UNIVERSIDADE ESTADUAL DE CAMPINAS
Instituto de Matemática, Estatística e Computação Científica

MICHELE CALEFE

CONSTRUÇÃO DE CONJUNTOS NUMÉRICOS: DOS NÚMEROS INTEIROS AOS HIPERREAIS

CAMPINAS
2016

MICHELE CALEFE

CONSTRUÇÃO DE CONJUNTOS NUMÉRICOS: DOS NÚMEROS INTEIROS AOS HIPERREAIS

Dissertação apresentada ao Instituto de Matemática, Estatística e Computação Científica da Universidade Estadual de Campinas como parte dos requisitos exigidos para a obtenção do título de Mestre em Matemática, junto ao Programa de Mestrado Profissional em Matemática em Rede Nacional - PROFMAT.

Pedro José Catuogno

ESTE EXEMPLAR CORRESPONDE À VERSÃO FINAL DA DISSERTAÇÃO DEFENDIDA PELA ALUNA MICHELE CALEFE, E ORIENTADA PELO PROF. DR. PEDRO JOSÉ CATUOGNO.

Assinatura do Orientador

_____

CAMPINAS

2016

Agência(s) de fomento e nº(s) de processo(s): CAPES

Ficha catalográfica
Universidade Estadual de Campinas
Biblioteca do Instituto de Matemática, Estatística e Computação Científica
Ana Regina Machado - CRB 8/5467

C128c

Calefe, Michele, 1981-
Construção de conjuntos numéricos : dos números inteiros aos hiperreais / Michele Calefe. – Campinas, SP : [s.n.], 2016.

Orientador: Pedro José Catuogno.
Dissertação (mestrado profissional) – Universidade Estadual de Campinas, Instituto de Matemática, Estatística e Computação Científica.

1. Números reais. 2. Números hiperreais. 3. Dedekind, Cortes de. I. Catuogno, Pedro José,1959-. II. Universidade Estadual de Campinas. Instituto de Matemática, Estatística e Computação Científica. III. Título.

Informações para Biblioteca Digital

Título em outro idioma: Construction of the numerical sets : from integer to hyperreal numbers
Palavras-chave em inglês:
Real numbers
Hyperreal numbers
Dedekind cuts
Área de concentração: Matemática em Rede Nacional
Titulação: Mestra
Banca examinadora:
Pedro José Catuogno [Orientador]
Roberto Andreani
Tomas Edson Barros
Data de defesa: 17-10-2016
Programa de Pós-Graduação: Matemática em Rede Nacional

Dissertação de Mestrado Profissional defendida em 17 de outubro de 2016 e aprovada Pela Banca Examinadora composta pelos Profs. Drs.

Prof(a). Dr(a). Pedro Jose Catuogno

Prof(a). Dr(a). Roberto Andreani

Prof(a). Dr(a). Tomas Edson Barros

Ata da defesa com as respectivas assinaturas dos membros
encontra-se no processo de vida acadêmica do aluno.

Às pessoas mais importantes da minha vida: Fábio, Samir e Kalila.

“Na maior parte das ciências uma geração põe abaixo
o que a outra construiu, e o que uma estabeleceu a outra desfaz.
Somente na matemática é que cada geração
constrói um novo andar sobre a antiga estrutura”
— HERMANN HANKEL

Agradecimentos

Ao meu orientador, Professor Doutor Pedro Jose Catuogno, que pacientemente me incentivou a finalizar essa dissertação.

Aos membros da Banca Examinadora, Prof. Dr. Roberto Andreani e Prof. Dr. Tomas Edson Barros, pela leitura e correção dos erros do meu trabalho.

À Unicamp, por me acolher como aluna mais uma vez e me proporcionar condições para a obtenção de um novo título.

À Sociedade Brasileira de Matemática, pela criação do PROFMAT.

Aos colegas da turma 2012 do PROFMAT, pela amizade e acolhimento durante as aulas de sexta-feira.

Aos professores que ministraram as aulas do PROFMAT 2012.

À colega Camila, por facilitar muito a minha vida, ao ceder algumas vezes o espaço da sua casa.

À minha mãe Sueli e à minha irmã Rafaela, pelas vezes que saíram de suas casas e me acompanharam até Campinas para cuidar dos meus filhos, a fim de que eu pudesse comparecer às aulas sem precisar ficar longe deles.

À Rafaela e ao Leonardo, que dedicaram parte de suas férias na digitação e formatação desse trabalho. Sem a ajuda deles meu trabalho não teria sido concluído.

Aos amigos que prestigiaram minha defesa: Vicente, Célia (mãe do Vicente), Prof. Dr. Paulo Ruffino, Rafaela, Leonardo, Fábio, Samir e Kalila.

Ao meu querido marido, por todo o apoio durante os anos que levei para concluir o Mestrado.

Aos meus amados filhos, por me proporcionarem alegria nos momentos mais difíceis da minha vida.

À CAPES, pelo apoio financeiro.

Resumo

Este trabalho tem por objetivo fazer a construção dos conjuntos numéricos dos inteiros, racionais, reais e hiperreais. Para a construção dos números inteiros e racionais foi utilizado o livro "Números Reais" de Jorge Aragona. No caso dos números reais o livro "Principles of Mathematical Analysis" de W. Rudin e, para a construção dos números hiperreais o texto "An Introduction to Non-Standard Analysis" de I. Davis. Os textos foram utilizados para nortear esse trabalho, que também contempla os detalhes não feitos pelos autores citados. A construção dos conjuntos numéricos, em geral, apresenta características bem parecidas. A partir de um conjunto que serve como base, define-se um elemento que posteriormente será identificado com os elementos do conjunto a ser criado através de um isomorfismo. As construções dos inteiros, racionais e hiperreais feitas aqui utilizam classes de equivalência, o que não acontece na construção dos reais feita utilizando cortes de Dedekind, presente nesta dissertação. Além dos cortes de Dedekind, existem outras maneiras de construir os números reais. Cantor, por exemplo, fez a construção utilizando sequências de Cauchy, o que será comentado brevemente aqui. Além das construções apontadas acima, o último capítulo desta dissertação dá sugestões de como introduzir os tópicos estudados na matemática do Ensino Médio, com exemplos de atividades e trechos da história da matemática que podem ser utilizados.

Palavras-chave: números reais, números hiperreais, construção de conjuntos numéricos.

Abstract

The goal of this work is to make the construction of the numerical sets of the integer, rational, real and hyperreal numbers. For the construction of the integer and rational numbers it was used the book "Números reais" by Jorge Aragona. In the case of the real numbers it was used the book "Principles of Mathematical Analysis" by Walter Rudin and for the construction of the hyperreal numbers it was used the text "An introduction to the Non-Standard Analysis" by Isaac Davis. These texts were used to guide this work, which also includes details not made by these authors. The construction of numerical sets, in general, shows very similar characteristics. From a set, which serves as a base to define an element that will be identified as elements in a new set, which will be created through isomorphism. The constructions of integer, rational and hyperreal numbers made here use equivalence classes, which does not happen in the construction of the real numbers that were made using the Dedekind cuts, in this dissertation. In addition to Dedekind cuts, there are other ways to construct real numbers. Cantor, for instance, made the construction of real numbers using Cauchy sequences, which are going to be commented briefly here. Besides the construction mentioned above, the last chapter gives suggestions about how to introduce studied topics in the high school mathematics level, exemplifying activities and passages about mathematics history that can be used.

Keywords: real numbers, hyperreal numbers, construction of the numerical sets.

Lista de Figuras

Sumário

Introdução

Essa dissertação tem por objetivo fazer a construção de alguns dos conjuntos numéricos mais utilizados por estudantes e estudiosos em diversas áreas.

A ideia é mostrar que, apesar de cada construção ter sido feita em uma época diferente e por matemáticos diferentes, as ideias centrais dessas construções coincidem em muitos tópicos.

Em quase todas elas começamos por encontrar o ponto "falho"de um conjunto numérico, o qual motiva a definição de um objeto matemático que posteriormente será identificado com o elemento do conjunto a ser criado.

Montamos nessa dissertação uma escada. O primeiro degrau é representado pelo conjunto dos números naturais, assumido como verdadeiro com as formalizações de *Giusepp Peano*. Ao avançarmos, construiremos o conjunto dos números inteiros, identificando a subtração de números naturais como ponto de partida para essa realização.

Em seguida, notando que a divisão de números inteiros nem sempre é possível, criamos uma relação de equivalência que torna viável a construção do conjunto dos números racionais.

Fizemos a construção de $\mathbb{Z}$ e $\mathbb{Q}$ com base no livro "*Números Reais*"de *Jorge Aragona*, seguindo os passos do exercício deixado pelo autor aos seus estudantes e leitores.

O próximo degrau corresponde à construção dos números reais com base nos números racionais. Para essa construção utilizamos o livro "*Principles of Mathematical Analysis*" de *Walter Rudin* como direcionamento . O autor fez a construção segundo *R. Dedekind*, utilizando a ideia de "cortes".

Por fim, construímos uma extensão do conjunto dos números reais para contemplar os números infinitos e infinitesimais, fazendo assim o estudo do chamado conjunto dos números hiperreais. Para isso utilizamos o texto de *Isaac Davis* "*An Introduction to Nonstandard Analysis*".

Historicamente a construção dos conjuntos numéricos começou a partir das discussões sobre o que é um número real, como os números racionais e irracionais se distribuem ao longo da reta e se a identificação de $\mathbb{R}$ com a reta é realmente possível.

Antes disso, associava-se a reta aos números reais sem uma formalização. Apenas a partir da segunda metade do século XIX, matemáticos como *George Cantor* e *Richard Dedekind* começaram a repensar sobre as evidências geométricas que os faziam associar a reta ao conjunto dos números reais e sentiram a necessidade de buscar uma construção desse conjunto que demonstrasse

realmente essa identificação.

Dedekind acabou por pensar na construção dos números reais com base na definição de corte, que ele mesmo criou. A ideia de *Dedekind* baseia-se no fato de os números racionais também estarem localizados na reta numérica. Assim, dado um ponto da reta, esse ponto divide-a em dois subconjuntos distintos A_1 e A_2 de $\mathbb{Q}$. Cada ponto fará isso de forma única. Se o ponto que realizou o "corte" for racional, ele será o maior elemento em A_1 ou o menor elemento em A_2. Caso o ponto não esteja em nenhum dos dois conjuntos, ou seja, não pertença a $\mathbb{Q}$, ele será colocado num novo conjunto: O conjunto dos números irracionais I, que unido a $\mathbb{Q}$ formará o conjunto dos números reais $\mathbb{R}$.

Mais tarde, *Bertrand Russel* proporá uma breve modificação dessa teoria, preocupando-se apenas com um dos conjuntos limitados pelo número que produziu o corte, já que o outro fica determinado pelo primeiro.

Depois disso, várias perguntas sobre conjuntos começaram a ser formuladas e respondidas e aos poucos a Teoria dos Conjuntos foi sendo criada. *Dedekind* propôs a caracterização dos naturais e racionais em termos de conjuntos.

Além dele e de *Cantor*, outros matemáticos como *Frege* e *Peano* se dedicaram à construção dos conjuntos dos números naturais, provando suas principais propriedades.

A construção de $\mathbb{R}$ também foi feita de outras formas, como por exemplo, utilizando sequências de *Cauchy*. Esse trabalho foi publicado em 1872 por *George Cantor*, mesmo ano em que *Dedekind* publicou seu livro "*Stetigkeit und irrational Zahlen*", que contém a construção de $\mathbb{R}$ através de cortes.

Quase um século depois outros pontos da *Análise* entraram em discussão. As ideias de números infinitos e infinitesimais eram utilizadas frequentemente no cálculo, mas ninguém havia ainda verificado a existência dos mesmos no conjunto dos números reais.

Nesse contexto, em 1960 *Abraham Robinson* desenvolveu a *Análise não-standard*, no qual os números reais foram estendidos para incluir os números infinitos e os números infinitesimais.

Esse corpo estendido passou a ser chamado corpo dos números hiperreais.

Capítulo 1

Conceitos iniciais

Neste 1^o capítulo iremos introduzir os conceitos que serão utilizados ao longo desta dissertação, na construção dos conjuntos numéricos.

Começaremos com as ideias iniciais de conjuntos na seção 1.1. Na seção 1.2 aprofundaremos as ideias iniciais dando importância às relações e aos conjuntos ordenados. Na seção 1.3 trabalharemos com as estruturas algébricas que serão utilizadas nos capítulos posteriores e na seção 1.5 é feita uma breve explanação sobre sequências.

1.1 Conjuntos

Conjunto é um conceito fundamental em matemática mas podemos ter uma ideia intuitiva de *conjunto* como uma lista de objetos, coisas, números, etc. Para nomear um conjunto utilizamos letra maiúscula do nosso alfabeto e, para nomear seus elementos utilizamos letra minúscula.

***Exemplo* 1.** O conjunto dos números naturais de 1 a 5 pode ser escrito como $A = \{1,\ 2,\ 3,\ 4,\ 5\}$.

Além de representar um conjunto explicitando seus elementos, podemos definir um conjunto por uma propriedade.

***Exemplo* 2.** $B = \{x/x \text{ é par}\}$. Sabemos que os elementos de B são $0,\ 2,\ 4,\ 6,\ 8,\ \cdots$.

A definição abaixo relaciona conjunto e elemento através da utilização dos símbolos $\in$ ou $\notin$(pertence e não pertence).

***Definição* 1.** Se A é um conjunto e x é um membro de A, podemos escrever $x \in A$. Caso contrário escrevemos $x \notin A$.

O conjunto que não contém elemento algum será chamado conjunto vazio e será representado por $\emptyset$ ou $\{\}$. Caso o conjunto tenha pelo menos um elemento, será chamado não vazio.

Se A e B são conjuntos e todo elemento de A é também um elemento de B, dizemos que A é um subconjunto de B e denotamos $A \subset B$. Caso exista um elemento de B que não esteja em A, então A será um *subconjunto próprio* de B.

Se $A \subset B$ e $B \subset A$, escrevemos $A = B$.

***Exemplo* 3.** Dado o conjunto $A = \{1,\ 2,\ 3,\ 4\}$, temos que o conjunto $B = \{1,\ 2\}$ é um subconjunto próprio de A e denotamos $B \subset A$.

O conjunto vazio $\emptyset$ é considerado um subconjunto de qualquer conjunto. Cada conjunto é um subconjunto de si mesmo.

Podemos também ter conjuntos cujos elementos são conjuntos. Nesse caso nos referimos ao *conjunto de conjuntos* como *família de conjuntos*. É comum nomearmos uma família de conjuntos com letras manuscritas. Como exemplos: $\mathscr{A}$, $\mathscr{B}$, $\mathscr{C}$, etc.

***Exemplo* 4.** O conjunto $\mathscr{A} = \{\{1,\ 2\},\ \emptyset,\ \{3\}\}$ é uma família de conjuntos. Seus elementos são os conjuntos $\{1,\ 2\}$, $\emptyset$ e $\{3\}$.

A família de todos os subconjuntos de um conjunto J é o *conjunto de potência* de J. Denotaremos o conjunto de potência de J por $P(J)$. O número de elementos de $P(J)$, denotado por $n(P(J))$ pode ser calculado pela fórmula $n(P(J)) = 2^{n(J)}$.

***Exemplo* 5.** Dado o conjunto $J = \{1,\ 2,\ 3\}$, o conjunto $P(J)$ terá os seguintes elementos:
$\emptyset,\ \{1\},\ \{2\},\ \{3\},\ \{1,\ 2\},\ \{1,\ 3\},\ \{2,\ 3\},\ \{1,\ 2,\ 3\} = J$.

Observemos que $\emptyset$ e J são o primeiro e o último elementos da lista e sempre entrarão no conjunto de potência de qualquer conjunto.

O número de elementos de $P(J)$ será calculado por $2^3 = 8$, já que 3 é o número de elementos do conjunto J.

***Definição* 2.** Uma relação R em um conjunto A é uma relação de equivalência se:

- R for reflexiva, isto é, para cada $a \in A,\ (a, a) \in R$;
- R for simétrica, isto é, se $(a, b) \in R$ então $(b, a) \in R$;
- R for transitiva, isto é, se $(a, b) \in R$, e $(b, c) \in R$ então $(a, c) \in R$.

A próxima seção tratará de conjuntos ordenados parcialmente e conjuntos ordenados totalmente, finalizando com o lema de Zorn, uma importante ferramenta matemática.

***Definição* 3.** Seja J um conjunto não vazio e $P(J)$ o conjunto das partes de J. Dizemos que um conjunto não vazio $\mathscr{P} \subset P(J)$ é uma partição do conjunto J se :

- $\forall A_1,\ A_2 \in \mathscr{P},\ A_1 \neq A_2 \Longrightarrow A_1 \cap A_2 = \emptyset$;

- $\bigcup_{A \in \mathscr{P}} A = J$.

***Exemplo* 6.** Sejam $\mathbb{N} = \{1,\ 2,\ 3,\ 4,\ \ldots\}$, $P = \{2,\ 4,\ 6,\ \ldots\}$ e $I = \{1,\ 3,\ 5,\ \ldots\}$.

Temos $P \cap I = \emptyset$ (já que P é o conjunto dos números naturais pares e I é o conjunto dos números naturais ímpares).

Além disso, $P \cup I = \mathbb{N}$.

Portanto, $\{P,\ I\}$ é uma partição de $\mathbb{N}$.

***Exemplo* 7.** Considere $A = \{1,\ 2,\ 3,\ 4,\ 5,\ 6\}$, $B = \{1,\ 2\}$, $C = \{5\}$ e $D = \{3,\ 6\}$.

Nesse caso, $A \neq B \cup C \cup D$ pois $4 \in A$ mas $4 \notin B \cup C \cup D$. Assim, $\{B,\ C,\ D\}$ não é uma partição do conjunto A.

***Definição* 4.** Um conjunto $X \subset \mathbb{R}$ chama-se *denso* em $\mathbb{R}$ quando todo intervalo aberto (a, b) contém algum ponto de X.

***Exemplo* 8.** $\mathbb{Q}$ é denso em $\mathbb{R}$. Tomando o intervalo aberto $(a, b) \in \mathbb{R}$, temos $b > a$, o que implica em $b - a > 0$. Assim, existe um número natural p tal que $0 < \frac{1}{p} < b - a$. Agora, para $n \in \mathbb{Z}$,

os números da forma $\frac{n}{p}$ decompõem a reta real em intervalos de comprimento $\frac{1}{p}$, como uma

régua com unidade básica $\frac{1}{p}$. Como $\frac{1}{p} < b - a$, para algum dos $\frac{n}{p}$ deve valer $a < \frac{n}{p} < b$,

ou seja, $\frac{n}{p}$, para algum $n \in \mathbb{Z}$ está no intervalo (a, b). Como $\frac{n}{p}$ é racional, $\mathbb{Q}$ é denso em $\mathbb{R}$.

1.2 Conjuntos Ordenados

***Definição* 5.** Uma ordem parcial em um conjunto A é uma relação R em A, com as propriedades:

- Reflexiva, isto é, $(a,\ a) \in R$ para cada $a \in A$;
- Anti-simétrica, isto é, $(a,\ b) \in R$ e $(b,\ a) \in R$ implica em $a = b$;
- Transitiva, isto é, $(a,\ b) \in R$ e $(b,\ c) \in R$ implica em $(a,\ c) \in R$.

***Exemplo* 9.** Seja $\mathscr{A}$ uma família de conjuntos. A relação R em $\mathscr{A}$ definida por "A é um subconjunto de B" é uma ordem parcial em $\mathscr{A}$.

De fato,

- (Reflexiva) $A \subset A$ para cada $A \in \mathscr{A}$ pois para todo $x \in A$ temos $x \in A$;

- (Anti-simétrica) Se $A \subset B$ então $\forall x \in A$, temos $x \in B$. Por outro lado, se $B \subset A,\ \forall x \in B$ temos $x \in A$. Portanto $A = B$;

- (Transitiva) Se $A \subset B$ e $B \subset C$, então, se $x \in A$ temos $x \in B$. Também, se $x \in B$ então $x \in C$. Podemos então concluir que se $x \in A$ temos $x \in C$. Portanto, $A \subset C$.

***Exemplo* 10.** Considere a relação R em um conjunto finito $A \subset \mathbb{N}$ definida por "x divide y". R é uma ordem parcial em A, pois:

- (Reflexiva) Se $x \in A,\ \ x \mid x,$ para todo $x \in A$;

- (Anti-simétrica) Se $\ x \mid y$, e $\ y \mid x,$ então $\exists\ a$ e $b \in \mathbb{N}$ tais que $y = a \cdot x$ e $x = b \cdot y$.

  Podemos então escrever $y = a \cdot (b \cdot y)$ e assim, $y = a \cdot b \cdot y$. Temos então $a \cdot b = 1$ e, como $a,\ b \in \mathbb{N},\ a = b = 1$, o que implica em $x = y$;

- (Transitiva) Se $\ x \mid y\ $ e $\ y \mid z,\ $ existem $a,\ b\ \in \mathbb{N}$ tais que $y = a \cdot x$ e $z = b \cdot y$.

  Juntando as duas igualdades, temos: $z = b \cdot (a \cdot x)$ o que implica em $z = (b \cdot a) \cdot x$. Substituindo $b \cdot a$ por c, concluímos que $\ x \mid z,\ $ como queríamos.

  Assim, a relação R é uma ordem parcial em $A \subset \mathbb{N}$.

***Definição* 6.** Um conjunto A, com uma relação R de ordem parcial em A, é chamado *conjunto parcialmente ordenado*.

Observemos que um conjunto parcialmente ordenado consiste em um conjunto A e uma relação R em A. Algumas vezes esse par é denotado por $(A,\ R)$ ou $(A,\ \precsim)$.

Dois elementos a e b, num conjunto parcialmente ordenado, podem ser ou não comparáveis. Por isso utiliza-se a palavra *parcial* na definição de ordem parcial num conjunto A.

Se, por outro lado, cada dois elementos de um conjunto dado A podem ser comparados segundo uma relação R, dizemos que existe uma *ordem total* em A, a qual definiremos abaixo:

***Definição* 7.** Uma ordem total num conjunto A é uma ordem parcial em A (ou seja, com as propriedades reflexiva, anti-simétrica e transitiva), com a propriedade adicional $a \prec b,\ a = b$ ou $a \succ b$ para quaisquer elementos a e b pertencentes a A. Um conjunto A com uma ordem total em A é chamado *conjunto totalmente ordenado*, ou simplesmente ordenado.

***Definição* 8.** Seja $(I,\ <)$ um conjunto totalmente ordenado. Uma família de conjuntos $F_i\ ,\ i \in I$ é uma cadeia se $F_i \subset F_j\ $ para $\ i < j,\ i \in I$.

***Exemplo* 11.** A ordem parcial em um conjunto A qualquer de números naturais com a ordem natural é, na verdade, uma ordem total, pois dois números quaisquer são comparáveis.

***Exemplo* 12.** Considere a relação R no conjunto $A = \{1,\ 2,\ 3,\ 4,\ 5\}$ definida por "x divide y". Vimos, num exemplo anterior, que R é uma *ordem parcial*.

Porém, não podemos dizer que R é uma ordem total pois, por exemplo, 3 e 4 não são comparáveis já que 3 não divide 4 e 4 não divide 3.

Seja B um subconjunto de um conjunto parcialmente ordenado A. Um elemento m em A é um *limite inferior* de B se, para todo $x \in B$ temos $m \leq x$.

Caso para todo $x \in B$ tenhamos $x \leq m,\ m \in A$, dizemos que m é um *limite superior* de B.

O maior limite inferior de um conjunto B é o *ínfimo* desse conjunto. Denotaremos esse limitante por $inf\ B$. Analogamente, o menor limite superior de um conjunto B é o *supremo* desse conjunto e será denotado por $sup\ B$.

***Exemplo* 13.** Considere o subconjunto B dos números inteiros:

$$B = \{x/x \in \mathbb{Z},\ 4 \leq x^2 \leq 16\}$$

Os elementos desse conjunto são: $-4,\ -3,\ -2,\ 2,\ 3,\ 4$.

Observemos que B possui infinitos limitantes inferiores e infinitos limitantes superiores em $\mathbb{Z}$. Podemos citar -5 e -4 como limitantes inferiores e 4 e 5 como limitantes superiores. Porém, observemos que:

- O número -4 é o maior limitante inferior do conjunto B, isto é, $inf\ B = -4$;

  Como $-4 \in B$, -4 é o menor elemento desse conjunto podendo ser chamado de mínimo.

- O número 4 é o menor limitante superior do conjunto B, isto é, $sup\ B = 4$.

  Como $4 \in B$, 4 é o maior elemento desse conjunto, podendo ser chamado máximo.

  Obs: se o conjunto considerado fosse $B = \{x/x \in \mathbb{Z}, 4 < x^2 < 16\}$, então teríamos ainda $infB = -4$ (mas não o mínimo) e, $supB = 4$ (mas não o máximo).

O próximo exemplo mostra que nem sempre um conjunto possui ínfimo ou supremo.

***Exemplo* 14.** Considere um subconjunto de $\mathbb{Q}$ (o conjunto dos números racionais) dado por:

$$B = \{x/x \in \mathbb{Q}_+^*,\ 3 \leq x^2 \leq 5\},$$

ou seja, o conjunto dos números racionais tais que o quadrado está entre 3 e 5. Novamente, o conjunto em questão possui infinitos limites inferiores e infinitos limites superiores, porém, nesse caso, não existem $inf\ B$ nem $sup\ B$ já que não é possível encontrar o menor número racional maior que $\sqrt{5}$ nem o maior número racional menor que $\sqrt{3}$.

