qual esse número se encontra da origem, ou seja, do número zero.

Exemplo 35. *Observe pela figura abaixo que a distância do número -2 ao número 0 é igual a 2 . Portanto $|-2| = 2$.*



Proposição 15. *Um conjunto $X \subseteq \mathbb{R}$ é limitado se, e somente se, existe $a > 0$ tal que $|x| \leq a$, para todo $x \in X$.*

Teorema 18. *Sejam $x, a \in \mathbb{R}$. As seguintes afirmações são equivalentes;*

- i) $-a \leq x \leq a$;
- ii) $x \leq a$ e $-a \leq x$;
- iii) $|x| \leq a$.

Demonstração. De fato, $-a \leq x \leq a \Leftrightarrow [-a \leq x \text{ e } x \leq a] \Leftrightarrow [a \geq x \text{ e } a \geq -x] \Leftrightarrow a \geq |x|$.

A última equivalência vem do fato do $|x| = \max\{x, -x\}$. □

¹Aqui estamos denotando o máximo (maior elemento do conjunto) por \max (veja a Definição 15).

Corolário 6. *Dados $a, x, b \in \mathbb{R}$ tem-se $|x - a| \leq b$ se, e somente se, $a - b \leq x \leq a + b$.*

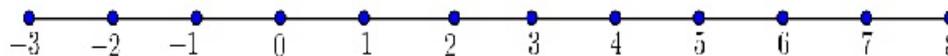
O corolário 6 nos diz que a distância de x a a ser menor ou igual a b é equivalente a dizer que x encontra-se entre $a - b$ e $a + b$.

O exemplo a seguir ilustra como se resolver uma equação envolvendo valor absoluto usando ideis geométricas.

Exemplo 36. *Vamos utilizar a ideia geométrica de módulo para resolver a equação e a inequação abaixo.*

a) $|x - 3| = 5$.

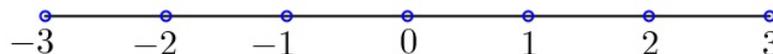
Solução:



Pela ideia geométrica de módulo temos que a distância do número x ao número 3 deve ser igual a 5. Portanto, os possíveis valores para x são, $x = 8$ ou $x = -2$.

b) $|x - 1| \leq 2$.

Solução:



A inequação nos diz que a distância do número x ao número 1 é menor ou igual a 2. Daí, $x \in [-1, 3]$ ou seja, $-1 \leq x \leq 3$.

Listamos a seguir as propriedades fundamentais do valor absoluto.

Teorema 19. *Para quaisquer que sejam $x, y, z \in \mathbb{R}$, valem as relações:*

i) $|x + y| \leq |x| + |y|$ (*desigualdade triangular*);

ii) $|x \cdot y| = |x| \cdot |y|$;

iii) $|x| - |y| \leq ||x| - |y|| \leq |x - y|$;

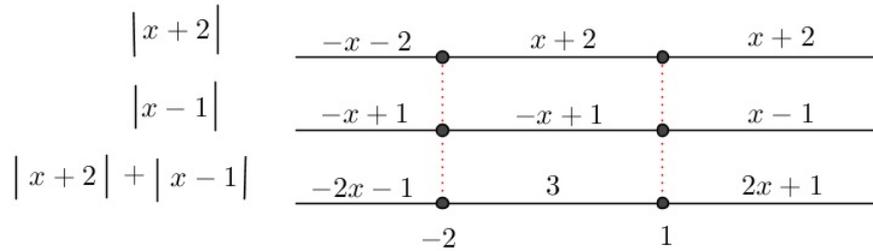
iv) $|x - z| \leq |x - y| + |y - z|$.

Demonstração. Prova do item i). Observe que $-|x| \leq x \leq |x|$ e $-|y| \leq y \leq |y|$, donde, por adição, $-(|x|+|y|) \leq x+y \leq |x|+|y|$. Portanto, pelo Teorema 18 segue que $|x+y| \leq |x|+|y|$.

A prova dos demais itens pode ser encontrada em [8], página 73. \square

Exemplo 37. Resolveremos a equação modular $|x + 2| + |x - 1| = 5$ usando a ideia geométrica.

solução: Observe o esquema abaixo:



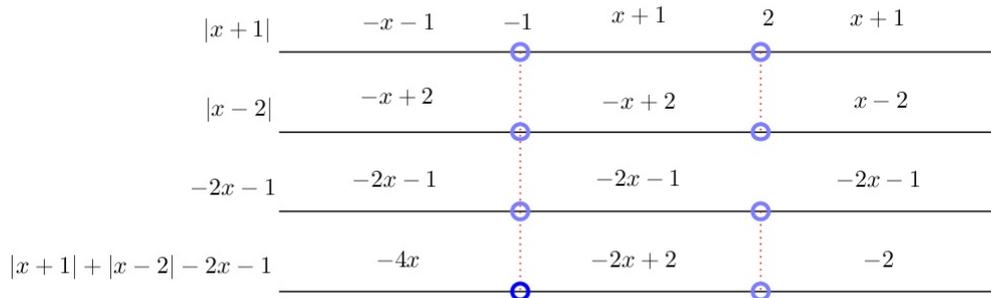
Observe que $|x + 2| + |x - 1| = \begin{cases} -2x - 1, & \text{se } x < -2, \\ 3, & \text{se } -2 \leq x \leq 1, \\ 2x + 1, & \text{se } x > 1. \end{cases}$

Portanto, $-2x - 1 = 5 \Leftrightarrow -2x = 6 \Leftrightarrow x = -3$ ou $2x + 1 = 5 \Leftrightarrow 2x = 4 \Leftrightarrow x = 2$.

Exemplo 38. Resolveremos a inequação modular $|x + 1| + |x - 2| \leq 2x + 1$ usando a ideia geométrica.

Solução: Resolver o problema $|x + 1| + |x - 2| \leq 2x + 1$ é equivalente a resolver o problema $|x + 1| + |x - 2| - 2x - 1 \leq 0$.

Observando o esquema abaixo temos:



Veja que $|x + 1| + |x - 2| - 2x - 1 = \begin{cases} -4x, & \text{se } x < -1, \\ -2x + 2, & \text{se } -1 \leq x \leq 2, \\ -2, & \text{se } x > 2. \end{cases}$. Analisando cada

uma das sentenças temos:

- I) $-4x \leq 0 \Rightarrow x \geq 0$ (Não serve!);
- II) $-2x + 2 \leq 0 \Rightarrow -2x \leq 2 \Rightarrow x \geq 1$, para $-1 \leq x \leq 2$;
- III) da mesma forma $-2 < 0$ para todo $x > 2$.

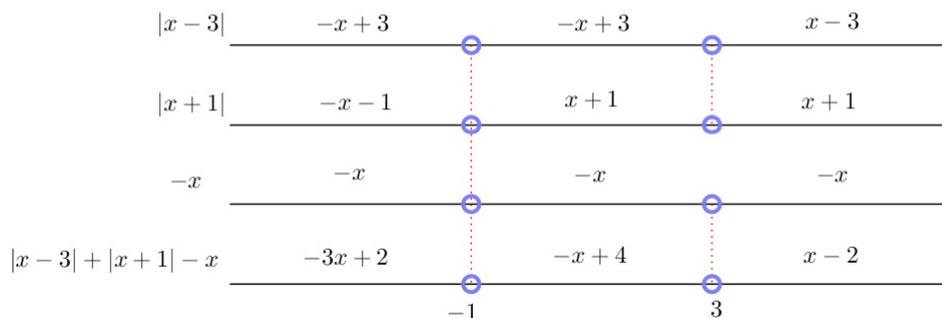
Portanto, a solução é dada pelo conjunto $S = \{x \in \mathbb{R} \mid x \geq 1\}$.

Segue logo abaixo mais um exemplo em que usaremos a ideia geométrica para resolvermos uma inequação modular. Veja que o esquema utilizado é muito útil para encontramos as sentenças que nos possibilitará a resolução do problema.

Exemplo 39. Utilizando a ideia geométrica resolveremos a inequação modular $|x - 3| + |x + 1| \geq x$.

Solução: Para iniciarmos observe que $|x - 3| + |x + 1| \geq x \Leftrightarrow |x - 3| + |x + 1| - x \geq 0$.