Observe que $\sqrt{3}$ e $\sqrt{5}$ não estão em $\mathbb{Q}$, por isso não podem ser considerados, respectivamente $inf\ B$ e $sup\ B$.

O próximo lema a ser enunciado será o Lema de Zorn. Esse lema será utilizado no capítulo 4, na demonstração do *lema do ultrafiltro*, no qual precisaremos mostrar a existência de um filtro maximal que será chamado ultrafiltro.

***Lema* 1.** (Lema de Zorn). Seja A um conjunto não-vazio ordenado parcialmente no qual todo subconjunto totalmente ordenado tem um limite superior em A. Então A contém pelo menos um elemento maximal.

***Definição* 9.** (Elemento maximal) Consideremos um conjunto ordenado A. Um elemento $a \in A$ é chamado de elemento maximal se $a \leq x$ implica em $a = x$.

Não será feita nessa dissertação a demonstração do lema de Zorn.

1.3 Algumas estruturas algébricas importantes

***Definição* 10.** Grupo: Um grupo é um conjunto G com uma operação, entre pares de G, denotada por $* : G \times G \to G$, denotada aqui por $(x,\ y) \longmapsto x * y$, com as seguintes propriedades:

1. Se $x \in G$ e $y \in G$, então $x * y$ está em G;
2. Associatividade: $(x * y) * z = x * (y * z)$ para todo $x,\ y,\ z \in G$;
3. G contém um elemento 0 tal que $0 * x = x * 0 = x$ para todo $x \in G$;
4. Para todo $x \in G$ corresponde um elemento $y \in G$ tal que $x * y = y * x = 0$.

***Definição* 11.** Grupo Abeliano: Um grupo abeliano é um grupo G cuja operação $*$ é comutativa, isto é, $x * y = y * x$ para todo $x,\ y \in G$.

***Exemplo* 15.** O conjunto dos números inteiros $\mathbb{Z}$ com a adição usual é um grupo abeliano.

***Exemplo* 16.** O conjunto das retas não horizontais e não verticais no plano $\mathbb{R}^2$ com coeficiente angular não nulo, isto é,

$$G = \{f : \mathbb{R} \to \mathbb{R} / f(x) = a \cdot x + b,\ a \neq 0,\ b \in \mathbb{R}\}$$

é um grupo com a operação "composição de funções". De fato,

- A composição de duas retas no plano, é uma reta no plano.

  Dadas duas retas no plano $f(x) = a \cdot x + b$ $(a \neq 0)$ e $g(x) = c \cdot x + d$ $(c \neq 0)$, temos

$$f \circ g(x) = a \cdot g(x) + b = a \cdot (c \cdot x + d) + b = (a \cdot c) \cdot x + (a \cdot d + b)$$

com $a \cdot c \neq 0$ (já que a e c são ambos não nulos).

Assim, $f \circ g(x) = (a \cdot c) \cdot x + (a \cdot d + b)$ é uma reta no plano.

- A composição de retas no plano é associativa.

  Dadas 3 retas $f(x) = a \cdot x + b,\ a \neq 0,\ \ g(x) = c \cdot x + d,\ \ c \neq 0$ e $h(x) = e \cdot x + f,\ \ e \neq 0$ temos:

  $$f \circ g(x) = (a \cdot c) \cdot x + (a \cdot d + b) \text{ (feito anteriormente) e,}$$

  $$(f \circ g) \circ h(x) = (a \cdot c) \cdot h(x) + (a \cdot d + b) = \ (a \cdot c) \cdot (e \cdot x + f) + a \cdot d + b = (a \cdot c \cdot e) \cdot x + (a \cdot c \cdot f + a \cdot d + b).$$

  Portanto, $(f \circ g) \circ h(x) = (a \cdot c \cdot e) \cdot x + (a \cdot c \cdot f + a \cdot d + b)$. Como $\ a,\ c$ e $e\ $ são não nulos, o produto $\ a \cdot c \cdot e\ $ é também não nulo.

  Agora, $g \circ h(x) = c \cdot h(x) + d = c \cdot (e \cdot x + f) + d = (c \cdot e) \cdot x + (c \cdot f + d)$ então, $f \circ (g \circ h)(x) = a \cdot ((c \cdot e) \cdot x + (c \cdot f + d)) + b = (a \cdot c \cdot e) \cdot x + (a \cdot c \cdot f + a \cdot d + b)$, como $a \cdot c \cdot e \neq 0$.

  Como $(f \circ g) \circ h(x) = f \circ (g \circ h)(x)$, a composição de funções de retas é associativa.

- A função identidade $f(x) = x$ é o elemento neutro da composição de funções pois, dada $g(x) = a \cdot x + b$, com $a \neq 0$ em G, temos $f \circ g(x) = g(x) = a \cdot x + b$ e $g \circ f(x) = a \cdot f(x) + b = a \cdot x + b$.

  Portanto, $f \circ g(x) = g \circ f(x) = g(x)$ para toda função $g(x)$ em G e $f(x) = x$ é o elemento neutro em G.

- Por último, para toda função $g(x) = a \cdot x + b,\ a \neq 0$ existe uma função $h(x) = g^{-1}(x)$ tal que $g \circ h(x) = h \circ g(x) = f(x)$ com $f(x) = x$ (a função identidade).

  A função $h(x)$ será dada por $h(x) = \dfrac{x}{a} - \dfrac{b}{a}$.

  Assim,

  $$g \circ h(x) = a \cdot \left(\frac{x}{a} - \frac{b}{a}\right) + b = a \cdot \frac{x}{a} - a \cdot \frac{b}{a} + b = x - b + b = x = f(x) \text{ e,}$$

  $$h \circ g(x) = \frac{a \cdot x + b}{a} - \frac{b}{a} = \frac{a \cdot x + b - b}{a} = \frac{a \cdot x}{a} = x = f(x).$$

Está provado então que o conjunto das retas não horizontais e não verticais no plano $\mathbb{R}^2$ com coeficiente angular diferente de 0 é um *grupo* cuja operação é a composição de funções.

Esse grupo não é abeliano pois, por exemplo, se tomarmos $f(x) = 2 \cdot x - 1$ e $g(x) = -x + 8$, temos, por um lado:

$f \circ g(x) = 2 \cdot g(x) - 1 = 2 \cdot (-x + 8) - 1 = -2 \cdot x + 16 - 1 = -2 \cdot x + 15$ e, por outro,

$$g \circ f(x) = -f(x) + 8 = -(2 \cdot x - 1) + 8 = -2 \cdot x + 1 + 8 = -2 \cdot x + 9.$$

Assim, $f \circ g(x) \neq g \circ f(x)$, o que prova que esse grupo não é abeliano.

Vamos definir agora a estrutura algébrica chamada *Anel*, na qual teremos *duas* operações.

***Definição* 12.** Anel: Um anel é um conjunto A com duas operações, adição e multiplicação, denotadas por + e $\cdot$ que satisfazem as seguintes propriedades:

1. Se $x \in A$ e $y \in A$, então a soma $x + y$ está em A;
2. A adição é comutativa: $x + y = y + x$ para todo $x, y \in A$;
3. A adição é associativa: $(x + y) + z = x + (y + z)$ para todo $x, y, z \in A$;
4. A contém um elemento 0 (elemento neutro) tal que $0 + x = x + 0 = x$ para todo $x \in A$. O elemento neutro é único;
5. Para cada $x \in A$ corresponde um único elemento $-x \in A$ tal que $x + (-x) = 0$;
6. Se $x,\ y \in A$, então o produto $x \cdot y \in A$;
7. A multiplicação é associativa: $(x \cdot y) \cdot z = x \cdot (y \cdot z)$ para todo $x, y, z \in A$;
8. Distributividade da multiplicação em relação à adição: Dados $x, y, z \in A$ temos $x \cdot (y + z) = = x \cdot y + x \cdot z$ e, $(x + y) \cdot z = x \cdot z + y \cdot z$.

***Definição* 13.** Caso a multiplicação admita um elemento $1 \in A$, $1 \neq 0$ tal que $x \cdot 1 = 1 \cdot x = x$, para todo $x \in A$, dizemos que A é um *anel com unidade*.

***Definição* 14.** Se $\forall\ x,\ y \in A,\ x \cdot y = y \cdot x$, dizemos que A é *comutativo*.

***Definição* 15.** Dizemos que A é um *anel sem divisores de zero* se, dados $x, y \in A$ temos $x \cdot y = 0 \Longrightarrow x = 0$ ou $y = 0$.

***Definição* 16.** Se um anel A for comutativo, com unidade e sem divisores de zero, ele será um *domínio de Integridade*.

***Exemplo* 17.** Um exemplo de anel não comutativo com unidade é o conjunto $M_{2\times 2}$ de todas as

$$\text{matrizes reais } 2 \times 2, \text{ da forma } \begin{pmatrix} a & b \\ c & d \end{pmatrix} \text{ com } a,\ b,\ c,\ d \in \mathbb{R}.$$

Para demonstrarmos a afirmação acima, precisamos definir igualdade de matrizes e as operações de adição e o produto de matrizes:

- Duas matrizes são iguais, ou seja, $\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} e & f \\ g & h \end{pmatrix}$, se e somente se $\begin{cases} a = e,\ b = f \\ c = g,\ d = h \end{cases}$

Operações com matrizes: Dados $a,\ b,\ c,\ d,\ e,\ f,\ g,\ h \in \mathbb{R}$, definimos:

- Adição: $\begin{pmatrix} a & b \\ c & d \end{pmatrix} + \begin{pmatrix} e & f \\ g & h \end{pmatrix} = \begin{pmatrix} a+e & b+f \\ c+g & d+h \end{pmatrix}$.

Observemos que cada um dos elementos $a+e,\ b+f,\ c+g,\ d+h$ pertence a $\mathbb{R}$ pois

$a,\ b,\ c,\ d,\ e,\ f,\ g,\ h \in \mathbb{R}$. Assim, $\begin{pmatrix} a+e & b+f \\ c+g & d+h \end{pmatrix} \in M_{2\times 2}$.

- Multiplicação: $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot \begin{pmatrix} e & f \\ g & h \end{pmatrix} = \begin{pmatrix} a\cdot e + b\cdot g & a\cdot f + b\cdot h \\ c\cdot e + d\cdot g & c\cdot f + d\cdot h \end{pmatrix}$.

Como $a\cdot e + b\cdot g,\ \ a\cdot f + b\cdot h,\ \ c\cdot e + d\cdot g,\ \ c\cdot f + d\cdot h$
pertencem a $\mathbb{R}$, $\begin{pmatrix} a\cdot e + b\cdot g & a\cdot f + b\cdot h \\ c\cdot e + d\cdot g & c\cdot f + d\cdot h \end{pmatrix} \in M_{2\times 2}$.

- O elemento neutro da adição é a matriz $0 = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$ (chamada matriz nula).

- O elemento neutro da multiplicação é dado por $1 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ (chamada matriz identidade).

Com isso, vamos mostrar que o conjunto M das matrizes reais $2\times$ 2 é um anel com unidade não comutativo.

Dados $a,\ b,\ c,\ d,\ e,\ f,\ g,\ h,\ i,\ j,\ k,\ l\ \in \mathbb{R}$ e as matrizes $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$, $B = \begin{pmatrix} e & f \\ g & h \end{pmatrix}$ e $C = \begin{pmatrix} i & j \\ k & l \end{pmatrix}$ temos:

- Comutatividade da adição. Devemos mostrar que $A + B = B + A$.

$$A + B = \begin{pmatrix} a & b \\ c & d \end{pmatrix} + \begin{pmatrix} e & f \\ g & h \end{pmatrix} = \begin{pmatrix} a+e & b+f \\ c+g & d+h \end{pmatrix} = \begin{pmatrix} e+a & f+b \\ g+c & h+d \end{pmatrix}$$

$$= \begin{pmatrix} e & f \\ g & h \end{pmatrix} + \begin{pmatrix} a & b \\ c & d \end{pmatrix} = B + A.$$

- Associatividade da adição:

$$(A+B)+C=\left[\begin{pmatrix}a & b\\ c & d\end{pmatrix}+\begin{pmatrix}e & f\\ g & h\end{pmatrix}\right]+\begin{pmatrix}i & j\\ k & l\end{pmatrix}=\begin{pmatrix}a+e & b+f\\ c+g & d+h\end{pmatrix}+\begin{pmatrix}i & j\\ k & l\end{pmatrix}$$

$$=\begin{pmatrix}(a+e)+i & (b+f)+j\\ (c+g)+k & (d+h)+l\end{pmatrix}=\begin{pmatrix}a+(e+i) & b+(f+j)\\ c+(g+k) & d+(h+l)\end{pmatrix}$$

$$=\begin{pmatrix}a & b\\ c & d\end{pmatrix}+\left[\begin{pmatrix}e & f\\ g & h\end{pmatrix}+\begin{pmatrix}i & j\\ k & l\end{pmatrix}\right]=A+(B+C).$$

- O elemento 0 definido acima como $0=\begin{pmatrix}0 & 0\\ 0 & 0\end{pmatrix}$ é o elemento neutro da adição.

  Vamos mostrar que $A+0=0+A=A$.

$$A+0=\begin{pmatrix}a & b\\ c & d\end{pmatrix}+\begin{pmatrix}0 & 0\\ 0 & 0\end{pmatrix}=\begin{pmatrix}a+0 & b+0\\ c+0 & d+0\end{pmatrix}=\begin{pmatrix}0+a & 0+b\\ 0+c & 0+d\end{pmatrix}=\begin{pmatrix}0 & 0\\ 0 & 0\end{pmatrix}+\begin{pmatrix}a & b\\ c & d\end{pmatrix}$$

  $=0+A=A$.

- O oposto de cada elemento $A=\begin{pmatrix}a & b\\ c & d\end{pmatrix}$ é o elemento $-A=-\begin{pmatrix}a & b\\ c & d\end{pmatrix}=\begin{pmatrix}-a & -b\\ -c & -d\end{pmatrix}$.

  Vamos mostrar que $A+(-A)=0$.

  Temos, $A+(-A)=\begin{pmatrix}a & b\\ c & d\end{pmatrix}+\begin{pmatrix}-a & -b\\ -c & -d\end{pmatrix}=\begin{pmatrix}a+(-a) & b+(-b)\\ c+(-c) & d+(-d)\end{pmatrix}=\begin{pmatrix}0 & 0\\ 0 & 0\end{pmatrix}=0.$

- A multiplicação é associativa. Vamos verificar que $(A\cdot B)\cdot C=A\cdot(B\cdot C)$.

$$(A\cdot B)\cdot C=\left[\begin{pmatrix}a & b\\ c & d\end{pmatrix}\cdot\begin{pmatrix}e & f\\ g & h\end{pmatrix}\right]\cdot\begin{pmatrix}i & j\\ k & l\end{pmatrix}=\left[\begin{pmatrix}a\cdot e+b\cdot g & a\cdot f+b\cdot h\\ c\cdot e+d\cdot g & c\cdot f+d\cdot h\end{pmatrix}\right]\cdot\begin{pmatrix}i & j\\ k & l\end{pmatrix}$$

$$=\begin{pmatrix}(a\cdot e+b\cdot g)\cdot i+(a\cdot f+b\cdot h)\cdot k & (a\cdot e+b\cdot g)\cdot j+(a\cdot f+b\cdot h)\cdot l\\ (c\cdot e+d\cdot g)\cdot i+(c\cdot f+d\cdot h)\cdot k & (c\cdot e+d\cdot g)\cdot j+(c\cdot f+d\cdot h)\cdot l\end{pmatrix}$$

$$=\begin{pmatrix}a\cdot e\cdot i+b\cdot g\cdot i+a\cdot f\cdot k+b\cdot h\cdot k & a\cdot e\cdot j+b\cdot g\cdot j+a\cdot f\cdot l+b\cdot h\cdot l\\ c\cdot e\cdot i+d\cdot g\cdot i+c\cdot f\cdot k+d\cdot h\cdot k & c\cdot e\cdot j+d\cdot g\cdot j+c\cdot f\cdot l+d\cdot h\cdot l\end{pmatrix}$$

$$= \begin{pmatrix} a\cdot(e\cdot i+f\cdot k)+b\cdot(g\cdot i+h\cdot k) & a\cdot(e\cdot j+f\cdot l)+b\cdot(g\cdot j+h\cdot l) \\ c\cdot(e\cdot i+f\cdot k)+d\cdot(g\cdot i+h\cdot k) & c\cdot(e\cdot j+f\cdot l)+d\cdot(g\cdot j+h\cdot l) \end{pmatrix}$$

$$= \begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot \begin{pmatrix} e\cdot i+f\cdot k & e\cdot j+f\cdot l \\ g\cdot i+h\cdot k & g\cdot j+h\cdot l \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot \left[\begin{pmatrix} e & f \\ g & h \end{pmatrix} \cdot \begin{pmatrix} i & j \\ k & l \end{pmatrix} \right] = A\cdot(B\cdot C).$$

- A multiplicação é distributiva em relação à adição. Vamos mostrar que $A\cdot(B+C)$ $= A\cdot B + A\cdot C$.

$$A\cdot(B+C) = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot \left[\begin{pmatrix} e & f \\ g & h \end{pmatrix} + \begin{pmatrix} i & j \\ k & l \end{pmatrix} \right] = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot \begin{pmatrix} e+i & f+j \\ g+k & h+l \end{pmatrix}$$

$$= \begin{pmatrix} a\cdot(e+i)+b\cdot(g+k) & a\cdot(f+j)+b\cdot(h+l) \\ c\cdot(e+i)+d\cdot(g+k) & c\cdot(f+j)+d\cdot(h+l) \end{pmatrix}$$

$$= \begin{pmatrix} (a\cdot e+b\cdot g)+(a\cdot i+b\cdot k) & (a\cdot f+b\cdot h)+(a\cdot j+b\cdot l) \\ (c\cdot e+d\cdot g)+(c\cdot i+d\cdot k) & (c\cdot f+d\cdot h)+(c\cdot j+d\cdot l) \end{pmatrix}$$

$$= \begin{pmatrix} a\cdot e+b\cdot g & a\cdot f+b\cdot h \\ c\cdot e+d\cdot g & c\cdot f+d\cdot h \end{pmatrix} + \begin{pmatrix} a\cdot i+b\cdot k & a\cdot j+b\cdot l \\ c\cdot i+d\cdot k & c\cdot j+d\cdot l \end{pmatrix}$$

$$= \left[\begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot \begin{pmatrix} e & f \\ g & h \end{pmatrix} \right] + \left[\begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot \begin{pmatrix} i & j \\ k & l \end{pmatrix} \right] = A\cdot B + A\cdot C.$$

Com a demonstração das propriedades acima verificamos que o conjunto $M_{2\times 2}$ das matrizes reais 2×2 é um anel. Para verificarmos que é um anel não comutativo, tomemos duas

matrizes $A = \begin{pmatrix} 1 & 2 \\ 0 & -3 \end{pmatrix}$ e $B = \begin{pmatrix} 3 & 2 \\ -2 & 0 \end{pmatrix}$.

O produto $A\cdot B$ será dado por $A\cdot B = \begin{pmatrix} 1 & 2 \\ 0 & -3 \end{pmatrix} \cdot \begin{pmatrix} 3 & 2 \\ -2 & 0 \end{pmatrix} = \begin{pmatrix} -1 & 2 \\ 6 & 0 \end{pmatrix}$. Por outro lado,

$B\cdot A = \begin{pmatrix} 3 & 2 \\ -2 & 0 \end{pmatrix} \cdot \begin{pmatrix} 1 & 2 \\ 0 & -3 \end{pmatrix} = \begin{pmatrix} 3 & 0 \\ -2 & -4 \end{pmatrix}$. Assim, $A\cdot B \neq B\cdot A$, o que mostra que o

conjunto $M_{2\times 2}$ das matrizes reais 2×2 é um anel não comutativo.

- Como a matriz $1 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ está em $M_{2\times 2}$ e, dada qualquer matriz $A \in M_{2\times 2}$ definida por

  $A = \begin{pmatrix} a & b \\ e & d \end{pmatrix}$ temos $A \cdot 1 = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} a & b \\ c & d \end{pmatrix} = 1 \cdot A = A,$

  o anel das matrizes 2×2, $M_{2\times 2}$ é um anel não comutativo com unidade.

- $M_{2\times 2}$ possui divisores de zero pois, podemos ter um produto de matrizes resultando na matriz nula sem que qualquer um dos fatores seja zero. Veja:

  Tomemos as matrizes $A = \begin{pmatrix} 1 & 2 \\ 0 & 0 \end{pmatrix}$ e $B = \begin{pmatrix} -2 & -4 \\ 1 & 2 \end{pmatrix}$.

  Ambas as matrizes são não nulas mas

$$A \cdot B = \begin{pmatrix} 1 & 2 \\ 0 & 0 \end{pmatrix} \cdot \begin{pmatrix} -2 & -4 \\ 1 & 2 \end{pmatrix} = \begin{pmatrix} -2+2 & -4+4 \\ 0+0 & 0+0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$$

A próxima estrutura a ser considerada é a mais completa e mais desejada para um conjunto numérico:

***Definição* 17.** Corpo: Um corpo é um conjunto F com duas operações, chamadas adição e multiplicação, que serão denotadas por + e $\cdot$ com as seguintes propriedades:

Axiomas da adição:

1. Se $x \in F$ e $y \in F$, então a soma $x + y$ está em F;
2. A adição é comutativa: $x + y = y + x$ para todo $x, y \in F$;
3. A adição é associativa: $(x + y) + z = x + (y + z)$ para todo $x, y, z \in F$;
4. Existência do elemento neutro aditivo. F contém um elemento 0 tal que $0 + x = x$ para todo $x \in F$;
5. Existência do elemento inverso aditivo (oposto). Para todo $x \in F$ corresponde um elemento $-x \in F$ tal que $x + (-x) = 0$.

Axiomas da mutiplicação:

1. Se $x \in F$ e $y \in F$, então o produto $x \cdot y$ está em F;

2. A multiplicação é comutativa: $x \cdot y = y \cdot x$ para todo $x, y \in F$;

3. A multiplicação é associativa: $(x \cdot y) \cdot z = x \cdot (y \cdot z)$ para todo $x, y, z \in F$;

4. Existência do elemento neutro multiplicativo. F contém um elemento $1 \neq 0$ tal que $x \cdot 1 = 1 \cdot x = x$ para todo $x \in F$;

5. Existência do inverso multiplicativo. Se $x \in F$ e $x \neq 0$ então existe um elemento $1/x \in F$ tal que $x \cdot (1/x) = 1$.

Lei Distributiva:

1. $x \cdot (y + z) = x \cdot y + x \cdot z$ se mantém para todo $x, y, z \in F$.

***Proposição* 1.** Os axiomas da adição implicam nas seguinte afirmações:

1. Lei do cancelamento aditivo: se $x+y = x+z$ então $y = z$. De fato, $y = 0+y = ((-x)+x)+y = (-x) + (x + y) = (-x) + (x + z) = (-x + x) + z = 0 + z = z$, isto é, $y = z$.

2. Unicidade do elemento neutro aditivo: se $x + y = x$, então $y = 0$. Se $x + y = x$, podemos escrever $x + y = x + 0$, o que implica, por (1), em $y = 0$.

3. Unicidade do inverso aditivo: se $x+y = 0$, então $y = -x$. Se $x+y = 0$, então $x+y = x+(-x)$ o que implica, por (1), em $y = -x$.

4. Oposto do oposto: $-(-x) = x$. Claramente, $-(-x) + (-x) = 0$. Assim, podemos escrever $-(-x) + (-x) = x + (-x)$, o que implica, por (1), em $-(-x) = x$.

***Proposição* 2.** Os axiomas da multiplicação implicam nas seguintes afirmações:

1. Lei do cancelamento multiplicativo: se $x \neq 0$ e $x \cdot y = x \cdot z$ então $y = z$.
   De fato, $y = 1 \cdot y = \left(\frac{1}{x} \cdot x\right) \cdot y = \frac{1}{x} \cdot (x \cdot y) = \frac{1}{x} \cdot (x \cdot z) = \left(\frac{1}{x} \cdot x\right) \cdot z = 1 \cdot z = z$, isto é, $y = z$.

2. Unicidade do elemento neutro multiplicativo: se $x \neq 0$ e $x \cdot y = x$ então $y = 1$.
   Se $x \cdot y = x$ então $x \cdot y = x \cdot 1$ e, por (1), temos $y = 1$.

3. Unicidade do inverso multiplicativo: se $x \neq 0$ e $x \cdot y = 1$, então $y = \frac{1}{x}$. De fato, $x \cdot y = 1$ implica em $x \cdot y = x \cdot \frac{1}{x}$ e, por (1), temos $y = \frac{1}{x}$.

4. Inverso do inverso: se $x \neq 0$ então $\frac{1}{1/x} = x$.
   Temos $\frac{1}{(1/x)} \cdot (1/x) = 1$, o que implica em $\frac{1}{(1/x)} \cdot (1/x) = x \cdot (1/x)$ e, por (1), $\frac{1}{(1/x)} = x$.

***Proposição* 3.** Os axiomas de corpo implicam nas seguintes afirmações, para todo $x,\ y,\ z \in F$:

1. Valem as igualdades $0 \cdot x = x \cdot 0 = 0$.

   Temos $0 \cdot x = (0+0) \cdot x \Longrightarrow 0 \cdot x = 0 \cdot x + 0 \cdot x$. Pela lei do cancelamento aditivo temos $0 \cdot x = 0$. Analogamente chegamos a $x \cdot 0 = 0$. E aí, $0 \cdot x = x \cdot 0 = 0$.

   Além disso, podemos concluir que $(-1) \cdot x = -x$ pois, $(-1) \cdot x + 1 \cdot x = ((-1)+1) \cdot x = 0 \cdot x = 0$. Assim, $(-1) \cdot x$ é o oposto de $1 \cdot x$, isto é, $(-1) \cdot x = -(1 \cdot x) = -x$.

2. Se $x \neq 0$ e $y \neq 0$, então $x \cdot y \neq 0$.

   Suponha $x \neq 0$ e $y \neq 0$, então existem $\dfrac{1}{x}$ e $\dfrac{1}{y}$ em F tal que o produto $\dfrac{1}{x} \cdot \dfrac{1}{y}$ existe e é igual a $\dfrac{1}{x \cdot y}$. Como $\dfrac{1}{x \cdot y}$ é o inverso de $x \cdot y$, devemos ter $x \cdot y \neq 0$.

3. $(-x) \cdot y = -(x \cdot y) = x \cdot (-y)$.

   Temos $(-x) \cdot y + x \cdot y = ((-x) + x) \cdot y = 0 \cdot y = 0$. Assim, $(-x) \cdot y = -(x \cdot y)$.

   Analogamente, $x \cdot (-y) + x \cdot y = x \cdot ((-y) + y) = x \cdot 0 = 0$. Assim, $x \cdot (-y)$ é o oposto de $x \cdot y$, isto é, $x \cdot (-y) = -(x \cdot y)$.

   Portanto, $(-x) \cdot y = -(x \cdot y) = x \cdot (-y)$.

4. $(-x) \cdot (-y) = x \cdot y$.

   Para verificar a igualdade acima, escrevemos:

   $(-x) \cdot (-y) + x \cdot (-y) = ((-x) + x) \cdot (-y) = 0 \cdot (-y) = 0$.

   Assim, $(-x) \cdot (-y)$ é o oposto de $x \cdot (-y) = -(x \cdot y)$, isto é, $(-x) \cdot (-y) = x \cdot y$.

***Definição* 18.** Um corpo ordenado é um corpo F que é também um conjunto ordenado tal que:

1. $x + y < x + z$ se $x, y, z \in F$ e $y < z$;

2. $x \cdot y > 0$ se $x \in F$, $y \in F$, $x > 0$, e $y > 0$.

   Se $x > 0$, x será chamado positivo; se $x < 0$, x será chamado negativo.

***Exemplo* 18.** O conjunto $\mathbb{Z}_p$ com p primo é um corpo.

Primeiramente observe que $\mathbb{Z}_p$ é o conjunto das classes residuais módulo p dado por $\{[0], [1], \ldots, [p-1]\}$, onde cada $[a] = \{x \in \mathbb{Z}, x \equiv a \mod p\}$. Em palavras mais simples $[a]$ é o conjunto dos números inteiros cujo resto da divisão de x por p é a. Assim, $x - a = k \cdot p,\ k \in \mathbb{Z}$. Além disso, em $\mathbb{Z}_p$ definiremos as seguintes operações:

- Adição: $[a] + [b] = [a + b]$ e,

- Multiplicação: $[a] \cdot [b] = [a \cdot b]$.

Com estas operações mostraremos que $\mathbb{Z}_p$ é um corpo para p primo. Comecemos verificando que as operações acima estão bem definidas, ou seja, ao mudarmos os representantes das classes $[a]$ e $[b]$, os valores de $[a+b]$ e $[a \cdot b]$ não se alterarão. Assim, tomando $a_1 \in [a]$ e $b_1 \in [b]$ temos $a_1 \equiv a \bmod p$ e $b_1 \equiv b \bmod p$ o que nos leva a $a_1 = a + k_1 \cdot p$ e $b_1 = b + k_2 \cdot p$ com $k_1,\ k_2 \in \mathbb{Z}$.

Assim, $a_1 + b_1 = (a+b) + (k_1+k_2)\cdot p \Rightarrow (a_1+b_1) \equiv (a+b) \mod p \Rightarrow a_1 + b_1 \in [a+b]$.

Assim, a classe da soma independe dos representantes das classes das parcelas. Portanto, a soma está bem definida em $\mathbb{Z}_p$.

Tomando os mesmos elementos acima temos:

$a_1 \cdot b_1 = (a + k_1 \cdot p) \cdot (b + k_2 \cdot p) = a \cdot b + a \cdot k_2 \cdot p + b \cdot k_1 \cdot p + k_1 \cdot p \cdot k_2 \cdot p = a \cdot b + (a \cdot k_2 + b \cdot k_1 + k_1 \cdot k_2 \cdot p)p$

ou seja, $a_1 b_1 \equiv (a \cdot b) \bmod p$.

Assim, a classe do produto independe dos representantes das classes dos fatores. Portanto, o produto está bem definido em $\mathbb{Z}_p$.

Agora verificaremos que $\mathbb{Z}_p$ é fechado com relação a adição. Para isso, considere $[a], [b] \in \mathbb{Z}_p$. Pela definição da adição em $\mathbb{Z}_p$ temos $[a] + [b] = [a + b]$, e, tomando $a_1 \in [a]$ e $b_1 \in [b]$, existem k_1 e $k_2 \in \mathbb{Z}$ tais que $a_1 = a + k_1 \cdot p$ e $b_1 = b + k_2 \cdot p$. Assim, podemos escrever:

$[a + b]$ é a classe das somas $a_1 + b_1$ com $a_1 \in [a]$ e $b_2 \in [b]$, o que implica em $a_1 + b_1 = (a+b)+(k_1+k_2)\cdot p$, o que nos leva a $a_1 + b_1 \equiv (a+b) \mod p$. Como $a_1 + b_1 \in [a+b],\ [a+b] \in \mathbb{Z}_p$.

Verificação das propriedades das operações $+$ e $\cdot$.

- A adição é comutativa pois $[a] + [b] = [a + b] = [b + a] = [b] + [a]$;
- A adição é associativa pois $([a] + [b]) + [c] = [a + b] + [c] = [(a + b) + c] = [a + (b + c)] = = [a] + [b + c] = [a] + ([b] + [c])$;
- O elemento $[0]$ está em $\mathbb{Z}_p$ e é o elemento neutro da adição, pois $[a] + [0] = [a + 0] = [a]$;
- O elemento inverso aditivo de $[a]$ denotado por $[-a]$ está em $\mathbb{Z}_p$ pois, $[a]+[-a] = [a+(-a)] = = [a - a] = [0]$;

  Agora vamos verificar que os axiomas da multiplicação são satisfeitos em $\mathbb{Z}_p$. Primeiramente mostraremos que, dados $[a], [b] \in \mathbb{Z}_p$, temos $[a] \cdot [b] \in \mathbb{Z}_p$. De fato, pela definição da multiplicação em $\mathbb{Z}_p$ temos $[a] \cdot [b] = [a \cdot b]$. Assim, tomando $a_1 \in [a]$ e $b_1 \in [b]$ temos $a_1 \equiv a \bmod p$ e $b_1 \equiv b \bmod p$, existindo $k_1, k_2 \in \mathbb{Z}$ tais que $a_1 = a + k_1 \cdot p$ e $b_1 = b + k_2 \cdot p$. Assim, $a_1 \cdot b_1 = (a + k_1 \cdot p) \cdot (b + k_2 \cdot p) = a \cdot b + k \cdot p$, com $k = a \cdot k_2 + b \cdot k_1 + k_1 \cdot k_2 \cdot p,\ k \in \mathbb{Z}$.

  Portanto, $a_1 \cdot b_1 \equiv a \cdot b \bmod p$, o que indica que $a_1 \cdot b_1$ pertence à classe residual de $[a \cdot b]$ módulo p, ou seja, $[a \cdot b] = [a] \cdot [b] \in \mathbb{Z}_p$.

- Agora, a multiplicação em $\mathbb{Z}_p$ é comutativa. De fato, dados $[a], [b] \in \mathbb{Z}_p$ temos $[a] \cdot [b] = = [a \cdot b] = [b \cdot a] = [b] \cdot [a]$;
- A multiplicação é associativa. Dados $[a], [b]$ e $[c] \in \mathbb{Z}_p$, temos $([a] \cdot [b]) \cdot [c] = [a \cdot b] \cdot [c] = = [(a \cdot b) \cdot c] = [a \cdot (b \cdot c)] = [a] \cdot [b \cdot c] = [a] \cdot ([b] \cdot [c])$;
- Existe o elemento neutro $[1]$ da multiplicação em $\mathbb{Z}_p$. De fato, $[1] \cdot [a] = [1 \cdot a] = [a]$;
- Dados $[a], [b]$ e $[c] \in \mathbb{Z}_p$, vale a distributiva da multiplicação em relação à adição. De fato, $[a] \cdot ([b] + [c]) = [a] \cdot [b + c] = [a \cdot (b + c)] = [a \cdot b + a \cdot c] = [a \cdot b] + [a \cdot c]$.

Falta verificar que os elementos não nulos de $\mathbb{Z}_p$ possuem inverso multiplicativo. Observemos então que, para que $[a] \in \mathbb{Z}_p$ seja invertível, deve existir $[b] \in \mathbb{Z}_p$ tal que $[a] \cdot [b] = [1]$. Assim, deve existir $k \in \mathbb{Z}$ tal que $a \cdot b - 1 = k \cdot p$, ou seja, $a \cdot b - k \cdot p = 1$. Concluímos então que a e p devem ser primos entre si. Como isso deve acontecer com todos os elementos de $\mathbb{Z}_p$, p deverá ser um número primo.

Assim, $\mathbb{Z}_p$ é um corpo para p primo.

Também vale a recíproca se $\mathbb{Z}_p$ é corpo então p é primo, pois se p não fosse primo, existiriam $c, d \in \{1, \cdots, p-1\}$ tais que $c \cdot d = p$, logo $[c] \cdot [d] = [0]$. Isto mostraria a existência de divisores de zero em $\mathbb{Z}_p$. Concluímos então que $\mathbb{Z}_p$ para p primo.

***Exemplo* 19.** O conjunto $\mathbb{Q} = \mathbb{Z} \times \mathbb{N}$ com a relação $(a, b) \equiv (c, d)$ se $a \cdot d = b \cdot c$ é um corpo. Observemos primeiramente que $\equiv$ é uma relação de equivalência. De fato, essa relação possui as propriedades reflexiva, simétrica e transitiva. Veja:

- $(a, b) \equiv (a, b)$ pois $a \cdot b = b \cdot a$, para todo $(a, b) \in \mathbb{Q}$ (reflexiva).
- Dados $(a, b), (c, d) \in \mathbb{Q}$, se $(a, b) \equiv (c, d)$, então $a \cdot d = b \cdot c$, o que implica em $d \cdot a = c \cdot b$ e $c \cdot b = d \cdot a$. Logo, $(c, d) \equiv (a, b)$ (simétrica).
- Por fim, dados $(a, b), (c, d)$ e (e, f) em $\mathbb{Q}$, se $(a, b) \equiv (c, d)$ e $(c, d) \equiv (e, f)$, é porque temos $a \cdot d = b \cdot c$ e $c \cdot f = d \cdot e$. Logo, podemos escrever $a \cdot d \cdot c \cdot f = b \cdot c \cdot d \cdot e$, o que implica, pela lei do cancelamento, em $a \cdot f = b \cdot e$, ou seja, $(a, b) \equiv (e, f)$ (transitiva).

Agora definiremos $\frac{a}{b} = [(a, b)] = \{(c, d)/(a, b) \equiv (c, d)\}$ e as operações adição dada por $\frac{a}{b} + \frac{c}{d} = [(a \cdot d + b \cdot c, b \cdot d)]$ e multiplicação dada por $\frac{a}{b} \cdot \frac{c}{d} = [(a \cdot c, b \cdot d)]$.
Vamos mostrar que as operações $+$ e $\cdot$ estão bem definidas.

- Adição

  Se $(a_1,\ b_1) \in [(a,\ b)]$ e $(c_1,\ d_1) \in [(c,\ d)]$, então $\begin{cases} a_1 \cdot b = b_1 \cdot a \\ c_1 \cdot d = d_1 \cdot c \end{cases}$ (1)

  Somando $(a_1,\ b_1)$ e $(c_1,\ d_1)$ temos $(a_1,\ b_1)+(c_1,\ d_1) = (a_1 \cdot d_1 + b_1 \cdot c_1,\ b_1 \cdot d_1)$. Para concluir nossa prova devemos verificar que $(a_1 \cdot d_1 + b_1 \cdot c_1,\ b_1 \cdot d_1) \equiv (a \cdot d + b \cdot c,\ b \cdot d)$. De fato, $(a_1 \cdot d_1 + b_1 \cdot c_1) \cdot b \cdot d = b_1 \cdot d_1 \cdot (a \cdot d + b \cdot c)$ pois $a_1 \cdot d_1 \cdot b \cdot d + b_1 \cdot c_1 \cdot b \cdot d = b_1 \cdot d_1 \cdot a \cdot d + b_1 \cdot d_1 \cdot b \cdot c$ já que, por (1) $a_1 b = b_1 a$ e $c_1 d = d_1 c$. Portanto, a soma está bem definida em $\mathbb{Q}$.

- Multiplicação

  Novamente, dados $(a_1,\ b_1) \in [(a,\ b)]$ e $(c_1,\ d_1) \in [(c,\ d)]$, temos $\begin{cases} a_1 \cdot b = b_1 \cdot a \\ c_1 \cdot d = d_1 \cdot c \end{cases}$ (1)

  Multiplicando $(a_1,\ b_1)$ e $(c_1,\ d_1)$ temos $(a_1,\ b_1) \cdot (c_1,\ d_1) = (a_1 \cdot c_1,\ b_1 \cdot d_1)$. Falta mostrar que $(a_1 \cdot c_1,\ b_1 \cdot d_1) \equiv (a \cdot c,\ b \cdot d)$. De fato, $a_1 \cdot c_1 \cdot b \cdot d = b_1 \cdot d_1 \cdot a \cdot c$, pois, por (1), trocando $a_1 \cdot b$ por $b_1 \cdot a$ e $c_1 \cdot d$ por $c \cdot d_1$ confirmamos a igualdade. Portanto, a multiplicação está bem definida em $\mathbb{Q}$.

Verificaremos abaixo que as operações definidas satisfazem as propriedades da definição de corpo.

- O conjunto $\mathbb{Q}$ é fechado com relação a adição. De fato, dados $(a,\ b), (c,\ d) \in \mathbb{Q}$ temos $(a,\ b) + (c,\ d) = (a \cdot d + b \cdot c,\ b \cdot d) \in \mathbb{Q}$ pois $a \cdot d + b \cdot c \in \mathbb{Z}$ e $b \cdot d \in \mathbb{N}$;

- A adição é comutativa. Tomando $(a,\ b), (c,\ d) \in \mathbb{Q}$ temos $(a,\ b)+(c,\ d) = (a \cdot d + b \cdot c,\ b \cdot d) =$ $= (c \cdot b + d \cdot a,\ d \cdot b) = (c,\ d) + (a,\ b)$;

- A adição é associativa. Tomando $(a,\ b), (c,\ d)$ e $(e,\ f) \in \mathbb{Q}$, temos $[(a,\ b) + (c,\ d)] + (e,\ f)$ $= (a \cdot d + b \cdot c,\ b \cdot d) + (e,\ f) = ((a \cdot d + b \cdot c) \cdot f + b \cdot d \cdot e,\ b \cdot d \cdot f) = (a \cdot d \cdot f + b \cdot c \cdot f + b \cdot d \cdot e,\ b \cdot d \cdot f)$ $= (a \cdot (d \cdot f) + b \cdot (c \cdot f + d \cdot e),\ b \cdot (d \cdot f)) = (a,\ b) + [(c \cdot f + d \cdot e,\ d \cdot f)] = (a,\ b) + [(c,\ d) + (e,\ f)]$;

- O elemento neutro de $\mathbb{Q}$ é $(0,\ 1)$ pois $(0,\ 1) + (c,\ d) = (0 \cdot d + 1 \cdot c,\ 1 \cdot d) = (c,\ d)$;

- O elemento inverso aditivo de $(a,\ b)$ em $\mathbb{Q}$, será denotado por $(-a,\ b)$, pois, $(a,\ b) + (-a,\ b) =$ $(a \cdot b + b \cdot (-a),\ b \cdot b)\ = (a \cdot b - b \cdot a,\ b^2) = (0,\ b^2) = (0,\ 1)$ para todo $b \in \mathbb{Q}$, pois $0 \cdot 1 = b^2 \cdot 0$;

- A multiplicação de dois elementos de $\mathbb{Q}$ está em $\mathbb{Q}$. De fato, tomando $(a,\ b), (c,\ d) \in \mathbb{Q}$ temos $(a,\ b) \cdot (c,\ d) = (a \cdot c,\ b \cdot d) \in \mathbb{Q}$, pois $a \cdot c \in \mathbb{Z}$ e $b \cdot d \in \mathbb{N}$;

- A multiplicação é comutativa. Podemos escrever $(a,\ b) \cdot (c,\ d) = (a \cdot c,\ b \cdot d)\ = (c \cdot a,\ d \cdot b) =$ $(c,\ d) \cdot (a,\ b)$;

- A multiplicação é associativa. Temos $[(a,\ b)\cdot(c,\ d)]\cdot(e,\ f) = (a\cdot c,\ b\cdot d)\cdot(e,\ f)$ $= ((a\cdot c)\cdot e,\ (b\cdot d)\cdot f) = (a\cdot(c\cdot e),\ b\cdot(d\cdot f)) = (a,\ b)\cdot[(c,\ d)\cdot(e,\ f)]$;

- Existe o elemento neutro $(1,1)\in\mathbb{Q}$ pois $(a,\ b)\cdot(1,1) = (a\cdot 1,\ b\cdot 1) = (a,\ b)$;

- Existe o elemento inverso multiplicativo de $(a,\ b)$, que será denotado por $(b,\ a)$. De fato, $(a,\ b)\cdot(b,\ a) = (a\cdot b,\ b\cdot a)$. Agora em $(a\cdot b,\ b\cdot a)$ temos $a\cdot b = b\cdot a$ o que implica em $a\cdot b\cdot 1 = b\cdot a\cdot 1$, ou seja, $(a\cdot b,\ b\cdot a) = (1,\ 1)$;

- Vale a distributiva da multiplicação em relação à adição. Dados $(a,\ b)$, $(c,\ d)$, $(e,\ f)$ em $\mathbb{Q}$, temos $(a,\ b)\cdot[(c,\ d)+(e,\ f)] = (a,\ b)\cdot(c\cdot f + d\cdot e,\ d\cdot f) = (a\cdot(c\cdot f + d\cdot e),\ b\cdot(d\cdot f))$ $= (a{\cdot}c{\cdot}f{+}a{\cdot}d{\cdot}e,\ b{\cdot}d{\cdot}f)$. Observemos que $(a{\cdot}c{\cdot}f{+}a{\cdot}d{\cdot}e,\ b{\cdot}d{\cdot}f)\equiv(a{\cdot}c{\cdot}f{\cdot}b{+}a{\cdot}d{\cdot}e{\cdot}b,\ b{\cdot}d{\cdot}f{\cdot}b)$, pois, $(a\cdot c\cdot f + a\cdot d\cdot e)\cdot b\cdot d\cdot f\cdot b = b\cdot d\cdot f\cdot(a\cdot c\cdot f\cdot b + a\cdot d\cdot e\cdot b)$.

  Assim, podemos escrever $(a,\ b)\cdot[(c,\ d)+(e,\ f)] = (a\cdot c\cdot f + a\cdot d\cdot e,\ b\cdot d\cdot f) =$ $(a\cdot c\cdot f\cdot b + a\cdot d\cdot e\cdot b,\ b\cdot d\cdot f\cdot b) = (a\cdot c\cdot(b\cdot f) + b\cdot d\cdot(a\cdot e),\ b\cdot d\cdot(b\cdot f)) =$ $(a\cdot c,\ b\cdot d)+(a\cdot e,\ b\cdot f) = (a,\ b)\cdot(c,\ d)+(a,\ b)\cdot(e,\ f)$.

  Concluímos que $\mathbb{Q} = \mathbb{Z}\times\mathbb{N}$ é um corpo com a relação $\equiv$ definida.

  No capítulo 2 faremos com mais detalhes essa demonstração utilizando uma notação mais apropriada.

***Definição* 19.** Um corpo F é chamado *completo* quando todo subconjunto não-vazio, limitado superiormente $X\subset F$, possui supremo em F.

***Exemplo* 20.** O subconjunto $X = \{x\in\mathbb{Q}\ /\ 0\leq x^2 < 5\}\subset\mathbb{Q}$ é não vazio pois $0\in X$, e é limitado superiormente. Porém, o menor limite superior de X não é um elemento de $\mathbb{Q}$ (já que $\sqrt{5}$ não é um número racional). Com esse contra-exempo concluímos que $\mathbb{Q}$ não é completo.

***Teorema* 1.** Num corpo ordenado F, as seguintes afirmações são equivalentes:

(i) $\mathbb{N}\subset F$ é ilimitado superiormente;

(ii) dados $a,b\in F$, com $a>0$, existe $n\in\mathbb{N}$ tal que $n\cdot a > b$;

(iii) dado qualquer $a>0$ em F, existe $n\in\mathbb{N}$ tal que $0<\dfrac{1}{n}<a$.

***Demonstração* 1.** (i) $\Rightarrow (ii)$

Como $\mathbb{N}$ é ilimitado, dados $a>0$ e $b\in F, \exists n\in\mathbb{N}$ tal que $\dfrac{b}{a}<n$ e, portanto, $b<a\cdot n$.

(ii) $\Rightarrow (iii)$

Dado $a>0$, existe por (ii), $n\in\mathbb{N}$ tal que $n\cdot a>1$. Então $0<\frac{1}{n}<a$.

(iii) $\Rightarrow (i)$

Dado qualquer $b > 0$ existe um $n \in \mathbb{N}$ tal que $\frac{1}{n} < \frac{1}{b}$, ou seja, $n > b$. Assim, nenhum elemento > 0 em F pode ser cota superior de $\mathbb{N}$. Também, nenhum elemento ≤ 0 pode ser. Logo $\mathbb{N}$ é ilimitado superiormente.

Um corpo ordenado F chama-se arquimediano quando nele é válida qualquer das três condições equivalentes do teorema acima.

***Exemplo* 21.** O corpo $\mathbb{Q}$ é arquimediano pois $\mathbb{N} \subset \mathbb{Q}$ é ilimitado superiormente.

1.4 Sequências

***Definição* 20.** Uma sequência de números reais é uma função $x : \mathbb{N} \to \mathbb{R}$, em que, para cada $n \in \mathbb{N}$, o valor $x(n) \in \mathbb{R}$ é representado por x_n e é chamado termo da sequência x de ordem n.

Uma sequência x pode ser representada por $(x_1,\ x_2, \cdots)$ ou $(x_n)_{n\in\mathbb{N}}$ ou (x_n).

***Definição* 21.** Uma sequência (x_n) é dita *limitada* quando o conjunto de seus termos é limitado, ou seja, quando existem $a, b \in \mathbb{R}$ tais que $a \leq x_n \leq b$ para todo $n \in \mathbb{N}$.

Observamos que, tomando $c = \max\{|a|,\ |b|\}$, podemos dizer que uma sequência é limitada

se $|x_n| \leq c$. Dizemos então, que (x_n) é limitada se e somente se $(|x_n|)$ é limitada.

Quando uma sequência (x_n) não é limitada, ela é dita *ilimitada*.

***Definição* 22.** Uma sequência (x_n) é *limitada superiormente* se existe $b \in \mathbb{R}$ tal que $x_n \leq b$ para todo $n \in \mathbb{N}$. Por outro lado, (x_n) é *limitada inferiormente* se existe $a \in \mathbb{R}$ tal que $x_n \geq a$ para todo $n \in \mathbb{N}$.

***Definição* 23.** Dada uma sequência $x = (x_n)_{x\in\mathbb{N}}$ de números reais, uma subsequência de x é a restrição da função x a um subconjunto infinito $\mathbb{N} = \{n_1 < n_2 < \cdots < n_i < \cdots\}$ de $\mathbb{N}$.

***Exemplo* 22.** $x_n = 1$ para todo $n \in \mathbb{N}$ é uma sequência *constante* da forma $(1, 1, 1, \cdots)$. Essa sequência é limitada pois o conjunto formado pelos seus termos é o conjunto unitário $\{1\}$ que é claramente limitado.

***Exemplo* 23.** $x_n = n$ para todo $n \in \mathbb{N}$ é a sequência $(1,\ 2,\ 3,\ \cdots,\ n,\ \cdots)$ que é limitada inferiormente apenas.

***Exemplo* 24.** A sequência de números reais $x_n = \frac{1}{n}$ para todo $n \in \mathbb{N}$, cujos termos são

$\left(1,\ \frac{1}{2},\ \frac{1}{3},\ \cdots,\ \frac{1}{n}, \cdots\right)$, é limitada pois seus termos estão entre 0 e 1.