Daí,



$$\text{Portanto, } |x - 3| + |x + 1| - x = \begin{cases} -3x + 2, & \text{se } x < -1 \\ -x + 4, & \text{se } -1 \leq x \leq 3 \\ x - 2, & \text{se } x > 3 \end{cases}$$

Analisando cada uma das sentenças e sendo S_1 , S_2 e S_3 a solução dos itens I), II) e III) respectivamente temos:

I) $-3x + 2 \geq 0 \Rightarrow -3x \leq -2 \Rightarrow x \leq \frac{2}{3} \Rightarrow S_1 = (-\infty, \frac{2}{3}]$;

II) $-x + 4 \geq 0 \Rightarrow x \leq 4 \Rightarrow S_2 = (-\infty, 4]$;

III) $x - 2 \geq 0 \Rightarrow x \geq 2 \Rightarrow S_3 = [2, +\infty)$.

$\therefore S = S_1 \cup S_2 \cup S_3 = \mathbb{R}$.

O Teorema abaixo tem como objetivo mostrar que o conjunto \mathbb{R} é arquimediano.

Teorema 20. Em \mathbb{R} as seguintes afirmações são equivalentes;

- a) $\mathbb{N} \subset \mathbb{R}$ é ilimitado superiormente;

²O símbolo \therefore significa portanto.

- b) dados $a, b \in \mathbb{R}$, com $a > 0$, existe $n \in \mathbb{N}$ tal que $n \cdot a > b$;
 c) dado qualquer $a > 0$ em \mathbb{R} , existe $n \in \mathbb{N}$ tal que $0 < \frac{1}{n} < a$.

Demonstração. ($a \Rightarrow b$). Como \mathbb{N} é ilimitado, dados $a > 0$ e $b \in \mathbb{R}$, existe $n \in \mathbb{N}$ tal que $\frac{b}{a} < n$ e, portanto, $b < a \cdot n$.

($b \Rightarrow c$). Dado $a > 0$, existe, em virtude de b , um $n \in \mathbb{N}$ tal que $n \cdot a > 1$. Então $0 < \frac{1}{n} < a$.

($c \Rightarrow a$) Dado qualquer $b > 0$ existe, por c) um $n \in \mathbb{N}$ tal que $\frac{1}{n} < \frac{1}{b}$, ou seja $n > b$. Portanto, nenhum elemento positivo em \mathbb{R} pode ser cota superior de \mathbb{N} . \square

Exemplo 40. *Mostraremos que dados $a, b \in \mathbb{R}$ com $a \neq b$, sempre existe $c \in \mathbb{Q}$.*

Demonstração. Suponhamos sem perda de generalidade que $a < b$. Com isso observe que $b - a > 0$, ou seja, existe $n \in \mathbb{N}$ suficientemente grande tal que $(b - a) > \frac{1}{n}$.

Seja $A = \{m \in \mathbb{Z} \mid \frac{m}{n} \geq b\}$. A é um conjunto não-vazio de números inteiros, limitado inferiormente por $b \cdot n$. Seja $m_0 \in A$ o menor elemento de A . Logo $b \leq \frac{m_0}{n}$ mas, como $m_0 - 1 < m_0$, tem-se $\frac{m_0 - 1}{n} < b$.

Afirmção: $a < \frac{m_0 - 1}{n} < b$. De fato, caso não fosse verdade teríamos $\frac{m_0 - 1}{n} \leq a < b \leq \frac{m_0}{n}$. Tal fato contraria que $b - a \leq \frac{m_0}{n} - \frac{m_0 - 1}{n} = \frac{1}{n}$. Portanto o número $\frac{m_0 - 1}{n} \in \mathbb{Q}$ está entre a e b . \square

4.3 Representação decimal dos números reais

Vamos falar um pouco sobre as expressões decimais, que é uma maneira eficiente de representar os números reais. Iremos considerar apenas os números reais positivos, pois, para o caso dos números negativos bastará colocar um sinal negativo à esquerda do número.

Definição 37. *Uma expressão decimal é um símbolo da forma*

$$\alpha = a_0, a_1 a_2 \dots a_i \dots,$$

onde a_0 é um número inteiro maior ou igual a zero e $a_1, a_2, \dots, a_i, \dots$ são números inteiros tais que $0 \leq a_i \leq 9$. O dígito a_i chama-se i -ésimo dígito (ou i -ésima casa) da expressão decimal de α com $i \in \mathbb{N}^*$. A representação decimal de um número real pode ser finita ou infinita.