***Definição* 24.** O número $a \in \mathbb{R}$ é *limite da sequência* (x_n) de números reais e, escreve-se $\lim\limits_n x_n = a$ quando para cada número real $\varepsilon > 0$, dado arbitrariamente, for possível obter um inteiro $n_0 \in \mathbb{N}$ tal que $|x_n - a| < \varepsilon$, sempre que $n > n_0$.

Assim, em uma linguagem menos formal, dizer que $a \in \mathbb{R}$ é o limite de uma sequência de números reais (x_n) significa dizer que seus termos se aproximam desse número a quando n assume valores muito grandes.

Quando $\lim\ x_n = a$, dizemos que a sequência (x_n) *converge* para a ou *tende* para a, escrevendo-se $x_n \to a$. Nesse caso a sequência x_n é denominada *convergente*. Caso contrário, a sequência é denominada divergente.

***Exemplo* 25.** A sequência $x_n = \dfrac{1}{n+1}$ é convergente e $\lim\ x_n = 0$ pois, para valores arbitrariamente grandes de n, $\dfrac{1}{n+1}$ tende para zero.

***Exemplo* 26.** A sequência $x_n = 2 \cdot n$ é divergente pois seus termos não se aproximam de nenhum valor quando tomamos valores de n arbitrariamente grandes.

***Teorema* 2.** Toda sequência limitada de números reais possui uma subsequência convergente.

***Demonstração* 2.** Seja (x_n) uma sequência. Como ela é limitada, suponha $x_n \in [a,\ b]$ para todo $n \in \mathbb{N}$. Consideremos o conjunto $A = \{t \in \mathbb{R};\ t \leq x_n$ para uma infinidade de índices $n\}$. Como $a \leq x_n \leq b$ para todo $n \in \mathbb{N}$, temos $a \in A$ e nenhum elemento de A é maior do que b. Portanto, A é não vazio e é limitado superiormente . Assim, existe $c = \sup A$. Para todo $\varepsilon > 0$, existe $t \in A$ com $c - \varepsilon < t$, logo há uma infinidade de índices n tais que $c - \varepsilon < x_n$. Por outro lado, como $c + \varepsilon \notin A$, existe apenas um número finito de índices n com $c + \varepsilon \leq x_n$. Concluímos então que, para uma infinidade de valores de n, temos $c - \varepsilon < x_n < c + \varepsilon$. Assim, c é limite de uma subsequência de (x_n).

***Definição* 25.** Seja (x_n) uma sequência de números reais. Ela se chama *sequência de Cauchy* quando, dado arbitrariamente um número real $\varepsilon > 0$, pode-se obter $n_0 \in \mathbb{N}$ tal que $m > n_0$ e $n > n_0$ implicam $|x_m - x_n| < \varepsilon$.

Mais simplificadamente, uma sequência (x_n) é de *Cauchy* se seus termos x_m e x_n se aproximam uns dos outros para valores arbitrariamente grandes de m e n.

***Teorema* 3.** Toda sequência convergente é de Cauchy.

***Demonstração* 3.** Seja $\lim\ x_n = a$. Assim, dado $\varepsilon > 0$, existe $n_0 \in \mathbb{N}$ tal que

$$m > n_0 \Rightarrow |x_m - a| < \frac{\varepsilon}{2} \text{ e } n > n_0 \Rightarrow |x_n - a| < \frac{\varepsilon}{2}.$$

Logo, $m, n > n_0 \Rightarrow |x_m - x_n| \leq |x_m - a| + |x_n - a| < \dfrac{\varepsilon}{2} + \dfrac{\varepsilon}{2} = \varepsilon$, o que mostra que (x_n) é uma sequência de Cauchy.

***Lema* 2.** Toda sequência de Cauchy é limitada.

***Demonstração* 4.** Seja (x_n) uma sequência de Cauchy. Assim, se $\varepsilon = 1$, obtemos $n_0 \in \mathbb{N}$ tal que $m, n \geq n_0 \Rightarrow |\ x_m - x_n\ | < 1$. Em particular $n \geq n_0 \Rightarrow\ |x_{n_0} - x_n| < 1$, ou seja, $n \geq n_0 \Rightarrow\ x_n \in (x_{n_0} - 1,\ x_{n_0} + 1)$.

Tomando agora o conjunto X formado pelos elementos $X = \{x_1,\ x_2,\ \cdots,\ x_{n_0} - 1,\ x_{n_0} + 1\}$, podemos encontrar α e β, respectivamente o menor e o maior elementos de X. Assim, $x_n \in [\alpha,\ \beta]$ para cada $n \in \mathbb{N}$. Logo, (x_n) é limitada.

***Lema* 3.** Se uma subsequência de Cauchy (x_n) possui uma subsequência convergindo para $a \in \mathbb{R}$ então $\lim\ x_n = a$.

***Demonstração* 5.** Dado $\varepsilon > 0$, existe $n_0 \in \mathbb{N}$ tal que $m, n\ >\ n_0\ \Rightarrow\ |x_m - x_n| < \dfrac{\varepsilon}{2}$.
Também existe $n_1 > n_0$ tal que $|x_{n_1} - a| < \dfrac{\varepsilon}{2}$. Portanto, $n > n_0\ \Rightarrow\ |x_n - a| \leq\ |x_n - x_{n_1}| + |x_{n_1} - a| < \dfrac{\varepsilon}{2} + \dfrac{\varepsilon}{2} = \varepsilon$. Assim, $\lim\ x_n = a$.

***Teorema* 4.** Toda sequência de Cauchy de números reais é convergente.

***Demonstração* 6.** Seja (x_n) uma sequência de Cauchy. Assim, ela é limitada. Logo, ela possui uma subsequência convergente. Pelo lema anterior (x_n) converge.

***Exemplo* 27.** A sequência $x_n = \dfrac{n}{n+1}$ converge para 1.

Notemos que $(x_n) = \left(\dfrac{1}{2},\ \dfrac{2}{3},\ \dfrac{3}{4},\ \cdots,\ \dfrac{n}{n+1},\ \cdots\right)$. Dado $\varepsilon > 0,\ |x_n - 1| = \left|\dfrac{n}{n+1} - 1\right|$

$= \left|\dfrac{n - n - 1}{n+1}\right| = \left|\dfrac{-1}{n+1}\right| = \dfrac{1}{n+1} < \varepsilon$ para $n > \dfrac{1}{\varepsilon} - 1$ (pois $\dfrac{1}{n+1} < \varepsilon\ \Rightarrow\ \dfrac{1}{\varepsilon} < n+1$

$\Rightarrow\ \dfrac{1}{\varepsilon} - 1 < n$).

Logo, dado $\varepsilon > 0$, existe $n_0 = \dfrac{1}{\varepsilon} - 1$ tal que $n > n_0\ \Rightarrow\ \left|\dfrac{n}{n+1} - 1\right| < \varepsilon$. O que implica em $\lim\limits_n\ \dfrac{n}{n+1} = 1$. Assim, (x_n) converge para 1.

Capítulo 2

Algumas construções iniciais

Para iniciarmos a construção dos conjuntos numéricos dos inteiros ($\mathbb{Z}$), racionais ($\mathbb{Q}$), reais ($\mathbb{R}$) e, posteriormente, do conjunto dos números Hiperreais, precisamos de um conjunto básico como ponto de partida. Esse conjunto básico será chamado *Conjunto dos Números Naturais* ($\mathbb{N}$) e a sua teoria foi fundamentada pela primeira vez em 1889 por *Giuseppe Peano* em seu livro "*Arithmetica Principia Nova Methodo Exposita*". A existência desse conjunto será admitida a partir de três conceitos primitivos e cinco axiomas conhecidos por *Axiomas de Peano*. Esses axiomas nos permitem conceber um conjunto de números ordenados sequencialmente no qual, cada elemento apresenta um sucessor. Assim, *Peano* nos propõe uma *teoria ordinal* (preocupada com a ordem e não com a ideia de quantidade, o que seria a preocupação de uma *teoria cardinal*).

Os conceitos adotados como primitivos por *Peano* são os seguintes: *número natural*, *zero*, *sucessor*. Os axiomas são os seguintes:

- 0 é um número natural;
- Todo número natural n possui um sucessor $\sigma(n)$;
- 0 não é sucessor de nenhum número;
- Se $\sigma(n) = \sigma(m)$, então $n = m$;
- Princípio da Indução Finita: seja S um conjunto de números naturais tal que:
  - $0 \in S$;
  - Se $n \in S$, então $\sigma(n) \in S$.

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

A partir desses axiomas, podemos definir as operações de adição e multiplicação nesse conjunto e verificar as suas propriedades operatórias.

Abaixo, listamos as operações adição e multiplicação, e algumas de suas proprie que serão utilizadas posteriormente.

Vamos indicar o conjunto dos números naturais por $\mathbb{N}$ e explicitar seus elementos:

$$\mathbb{N} = \{0, 1, 2, 4, \cdots\}$$

Além disso, definiremos as operações de adição por $(a, b) \mapsto a + b$ e de multiplicação por $(a, b) \mapsto a \cdot b$.

Assim, podemos escrever:

- As operações de adição e de multiplicação são bem definidas:

  $\forall a_1, b_1, a_2, b_2 \in \mathbb{N}$, $a_1 = a_2$ e $b_1 = b_2 \Rightarrow a_1 + b_1 = a_2 + b_2$ e $a_1 \cdot b_1 = a_2 \cdot b_2$.

- A adição e a multiplicação são comutativas.

  $\forall a, b \in \mathbb{N}$, temos $a + b = b + a$ e $a \cdot b = b \cdot a$.

- A adição e a multiplicação são associativas:

  $\forall a, b, c \in \mathbb{N}$, temos $(a + b) + c = a + (b + c)$ e $(a \cdot b) \cdot c = a \cdot (b \cdot c)$

- A adição e a multiplicação possuem elementos neutros, dados respectivamente por 0 e 1:

  Dado, $\forall a \in \mathbb{N}$, temos $a + 0 = 0 + a = a$ e $a \cdot 1 = 1 \cdot a = a$.

- A multiplicação é distributiva com relação à adição:

  $\forall a, b, c \in \mathbb{N}$, $a \cdot (b + c) = a \cdot b + a \cdot c$.

  Definiremos $\mathbb{N}^*$ como o conjunto dos números naturais não nulos. Temos $\mathbb{N}^* = \{1, 2, 3, 4, \cdots\}$.

  Além das propriedades acima, o conjunto dos números naturais também possui as seguintes propriedades:

- Integridade:

  Dados $a, b \in \mathbb{N}^*$, temos $a \cdot b \in \mathbb{N}^*$, ou seja, $\forall a, b \in \mathbb{N},\ a \cdot b = 0 \Rightarrow a = 0$ ou $b = 0$.

- Tricotomia:

  Dados $a, b \in \mathbb{N}$, uma e somente uma das relações abaixo é válida em $\mathbb{N}$:

  (i) $a = b$.

  (ii) $\exists c \in \mathbb{N}^*$, tal que $b = a + c$, ou equivalentemente, $a < b$.

  (iii) $\exists c \in \mathbb{N}^*$, tal que $a = b + c$, ou equivalentemente, $a > b$.

Além disso, $0 < a$ para todo $a \in \mathbb{N}^*$ (pois $0 + a = a$) e, se $a + b = 0$, então $a = b = 0$ (pois se $a \neq 0$ então $b < 0$, o que é absurdo; logo, $a = 0$).

Algumas proposições úteis:

***Proposição* 4.** $a \cdot 0 = 0\ \forall\ a \in \mathbb{N}$.

De fato, $a \cdot 0 = a \cdot (0 + 0) = a \cdot 0 + a \cdot 0$. Se $a \cdot 0 \neq 0$, então $a \cdot 0 \in \mathbb{N}^*$, e aí, $a \cdot 0 < a \cdot 0$, o que é absurdo. Logo, $a \cdot 0 = 0$.

***Proposição* 5.** A relação $<$ (menor do que) é transitiva:

$$\forall a, b, c \in \mathbb{N},\ a < b \text{ e } b < c \Rightarrow a < c.$$

De fato, se $a < b$ e $b < c$, temos que existem $d, f \in \mathbb{N}^*$ tais que $b = a + d$ e $c = b + f$.

Logo, usando a associatividade da adição, temos: $c = b + f = (a + d) + f = a + (d + f)$, com $d + f \in \mathbb{N}^*$. O que implica em $a < c$.

***Proposição* 6.** A adição é compatível e comutativa com respeito à relação "menor do que":

$$\forall a, b, c \in \mathbb{N},\ a < b \Leftrightarrow a + c < b + c.$$

De fato, se $a < b$, existe $d \in \mathbb{N}^*$, tal que $b = a + d$. Somando c a ambos os lados da última igualdade, pela comutatividade e associatividade da adição, temos:

$b + c = c + b = c + (a + d) = (c + a) + d = (a + c) + d$ o que mostra que $a + c < b + c$.

Reciprocamente, se $a + c < b + c$, pela tricotomia, temos:

(i) $a = b$, o que acarretaria $a + c = b + c$, que é falso;

(ii) $b < a$, o que acarretaria $b + c < a + c$, que é falso;

(iii) $a < b$, que é a possibilidade válida.

***Proposição* 7.** A multiplicação é compatível e comutativa com respeito à relação "menor do que":

$$\forall a, b \in \mathbb{N},\ \forall c \in \mathbb{N}^*, a < b \Leftrightarrow a \cdot c < b \cdot c$$

De fato, suponha $a < b$. Assim, $\exists d \in \mathbb{N}^*$ tal que $b = a + d$. Multiplicando esta igualdade por c de ambos os lados temos:

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

o que implica em $a \cdot c < b \cdot c$ pois, pela integridade temos $c \cdot d \in \mathbb{N}^*$

Reciprocamente, se $a \cdot c < b \cdot c$, pela tricotomia podemos ter:
(i) $a = b$, o que acarretaria $a \cdot c = b \cdot c$, o que é falso;

(ii) $b < a$, o que acarretaria $b \cdot c < a \cdot c$, o que é falso;

(iii) $a < b$, que é a possibilidade válida.

***Proposição* 8.** A adição é comparável e comutativa com respeito à igualdade:

$$\forall a, b, c \in \mathbb{N},\ a = b \Leftrightarrow a + c = b + c.$$

De fato, $a = b \Rightarrow a + c = b + c$ pois a adição é uma operação bem definida.

Agora, supondo $a + c = b + c$, podemos ter três possibilidades:
(i) $a < b$, o que implicaria em $a + c < b + c$ o que é falso;

(ii) $b < a$, o que implicaria em $b + c < a + c$, o que é falso;

(iii) $a = b$, que é a possibilidade válida.

***Proposição* 9.** A multiplicação é compatível e cancelativa com respeito à igualdade:

$$\forall a, b \in \mathbb{N},\ \forall c \in \mathbb{N}^*,\ a = b \Leftrightarrow a \cdot c = b \cdot c.$$

De fato, $a = b \Rightarrow a \cdot c = b \cdot c$ decorre do fato de a multiplicação ser uma operação bem definida em $\mathbb{N}$.

Agora, se $a \cdot c = b \cdot c$, então podemos ter três possibilidades:
(i) $a < b$, o que acarretaria $a \cdot c < b \cdot c$, o que é falso;

(ii) $b < a$, o que acarretaria $b \cdot c < a \cdot c$, o que é falso;

(iii) $a = b$, que é a possibilidade válida.

Para finalizar, notemos que $<$ não é uma relação de ordem, pois $<$ não é reflexiva. Mas, a relação $\leq$ (menor ou igual que) é,

- $\forall a \in \mathbb{N},\ a \leq a$ (reflexividade);

- $\forall a, b \in \mathbb{N},\ a \leq b$ e $b \leq a \Rightarrow a = b$ (anti-simetria);

- $\forall a, b, c \in \mathbb{N},\ a \leq b$ e $b \leq c \Rightarrow a \leq c$ (transitividade).

Usaremos também a notação $a \geq b$ se a é maior ou igual a b.

2.1 Construção do conjunto dos números inteiros

Os motivos que levaram o ser humano a pensar em números diferentes daqueles utilizados para contar estão ligados a questões práticas e operacionais. Mesmo o número zero (que não é tão "natural"quanto parece) demorou a ser visto como um número. Pensando assim, os números negativos só puderam ser pensados depois, já que o sinal negativo está ligado à posição do número em relação ao zero. De acordo com *Georges Ifrah* "A humanidade lutou durante milênios com sistemas inadequados e inoperantes, desprovidos de um símbolo que representasse o "nulo"ou "nada". Durante muito tempo, ela viveu também na impossibilidade de conceber os números "negativos"(-1, -2, -3, -4 etc), dos quais nos servimos correntemente hoje em dia para exprimir, por exemplo, uma temperatura abaixo de zero, ou ainda um saldo devedor numa conta bancária. Assim, durante muito tempo uma subtração como $3 - 5$ foi considerada impossível. Sabemos como a descoberta do zero varreu este obstáculo e

permitiu, de acordo com a famosa "regra dos sinais", a extensão dos números aritméticos ordinários (ditos"naturais") até os números "relativos", por adjunção a eles de seus "simétricos"em relação a zero".

A formalização do conceito de conjuntos numéricos não está ligada às ideias práticas do uso dos mesmos, mas a um movimento de construção da Teoria dos Conjuntos que ocorreu apenas no século XIX.

Este capítulo é dedicado à construção de dois conjuntos numéricos: o dos inteiros ($\mathbb{Z}$) e o conjunto dos números racionais ($\mathbb{Q}$). A construção de ambos os conjuntos será feita de acordo com a sequência que *Jorge Aragona* propôs em seu livro: *"Números Reais"*, no exercício 2 que se encontra nas páginas 30 a 36.

Para a construção do conjunto dos números inteiros, precisamos criar uma boa definição para os números pertencentes ao novo conjunto que se quer criar. Observemos que os elementos do conjunto serão definidos a partir do que temos, bucando uma nova definição para os resultados que não pertencem a $\mathbb{N}$. Assim, se quisermos construir $\mathbb{Z}$ a partir de $\mathbb{N}$, a subtração será um bom ponto de partida.

Quando $a, b \in \mathbb{N}$ e $a > b$, a diferença $a - b$ é um número de $\mathbb{N}$. Porém, quando $a < b$, é necessário criar uma boa definição para $a - b$, de modo que se $x,\ y,\ u,\ v \in \mathbb{N}$, com $x \geq y$, $u \geq v$ e, $x - y = u - v$, tenhamos, $y - x = v - u$. Assim, precisamos de alguma expressão equivalente à expressão $y - x = v - u$ dada.

Consideremos então a expressão equivalente a $y - x = v - u$, dada por $x + v = y + u$, que será condição necessária e suficiente para que as diferenças entre dois pares de números sejam iguais. Desse modo, trabalharemos apenas dentro de $\mathbb{N}$. Como a relação que associa cada par de números naturais à sua soma pode levar diversos pares diferentes a um mesmo resultado (como exemplo temos: $7 + 8 = 10 + 5 = 6 + 9$), tomaremos o quociente do conjunto $\mathbb{N} \times \mathbb{N}$ (já que estamos pegando um par de valores naturais) pela relação de equivalência descrita, ou seja, $\mathbb{N}^2/\equiv$, onde $\overline{(a, b)} \equiv \overline{(c, d)} \iff a + d = b + c$.

Podemos verificar que a relação $\equiv$ dada acima é uma relação de equivalência. De fato, $\equiv$ satisfaz as seguintes propriedades:

- Reflexividade: dado $(a, b) \in \mathbb{N}^2$, temos $(a, b) = (a, b)$ pois $a + b = b + a$, já que a adição é comutativa em $\mathbb{N}$;
- Simetria: tomando $(a, b), (c, d) \in \mathbb{N}^2$, tais que $(a, b) \equiv (c, d)$, podemos escrever $a + d = b + c \iff d + a = c + b \iff c + b = d + a \iff (c, d) \equiv (a, b)$;
- Transitividade: dados $(a, b), (c, d)$ e $(e, f) \in \mathbb{N}^2$ tais que $(a, b) \equiv (c, d)$ e $(c, d) \equiv (e, f)$, temos $a+d = b+c$ e $c+f = d+e$. O que nos permite escrever $(a+d)+(c+f) = (b+c)+(d+e) \iff a + (d + c) + f = b + (c + d) + e$.

$$\begin{cases} (a,b) \equiv (a_1,b_1) \Rightarrow a+b_1 = b+a_1 \ (1) \text{ e} \\ (c,d) \equiv (c_1,d_1) \Rightarrow c+d_1 = d+c_1 \ (2) \end{cases}$$

Assim, pela definição da soma podemos escrever:

$(a,b)+(c,d) = (a+c, b+d)$ e $(a_1,b_1)+(c_1,d_1) = (a_1+c_1, b_1+d_1)$.

Para que a adição esteja bem definida, devemos ter, $(a_1+c_1, b_1+d_1) \equiv (a+c, b+d)$.

De fato, $a_1+c_1+b+d = (a_1+b)+(c_1+d)$ e, pelas igualdades (1) e (2) ficamos com $a_1+c_1+b+d = (a_1+b)+c_1+d = a+b_1+c+d_1 = b_1+d_1+a+c$.

Isso mostra que $(a_1+c_1, b_1+d_1) \equiv (a+c, b+d)$ o que implica na boa definição da operação adição.

Pela lei do cancelamento com respeito a igualdade ficamos com $a+f = b+e$ o que implica em $(a,b) \equiv (e,f)$.

Temos então que a relação $\equiv$ dada acima é uma relação de equivalência. Posteriormente definiremos o número inteiro como a classe de equivalência de um par $(a,b) \in \mathbb{N}^2$ módulo a relação de equivalência dada acima, ou seja, o número inteiro será a diferença $a-b$ com $(a,b) \in \mathbb{N}^2$.

Agora introduziremos as seguintes operações em $\mathbb{N} \times \mathbb{N}/\equiv$:

$$\text{Adição: } \overline{(a,b)} + \overline{(c,d)} := \overline{(a+c, b+d)}$$
$$\text{Multiplicação: } \overline{(a,b)} \cdot \overline{(c,d)} := \overline{(a \cdot c + b \cdot d, a \cdot d + b \cdot c)}$$

Mostraremos que essas operações estão bem definidas em $\mathbb{N}^2/\equiv$, isto é, que as operações definidas independem dos representantes (a_1,b_1) e (c_1,d_1) respectivamente das classes $\overline{(a,b)}$ e $\overline{(c,d)}$ em $\mathbb{N}^2$.

- Adição: tomando as classes $\overline{(a,b)}$ e $\overline{(c,d)}$ e representantes (a_1,b_1) e (c_1,d_1) respectivamente dessas classes, temos $(a,b) \equiv (a_1,b_1)$, o que implica em $a+b_1 = b+a_1$ (1) e, $(c,d) \equiv (c_1,d_1)$, o que implica em $c+d_1 = d+c_1$ (2). Podemos então escrever $(a_1+b_1)+(c_1+d_1) = (a_1+c_1,\ b_1+d_1)$ que é equivalente a $(a+c,\ b+d)$ pois, nesse caso, por (1) e (2), $a_1+c_1+b+d = b_1+d_1+a+c \Rightarrow a+c_1+b_1+d = a+c_1+b_1+d$. Portanto, a soma independe dos representantes escolhidos, isto é, está bem definida.

- Multiplicação: tomando as classes $\overline{(a,b)}$ e $\overline{(c,d)}$ e representantes (a_1,b_1) e (c_1,d_1) respectivamente nessas classes, temos $(a,b) \equiv (a_1,b_1)$, o que implica em $a+b_1 = b+a_1$ (1a) e, $(c,d) \equiv (c_1,d_1)$, o que implica em $c+d_1 = d+c_1$ (1b).

  A partir dessas igualdades devemos mostrar que

(a $\cdot c + b \cdot d,\ a \cdot d + b \cdot c) \equiv (a_1 \cdot c_1 + b_1 \cdot d_1,\ a_1 \cdot d_1 + b_1 \cdot c_1)$, que é equivalente mostrar que

$$a \cdot c + b \cdot d + a_1 \cdot d_1 + b_1 \cdot c_1 = a \cdot d + b \cdot c + a_1 \cdot c_1 + b_1 \cdot d_1 \qquad (2)$$

A verificação de (2), usando $(1a)$ e $(1b)$ segue de:

$$\begin{aligned}
a \cdot c + b \cdot d + a_1 \cdot d_1 + b_1 \cdot c_1 + b_1 \cdot c &= (a + b_1) \cdot c + b \cdot d + a_1 \cdot d_1 + b_1 \cdot c_1 \\
&= (b + a_1) \cdot c + b \cdot d + a_1 \cdot d_1 + b_1 \cdot c_1 \\
&= b \cdot c + a_1 \cdot c + b \cdot d + a_1 \cdot d_1 + b_1 \cdot c_1 \\
&= b \cdot c + a_1 \cdot (c + d_1) + b \cdot d + b_1 \cdot c_1 \\
&= b \cdot c + a_1 \cdot (d + c_1) + b \cdot d + b_1 \cdot c_1 \\
&= b \cdot c + a_1 \cdot d + a_1 \cdot c_1 + b \cdot d + b_1 \cdot c_1 \\
&= b \cdot c + (a_1 + b) \cdot d + a_1 \cdot c_1 + b_1 \cdot c_1 \\
&= b \cdot c + (a + b_1) \cdot d + a_1 \cdot c_1 + b_1 \cdot c_1 \\
&= b \cdot c + a \cdot d + b_1 \cdot d + a_1 \cdot c_1 + b_1 \cdot c_1 \\
&= b \cdot c + a \cdot d + b_1 \cdot (d + c_1) + a_1 \cdot c_1 \\
&= b \cdot c + a \cdot d + b_1 \cdot (d_1 + c) + a_1 \cdot c_1 \\
&= b \cdot c + a \cdot d + b_1 \cdot d_1 + b_1 \cdot c + a_1 \cdot c_1 \\
&= a \cdot d + b \cdot c + a_1 \cdot c_1 + b_1 \cdot d_1 + b_1 \cdot c.
\end{aligned}$$

Portanto, a multiplicação independe dos representantes escolhidos, ou seja, está bem definida.

Concluímos então que a soma e o produto estão bem definidos em $\mathbb{N}^2/\equiv$. Vamos mostrar agora que $\mathbb{N}^2/\equiv$ é um anel unitário e comutativo.

Agora verificaremos que o conjunto $\mathbb{N}^2/\equiv$ munido das operações adição e multiplicação definidas acima é um anel unitário e comutativo. Para isso, verificaremos que esse conjunto satisfaz as condições da definição desta estrutura algébrica.

Dados $(\overline{a, b})$, $(\overline{c, d}) \in \mathbb{N}^2/\equiv$, temos $(\overline{a, b}) + (\overline{c, d}) = (\overline{a + c,\ b + d})$. Como $a, b, c, d \in \mathbb{N}$, $a + c$ e $b + d \in \mathbb{N}$, e aí, $(\overline{a + c,\ b + d}) \in \mathbb{N}^2/\equiv$.

- A adição é comutativa. Dados $\overline{(a, b)}$, $\overline{(c, d)} \in \mathbb{N}^2/\equiv$, temos $\overline{(a, b)} + \overline{(c, d)} = \overline{(a + c, b + d)}$ $= \overline{(c + a, d + b)} = \overline{(c, d)} + \overline{(a, b)}$.

- A adição é associativa. Sejam $\overline{(a, b)}, \overline{(c, d)}, \overline{(e, f)} \in \mathbb{N}^2/\equiv$. Temos então $(\overline{(a, b)} + \overline{(c, d)}) +$ $\overline{(e, f)} = \overline{(a + c, b + d)} + \overline{(e, f)} = \overline{((a + c) + e, (b + d) + f)} = \overline{(a + (c + e), b + (d + f))}$ $= \overline{(a, b)} + (\overline{(c, d)} + \overline{(e, f)})$.

- Existe o elemento neutro da adição e ele é único. Esse elemento neutro será o elemento $\overline{(0,0)}$. De fato, ao somarmos qualquer elemento $\overline{(a,b)} \in \mathbb{N}^2/\equiv$ com o elemento $\overline{(0,0)}$ temos: $\overline{(a,b)} + \overline{(0,0)} = \overline{(a+0, b+0)} = \overline{(a,b)}$.

- Existe o inverso aditivo e ele é único. O inverso do elemento $\overline{(a,b)} \in \mathbb{N}^2/\equiv$ será dado por $-\overline{(a,b)} = \overline{(b,a)}$. De fato, temos $\overline{(a,b)} + \overline{(b,a)} = \overline{(a+b, b+a)}$. Observemos que $\overline{(a+b, b+a)} = \overline{(0,0)}$, pois $a+b+0 = b+a+0$.

  Dados $(\overline{a,b}),\ (\overline{c,\ d}) \in \mathbb{N}^2/\equiv$, temos $(\overline{a,b})\cdot(\overline{c,d}) = (\overline{a\cdot c + b\cdot d,\ a\cdot d + b\cdot c})$. Como $a, b, c, d \in \mathbb{N},\ a\cdot c + b\cdot d$ e $a\cdot d + b\cdot c \in \mathbb{N}$ e aí, $(\overline{a\cdot c + b\cdot d,\ a\cdot d + b\cdot c}) \in \mathbb{N}^2/\equiv$.

- A multiplicação é associativa. Para ver isso, tome $\overline{(a,b)}, \overline{(c,d)}, \overline{(e,f)} \in \mathbb{N}^2/\equiv$.

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

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

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

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

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

- Vale a distributiva da multiplicação em relação à adição. Sejam $\overline{(a,b)}, \overline{(c,d)}, \overline{(e,f)} \in \mathbb{N}^2/\equiv$. Temos $\overline{(a,b)} \cdot (\overline{(c,d)} + \overline{(e,f)}) = \overline{(a,b)} \cdot \overline{(c+e, d+f)}$

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

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

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

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

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

Com as seis propriedades acima o conjunto $\mathbb{N}^2/\equiv$ é um anel.

Abaixo verificaremos que a multiplicação é comutativa e que possui um elemento unitário (o elemento neutro da multiplicação).

- A multiplicação é comutativa. Para ver isto, tome $\overline{(a,b)},\ \overline{(c,d)} \in \mathbb{N}^2/\equiv$. Temos $\overline{(a,b)} \cdot \overline{(c,d)} = \overline{(a\cdot c + b\cdot d, a\cdot d + b\cdot c)} = \overline{(c\cdot a + d\cdot b, c\cdot b + d\cdot a)} = \overline{(c,d)} \cdot \overline{(a,b)}$, como queríamos. Com essa propriedade temos um anel comutativo.

- Existe o elemento neutro da multiplicação. Esse elemento será o $\overline{(1,0)}$. De fato, dado $\overline{(a,b)} \in \mathbb{N}^2/\equiv$, temos $\overline{(a,b)} \cdot \overline{(1,0)} = \overline{(1\cdot a + 0\cdot b, 0\cdot a + 1\cdot b)} = \overline{(a,b)}$.

Mostraremos agora que a relação $\leq$ entre os elementos de $\mathbb{N}^2/\equiv$, definida por $\overline{(a,b)} \leq \overline{(c,d)} \iff a+d \leq b+c$ é uma relação de ordem. Para isso, provaremos que $\leq$ está bem definida e verifica as propriedades reflexiva, anti-simétrica e transitiva. Veja:

- A relação $\overline{(a,b)} \leq \overline{(c,d)} \iff a+d \leq b+c$ está bem definida. De fato, considere $\overline{(a_1,b_1)} \equiv \overline{(a,b)}$ e $\overline{(c_1,d_1)} \equiv \overline{(c,d)}$. Então, podemos escrever $a_1+b=b_1+a$ e $c_1+d=d_1+c$. Somando as igualdades membro a membro temos $a_1+b+d_1+c=b_1+a+c_1+d$ (1). Desde que $\overline{(a,b)} \leq \overline{(c,d)}$, temos $a+d \leq b+c$ (2). Assim, por (1) e (2) concluímos que $a_1+d_1 \leq b_1+c_1$. O que mostra que a relação $\leq$ está bem definida.

- Reflexividade. Se $\overline{(a,b)} \in \mathbb{N}^2/\equiv$, então $\overline{(a,b)} \leq \overline{(a,b)}$, pois $a+b \leq b+a$;

- Anti-simetria. Se $\overline{(a,b)} \leq \overline{(c,d)}$, então, $a+d \leq b+c$. Por outro lado, se $\overline{(c,d)} \leq \overline{(a,b)}$, temos $b+c \leq a+d$. Concluímos então que $a+d=b+c$, ou seja, se $\overline{(a,b)} \equiv \overline{(c,d)}$;

- Transitividade. Tome $\overline{(a,b)}, \overline{(c,d)}, \overline{(e,f)} \in \mathbb{N}^2/\equiv$. Suponha $\overline{(a,b)} \leq \overline{(c,d)}$ e $\overline{(c,d)} \leq \overline{(e,f)}$. Temos então $a+d \leq b+c$ e $c+f \leq d+e$. Somando ambas as desigualdades ficamos com $a+d+c+f \leq b+c+d+e$, o que implica em $a+f \leq b+e$, ou seja, $\overline{(a,b)} \leq \overline{(e,f)}$.

Portanto, temos uma ordem parcial em $\mathbb{N}^2/\equiv$.

Agora, para que a ordem definida seja total, dados dois elementos $\overline{(a,b)},\ \overline{(c,d)} \in \mathbb{N}^2/\equiv$, devemos ter necessariamente uma e somente uma das três relações abaixo:

$$\overline{(a,b)} < \overline{(c,d)},\ \overline{(a,b)} = \overline{(c,d)} \text{ ou } \overline{(a,b)} > \overline{(c,d)}.$$

De fato, suponha que não aconteça $\overline{(a,b)} \leq \overline{(c,d)}$.

Então, não podemos escrever $a+d \leq b+c$. Como, $a,\ b,\ c$ e d pertencem ao conjunto dos números naturais onde temos uma ordem, se não acontece $a+d \leq b+c$, então $a+d > b+c$, o que implica em $\overline{(a,b)} > \overline{(c,d)}$. Assim, pelo menos uma das três acontece.

Agora, caso $\overline{(a,b)} < \overline{(c,d)}$ teríamos $a+d < b+c$, pois se $a+d \geq b+c$, então $\overline{(a,b)} \geq \overline{(c,d)}$ o que mostra que no máximo uma das relações acontece.

Concluímos então que $\mathbb{N}^2/\equiv$ é um conjunto ordenado totalmente.

Finalmente, para poder criar o conjunto $\mathbb{Z}$ é necessário exibir uma função que inclua $\mathbb{N}$ dentro desse conjunto preservando características como ordem, soma, produto e injetividade.

Essa função será a função $\Phi : a \in \mathbb{N} \mapsto \overline{(a,0)} \in \mathbb{Z}$.

Em seguida, criaremos a função $\Psi : a \in \mathbb{N} \mapsto \overline{(0,a)} \in \mathbb{Z}$, que levará os elementos de $\mathbb{N}$ no oposto de cada elemento $\overline{(a,0)}$, dado por $-\overline{(a,0)} = \overline{(0,a)}$. Observe que cada um dos elementos $\overline{(a,0)},\ \overline{(0,a)},\ a \in \mathbb{N}$ pertence a $\mathbb{N}^2/\equiv$. As funções Φ e Ψ serão partes do isomorfismo que finaliza a construção de $\mathbb{Z}$.

Função $\Phi : a \in \mathbb{N} \mapsto \overline{(a,0)} \in \mathbb{Z}$:

- A função Φ é injetora. De fato, sejam $a, b \in \mathbb{N}$, tais que $\Phi(a) = \Phi(b)$. Assim, pela definição da função Φ dada acima temos $\overline{(a,0)} = \Phi(a) = \Phi(b) = \overline{(b,0)}$, ou seja, $a + 0 = 0 + b \Longrightarrow a = b$. Portanto, a função dada é injetora;

- A função Φ preserva a soma e o produto, ou seja, $\Phi(a+b) = \Phi(a)+\Phi(b)$ e $\Phi(a\cdot b) = \Phi(a)\cdot\Phi(b)$, para todo $a, b \in \mathbb{N}$.

  Assim, sejam $a, b \in \mathbb{N}$. Então, $\Phi(a + b) = \overline{(a + b, 0)} = \overline{(a + b, 0 + 0)} = \overline{(a, 0)} + \overline{(b, 0)} = \Phi(a) + \Phi(b)$. Além disso, $\Phi(a \cdot b) = \overline{(a \cdot b, 0)} = \overline{(a \cdot b + 0 \cdot 0, a \cdot 0 + 0 \cdot b)} = \overline{(a, 0)} \cdot \overline{(b, 0)} = \Phi(a) \cdot \Phi(b)$.

  Portanto, a função Φ preserva a soma e o produto;

- A função Φ preserva a ordem, ou seja, $a \leq b \Longrightarrow \Phi(a) \leq \Phi(b)$.

  Considere $a, b \in \mathbb{N}$. Vamos supor $a \leq b$ e $\Phi(b) < \Phi(a)$. Assim, teríamos $\overline{(b, 0)} < \overline{(a, 0)}$, o que implicaria em $b + 0 < 0 + a \Longrightarrow b < a$, o que é absurdo, pois, por hipótese temos $a \leq b$. Portanto, $\Phi(a) \leq \Phi(b)$.

  Como um caso particular importante, temos $\overline{(0, 0)} \leq \Phi(a)$ para todo $a \in \mathbb{N}$. De fato, se tivéssemos $\Phi(a) < \overline{(0, 0)}$, então $\overline{(a, 0)} < \overline{(0, 0)}$, isto é $a + 0 < 0 + 0 \Longrightarrow a < 0$, o que seria absurdo, pois todo $a \in \mathbb{N}$ é um número positivo.

Assim, $Im(\Phi)$ é uma cópia de $\mathbb{N}$ dentro do novo conjunto $\mathbb{Z}$. Os elementos de $Im(\Phi)$ serão os números inteiros não negativos $(\mathbb{Z}_+)$. Denotaremos o conjunto dos números positivos por $\mathbb{Z}_+^*$.

Construiremos agora uma função $\Psi : a \in \mathbb{N} \longrightarrow \overline{(0, a)} \in \mathbb{Z}$. Observe que $Im(\Psi)$ terá como elementos os opostos de $\mathbb{N}$, pois $\overline{(0, a)} = -\overline{(a, 0)}$. Algumas características importantes:

- A função Ψ é injetora. Dados $a, b \in \mathbb{N}$, suponha $\Psi(a) = \Psi(b)$. Assim, temos, $\overline{(0, a)} = \Psi(a) = \Psi(b) = \overline{(0, b)}$. Portanto, $0 + b = a + 0 \Longrightarrow b = a$;

- A função Ψ preserva a soma pois $\Psi(a + b) = \overline{(0 + 0, a + b)} = \overline{(0, a)} + \overline{(0, b)} = \Psi(a) + \Psi(b)$;

- Quanto ao produto, temos $\Psi(a \cdot b) = \overline{(0, a \cdot b)} = \overline{(a \cdot 0 + 0 \cdot b, a \cdot b + 0 \cdot 0)} = \overline{(a, 0)} \cdot \overline{(0, b)} = -\overline{(0, a)} \cdot \overline{(0, b)} = -\Psi(a) \cdot \Psi(b)$. Também $\Psi(a \cdot b) = \overline{(0,\ a \cdot b)} = \overline{(0 \cdot b + a \cdot 0,\ 0 \cdot 0 + a \cdot b)} = \overline{(0, a)} \cdot \overline{(b, 0)} = \overline{(0, a)} \cdot (-\overline{(0, b)}) = \Psi(a) \cdot (-\Psi(b)) = -\Psi(a) \cdot \Psi(b)$.

- Agora, suponha $a \leq b$ e $\Psi(b) > \Psi(a)$. Assim, podemos escrever $\overline{(0, b)} > \overline{(0, a)}$, o que implica em $0 + a > 0 + b$, ou seja, $a > b$, o que é absurdo pois $a \leq b$.

Podemos ver também do seguinte modo: $a \leq b \Rightarrow \overline{(a,0)} \leq \overline{(b,0)} \Rightarrow a+0 \leq 0+b \Rightarrow 0+a \leq b+0 \Rightarrow \overline{(0,b)} \leq \overline{(0,a)}$.

Logo, $a \leq b$ implica em $\Psi(b) \leq \Psi(a)$ (a desigualdade em $Im(\Psi)$ inverte em relação à desigualdade em $\mathbb{N}$).

Os elementos de $Im(\Psi)$ serão chamadas de números inteiros não positivos e serão representadas por $(\mathbb{Z}_-)$. Denotaremos o conjunto dos números negativos por $\mathbb{Z}_-^*$.

Ficamos então com $\mathbb{Z}_+^* = Im(\Phi)$ e $\mathbb{Z}_-^* = Im(\Psi)$.

Falta compararmos os elementos de $\mathbb{Z}_+^*$ e $\mathbb{Z}_-^*$ e 0. Para isso, definamos $\alpha,\ \beta \in \mathbb{Z}$ e $\alpha < \beta$ por $\alpha < \beta \iff \alpha \leq \beta$ e $\alpha \neq \beta$.

Se $\alpha \in \mathbb{Z}_-^*$ e $\beta \in \mathbb{Z}_+^*$ vamos mostrar que $\alpha < \overline{(0,0)} < \beta$.

1) Suponha $\alpha \in \mathbb{Z}_-^*$ e $\overline{(0,0)} < \alpha$.

Como $\alpha = \overline{(0,\alpha)}$, podemos escrever $\overline{(0,0)} < \overline{(0,\alpha)}$, o que implica em $0+\alpha > 0+0$, isto é $\alpha > 0$, o que é absurdo, já que $\alpha \in \mathbb{Z}_-^*$ (lembremos que a desigualdade em $\mathbb{Z}_-^*$ inverte em relação a $\mathbb{N}^2/\equiv$). Portanto, $\alpha < \overline{(0,0)}$.

2) Suponha $\beta \in \mathbb{Z}_+^*$ e $\beta < \overline{(0,0)}$. Como $\beta = \overline{(\beta,0)}$, podemos escrever $\overline{(\beta,0)} < \overline{(0,0)}$, o que nos fornece $\beta + 0 < 0 + 0$, isto é, $\beta < 0$, o que é absurdo pois $\beta \in \mathbb{Z}_+^*$. Portanto, $\overline{(0,0)} < \beta$.

Concluímos então que $\alpha < \overline{(0,0)} < \beta$.

Agora, vamos mostrar que $\mathscr{P} = \{\mathbb{Z}_-^*, \{\overline{(0,0)}\}, \mathbb{Z}_+^*\}$ é uma partição de $\mathbb{Z}$.

Para isso, devemos mostrar que:

(a) A interseção dos elementos de $\mathscr{P}$, dois a dois, é vazia. De fato, tomando $\alpha \in \mathbb{Z}_-^*$, α não pode pertencer a $\{\overline{(0,0)}\}$, caso contrário, $\alpha = \overline{(0,\alpha)} = \overline{(0,0)}$ isto é, $0+0 = \alpha+0$, o que implicaria em $\alpha = 0$. Portanto, $\mathbb{Z}_-^* \cap \{\overline{(0,0)}\} = \emptyset$.

Analogamente $\mathbb{Z}_+^* \cap \{\overline{(0,0)}\} = \emptyset$.

Agora, suponha que $\exists\ x \in \mathbb{Z}_-^* \cap \mathbb{Z}_+^*$, então $x = \overline{(0,x)}$ e $x = \overline{(x,0)}$ isto é, $\overline{(0,x)} = \overline{(x,0)}$, o que implica em $0+0 = x+x$, ou seja $x = 0$, o que não pode acontecer, já que $x \in \mathbb{Z}_-^*$, por exemplo.

Portanto, a interseção dos elementos de $\mathscr{P}$, dois a dois é vazia.

(b) Agora, tomando qualquer elemento γ em $\mathbb{Z}$, ou γ é da forma $\overline{(\gamma,0)}$ ou $\overline{(0,\gamma)}$ ou $\overline{(0,0)}$, ou seja, a união $\mathbb{Z}_-^* \cup \{\overline{(0,0)}\} \cup \mathbb{Z}_+^*$ é todo o conjunto $\mathbb{Z}$.

Assim, existe uma bijeção entre os elementos do conjunto $\mathbb{N}^2/\equiv$ (que são classes de equivalência) e os elementos de $\mathbb{Z}$ (que são os números inteiros).

Apesar de os elementos dos dois conjuntos serem diferentes, a bijeção (que no texto indicamos por Φ e Ψ) garante que podemos identificar de maneira única esses dois conjuntos.

Para clarear as ideias, quando tomamos a função $\Phi : \mathbb{N} \to \mathbb{Z}$ e escrevemos $\Phi(a) = \overline{(a,0)}$, estamos pegando $a \in \mathbb{N}$ e elementos de $\mathbb{N}^2$ da forma $\overline{(k+a,k)}$ com $k \in \mathbb{N}$. A ideia de tomar o

quociente de $\mathbb{N}^2$ por uma relação de equivalência permite considerar apenas o elemento $\overline{(a,0)}$ como representante de todos os $(k+a,k)$ possíveis.

Assim, cada $\overline{(a,0)} \in \mathbb{N}^2/\equiv$ é o elemento $a-0=a \in \mathbb{Z}$ e cada $\overline{(0,a)} \in \mathbb{N}^2/\equiv$ é o elemento $0-a=-a \in \mathbb{Z}$. O elemento $\overline{(0,0)} \in \mathbb{N}^2/\equiv$ é o $0 \in \mathbb{Z}$.

Nosso conjunto $\mathbb{Z}$ está completo.

2.2 Construção do conjunto dos números racionais

A construção do conjunto dos números racionais é semelhante à construção dos números inteiros feita anteriormente. Essa construção será a busca de um conjunto numérico contendo $\mathbb{Z}$ no qual o quociente $\frac{a}{b}$ esteja definido, quaisquer que sejam $a,b \in \mathbb{Z}$ com $b \neq 0$. Além disso, como existe um número infinito de frações equivalentes a $\frac{a}{b}$, ou seja, frações $\frac{c}{d}$, de modo que $\frac{a}{b}=\frac{c}{d}$ (e isso nos leva a escrever $a \cdot d = b \cdot c$), criaremos uma relação de equivalência na qual $(a,b) \equiv (c,d) \iff a \cdot d = b \cdot c$. Assim, o conjunto dos números racionais será a classe de equivalência de um par odenado $(a,b) \in \mathbb{Z} \times \mathbb{Z}$, módulo a relação de equivalência $\equiv$ definida acima. Comecemos a construção verificando que a relação definida é uma relação de equivalência.

Dados $(a,b),(c,d),(e,f) \in \mathbb{Z}^2$, temos:

- A relação $\equiv$ é reflexiva, pois, $(a,b) \equiv (a,b)$ já que $a \cdot b = b \cdot a$;
- A relação é simétrica. Se $(a,b) \equiv (c,d)$, temos $a \cdot d = b \cdot c$, o que nos leva a $b \cdot c = a \cdot d \iff c \cdot b = d \cdot a \iff (c,d) \equiv (a,b)$;
- A relação é transitiva. De fato, se $(a,b) \equiv (c,d)$ e $(c,d) \equiv (e,f)$, temos $a \cdot d = b \cdot c$ e $c \cdot f = d \cdot e$. Multiplicando as igualdades membro a membro temos $(a \cdot d) \cdot (c \cdot f) = (b \cdot c) \cdot (d \cdot e)$, o que implica em $a \cdot d \cdot c \cdot f = b \cdot c \cdot d \cdot e$. Pela lei do cancelamento ficamos com $a \cdot f = b \cdot e$, o que implica em $(a,b) \equiv (e,f)$.

A relação $\equiv$ de equivalência definida acima possui as seguintes propriedades:

$$\begin{cases} (a,b) \equiv (a',b') \\ \text{e } (c,d) \equiv (c',d') \end{cases} \Rightarrow \begin{cases} (a \cdot d + b \cdot c, b \cdot d) \equiv (a' \cdot d' + b' \cdot c', b' \cdot d') \\ (a \cdot c, b \cdot d) \equiv (a' \cdot c', b' \cdot d') \end{cases}$$

- Se $(a,b) \equiv (a',b')$ e $(c,d) \equiv (c',d')$ então $a \cdot b' = b \cdot a'$ (1) e $c \cdot d' = d \cdot c'$ (2). Multiplicando (1) por $d \cdot d'$ e (2) por $b \cdot b'$, e somando as igualdades resultantes membro a membro ficamos com $a \cdot d \cdot b' \cdot d' + b \cdot c \cdot b' \cdot d' = b \cdot d \cdot a' \cdot d' + b \cdot d \cdot b' \cdot c' \implies (a \cdot d + b \cdot c) \cdot b' \cdot d' = b \cdot d \cdot (a' \cdot d' + b' \cdot c') \implies (a \cdot d + b \cdot c, b \cdot d) \equiv (a' \cdot d' + b' \cdot c', b' \cdot d')$, como queríamos.

- Se $(a,b) \equiv (a^{'},b^{'})$ e $(c,d) \equiv (c^{'},d^{'})$ então $a \cdot b^{'} = b \cdot a^{'}$ (1) e $c \cdot d^{'} = d \cdot c^{'}$ (2). Multiplicando as igualdades (1) e (2) membro a membro ficamos com $a \cdot c \cdot b^{'} \cdot d^{'} = b \cdot d \cdot a^{'} \cdot c^{'}$, o que implica em $(a \cdot c, b \cdot d) \equiv (a^{'} \cdot c^{'}, b^{'} \cdot d^{'})$.

Concluímos então, que a relação de equivalência $\equiv$ definida acima possui as propriedade citadas. Além disso, pensando em (a,b) como uma classe, e indicando-a por $\overline{(a,b)}$, verificamos acima que as propriedades são válidas independente dos representantes dessas classes, o que mostra que as operações acima (que serão chamadas respectivamente de adição e multiplicação) estão bem definidas.

Podemos então escrever:

$$\overline{(a,b)} + \overline{(c,d)} := \overline{(a \cdot d + b \cdot c, b \cdot d)} \qquad \text{(adição)}$$
$$\overline{(a,b)} \cdot \overline{(c,d)} := \overline{(a \cdot c, b \cdot d)} \qquad \text{(multiplicação)}$$

Agora mostraremos que, com essas operações, o conjunto $\mathbb{Z} \times \mathbb{Z}^*/\equiv$ é um corpo. Para, isso, mostraremos que as propriedades de corpo são válidas para as operações definidas acima.