Observação 12. A expressão $\alpha = a_0, a_1 a_2 \dots a_i \dots$ representa o número

$$\alpha = a_0 + \frac{a_1}{10} + \frac{a_2}{100} + \frac{a_3}{1000} + \dots + \frac{a_i}{10^i} + \dots.$$

Exemplo 41. $m = 3, 12121212\dots$, $n = 4, 85$ são exemplos de representações decimais, sendo o primeiro deles um número cuja representação decimal é infinita e o segundo com representação decimal finita.

Teorema 21. Seja α um número real positivo, então existem inteiros positivos

$$a_0, a_1, a_2, \dots, a_i, \dots \in \mathbb{Z}, \text{ com } 0 \leq a_i \leq 9,$$

tais que $\alpha = a_0, a_1 a_2 a_3 \dots$

Demonstração. Seja $\lfloor \alpha \rfloor = a_0$. Então $a_0 \leq \alpha < a_0 + 1$. Se $\alpha = a_0$, então o próprio a_0 é a representação procurada. Caso $a_0 < \alpha < a_0 + 1$, iremos considerar o maior dos números

$$a_0, a_0 + \frac{1}{10}, a_0 + \frac{2}{10}, \dots, a_0 + \frac{9}{10}$$

que não supera α . Suponhamos que $a_0 + \frac{a_1}{10}$ seja o número procurado, então

$$\alpha_1 = a_0 + \frac{a_1}{10} \leq \alpha < a_0 + \frac{a_1 + 1}{10} = \beta_1.$$

Se $\alpha = \alpha_1$ a demonstração se encerra com $\alpha = a_0, a_1$. Caso contrário, toma-se o maior dos números,

$$a_0 + \frac{a_1}{10}, a_0 + \frac{a_1}{10} + \frac{1}{100}, \dots, a_0 + \frac{a_1}{10} + \frac{9}{100}$$

que não supera α . Se $a_0 + \frac{a_1}{10} + \frac{a_2}{100}$ é esse número, então

$$\alpha_2 = a_0 + \frac{a_1}{10} + \frac{a_2}{100} \leq \alpha < a_0 + \frac{a_1}{10} + \frac{a_2 + 1}{100} = \beta_2.$$

Se $\alpha = \alpha_2$, então $\alpha = a_0, a_1 a_2$ ficando assim concluída a demonstração. Caso $\alpha \neq \alpha_2$ repete-se o mesmo raciocínio. Daí termos duas possibilidades:

1^a) α tem uma representação decimal finita, ou seja, $\alpha = a_0, a_1 a_2 \dots a_p$ para algum índice p .

2^a) Não é possível encontrar inteiros positivos $a_0, a_1, a_2, \dots, a_p$, com $0 \leq a_i \leq 9$, para os quais tem-se $\alpha = a_0, a_1 a_2 \dots a_p$. Neste caso, devemos observar os seguintes subconjuntos de \mathbb{R} :

$$A = \{\alpha_1, \alpha_2, \dots\} \text{ e } B = \{\beta_1, \beta_2, \dots\}$$

Veja que qualquer elemento de A é menor que o respectivo elemento de B .

Por outro lado temos que dado um número real $\epsilon > 0$, seja p um número natural tal que seja válida $\frac{1}{10^p} < \epsilon$. Então,

$$\alpha_p - \beta_p = \left(a_0 + \frac{a_1}{10} + \dots + \frac{a_{p-1}}{10^{p-1}} + \frac{a_p + 1}{10^p} \right) - \left(a_0 + \frac{a_1}{10} + \dots + \frac{a_{p-1}}{10^{p-1}} + \frac{a_p}{10^p} \right) = \frac{1}{10^p} < \epsilon.$$

$$\alpha_p \leq \alpha < \beta_p \Rightarrow \alpha - \alpha_p < \beta_p - \alpha_p \Rightarrow \alpha - \alpha_p < \epsilon.$$

Considerando $n \geq p$ temos $\alpha_p \leq \alpha_n \leq \alpha$, e então $\alpha - \alpha_n \leq \alpha - \alpha_p < \epsilon$.