- Dados $\overline{(a,b)}$ e $\overline{(c,d)} \in \mathbb{Z} \times \mathbb{Z}^*/\equiv$, temos $\overline{(a,b)} + \overline{(c,d)} = \overline{(a \cdot d + b \cdot c, b \cdot d)}$. Como $a, c \in \mathbb{Z}$ e $b, d \in \mathbb{Z}^*$, temos $a \cdot d + b \cdot c \in \mathbb{Z}$ e $b \cdot d \in \mathbb{Z}^*$. Assim, $\overline{(a \cdot d + b \cdot c, b \cdot d)} \in \mathbb{Z} \times \mathbb{Z}^*/\equiv$;

- Comutatividade da soma. Se $\overline{(a,b)}$ e $\overline{(c,d)} \in \mathbb{Z} \times \mathbb{Z}^*/\equiv$, podemos escrever $\overline{(a,b)} + \overline{(c,d)} = \overline{(a \cdot d + b \cdot c, b \cdot d)} = \overline{(c \cdot b + d \cdot a, d \cdot b)} = \overline{(c,d)} + \overline{(a,b)}$;

- Associatividade da soma. Se $\overline{(a,b)}$, $\overline{(c,d)}$ e $\overline{(e,f)} \in \mathbb{Z} \times \mathbb{Z}^*/\equiv$, temos $(\overline{(a,b)} + \overline{(c,d)}) + \overline{(e,f)}$
$= \overline{(a \cdot d + b \cdot c, b \cdot d)} + \overline{(e,f)} = \overline{((a \cdot d + b \cdot c) \cdot f + (b \cdot d) \cdot e, (b \cdot d) \cdot f)}$
$= \overline{(a \cdot d \cdot f + b \cdot c \cdot f + b \cdot d \cdot e, b \cdot d \cdot f)} = \overline{(a \cdot (d \cdot f) + b \cdot (c \cdot f + d \cdot e), b \cdot (d \cdot f))}$
$= \overline{(a,b)} + \overline{(c \cdot f + d \cdot e, d \cdot f)} = \overline{(a,b)} + (\overline{(c,d)} + \overline{(e,f)})$, como queríamos;

- O elemento neutro da adição existe e é único. Ele será o elemento $\overline{(0,1)}$. De fato, dados $\overline{(0,1)}$ e $\overline{(a,b)} \in \mathbb{Z} \times \mathbb{Z}^*/\equiv$, temos $\overline{(0,1)} + \overline{(a,b)} = \overline{(0 \cdot b + 1 \cdot a, 1 \cdot b)} = \overline{(a,b)} = \overline{(a \cdot 1 + b \cdot 0, b \cdot 1)} = \overline{(a,b)}$.

- Existe o inverso aditivo $-\overline{(a,b)}$, de todo $\overline{(a,b)} \in \mathbb{Z} \times \mathbb{Z}^*/\equiv$, e ele é único. Esse elemento será denotado por $\overline{(-a,b)}$ ou $\overline{(a,-b)}$. De fato, $\overline{(a,b)} + (-\overline{(a,b)}) = \overline{(a,b)} + \overline{(-a,b)}$
$= \overline{(a \cdot b + b \cdot (-a), b \cdot b)} = \overline{(a \cdot b - b \cdot a, b^2)} = \overline{(0,b^2)} = \overline{(0,1)}$. Temos também $\overline{(a,b)} + \overline{(a,-b)}$
$= \overline{(a \cdot (-b) + b \cdot a, b \cdot (-b))} = \overline{(-a \cdot b + b \cdot a, -b^2)} = \overline{(0,-b^2)} = \overline{(0,1)}$, pois $0 \cdot 1 = -b^2 \cdot 0$.

- Dados $\overline{(a,b)}$ e $\overline{(c,d)}$ em $\mathbb{Z} \times \mathbb{Z}^*/\equiv$, temos $\overline{(a \cdot c, b \cdot d)} \in \mathbb{Z} \times \mathbb{Z}^*/\equiv$ pois $a \cdot c \in \mathbb{Z}$ e $b \cdot d \in \mathbb{Z}^*$;

- Dados dois elementos $\overline{(a,b)}$ e $\overline{(c,d)} \in \mathbb{Z} \times \mathbb{Z}^*/\equiv$, o produto $\overline{(a,b)} \cdot \overline{(c,d)}$ é comutativo. De fato, $\overline{(a,b)} \cdot \overline{(c,d)} = \overline{(a \cdot c, b \cdot d)} = \overline{(c \cdot a, d \cdot b)} = \overline{(c,d)} \cdot \overline{(a,b)}$;

- Associatividade da multiplicação. Tomando os elementos $\overline{(a,b)}$, $\overline{(c,d)}$ e $\overline{(e,f)}$ em $\mathbb{Z}\times\mathbb{Z}/\equiv$, temos $(\overline{(a,b)}\cdot\overline{(c,d)})\cdot\overline{(e,f)} = \overline{(a\cdot c, b\cdot d)}\cdot\overline{(e,f)} = \overline{(a\cdot c\cdot e, b\cdot d\cdot f)} = \overline{(a\cdot(c\cdot e), b\cdot(d\cdot f))} = \overline{(a,b)}\cdot\overline{(c\cdot e, d\cdot f)} = \overline{(a,b)}\cdot(\overline{(c,d)}\cdot\overline{(e,f)})$;

- Existe o elemento neutro da multiplicação e ele é único. O elemento neutro será $\overline{(1,1)} \in \mathbb{Z}\times\mathbb{Z}^*/\equiv$. De fato, dado qualquer $\overline{(a,b)} \in \mathbb{Z}\times\mathbb{Z}^*/\equiv$, temos $\overline{(a,b)}\cdot\overline{(1,1)} = \overline{(a\cdot 1, b\cdot 1)} = \overline{(1\cdot a, 1\cdot b)} = \overline{(a,b)}$.

- Existência do inverso multiplicativo. Dado qualquer elemento $\overline{(a,b)} \in \mathbb{Z}\times\mathbb{Z}^*/\equiv$, o seu inverso multiplicativo será o elemento $\overline{(b,a)}$ pois $\overline{(a,b)}\cdot\overline{(b,a)} = \overline{(a\cdot b, b\cdot a)} = \overline{(1,1)}$.

- Vale a distributiva da multiplicação em relação à adição.

  Dados $\overline{(a,b)}$, $\overline{(c,d)}$ e $\overline{(e,f)}$ em $\mathbb{Z}\times\mathbb{Z}^*/\equiv$, temos $\overline{(a,b)}\cdot(\overline{(c,d)}+\overline{(e,f)}) = \overline{(a,b)}\cdot\overline{(c\cdot f + d\cdot e, d\cdot f)}$

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

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

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

  Assim, $\mathbb{Z}\times\mathbb{Z}^*/\equiv$ é um corpo com as operações $+$ e $\cdot$ definidas.

Vamos agora definir como ficarão os sinais dos elementos de $\mathbb{Q}$.

Suponha $\alpha \in \mathbb{Q}$. Como $\mathbb{Q}$ será identificado com o conjunto $\mathbb{Z}\times\mathbb{Z}^*/\equiv$, cada elemento de $\mathbb{Q}$ será, inicialmente, uma classe de equivalência. Suponha então que (a,b) e (c,d) sejam representantes de α. Assim $\overline{(a,b)} \equiv \overline{(c,d)}$, isto é, $a\cdot d = b\cdot c$. Se $b>0$ e $d>0$, então, para que a igualdade se mantenha devemos ter a e c com mesmo sinal, ou seja $a\cdot c > 0$.

Vamos agora definir quando teremos um número racional *positivo* e quando teremos um número racional *negativo*.

$\alpha \in \mathbb{Q},\ \alpha \neq 0$ será *positivo* se existir um representante $\dfrac{a}{b}$ de α tal que $a>0$ e $b>0$, pois, nesse caso, qualquer outro representante $\dfrac{c}{d}$ de α com $d>0$ terá $c>0$. Nesse caso escrevemos $\alpha > 0$.

$\alpha \in \mathbb{Q},\ \alpha \neq 0$ será dito *negativo* se, dado $\dfrac{a}{b}$ um representante de α temos $b>0$ e $a<0$. Escrevemos, nesse caso, $\alpha < 0$.

Se $a=0$ e $b>0$ em $\dfrac{a}{b}$, então $\alpha = 0$.

Agora vamos definir uma relação de ordem $\leq$ sobre $\mathbb{Q}$ por

$$\alpha \leq \beta \iff \alpha - \beta \leq 0$$

Assim, dados $\alpha,\ \beta,\ \gamma \in \mathbb{Q}$, temos:

- Essa relação é reflexiva, pois $\alpha \leq \alpha \Longrightarrow \alpha - \alpha \leq 0$;

- Essa relação é anti-simétrica, pois, se $\alpha \leq \beta$ e $\beta \leq \alpha$, então $\alpha - \beta \leq 0$ e $\beta - \alpha \leq 0$. Isso só acontece se $\alpha = \beta$.

- A relação é transitiva, ou seja, se $\alpha \leq \beta$ e $\beta \leq \gamma$, então, $\alpha - \beta \leq 0$ e $\beta - \gamma \leq 0$. Assim, somando as desigualdades membro a membro temos $(\alpha - \beta) + (\beta - \gamma) \leq 0 + 0$ o que implica em $\alpha - \beta + \beta - \gamma \leq 0$, isto é, $\alpha - \gamma \leq 0$. Portanto, $\alpha \leq \gamma$.

Falta mostrar que, dados $\alpha, \beta \in \mathbb{Q},\ \alpha < \beta$ ou $\alpha = \beta$ ou $\alpha > \beta$.

Suponha que α não seja menor que nem igual a β. Então a diferença $\alpha - \beta$ não pode ser negativa nem zero. Assim, a diferença tem que ser positiva, o que implica em $\alpha > \beta$.

Portanto $\leq$ é uma relação de ordem $\mathbb{Q}$.

Falta agora criarmos uma bijeção entre os conjuntos $\mathbb{Z} \times \mathbb{Z}^*/\equiv$ e $\mathbb{Q}$. A função candidata a ser essa bijeção é a aplicação $\Phi := a \in \mathbb{Z} \longmapsto \overline{(a, 1)} \in \mathbb{Q}$.

- Φ é injetora. De fato, se $\Phi(a) = \Phi(b),\ a,\ b \in \mathbb{Z}$, então $\overline{(a, 1)} = \overline{(b, 1)}$, o que implica em $a \cdot 1 = 1 \cdot b$, isto é, $a = b$;

- Φ preserva a soma. Tomando $a,\ b \in \mathbb{Z},\ \Phi(a + b) = \overline{(a + b,\ 1)} = \overline{(a \cdot 1 + b \cdot 1, 1 \cdot 1)} = \overline{(a, 1)} + \overline{(b, 1)} = \Phi(a) + \Phi(b)$;

- Φ preserva o produto. Se $a,\ b \in \mathbb{Z},\ \Phi(a \cdot b) = \overline{(a \cdot b, 1)} = \overline{(a, 1)} \cdot \overline{(b, 1)} = \Phi(a) \cdot \Phi(b)$;

- Φ preserva a ordem. Se $a,\ b \in \mathbb{Z}$ e $a \leq b$, temos $\Phi(a) - \Phi(b) = \overline{(a, 1)} - \overline{(b, 1)} = \overline{(a, 1)} + \overline{(-b, 1)} = \overline{(a \cdot 1 - b \cdot 1, 1 \cdot 1)} = \overline{(a - b, 1)}$. Como $a \leq b,\ a - b \leq 0$. Assim, $\overline{(a - b, 1)} \leq 0$, isto é, $\Phi(a) - \Phi(b) \leq 0 \Longrightarrow \Phi(a) \leq \Phi(b)$.

Assim, construímos o conjunto dos números racionais com base no conjunto dos números inteiros.

Capítulo 3

Construção dos números reais via cortes de Dedekind

3.1 Entendendo o significado dos cortes de Dedekind

Ao refletir sobre a continuidade da reta numérica e a relação entre ela e o conjunto dos números reais, *Dedekind* observou que a continuidade de um segmento de reta se deve *"...à natureza da divisão do segmento em duas partes por um ponto sobre o segmento"*, segundo *Carl B.Boyer*. *Dedekind* percebeu que podemos fazer uma divisão dos pontos do segmento em duas classes da seguinte forma: cada ponto pertence a uma e somente uma classe; todo ponto numa classe está a esquerda de todo ponto da outra e existe um e um só ponto que realiza essa divisão.

Assim, o domínio dos números racionais pode ser completado até formar um contínuo, segundo *Carl B. Boyer*.

Se o ponto que realiza o corte já está no conjunto dos números racionais, permanece. Caso contrário, colocamos esse ponto num novo conjunto, que posteriormente será chamado de *conjunto dos números irracionais*. A união desse novo conjunto, ao conjunto $\mathbb{Q}$ será o *conjunto dos números reais* ($\mathbb{R}$).

Como exemplos, se tomarmos o número 2, esse número divide o conjunto dos números racionais nos conjuntos $A = \{x \in \mathbb{Q}/x \leq 2\}$ e $B = \{x \in \mathbb{Q}/x > 2\}$. Como $2 \in \mathbb{Q}$, não há o que fazer. Por outro lado, se tomarmos, para fazer a divisão do conjunto dos números racionais, o número tal que o quadrado é igual a 2, temos que a divisão de $\mathbb{Q}$ será feita pelas classes $A = \{x \in \mathbb{Q}/x^2 < 2\}$ e $B = \{x \in \mathbb{Q}/x^2 > 2\}$. Como $x \notin \mathbb{Q}$, ele não pode pertencer a nenhum dos conjuntos A e B e, assim, será colocado num novo conjunto, que será o complementar do conjunto dos números racionais em relação ao conjunto dos números reais, completando a reta numérica.

Posteriormente o matemático *Bertrand Russel* $(1872 - 1970)$ propôs uma pequena modificação na definição de *Dedekind*. Ele observou que, como qualquer uma das classes A e B pode ser univocamente determinda pela outra, basta uma para determinarmos um número real. Assim, o

número $\sqrt{2}$ pode ser definido simplesmente como o conjunto dos números racionais positivos cujos quadrados são menores que 2 e também de todos os números racionais negativos.

A partir disso podemos iniciar a construção dos números reais segundo a ideia de *Richard Dedekind*. Seguiremos os passos de *Walter Rudin* em seu livro *"Principles of mathematical analysis"*, não economizando em detalhes.

***Definição* 26.** Um corte é, por definição, qualquer conjunto $\alpha \subset \mathbb{Q}$ com as seguintes propriedades:

1. α é não vazio, e $\alpha \neq \mathbb{Q}$.
2. Se $p \in \alpha$, $q \in \mathbb{Q}$, e $q < p$, então $q \in \alpha$.
3. Se $p \in \alpha$, então $p < r$ para algum $r \in \alpha$.

A partir do item 2 podemos concluir:

1. Se $p \in \alpha$ e $q \notin \alpha$ então $p < q$.
2. Se $r \notin \alpha$ e $r < s$ então $s \notin \alpha$.

O item 3 da definição acima exclui um possível maior elemento no conjunto α, o que sugere que os cortes são subconjuntos abertos de $\mathbb{Q}$. De fato, supondo por contradição que exista um maior elemento $s \in \alpha$, chegamos à conclusão de que, por 3, deve existir em α algum $t > s$. O que contradiz o fato de que s é o maior elemento de α.

***Exemplo* 28.** Se $r \in \mathbb{Q}$, então $\alpha_r = \{x \in \mathbb{Q} : x < r\}$ é um corte. De fato,

1. Dado $r \in \mathbb{Q}$, existe $s = r - 1$ tal que $s \in \alpha_r$ (já que $s = r - 1 < r$) e, $s' = r + 1$ tal que $s' \notin \alpha_r$ (já que $s' = r + 1 > r$) e $s' \in \mathbb{Q}$. Assim, $\alpha_r \neq$ e $\alpha_r \neq \mathbb{Q}$.
2. Dado $p \in \alpha_r,\ q \in \mathbb{Q}$ e $q < p$, temos $p < r$ e por consequência $q < p < r$, o que implica em $q \in \alpha_r$.
3. Dado $p \in \alpha_r$, temos $p < r$. Tomando $s = \frac{p+r}{2}$, temos $s > p$ e $s < r$, o que implica em $s \in \alpha_r$. Portanto α_r é corte.

Como exemplo de corte temos o conjunto $\alpha \subset \mathbb{Q}$ definido por
$\alpha = \{q \in \mathbb{Q}/q \leq 0\} \cup \{q \in \mathbb{Q}/q \geq 0, q^2 < 2\}$.

De fato, o item 1 da definição de corte dada acima está satisfeito já que $-1 \in \alpha$ (logo α é não vazio) e $3 \in \mathbb{Q}$ mas $3 \notin \alpha$ pois $3^2 = 9 > 2$ (assim $\alpha \neq \mathbb{Q}$).

Para verificarmos que o item 2 da definição de corte é válido, tome $p \in \alpha$, $q \in \mathbb{Q}$ e $q < p$. Se $q \leq 0$ temos $q \in \alpha$. Caso $q \geq 0$, então podemos escrever $q^2 < p^2$ (pois $q < p$). Como $p \in \alpha$, temos $q^2 < p^2 < 2$. Assim, $q \in \alpha$.

Falta verificar que α não possui maior elemento. Para isso, dado $p \in \alpha$, vamos mostrar que existe $q \in \mathbb{Q}$, $q > p$ tal que $q \in \alpha$. Assim, considere:

$$q = p - \frac{p^2-2}{p+2} = \frac{p\cdot(p+2)-(p^2-2)}{p+2} = \frac{p^2+2\cdot p-p^2+2}{p+2} = \frac{2\cdot p+2}{p+2}.$$

Podemos ver que $q > p$ pois se $p > 0$ temos $p^2 - 2 < 0$ e $p + 2 > 0$. Logo, $\frac{p^2-2}{p+2} < 0$, o que implica em $q = p - \frac{p^2-2}{p+2} > p$. Além disso, $q^2 < 2$, pois,

$$\left(\frac{2\cdot p+2}{p+2}\right)^2 - 2 = \frac{4\cdot p^2+8\cdot p+4-2\cdot p^2-8\cdot p-8}{(p+2)^2} = \frac{2\cdot p^2-4}{(p+2)^2} = \frac{2\cdot(p^2-2)}{(p+2)^2}.$$

Como $p^2 - 2 < 0$ temos $q^2 - 2 < 0$. Assim, $q^2 < 2$ e $q \in \alpha$.

Concluímos, então, que o conjunto $\alpha \subset \mathbb{Q}$ definido por $\alpha = \{q \in \mathbb{Q}/q \leq 0\} \cup \{q \in \mathbb{Q}/q \geq 0, q^2 < 2\}$ é um corte.

3.2 Construindo o conjunto dos números reais

Agora, faremos a construção dos números reais propriamente dita. Para provar que esse novo conjunto existe inicialmente precisamos identificar quais serão seus elementos. *R. Dedekind*, identificou cada número de $\mathbb{Q}$ e os que não pertenciam a $\mathbb{Q}$ com um corte, definido anteriormente.

O teorema a seguir motivará nossa construção:

***Teorema* 5.** Existe um corpo ordenado $\mathbb{R}$ com a propriedade do supremo no qual o conjunto dos números racionais é um conjunto denso. Mais do que isso, $\mathbb{R}$ contém $\mathbb{Q}$ como subcorpo.

Demonstrar esse teorema significa completar o conjunto dos números racionais de modo a formar um contínuo.

Primeiramente verificaremos que o conjunto de cortes é um conjunto ordenado. Para isso definiremos uma relação de ordem entre seus elementos. Como os cortes são conjuntos, é natural que a relação de ordem utilizada seja a inclusão.

Após verificarmos a existência de uma ordem no conjunto de cortes, iremos mostrar que o conjunto em questão possui a propriedade do supremo.

E, finalmente, será demonstrado que o conjunto de cortes é um corpo.

Passo 1: O conjunto de cortes possui uma ordem.

Como dito acima, a relação de ordem entre os elementos do conjunto de cortes será denotada por $<$. A expressão $\alpha \leq \beta$ será válida quando α for um subconjunto de β, ou seja, quando $\alpha \subseteq \beta$.

Para que tenhamos uma *ordem* no conjunto de cortes, a relação denotada por $\subseteq$ deverá satisfazer a definição de ordem dada no capítulo 1, que é trivial.

Abaixo veremos que essa ordem é total.

Se α, β pertencem ao conjunto de cortes então é válida somente uma das relações:

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

Sabemos que, no máximo uma das três relações dadas em 1 se mantém, pois, supondo $\alpha < \beta$, existe $x \in \beta$ tal que $x \notin \alpha$. Logo, não podemos ter $\alpha = \beta$ nem $\beta < \alpha$. Supondo $\beta < \alpha$ chegamos, analogamente à mesma conclusão. Agora, caso $\alpha = \beta$, não existe $x \in \alpha$ tal que $x \notin \beta$ e não existe $x \in \beta$ tal que $x \notin \alpha$, o que exclui as desigualdades $\alpha < \beta$ e $\beta < \alpha$. Portanto, no máximo uma das três relações acima é válida.

Resta verificar que pelo menos uma delas acontece. Para isso, suponha que as duas primeiras relações dadas falham. Assim, se α não é suconjunto de β, então existe $p \in \alpha$ tal que $p \notin \beta$. Logo, se $q \in \beta$, temos $q < p$ e aí, concluimos que $q \in \alpha$. Como $\alpha \neq \beta$, temos $\beta < \alpha$.

Concluímos, então, que o conjunto de cortes é um conjunto ordenado.

Passo 2: O conjunto de cortes possui a propriedade do supremo (vide definição do capítulo 1).

Para provar isso, considere A um subconjunto não vazio do conjunto de cortes e assuma que β pertença ao conjunto de cortes e seja um limitante superior de A. Assim, $\alpha \leq \beta$ para todo $\alpha \in A$. Defina γ como a união de todos os $\alpha \in A$. Isso significa que $p \in \gamma$ se e somente se $p \in \alpha$ para algum $\alpha \in A$. Provaremos que γ é um corte e que $\gamma = \textit{sup } A$.

Vamos mostrar que γ é um corte. Desde que A é um conjunto não vazio (por suposição), existe $\alpha_0 \in A$. Desde que $\alpha_0 < \gamma$, γ é um conjunto não vazio. Depois, $\gamma < \beta$ (pois $\alpha < \beta$ para todo $\alpha \in A$ já que β é um limitante superior de A). Assim, $\gamma \neq \mathbb{Q}$. Portanto, está satisfeita a propriedade 1 da definição de corte. Quanto a propriedade 2, considere $p \in \gamma$. Então $p \in \alpha_1$ para algum $\alpha_1 \in A$. Assim, se $q < p$, então $q \in \alpha_1$ (pois α_1 é corte) e aí $q \in \gamma$. Isso prova 2. Agora, se $p \in \alpha_1$ podemos escolher $r \in \alpha_1$ de modo que $p < r$ (pois α_1 é um corte). Aí concluímos que $r \in \gamma$ o que implica que a propriedade 3 está satisfeita. Portanto, γ é corte.

Sabemos que $\alpha \leq \gamma$ para todo $\alpha \in A$. Tome $\delta < \gamma$. Então existe $s \in \gamma$ tal que $s \notin \delta$. Desde que $s \in \gamma$, temos que $s \in \alpha$ para algum $\alpha \in A$. Daí $\delta < \alpha$ e δ não é um limitante superior de A. Isso nos leva ao resultado desejado: $\gamma = \textit{sup } A$.

Assim, o conjunto de cortes é um conjunto ordenado que tem a propriedade do supremo. Abaixo vamos demonstrar que esse conjunto ordenado é um corpo. Para isso definiremos duas ope-

rações entre os elementos do conjunto de cortes: adição e multiplicação e, verificaremos que as propriedades dessas operações satisfazem as propriedades operatórias de um corpo.

Começaremos com a soma de cortes.

Passo 3: Soma de cortes.

Se α e β pertencem ao conjunto de cortes, definiremos $\alpha + \beta$ como sendo o conjunto das somas $r + s$, onde $r \in \alpha$ e $s \in \beta$.

1. Temos que mostrar que $\alpha + \beta$ é um corte.

   De fato, como α e β são cortes, existem $r_0 \in \alpha$ e $s_0 \in \beta$. Portanto, $r_0 + s_0 \in \alpha + \beta$ e aí $\alpha + \beta$ é não vazio. Além disso, $\alpha + \beta \neq \mathbb{Q}$ pois, tomando $r' \notin \alpha$ e $s' \notin \beta$ (existem pois $\alpha, \beta \neq \mathbb{Q}$), temos que $r' > r$ e $s' > s$ para todo $r \in \alpha$, $s \in \beta$. E aí podemos escrever $r' + s' > r + s$. Como a desigualdade anterior é válida para todo $r \in \alpha$ e $s \in \beta$ concluímos então que $r' + s' \notin \alpha + \beta$. Portanto, $\alpha + \beta \neq \mathbb{Q}$ e a propriedade 1 está satisfeita.

   Para mostrar a propriedade 2, tome $p \in \alpha + \beta$. Então $p = r + s$, com $r \in \alpha$ e $s \in \beta$. Se $q < p$, então podemos escrever $q < r+s$, e aí $q-s < r$ o que nos dá $q-s \in \alpha$ e $q = (q-s)+s \in \alpha+\beta$. Assim, é válida a propriedade 2 para $\alpha + \beta$.

   Falta a propriedade 3. Sejam $r \in \alpha$, $s \in \beta$ e escolha $t \in \alpha$ tal que $t > r$. Isso é possível pois α é um corte. Então $p = r + s < t + s$ e, $t + s \in \alpha + \beta$. Logo, 3 se mantém.

   Concluímos então que $\alpha + \beta$ é um corte.

2. A adição de cortes é comutativa.

   Considere $r + s \in \alpha + \beta$. Como $r, s \in \mathbb{Q}$, temos $r + s = s + r$. Como os elementos da forma $s + r$ pertencem ao conjunto $\beta + \alpha$, temos que os elementos de $\alpha + \beta$ e $\beta + \alpha$ são os mesmos. Portanto, $\alpha + \beta = \beta + \alpha$.

3. A adição de cortes é associativa.

   O conjunto $(\alpha + \beta) + \gamma$ tem elementos da forma $(r + s) + t$, onde $r \in \alpha$, $s \in \beta$ e $t \in \gamma$. Como $\alpha, \beta, \gamma \in \mathbb{Q}$, vale a associatividade entre os elementos dos cortes. Portanto, $(r + s) + t = r + (s + t)$. Como os elementos da forma $r + (s + t)$ pertencem a $\alpha + (\beta + \gamma)$, temos $(\alpha + \beta) + \gamma = \alpha + (\beta + \gamma)$.

4. Existe o elemento neutro da adição, o qual chamaremos de 0^*. Além disso, $\alpha + 0^* = \alpha$ com α pertencente ao conjunto de cortes.

   Vamos definir 0^* como o conjunto de todos os números racionais negativos. É fácil ver que 0^* é um corte. De fato, 0^* é não vazio (contém os números negativos). $0^* \neq \mathbb{Q}$ pois, por exemplo,

$2 \notin 0^*$. Além disso, se $p \in 0^*$, então $p < 0$. Tomando $q < p$ temos $q < 0$ e aí $q \in 0^*$. Isso satisfaz 2. Resta verificar a propriedade 3. Tomando $p \in 0^*$, temos $p < 0$. Escolhendo $q = p/2$ temos $p < q$ e $q \in 0^*$. Com isso concluímos que 0^* é um corte.

Sabendo que 0^* é um corte, tome $r \in \alpha$ e $s \in 0^*$. Assim, $r + s \in \alpha + 0^*$. Como $s < 0$ temos $r + s < r$ o que nos permite dizer $\alpha + 0^* \subset \alpha$. Para mostrarmos que $\alpha \subset \alpha + 0^*$, tome $p, q \in \alpha$, com $p < q$. Assim, $p - q \in 0^*$, e aí $p = q + (p - q) \in \alpha + 0^*$. Portanto, $\alpha \subset \alpha + 0^*$. Concluímos então que $\alpha = \alpha + 0^*$.

5. Existe o oposto de um corte α. Esse oposto será denotado por $-\alpha$.

   Para demonstrarmos a afirmação acima, fixe α no conjunto de cortes e considere β o conjunto de todos os p com a seguinte propriedade: Existe $r > 0$ tal que $-p - r \notin \alpha$. Em outras palavras, algum número racional menor que $-p$ não está em α. Nós provaremos que β está no conjunto de cortes e que $\alpha + \beta = 0^*$.

   Primeiramente, observemos que β é um corte. Para isso, vamos mostrar que a definição de corte é válida para esse conjunto. Tomemos então $s \notin \alpha$ e $p = -s - 1$, então $s = -p - 1 \notin \alpha$, e aí $p \in \beta$. Então β é não vazio. Se $q \in \alpha$, então $-q \notin \beta$, pois, se $-q \in \beta$, pela definição de β existiria $s > 0$ tal que $-(-q) - s = q - s \notin \alpha$, o que não acontece pois, α é corte e, sendo assim qualquer elemento menor que q está em α. Assim, $\beta \neq \mathbb{Q}$. Portanto a primeira propriedade se mantém.

   Agora escolha $p \in \beta$, e seja $r > 0$, tal que $-p - r \notin \alpha$. Se $q < p$, $-q - r > -p - r$, então, $-q - r \notin \alpha$, e aí $q \in \beta$. Assim, a propriedade II se mantém. Para verificarmos que a propriedade III se mantém, tome $p \in \beta$ e seja $r \in \mathbb{Q}, r > 0$ tal que $-p - r \notin \alpha$. Escolha $t = p + (r/2)$ com $r > 0$. Então $t > p$, e $-t - (r/2) = -(p + (r/2)) - (r/2) = -p - r \notin \alpha$. Assim, $t \in \beta$. Temos então que β é um corte.

   Agora mostraremos que $\alpha + \beta = 0^*$. Se $r \in \alpha$ e $s \in \beta$, então $-s \notin \alpha$, pois se $-s \in \alpha$, então para todo $r > 0$ teríamos $-s - r \in \alpha$, o que nos levaria a deduzir que $s \notin \beta$ (contradição). Logo $-s \notin \alpha$ e daí $r < -s$, $r + s < 0$. Assim, $\alpha + \beta \subset 0^*$.

   Para provar que $0^* \subset \alpha + \beta$, tome $v \in 0^*$ e considere $w = -v/2$. Claramente $w > 0$ e existe um natural n tal que $n \cdot w \in \alpha$, mas $(n + 1) \cdot w \notin \alpha$ (pois $\mathbb{Q}$ é um corpo arquimediano). Tomando $p = -(n + 2) \cdot w$, temos que $p \in \beta$, pois $-p - w = (n + 1) \cdot w \notin \alpha$. Além disso, $v = -2 \cdot w = n \cdot w + p \in \alpha + \beta$.

   Assim, $0^* \subset \alpha + \beta$.

   Concluímos então que $\alpha + \beta = 0^*$.

   β será denotado por $-\alpha$.

Passo 4: Sabendo agora que os axiomas da adição são válidos, concluímos que são válidas também as afirmações abaixo:

1^a afirmação: lei do cancelamento: Se $\alpha + \beta = \alpha + \gamma$, então $\beta = \gamma$.
2^a afirmação: unicidade do elemento neutro: Se $\alpha + \beta = \alpha$ então $\beta = 0^*$.
3^a afirmação: unicidade do oposto $-\alpha$ de α. Se $\alpha + \beta = 0^*$, então $\beta = -\alpha$.
4^a afirmação: o oposto do oposto de α é α: $-(-\alpha) = \alpha$.

Agora, considere os cortes $\alpha,\ \beta,\ \gamma$ com $\beta < \gamma$. Vamos verificar que $\alpha + \beta < \alpha + \gamma$. De fato, seja $x + y \in \alpha + \beta$ com $x \in \alpha$ e $y \in \beta$. Como, por hipótese $\beta < \gamma$ temos $y \in \gamma$, e aí concluímos que $x + y \in \alpha + \gamma$. Isso mostra que $\alpha + \beta < \alpha + \gamma$.

Podemos afirmar também que $\alpha > 0^*$ se e somente se $-\alpha < 0^*$.

Para isso , suponha primeiramente que $\alpha > 0^*$ e tome $p \in -\alpha$. Então existe $r > 0$ tal que $-p - r \notin \alpha$. Como $\alpha > 0^*$, $-p - r > 0$ o que nos dá $p < -r$. Como $r > 0$ temos $-r < 0$, portanto, $p < 0$ e $p \in 0^*$. Assim, $-\alpha < 0^*$.

Agora suponha $-\alpha < 0^*$. Vamos mostrar que $\alpha > 0^*$.

Considere $p \in 0^*$. Então $-p > 0$, ou seja, $-p$ é uma cota superior de $-\alpha$ e $-p \notin -\alpha$. Logo, existe $r > 0$ tal que $-p - r \notin -\alpha$. Isto é, $p \in \alpha$.

Passo 5: Neste passo demonstraremos que os axiomas de multiplicação da definição de corpo são válidos no conjunto de cortes. Para isso, trabalharemos inicialmente com cortes do tipo $\alpha > 0^*$.

Sejam α e β cortes nas condições acima. Definiremos $\alpha \cdot \beta$ o conjunto de todos os p tais que $p \leq r \cdot s$ para alguma escolha de $r \in \alpha$ e $s \in \beta$, sendo $r, s > 0$. Definiremos 1^* como o conjunto de todos os $q \in \mathbb{Q}$ tais que $q < 1$.

1. Se α e β são cortes, mostraremos que $\alpha \cdot \beta$ é um corte.

   De fato, como α e β são não vazios (pois ambos são cortes), existem $r \in \alpha$ e $s \in \beta$, ambos maiores que zero. Assim, existe $p \leq r \cdot s$ (por exemplo $\frac{r \cdot s}{2}$). Logo, $\alpha \cdot \beta$ é não vazio. Agora, como α e β são diferentes de $\mathbb{Q}$, existem $r \in \mathbb{Q}$ e $s \in \mathbb{Q}$, ambos maiores que zero tais que $r \notin \alpha$ e $s \notin \beta$. Assim, $r > p$ para todo $p \in \alpha$ e $s > q$ para todo $q \in \beta$. Temos então que $r \cdot s > p \cdot q,\ \forall p \in \alpha$ e$\forall q \in \beta$ o que implica em $r \cdot s \notin \alpha\beta$, mas $r \cdot s \in \mathbb{Q}$. Concluímos então

que $\alpha \cdot \beta \neq \mathbb{Q}$.

Agora tome $p \in \alpha \cdot \beta,\ \forall p \in \alpha$ e $\forall q \in \beta$ e $q \in \mathbb{Q}$ de modo que $q < p$. Assim, $p \leq r \cdot s$ para alguma escolha de $r \in \alpha$ e $s \in \beta$. Como $q < p$, temos $q \leq r \cdot s$, e aí concluímos que $q \in \alpha \cdot \beta$.

Falta verificar que o conjunto $\alpha \cdot \beta$ não possui maior elemento. De fato, se $p \in \alpha \cdot \beta$ então $p \leq r \cdot s$ para alguma escolha de $r \in \alpha$ e $s \in \beta$. Como α e β são cortes, ambos não possuem maior elemento. Assim, podemos escolher $u \in \alpha$ com $u > r$ e $v \in \beta$ com $v > s$. Temos então $p < r \cdot s < u \cdot v$ e $u \cdot v \in \alpha \cdot \beta$. Portanto, $\alpha \cdot \beta$ não possui maior elemento.

Concluímos então que $\alpha \cdot \beta$ é corte.

2. Comutatividade da multiplicação de cortes. Mostraremos que $\alpha \cdot \beta = \beta \cdot \alpha$.

   De fato, temos que $\alpha \cdot \beta$ é o conjunto dos $p \in \mathbb{Q}$ tais que $p \leq r \cdot s$ para algum $r \in \alpha$ e algum $s \in \beta$. Como $r, s \in \mathbb{Q}$, temos $r \cdot s = s \cdot r$ e aí $p \leq s \cdot r$ o que implica em $p \in \beta \cdot \alpha$. Portanto, $\alpha \cdot \beta = \beta \cdot \alpha$.

3. Associatividade da multiplicação. Vamos mostrar que $(\alpha \cdot \beta) \cdot \gamma = \alpha \cdot (\beta \cdot \gamma)$.

   Considere os cortes α, β e γ. Assim, dado $p \in (\alpha \cdot \beta) \cdot \gamma$, temos $p \leq (r \cdot s) \cdot t$ para alguma escolha de $r \in \alpha$, $s \in \beta$ e $t \in \gamma$. Como r, s e $t \in \mathbb{Q}$, e em $\mathbb{Q}$ a multiplicação é associativa, temos $(r \cdot s) \cdot t = r \cdot (s \cdot t)$, o que implica em $p \in \alpha \cdot (\beta \cdot \gamma)$.

4. Existência do elemento neutro da multiplicação de cortes.

   Devemos mostrar que $1^* \cdot \alpha = \alpha$ para todo o corte α, com 1^* o conjunto dos $q \in \mathbb{Q}$ tais que $q < 1$.

   Assim, se $r \in 1^* \cdot \alpha$, então $r \leq q \cdot p$ para algum $q \in 1^*$ e $p \in \alpha$. Como $q \in 1^*$, temos $q < 1$ o que implica em $q \cdot p < p$. Concluímos então que $r < p$ e aí $r \in \alpha$. Portanto, $1^* \cdot \alpha \subset \alpha$.

   Por outro lado, considere $p \in \alpha$. Então existe $r \in \alpha$ tal que $p < r$. Escrevendo p na forma $p = \dfrac{p}{r} \cdot r$, temos $\dfrac{p}{r} \in 1^*$ (pois $p < r$) e $r \in \alpha$, o que nos dá $p \in 1^* \cdot \alpha$. Assim, $\alpha \subset 1^* \cdot \alpha$
   Portanto, $1^* \cdot \alpha = \alpha$.

5. Definição do inverso multiplicativo.

   Se $\alpha > 0$ definiremos $\alpha^{-1} = \{r : r < \dfrac{1}{p}, p \notin \alpha\}$.

   Se $\alpha < 0$ definiremos $\alpha^{-1} = \{r : r < \dfrac{1}{p},\ p \notin \alpha,\ p < 0\}$.

   α^{-1} é um corte $(\alpha > 0)$. De fato:

- $\alpha^{-1} \neq \emptyset$.

  Seja $x > 0$ tal que $x \notin \alpha$. Assim, $-1 < \dfrac{1}{x}$, isto é, $-1 \in \alpha^{-1}$.

- Sejam $p \in \alpha^{-1}$ e $q \in \mathbb{Q}$ tal que $q < p$. Assim, dado $x > 0$ tal que $x \notin \alpha$ temos $p < \dfrac{1}{x}$. Como $q < p$, temos $q < \dfrac{1}{x}$, o que implica em $q \in \alpha^{-1}$.

- Agora seja $p \in \alpha^{-1}$.

  Seja $x > 0$ tal que $x \notin \alpha$ e $p < \dfrac{1}{x}$. Como entre dois racionais existe outro racional, temos que existe $q \in \mathbb{Q}$ tal que $p < q < \dfrac{1}{x}$. Logo $q \in \alpha^{-1}$ e $p < q$.

  Concluímos então que α^{-1} definido acima é um corte.

Agora vamos mostrar que $\alpha \cdot \alpha^{-1} = \alpha^{-1} \cdot \alpha = 1^*$.

- $\alpha \cdot \alpha^{-1} \subset 1^*$.

  Sejam $p \in \alpha$ e $q \in \alpha^{-1}$. Como $\alpha > 0$ temos que $\alpha^{-1} > 0$, logo, assumimos $p, q > 0$. Sabemos que existe $x \notin \alpha,\ x > 0$ tal que $q < \dfrac{1}{x}$. Também que $p < x$.

  Concluímos então que $p \cdot q < p \cdot \dfrac{1}{x} < x \cdot \dfrac{1}{x} = 1$, isto é , $p \cdot q \in 1^*$. Assim, $\alpha \cdot \alpha^{-1} \subset 1^*$.

- $1^* \subset \alpha \cdot \alpha^{-1}$.

  Como $\alpha > 0$ resulta que existe um $n_0 \in \mathbb{N}$ tal que para todo $n > n_0$ existe $k_n \in \mathbb{N}$ com a propriedade que $\dfrac{k_n}{n} \in \alpha$ e $\dfrac{k_{n+1}}{n} \notin \alpha$. Observar que $k_n < k_{n+1}$.

  Seja $p \in 1^*$. Claro que existem $n \in \mathbb{N}$ e seu correspondente k_n tal que $p < \dfrac{k_n}{k_{n+1}}$.

  Como $\dfrac{p \cdot n}{k_n} < (\dfrac{k_{n+1}}{n})^{-1}$ e entre dois racionais sempre tem outro racional, existe S_n tal que $\dfrac{p \cdot n}{k_n} < S_n < (\dfrac{k_{n+1}}{n})^{-1}$. Claro que $S_n \in \alpha^{-1}$ e $p < \dfrac{k_n}{n} \cdot S_n$. Isto é, $p \in \alpha \cdot \alpha^{-1}$. Assim, $1^* \subset \alpha \cdot \alpha^{-1}$.

  Portanto, $1^* = \alpha \cdot \alpha^{-1}$.

Passo 6: Completaremos a definição de multiplicação mostrando que: $\alpha \cdot 0^* = 0^* \cdot \alpha = 0^*$.

De fato, dado $p \in \alpha \cdot 0^*,\ \exists\ r \in \alpha$ e $s \in 0^*$. tal que $p \leq r \cdot s$. Como $r,\ s$ são números racionais, temos $r \cdot s = s \cdot r$, o que implica em $p \leq r \cdot s = s \cdot r$, ou seja, $p \in 0^* \cdot \alpha$. Assim, $\alpha \cdot 0^* \subset 0^* \cdot \alpha$. Analogamente, $0^* \cdot \alpha \subset \alpha \cdot 0^*$. Portanto $\alpha \cdot 0^* = \alpha \cdot 0^*$.

Agora, falta mostrar a segunda igualdade, ou seja, que $0^* \cdot \alpha = 0^*$. Para isto, considere $p \in 0^* \cdot \alpha$. Então $p \leq r \cdot s$ para $r \in 0^*$ (assim $r < 0$) e $s \in \alpha$.

Como estamos trabalhando com os números racionais positivos $s > 0$, e aí $r \cdot s < 0$, o que implica em $p \in 0^*$.

Assim, temos $0^* \cdot \alpha = \alpha \cdot 0^* \subset 0^*$. Vamos mostrar que $0^* \subset \alpha \cdot 0^*$.

Para isso, tome $p \in 0^*$. Assim, $p < 0$, o que pode ser escrito $p < r \cdot 0$, para todo $r \in \mathbb{Q}$. Em particular, considere $r > 0$ e suponha $r \in \alpha$. Nesse caso, $p \in \alpha \cdot 0^*$.

Portanto $0^* \subset \alpha \cdot 0^*$. Assim, temos $0^* \cdot \alpha = \alpha \cdot 0^* = 0^*$.

Vamos agora definir:

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

Observemos que os produtos foram definidos no passo anterior.

São eles:

a) $\alpha \cdot \beta = \beta \cdot \alpha$;

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

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

d) $\alpha \cdot 0^* = 0^* \cdot \alpha = 0^*$;

e) $1^* \cdot \alpha = \alpha$;

f) $\alpha \cdot \alpha^{-1} = \alpha^{-1} \cdot \alpha = 1^*$.

Sabendo que os axiomas da multiplicação são válidos para cortes pertencentes a $\mathbb{R}_+$ podemos verificar que os mesmos são válidos em $\mathbb{R}$ simplesmente aplicando as definições anteriores e a igualdade $-(-\gamma) = \gamma$. Faremos alguns casos:

a)$\alpha \cdot \beta = \beta \cdot \alpha$. Se $\alpha < 0^*$ e $\beta < 0^*$ temos $\alpha \cdot \beta = (-\alpha) \cdot (-\beta) = (-\beta) \cdot (-\alpha) = \beta \cdot \alpha$;

Se $\alpha < 0^*$ e $\beta > 0^*$ temos $\alpha \cdot \beta = -[(-\alpha) \cdot \beta] = -[\beta \cdot (-\alpha)] = \beta \cdot \alpha$;

Se $\alpha > 0^*$ e $\beta < 0^*$ temos $\alpha \cdot \beta = -[\alpha \cdot (-\beta)] = -[(-\beta) \cdot \alpha] = \beta \cdot \alpha$.

b) $(\alpha \cdot \beta) \cdot \gamma = \alpha \cdot (\beta \cdot \gamma)$

Como exemplo, considere $\alpha < 0^*,\ \beta < 0^*$ e $\gamma > 0^*$.

Temos $(\alpha \cdot \beta) \cdot \gamma = ((-\alpha) \cdot (-\beta)) \cdot \gamma$

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

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

Para uma demonstração completa deste item devemos verificar todos os casos possíveis.

c) $\alpha \cdot (\beta + \gamma) = \alpha \cdot \beta + \alpha \cdot \gamma$.
Como exemplo, considere $\alpha > 0^*,\ \beta < 0^*$ e $\beta + \gamma > 0^*$.
Então $\gamma = (\beta+\gamma)+(-\beta) \Rightarrow \alpha \cdot \gamma = \alpha \cdot (\beta+\gamma)+\alpha \cdot (-\beta) \Rightarrow \alpha \cdot \gamma = \alpha \cdot (\beta+\gamma)-\alpha \cdot \beta$
$\Rightarrow \alpha \cdot \beta + \alpha \cdot \gamma = \alpha \cdot (\beta + \gamma)$.

d) Se $\alpha < 0^*$, então podemos escrever:
$(-\alpha) \cdot 0^* + (-\alpha) \cdot 1^* = (-\alpha) \cdot (0^* + 1^*) = (-\alpha) \cdot 1^*$.
Assim, pela lei do cancelamento temos $(-\alpha) \cdot 0^* = 0^*$.

e) Se $\alpha < 0^*$, então:
$1^* \cdot \alpha + (-\alpha)$
$= 1^* \cdot \alpha + 1^* \cdot (-\alpha)$
$= 1^* \cdot \alpha - 1^* \cdot \alpha = 0^* \cdot \alpha = 0^*$.
Assim, $1^* \cdot \alpha = -(-\alpha) = \alpha$.

Concluímos que o conjunto de cortes é um corpo ordenado com a propriedade do supremo.

Passo 7: Esse passo faz a ponte entre o conjunto de corte e o conjunto $\mathbb{Q}$. Nós associaremos a cada $r \in \mathbb{Q}$ o conjunto r^* que consiste de todos os $p \in \mathbb{Q}$ tais que $p < r$. Afirmamos que cada r^* é um corte. De fato, temos:

1. Cada r^* é não vazio, pois existe $p = r - 1$, de modo que $p < r$ e $p \in \mathbb{Q}$. Assim, $p \in r^*$. Além disso, $r^* \neq \mathbb{Q}$ pois $s = r + 1 \in \mathbb{Q}$, mas $s \notin r^*$ (pois $s > r$), para cada $r \in \mathbb{Q}$.

2. Para cada $r \in \mathbb{Q}$ tomando $p \in r^*$, $q \in \mathbb{Q}$ e $q < p$, temos $q < p < r$, o que implica em $q \in r^*$.

3. Podemos verificar que r^* não possui maior elemento. De fato, se $p \in r^*$, temos $p < r$. Como $\mathbb{Q}$ é denso e o intervalo $(p, r) \in \mathbb{Q}$, existe $q \in \mathbb{Q}$ nesse intervalo, ou seja, $q > p$ e, $q < r$, o que

implica em $q \in r^*$.

Concluímos, então, que r^* com $r \in \mathbb{Q}$, para cada $r \in \mathbb{Q}$ é um corte.

Esses cortes, satisfazem as seguintes relações:

1. $r^* + s^* = (r+s)^*$;

   De fato, se $p \in r^* + s^*$ então p pode ser escrito como $p = u + v$ com $u < r$ e $v < s$ o que implica em $p < r + s$, ou seja, $p \in (r+s)^*$. Por outro lado, se $p \in (r+s)^*$, temos $p < r + s$. Escolhendo t tal que $2 \cdot t = r + s - p$ podemos escrever $u = r - t$ e $v = s - t$. Então $u \in r^*$ e $v \in s^*$ e aí temos $p = u + v \in r^* + s^*$. Portanto, $r^* + s^* = (r+s)^*$.

2. $r^* \cdot s^* = (r \cdot s)^*$;

   Tomando $p \in r^* \cdot s^*$, temos $p \leq u \cdot v$ para alguma escolha de $u \in r^*$ e $v \in s^*$, o que implica em $u < r$ e $v < s$. Assim, podemos escrever $p \leq u \cdot v < r \cdot s$. Logo, $p < r \cdot s$ e aí $p \in (r \cdot s)^*$. Por outro lado, se $p \in (r \cdot s)^*$, então $p < r \cdot s$, o que implica que $p \leq r \cdot s$ e, portanto, $p \in r^* \cdot s^*$. Podemos então dizer $r^* \cdot s^* = (r \cdot s)^*$.

3. $r^* < s^*$ se e somente se $r < s$.

   Suponha primeiramente que $r < s$. Então, $r \in s^*$ mas $r \notin r^*$. Assim, $r^* < s^*$. Supondo agora $r^* < s^*$, temos que existe $p \in s^*$ tal que $p \notin r^*$. Logo, $r \leq p < s$. Portanto $r < s$. Concluímos então que $r^* < s^*$ se e somente se $r < s$.

4. $-(r^*) = (-r^*)$
   Temos $-(r^*) = 0^* - (r^*) = (-r + r)^* - (r^*) = (-r)^* + (r^* - (r^*)) = (-r)^* + 0^* = (-r)^*$.

5. $(r^*)^{-1} = (r^{-1})^*$
   Temos $(r^*)^{-1} = (r^*)^{-1} \cdot 1^* = (r^*)^{-1} \cdot (r \cdot r^{-1})^* = (r^*)^{-1} \cdot (r^* \cdot (r^{-1})^*) = ((r^*)^{-1} \cdot r^*) \cdot (r^{-1})^* = 1^* \cdot (r^{-1})^* = (r^{-1})^*$

Passo 8: no passo anterior fizemos algo de extrema importância: identificamos o conjunto de *cortes racionais* com os *números racionais*. Essa identificação acontece através de uma função entre o conjunto de cortes e $\mathbb{Q}$ que preserva a soma, o produto e a ordem e que, por isso, permite que $\mathbb{Q}$ seja um subcorpo de $\mathbb{R}$.

Chegamos então ao fim da construção do conjunto dos números reais, caracterizando-o como um corpo ordenado completo, onde $\mathbb{Q}$ é um subcorpo.

Notemos que, $\mathbb{Q}$ é também um corpo ordenado, porém não é completo. No capítulo 1 mostramos essa afirmação.

Além de corpo ordenado completo, $\mathbb{R}$ é arquimediano, isto é, $\mathbb{N}$ é um subconjunto ilimitado superiormente em $\mathbb{R}$.