Por outro lado $|\alpha - \alpha_n| = \alpha - \alpha_n \Rightarrow |\alpha - \alpha_n| < \epsilon$, para todo $n \geq p$. Portanto, α se aproxima tanto quanto queiramos de algum α_n , ou seja,

$$a_0 + \frac{a_1}{10} + \frac{a_2}{10^2} + \dots = \alpha.$$

Logo, $\alpha = a_0, a_1 a_2 \dots$. □

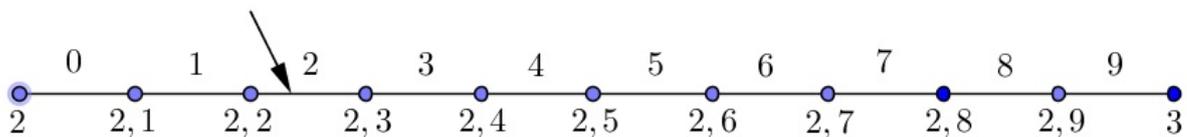
Na representação decimal de um número real $\alpha \geq 0$ temos aqui: a_0 é a parte inteira; a_1 é a primeira casa decimal; a_2 é a segunda casa decimal; \dots a_i é a i -ésima casa decimal, e assim por diante.

Se $\alpha < 0$ teremos $\alpha = -a_0, a_1 a_2 \dots$.

Exemplo 42. Faremos a representação decimal do número $\sqrt{5}$, até a terceira casa decimal utilizando o método usado na demonstração do Teorema 21.

Observe que $\lfloor \sqrt{5} \rfloor = 2$. Daí devemos procurar na sequência

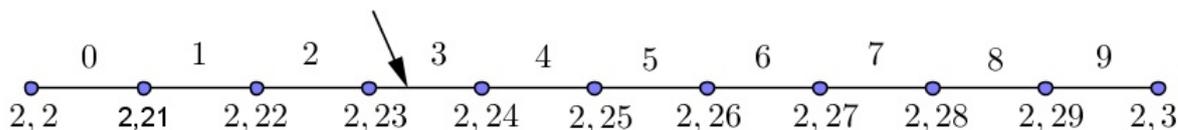
$$2, 2 + \frac{1}{10}, 2 + \frac{2}{10}, \dots, 2 + \frac{9}{10}$$



o maior número que não supere $\sqrt{5}$. Observe que $(2,2)^2 = 4,84$ e $(2,3)^2 = 5,29$; então esse número é 2,2. Usando a notação do teorema 21 temos $a_1 = 2$.

Assim, na sequência

$$2 + \frac{2}{10}, 2 + \frac{2}{10} + \frac{1}{100}, \dots, 2 + \frac{2}{10} + \frac{9}{100}$$



procure o maior número que não supere $\alpha = \sqrt{5}$. Como $(2, 23)^2 = 4,9729$ e $(2, 24)^2 = 5,0176$, esse número é $2, 23$. Logo, $\alpha_2 = 3$.

Vejamos agora em

$$2 + \frac{2}{10} + \frac{3}{100} + \frac{1}{1000}, 2 + \frac{2}{10} + \frac{3}{100} + \frac{2}{1000}, \dots, 2 + \frac{2}{10} + \frac{3}{100} + \frac{9}{1000}$$

o maior número que não supera $\sqrt{5}$.

Observando que $(2, 236)^2 = 4,999696$ e $(2, 237)^2 = 5,004169$, a resposta procurada é $2, 236$. Portanto,

$$\alpha_3 = 6 \text{ e } \sqrt{5} = 2, 236\dots$$

Com isso percebe-se que a representação decimal de um número real é apenas uma dentre infinitas outras representações. Nos dias atuais, além da representação decimal, é muito comum representar números reais na base dois (representação binária) e na base sessenta (representação sexagesimal). A representação binária é muito usada para se trabalhar com os números computacionalmente: qualquer cálculo em computadores e calculadoras é feito com números na forma binária. Há também vários jogos quebra-cabeças, como o bem conhecido jogo Nim e o quebra-cabeça dos anéis chineses, em que suas soluções dependem dessa base.

Já o sistema sexagesimal (base 60) foi muito usado pelos Babilônios, e ainda é utilizada para representar ângulos, minutos, segundos, e ano comercial.

O exemplo a seguir pode ser encontrado em [5].

Exemplo 43. Mostremos como se pode pesar, com uma balança de pratos simples, um peso ω de um número inteiro de libras, usando-se pesos de uma libra, duas libras, 2^2 libras, 2^3 libras e assim por diante, havendo apenas um peso de cada tipo.

Solução: Para resolver tal problema basta expressar ω na base 2. Para entendermos tomemos $\omega = 27$ libras. A representação binária do número 27 é 11011, daí temos que o número 27 pode ser escrito da forma $1 \cdot 2^4 + 1 \cdot 2^3 + 0 \cdot 2^2 + 1 \cdot 2^1 + 1 \cdot 2^0$, concluímos assim que para pesar um peso de 27 libras precisaremos de um peso de 16 libras, um peso de 8 libras, um peso de duas libras e um peso de uma libra.

Proposição 16. *Um número racional, na forma irredutível $\frac{a}{b}$, tem representação decimal finita se, e somente se, b possui apenas 2 e 5 como fatores primos.*

Demonstração. (\Rightarrow) Considere α um número cuja representação decimal seja finita, é sempre possível colocá-lo na forma $\frac{a}{b}$, com b sendo uma potência de 10. Lembre-se que qualquer potência de 10 tem apenas o 2 e o 5 como fatores primos.

(\Leftarrow) Suponha que seja possível escrever b da forma $2^m 5^n$, com m e n inteiros positivos ou nulos. Então, teremos duas possibilidades:

- 1) ou m é menor do que n ou igual a n ($m \leq n$);
- 2) ou então m é maior do que n ($m > n$).

Se $m \leq n$, multiplicaremos o numerador e o denominador da fração por 5^{m-n} .

$$\alpha = \frac{a}{2^m 5^n} \Rightarrow \alpha = \frac{a 5^{m-n}}{2^m 5^n 5^{m-n}} = \frac{a 5^{m-n}}{2^m 5^m} = \frac{a 5^{m-n}}{10^m}.$$

Portanto α tem representação finita.

O caso em que $n > m$ é feito de modo análogo. □

4.3.1 Dízimas Periódicas

Definição 38. *Uma expressão decimal $\alpha = 0, a_1 a_2 a_3 \dots$ chama-se uma dízima periódica simples, de período $a_1 a_2 a_3 \dots a_p$, quando os primeiros p dígitos após a vírgula se repetem indefinidamente na mesma ordem.*

Exemplo 44. *São dízimas periódicas simples as expressões:*

- 1) 0,333...
- 2) 0,4141...
- 3) 0,999...

A fração que representa a dízima periódica chama-se fração geratriz ou simplesmente geratriz. Para determiná-la procederemos da seguinte maneira:

$$\alpha = 0,333\dots \Rightarrow 10 \cdot \alpha = 3,333\dots \Rightarrow 9 \cdot \alpha = 3 \text{ pois fizemos } 10 \cdot \alpha - \alpha. \text{ Daí, } \alpha = \frac{3}{9} \Rightarrow \alpha = \frac{1}{3}.$$

Portanto, a geratriz de uma dízima periódica simples é a fração cujo numerador é formado pelo período da dízima e o denominador é formado por tantos noves quantos são os algarismos do período.

Definição 39. *Dízimas periódicas compostas são aquelas que após a vírgula possuem uma parte que não se repete, seguida de uma parte periódica.*

Por exemplo temos: $\alpha = 0,01222\dots$

Para determinar a fração geratriz da dízima acima, procederemos da seguinte forma:

$$\begin{aligned} \alpha = 0,01222\dots &\Rightarrow 100 \cdot \alpha = 1,222\dots \Rightarrow 100 \cdot \alpha = 1 + 0,222\dots \Rightarrow 100 \cdot \alpha = 1 + \frac{2}{9} \\ \Rightarrow 100 \cdot \alpha &= \frac{(9 \cdot 1) + 2}{9} \Rightarrow 100 \cdot \alpha = \frac{[(10 - 1) \cdot 1] + 2}{9} \Rightarrow 100 \cdot \alpha = \frac{10 - 1 + 2}{9} = \frac{12 - 1}{9} \\ &\Rightarrow 100 \cdot \alpha = \frac{12 - 1}{9} \Rightarrow \alpha = \frac{12 - 1}{900}. \end{aligned}$$

Portanto, toda representação decimal periódica representa um número racional.

Chegamos assim a uma regra muito utilizada na educação básica:

A fração geratriz de uma dízima periódica composta é a fração cujo numerador é formado pela parte não periódica, seguido do período menos a parte não periódica e cujo denominador é formado por tantos noves quantos são os algarismos do período seguido de tantos zeros quantos são os algarismos da parte não periódica.

4.4 Considerações Finais

Este trabalho consistiu na construção do conjunto dos números reais através dos cortes de Dedekind. No primeiro capítulo demos um embasamento teórico sobre os principais conceitos que serviriam de base para o desenvolvimento da dissertação. No segundo capítulo fizemos a construção do números racionais via relação de equivalência e com isso vimos que o conjunto dos números racionais têm algumas lacunas, por exemplo, $\sqrt{2}$ que é irracional.

No terceiro capítulo tratamos sobre a construção dos números reais, fazendo uma pequena mudança na definição que originalmente fora dada por Dedekind, tal mudança nos forneceu um arduo mas gratificante trabalho. O quarto capítulo trata sobre o valor absoluto de um número real, em que procuramos dar um breve embasamento sobre tal assunto, além disso falamos um pouco de um método bastante eficiente para representar a raiz quadrada de um número real, que é por aproximação de sequências de números racionais, finalizando assim esta dissertação.

Referências Bibliográficas

- [1] Boyer, C. B. História da Matemática. Editora da Universidade de São Paulo, São Paulo, 1974.
- [2] Carvalho, M.S., Lopes, M. L. M. L., Sousa. J. de M e., Fundamentos da Matemática Elementar. Editora Campus - Rio de Janeiro, 1984.
- [3] Domingues, Hygino, H. Fundamentos de Aritmética,. Editora da UFSC, Florianópolis, 2009.
- [4] Dulce, Osvaldo; Pompeo, José, N. Fundamentos de Matemática elementar, volume 9. Atual Editora, São Paulo, 2013.
- [5] Eves, H. Introdução à História da Matemática., Tradução, Domingues, Hygino, H. Editora Unicamp, Campinas - SP, 2004.
- [6] Ferreira, J. A Construção dos Números. Coleção Textos Universitários - SBM, Rio de Janeiro, 2011.
- [7] Grupo Escolar, Origem dos números inteiros. Disponível em:
<<http://www.grupoescolar.com/pesquisa/origem-dos-numeros-inteiros.html>> .
Acesso em 15.07.2016.
- [8] Lima, E. L. Curso de Análise, vol. 1. 12ª edição. Projeto Euclides, IMPA, 2008.
- [9] Lima, E. L; Carvalho, P. C. P; Morgado, A. C; Wagner, Eduardo. A Matemática do Ensino Médio, volume 1. Editora SBM, Rio de Janeiro, 1996.
- [10] Machado, G, M. A construção dos números. Trabalho de conclusão de curso, UFSCar, 2014.

- [11] Mec, Números Racionais. Disponível em:
<<http://webeduc.mec.gov.br/portaldoprofessor/matematica/condigital2/campos-numericos/numeros-rationais.html>>. Acesso em 15.07.2016.
- [12] Moura, R. P. Notas de aulas de Fundamentos de Matemática Elementar, UFPI 2014.
- [13] Neri, C e Cabral, M. Curso de Análise Real, 2^a ed. V2.4, Rio de Janeiro, 2011.
- [14] Neto, A. C. M. Tópicos de Matemática elementar, volume 1. Editora SBM, Rio de Janeiro, 2013.
- [15] Rudin, W. Princípios de Análise Matemática, Ao livro Técnico S.A. e Editora Universidade de Brasília, 1971.
- [16] Só matemática, Dedekind. Disponível em:
<<http://www.somatematica.com.br/biograf/dedekind.php>>. Acesso em 03.08.2016.
- [17] Só Matemática, Irracionais. Disponível em:
<<http://www.somatematica.com.br/irracionais.php>>. Acesso em 15.07.2016.
- [18] USP, Dedekind. Disponível em:
<<http://ecalculo.if.usp.br/historia/dedekind.htm>>. Acesso em 15.07.2016.