Diferentemente das construções de $\mathbb{Z}$ e $\mathbb{Q}$ feitas anteriormente, a construção feita através dos cortes de Dedekind não envolveu a criação de uma relação de equivalência, o que não acontece quando a construção é feita utilizando sequências de Cauchy de números racionais, método utilizado por George Cantor também na segunda metade do século XIX.

Capítulo 4

Construção dos números hiperreais

Por muito tempo matemáticos e físicos utilizavam as ideias de "infinito" e de "infinitésimo" resolvendo problemas sem se preocupar com uma formalização desses conceitos.

Archimedes encontrou a fórmula para área do círculo, no século III a.c, pensando no círculo como um polígono de infinitos lados infinitamente pequenos. *G.W. Leibniz*, no século XVII, utilizou extensivamente os números infinitesimais quando pretendia chegar tão perto do zero quanto se queria.

Independentemente do período ou do contexto histórico os números infinitamente pequenos ou infinitamente grandes fizeram parte da resolução de problemas matemáticos ou físicos mas nunca tiveram a atenção merecida no sentido de sair da ideia intuitiva e passar por uma formalização, fazendo parte efetivamente de um conjunto numérico.

Quem finalmente resolveu este problema, fazendo a construção de um conjunto numérico que contemplasse a existência dos *infinitos* e *infinitésimos* foi o matemático *Abraham Robinson* na década de 1960.

Ele desenvolveu o estudo da *Análise não-standard*, construindo o corpo dos *números hiperreais*, a partir da extensão rigorosa do conjunto dos números reais.

Nesse novo sistema definiu-se como *infinitésimo* um número maior que zero que seja menor que qualquer número real positivo e *infinito* como um número maior que zero e maior que qualquer número real maior que zero.

A criação dos números hiperreais faz uso de sequências reais de um modo diferente do que era usado na época, pois a preocupação de *Abraham Robinson* não era com a convergência das mesmas, mas como cada sequência poderia representar um número real *standard* e números reais *não-standard*, que seriam uma extensão do primeiro conjunto.

O corpo de sequências de valor real identificaria cada número real com uma sequência constante cujas entradas são o próprio número.

Nós começaremos considerando o conjunto das sequências de valor real, que será denotado por $\mathbb{R}^{\mathbb{N}}$ com a adição e multiplicação feitas ponto a ponto. Claramente se somarmos ou multi-

plicarmos duas sequências de valor real ponto a ponto conseguiremos outra sequência de valor real, o que nos permite falar que o conjunto $\mathbb{R}^{\mathbb{N}}$ é um conjunto fechado com relação a essas duas operações. Do mesmo modo, toda sequência de valor real tem um inverso aditivo. Basta tomarmos o inverso aditivo de cada entrada da sequência. Temos então que o conjunto $\mathbb{R}^{\mathbb{N}}$ forma um anel comutativo com identidade. Porém se quisermos verificar se o nosso conjunto é um corpo (o que seria conveniente), esbarramos no problema dos divisores de zero, pois podemos ter duas sequências não nulas cujo produto é nulo. Considere, por exemplo, as sequências $a = 0,\ 1,\ 0,\ 1,\ 0, \ldots$ e $b = 1,\ 0,\ 1,\ 0,\ 1, \ldots$. Nenhuma delas é nula, porém o produto delas é nulo. Veja, $a \cdot b = 0 \cdot 1,\ 1 \cdot 0,\ 0 \cdot\ 1,\ \ldots = 0, 0, 0, 0, \ldots$. Assim, $\mathbb{R}^{\mathbb{N}}$ não seria um corpo.

Para resolver esse problema foi desenvolvida uma teoria (a dos *números hiperreais*). Primeiramente é necessário introduzir a noção de ultrafiltro livre.

***Definição* 27.** (Filtros) Um filtro $\mathscr{U}$ sobre um conjunto J é um subconjunto de $P(J)$, o conjunto de potência de J, satisfazendo as seguintes propriedades:

1. Subconjunto próprio: $\emptyset \notin \mathscr{U}$,
2. Propriedade da intersecção finita: Se A, $B \in \mathscr{U}$, então $A \cap B \in \mathscr{U}$,
3. Propriedade de superconjunto: Se $A \in \mathscr{U}$ e $A \subseteq B$, então $B \in \mathscr{U}$.

Como exemplos de filtros podemos citar:

***Exemplo* 29.** O conjunto $F = \{B \subseteq \mathbb{N} \mid A_0 \subseteq B\}$, com $A_0 \subseteq \mathbb{N}$, A_0 não vazio.

Podemos observar que F é um filtro sobre $\mathbb{N}$ pois:

- O conjunto vazio não pertence a F pois $A_0 \subseteq B$ e A_0 é não vazio.
- Dados dois conjuntos B_1 e B_2 em F, temos $A_0 \subseteq B_1$, e $A_0 \subseteq B_2$, o que implica em $A_0 \subseteq B_1 \cap B_2$. Portanto, $B_1 \cap B_2 \in F$.
- Se A está em F, então $A_0 \subset A$. Dado B tal que $A \subseteq B$, temos $A_0 \subseteq B$, o que significa $B \in F$.

***Exemplo* 30.** Dado um conjunto infinito S, a família de todos os subconjuntos cofinitos de S é um filtro.

Lembremos que um conjunto $A \subseteq S$ é cofinito se A é o complementar de um conjunto finito em S.

Considere a família de todos os subconjuntos cofinitos $\mathscr{C} = \{A_i\}$ de S. Temos, então:

- O conjunto vazio $\emptyset$ não pertence a $\mathscr{C}$ pois o complementar de $\emptyset$ em S é $S - \emptyset = S$, que é infinito.

- Dados dois conjuntos cofinitos A_i e A_j pertencentes a $\mathscr{C}$, temos que $S - (A_i \cap A_j) = (S - A_i) \cup (S - A_j)$. Como A_i e A_j são cofinitos, os complementares de A_i e A_j dados respectivamente por $S - A_i$ e $S - A_j$ são finitos. Assim, $S - (A_i \cap A_j) = (S - A_i) \cup (S - A_j)$ é finito, o que implica em $S - (A_i \cap A_j)$ é finito. Logo, $A_i \cap A_j \in \mathscr{C}$.
- Agora suponha $A_i \in \mathscr{C}$. Assim, pela definição do conjunto $\mathscr{C}$ temos que $S - A_i$ é finito. Tomando agora $A_j \in S$ tal que $A_i \subset A_j$, temos $S - A_j \subseteq S - A_i$. Como $S - A_i$ é finito, temos $S - A_j$ finito. Logo $A_j \in \mathscr{C}$.

Portanto, a família $\mathscr{C}$ de todos os subconjuntos cofinitos de S é um filtro sobre S.

***Definição* 28.** Um filtro $\mathscr{U}$ será chamado *ultrafiltro* sobre J se, para todo $A \subseteq J$ temos $A \in \mathscr{U}$ ou $J - A \in \mathscr{U}$.

Posteriormente veremos que os ultrafiltros são os filtros maximais.

***Definição* 29.** Um ultrafiltro $\mathscr{U}$ sobre J será chamado livre se ele não contém subconjuntos finitos de J.

O lema abaixo garante que, dado qualquer ultrafiltro $\mathscr{U}$ sobre $\mathbb{N}$ e qualquer coleção finita de subconjuntos disjuntos de $\mathbb{N}$ cuja união é $\mathbb{N}$, resulta que exatamente um desses subconjuntos deverá pertencer ao ultrafiltro.

***Lema* 4.** Seja $\mathscr{U}$ um ultrafiltro sobre $\mathbb{N}$, e seja $\{A_1, \ldots, A_n\}$ uma coleção finita de subconjuntos disjuntos tal que $\bigcup_{j=1}^{n} A_j = \mathbb{N}$. Então existe um único j tal que $A_j \in \mathscr{U}$.

***Demonstração* 7.** Provaremos que existe $A_i \in \mathscr{U}$.

Para isso, suponha, por absurdo, que $\mathscr{U}$ não contenha nenhum dos subconjuntos $A_1, \ldots, A_n$. Então, $\mathscr{U}$ precisa conter o complementar de cada subconjunto, ou seja, os conjuntos $\mathbb{N} - A_1, \ldots, \mathbb{N} - A_n$ estão em $\mathscr{U}$. Portanto, $\mathscr{U}$ contém a intersecção desses complementares dada por:

$$\bigcap_{j=1}^{n}(A_j^c) = (\bigcup_{j=1}^{n} A_j)^c = (\mathbb{N})^c = \emptyset$$

Como $\mathscr{U}$ não contém o conjunto vazio, temos um absurdo. Logo, $\mathscr{U}$ contém um dos conjuntos $A_1, \ldots, A_n$.

Agora suponha que $\mathscr{U}$ contenha A_i e A_j para $i \neq j$. Então $\mathscr{U}$ precisa também conter $A_i \cap A_j$. Porém, A_i e A_j são disjuntos, ou seja $A_i \cap A_j = \emptyset$. Como $\mathscr{U}$ não contém o conjunto vazio temos que $\mathscr{U}$ pode conter apenas um dos subconjuntos $A_1, \ldots, A_n$.

O lema a seguir mostra que qualquer filtro pode ser estendido a um ultrafiltro. Basta utilizarmos o Lema de Zorn para provar a existência de um filtro maximal e depois disso verificarmos que esse filtro maximal satisfaz a propriedade de ultrafiltro.

***Lema* 5.** Lema do Ultrafiltro. Seja J um conjunto e $F_0 \subset P(J)$ um filtro sobre J. Então F_0 pode ser estendido a um ultrafiltro $\mathscr{F}$ sobre J.

***Demonstração* 8.** 1^o passo: mostraremos a existência de um filtro maximal. Considere o conjunto Φ dos filtros sobre J que contém F_0. Isso forma um conjunto parcialmente ordenado pela relação de inclusão. Agora considere qualquer cadeia $\{F_i\}_{i\in I}$ de filtros em Φ. A cadeia $\{F_i\}_{i\in I}$ é um subconjunto totalmente ordenado de Φ. Afirmamos que o conjunto $\cup F_i = G$ é um limitante superior da cadeia. De fato, como $\emptyset \notin F_i$ para todo $i \in I$ (pois cada F_i é um filtro), temos que $\emptyset \notin G$.

Similarmente, para todos $a \in G$, temos $a \in F_i$ para algum i. Então, para todo b tal que $a \subseteq b$, temos $b \in F_i \subset G$, o que satisfaz a propriedade de superconjunto do filtro G. Por último, suponha $a,\ b \in G$. Assim, $a \in F_i$ e $b \in F_j$ para $i,\ j \in I$. Suponha $i \leq j$. Então $F_i \subset F_j$ e, aí $a,\ b \in F_j$, o que, pela propriedade da interseção finita mostra que $a \cap b \in F_j \subset G$. Portanto, G também satisfaz a propriedade da interseção finita, o que nos leva a concluir que $G \in \Phi$ é também um filtro.

Logo, Φ é um conjunto não vazio, ordenado parcialmente tal que todo subconjunto ordenado totalmente (cadeia de filtros) tem um limitante superior em Φ. Essas são as hipóteses do Lema de Zorn. Assim, por esse lema, Φ possui pelo menos um elemento maximal, que será denotado por $\mathscr{F}$.

2^o passo: Agora vamos mostrar que o filtro maximal $\mathscr{F}$ encontrado é um ultrafiltro. Para isso, vamos verificar que, para todo $X \subseteq J$ ou X ou $J - X$ pertence ao ultrafiltro $\mathscr{F}$.

Seja $X \subseteq A$ e suponha que $\mathscr{F}$ não contenha nem X nem $A - X$. Então $\mathscr{F}$ precisa conter algum $a \in \mathscr{F}$ tal que $a \cap X = \emptyset$. Se não, então $\mathscr{F} \cup \{X\}$ seria um filtro, o que viola a maximalidade de $\mathscr{F}$.

Similarmente, $\mathscr{F}$ precisa conter algum b tal que $b \cap (A - X) = \emptyset$. Pela propriedade da interseção finita devemos ter então $a \cap b \neq \emptyset$. Mas isso é impossível pois a está inteiramente fora de X e b está inteiramente fora de $A - X$.

Portanto $\mathscr{F}$ precisa conter X ou $A - X$.

A existência de ultrafiltros livres (que não contém subconjuntos finitos de J) segue imediatamente do lema anterior. Basta tomar o filtro consistindo de todos os conjuntos cofinitos (cujo complementar é finito) e estender a um ultrafiltro. Como esse filtro não terá conjuntos finitos e o ultrafiltro resultante contém esses conjuntos ou seus complementares, o ultrafiltro maximal resultante poderá ser formado apenas por conjuntos infinitos, o que é uma condição para termos um *ultrafiltro livre*.

Agora precisamos juntar a ideia de ultrafiltro livre vista até aqui e as sequências de números reais que representarão os números hiperreais.

Para isso, nós precisamos saber quando igualar duas sequências criando uma relação de equivalência.

Mas quando duas sequências serão iguais? Quando o conjunto dos índices dos termos iguais (que é um subconjunto dos números naturais) formar um conjunto grande (todos exceto por uma quantidade finita de termos).

Para completar é primordial entendermos que justamente os subconjuntos grandes de $\mathbb{N}$ serão o ultrafiltro procurado, em relação ao qual definiremos abaixo a equivalência módulo ultrafiltro.

***Definição* 30.** (Equivalência Módulo Ultrafiltro) Dado um ultrafiltro livre $\mathscr{U}$ sobre $\mathbb{N}$, e sequências de valor real $a,\ b \in \mathbb{R}^{\mathbb{N}}$, nós definimos a relação $=_{\mathscr{U}}$ por $a =_{\mathscr{U}} b$ se $\{j \in \mathbb{N} / a_j = b_j\} \in \mathscr{U}$.

***Demonstração* 9.** Mostraremos que a relação acima definida é, de fato, uma relação de equivalência. Para isso, devemos mostrar que $=_{\mathscr{U}}$ satisfaz as propriedades reflexividade, simetria e transitividade.

- Reflexividade: Tomando uma sequência $a \in \mathbb{R}^{\mathbb{N}}$, temos que o conjunto $\{j \in \mathbb{N} / a_j = a_j\}$ é o conjunto dos números naturais. Temos, $\mathbb{N} \in \mathscr{U}$, pois se $\mathbb{N} \notin \mathscr{U}$, então $\emptyset = \mathbb{N} - \mathbb{N} \in \mathscr{U}$, o que é impossível. Assim $a =_{\mathscr{U}} a$.
- Simetria: Para quaisquer sequências a e b pertencentes a $\mathbb{R}^{\mathbb{N}}$ tais que $a =_{\mathscr{U}} b$, temos que se $\{j \in \mathbb{N} / a_j = b_j\} \in \mathscr{U}$, então $\{j \in \mathbb{N} / b_j = a_j\} \in \mathscr{U}$. Assim, $a =_{\mathscr{U}} b$ implica em $b =_{\mathscr{U}} a$.
- Transitividade: Considere as sequências $a,\ b,\ c \in \mathbb{R}^{\mathbb{N}}$. Suponhamos $a =_{\mathscr{U}} b$ e $b =_{\mathscr{U}} c$. Então os conjuntos $\{j \in \mathbb{N} / a_j = b_j\}$ e $\{j \in \mathbb{N} / b_j = c_j\}$ são ambos elementos de $\mathscr{U}$. Porém, os conjuntos nos quais $a_j = b_j$ e $b_j = c_j$ podem ser escritos na forma $\{j \in \mathbb{N} / a_j = b_j \ \& \ b_j = c_j\}$. Como $\{j \in \mathbb{N} / a_j = b_j\} \in \mathscr{U}$ e $\{j \in \mathbb{N} / b_j = c_j\} \in \mathscr{U}$, temos $\{j \in \mathbb{N} / a_j = b_j\} \cap \{j \in \mathbb{N} / b_j = c_j\} \in \mathscr{U}$(propriedade da intersecção finita).
  Como $\{j \in \mathbb{N} / a_j = b_j\} \cap \{j \in \mathbb{N} / b_j = c_j\} \subseteq \{j \in \mathbb{N} / a_j = c_j\}$, temos $\{j \in \mathbb{N} / a_j = c_j\} \in \mathscr{U}$ (propriedade de superconjunto).
  Assim, $a =_{\mathscr{U}} b$ e $b =_{\mathscr{U}} c$ implica em $a =_{\mathscr{U}} c$, o que prova a transitividade.

Portanto, a relação $=_{\mathscr{U}}$ é uma relação de equivalência. Denotaremos a classe de equivalência da sequência a por $[a]$.

Agora que já está definida a relação de equivalência que fará do conjunto de sequências de valor real um corpo, devemos definir as operações desse conjunto e posteriormente verificar que essas operações satisfazem as propriedades operatórias de um corpo. A ideia intuitiva de que se $a_1 =_{\mathscr{U}} a_2$ e $b_1 =_{\mathscr{U}} b_2$ então $a_1 + b_1 =_{\mathscr{U}} a_2 + b_2$ deverá ser verificada, ou seja, devemos mostrar que a adição está bem definida no nosso conjunto. O mesmo deverá acontecer com a multiplicação. Para fazer isso, provaremos o lema abaixo:

***Lema* 6.** A adição e a multiplicação ponto a ponto são operações binárias bem definidas no conjunto de sequências de valor real sobre ultrafiltro equivalência.

***Demonstração* 10.** A demonstração desse lema será feita considerando-se a notação a_{ki} com k denotando a que sequência estamos nos referindo e i denotando a posição de cada termo da sequência. Considere as sequências reais a_1, a_2, b_1 e b_2 e suponha que $a_1 =_{\mathscr{U}} a_2$ e $b_1 =_{\mathscr{U}} b_2$. Isso significa que $\{i \in \mathbb{N}/a_{1i} = a_{2i}\} \in \mathscr{U}$ e $\{k \in \mathbb{N}/b_{1k} = b_{2k}\} \in \mathscr{U}$. Então, pela propriedade da intersecção finita sabemos que $\{i \in \mathbb{N}/a_{1i} = a_{2i}\} \cap \{k \in \mathbb{N}/b_{1k} = b_{2k}\} \in \mathscr{U}$, o que significa dizer $\{j \in \mathbb{N}/a_{1j} = a_{2j}\ \&\ b_{1j} = b_{2j}\} \in \mathscr{U}$. Sendo assim, temos que $\{j \in \mathbb{N}/a_{1j} + b_{1j} = a_{2j} + b_{2j}\} \in \mathscr{U}$, o que implica em $\{j \in \mathbb{N}/(a_1 + b_1)_j = (a_2 + b_2)_j\} \in \mathscr{U}$. Portanto, $a_1 + b_1 =_{\mathscr{U}} a_2 + b_2$, ou seja, a adição está bem definida. Para verificarmos que a multiplicação está bem definida, tome novamente $a_1 =_{\mathscr{U}} a_2$ e $b_1 =_{\mathscr{U}} b_2$. Então $\{i \in \mathbb{N}/a_{1i} = a_{2i}\} \in \mathscr{U}$ e $\{k \in \mathbb{N}/b_{1k} = b_{2k}\} \in \mathscr{U}$. Pela propriedade da intersecção finita sabemos que $\{i \in \mathbb{N}/a_{1i} = a_{2i}\} \cap \{k \in \mathbb{N}/b_{1k} = b_{2k}\} \in \mathscr{U}$, o que significa dizer $\{j \in \mathbb{N}/a_{1j} = a_{2j}\ \&\ b_{1j} = b_{2j}\} \in \mathscr{U}$. Sendo assim, podemos escrever $\{j \in \mathbb{N}/a_j \cdot b_{1j} = a_{2j} \cdot b_{2j}\} \in \mathscr{U}$, o que implica em $\{j \in \mathbb{N}/(a_1 \cdot b_1)_j = (a_2 \cdot b_2)_j\} \in \mathscr{U}$. Portanto, $a_1 \cdot b_1 =_{\mathscr{U}} a_2 \cdot b_2$ o que significa que a multiplicação está bem definida em $\mathbb{R}^{\mathbb{N}}$.

O conjunto dos números hiperreais será o conjunto das sequências de valor real módulo ultrafiltro, e será denotado por ${}^*\mathbb{R}$.

Sabendo que as operações (+ e $\cdot$) acima estão bem definidas nesse conjunto, vamos verificar que, para essas operações são válidas as propriedades de corpo, através do teorema a seguir.

***Teorema* 6.** O conjunto ${}^*\mathbb{R}$ com a adição e multiplicação ponto a ponto é um corpo.

***Demonstração* 11.** A adição é comutativa. De fato, dadas duas sequências $a,\ b \in {}^*\mathbb{R}$, temos que $[a + b]$ será o conjunto dos $c \in {}^*\mathbb{R}$ tais que $a + b =_{\mathscr{U}} c$, o que implica em $\{j \in \mathbb{N}/(a + b)_j = c_j\} = \{j \in \mathbb{N}/a_j + b_j = c_j\} = \{j \in \mathbb{N}/b_j + a_j = c_j\} = \{j \in \mathbb{N}/(b+a)_j = c_j\} \in \mathscr{U}$. Portanto, $b + a =_{\mathscr{U}} c$. Assim, podemos dizer que $a + b =_{\mathscr{U}} b + a$, ou seja, a adição é comutativa em ${}^*\mathbb{R}$.

2. A adição é associativa. Sejam $a, b, c \in {}^*\mathbb{R}$. Assim, $[(a + b) + c]$ será o conjunto dos $d \in {}^*\mathbb{R}$ tais que $(a + b) + c =_{\mathscr{U}} d$, o que implica em $\{j \in \mathbb{N}/((a + b) + c)_j = d_j\} = \{j \in \mathbb{N}/(a_j + b_j) + c_j = d_j\} = \{j \in \mathbb{N}/a_j + (b_j + c_j) = d_j\} = \{j \in \mathbb{N}/(a + (b + c))_j = d_j\} \in \mathscr{U}$. Portanto, $(a+b)+c =_{\mathscr{U}} a+(b+c)$, ou seja, a adição é associativa.

3. Existe o elemento neutro da adição e ele é único. Esse elemento será denotado por 0 e será a sequência constante nula em ${}^*\mathbb{R}$. De fato, dado $a \in {}^*\mathbb{R}$, temos $\{j \in \mathbb{N}/a_j = a_j + 0_j\} = \{j \in \mathbb{N}/a_j = (a+0)_j\} \in \mathscr{U}$, o que implica em $a =_{\mathscr{U}} a + 0$. Agora suponha que exista $e \in {}^*\mathbb{R}$ tal que para todo $a \in {}^*\mathbb{R}$ se tenha $e + a =_{\mathscr{U}} a$. Então $\{j \in \mathbb{N}/e_j + a_j = a_j\} \in \mathscr{U}$. Pela unicidade do elemento neutro aditivo em $\mathbb{R}$ $e_j = 0$ para cada $j \in \mathbb{N}$, o que nos permite concluir que a sequência constante nula é o único elemento neutro da adição em ${}^*\mathbb{R}$.

4. Existe o inverso aditivo para todo $a \in {}^*\mathbb{R}$ e ele é único. Para qualquer hiperreal a podemos definir seu inverso aditivo como $-a$, isto é, $-a$ possui todas as entradas opostas às entradas de a. Vamos mostrar que esse inverso aditivo é único. Para isso, suponha que existam $x,\ y \in {}^*\mathbb{R}$ tais que $x + a =_{\mathscr{U}} a + x =_{\mathscr{U}} 0$ e $y + a =_{\mathscr{U}} a + y =_{\mathscr{U}} 0$. Então, pelas propriedades associatividade e existência do elemento neutro podemos escrever: $y =_{\mathscr{U}} y + 0 =_{\mathscr{U}} y + (a + x) =_{\mathscr{U}} (y + a) + x =_{\mathscr{U}} 0 + x =_{\mathscr{U}} x$. Pela transitividade da relação de equivalência $=_{\mathscr{U}}$ temos $y =_{\mathscr{U}} x$. Portanto, o inverso aditivo dos elementos de ${}^*\mathbb{R}$ é único para cada elemento.

5. A multiplicação é comutativa. Tomando $a,\ b \in {}^*\mathbb{R}$ temos que $[a \cdot b]$ é a classe dos elementos $c \in {}^*\mathbb{R}$, tais que $a \cdot b =_{\mathscr{U}} c$ ou seja, tal que $\{j \in \mathbb{N} / (a \cdot b)_j = c_j\} \in \mathscr{U}$. Como a multiplicação em $\mathbb{R}$ é comutativa, temos $\{j \in \mathbb{N} / (b \cdot a)_j = c_j\} \in \mathscr{U}$ o que implica em $a \cdot b =_{\mathscr{U}} b \cdot a$, ou seja, a multiplicação é comutativa em ${}^*\mathbb{R}$.

6. A multiplicação é associativa. Sejam $a, b, c \in {}^*\mathbb{R}$. Assim $[(a \cdot b) \cdot c]$ será o conjunto dos elementos $d \in {}^*\mathbb{R}$ tais que $(a \cdot b) \cdot c =_{\mathscr{U}} d$, o que implica em $\{j \in \mathbb{N} / ((a \cdot b) \cdot c)_j = d_j\} \in \mathscr{U}$. Como a multiplicação de números reais é associativa, temos $\{j \in \mathbb{N} / (a \cdot (b \cdot c))_j = d_j\} \in \mathscr{U}$, o que nos permite concluir que $(a \cdot b) \cdot c =_{\mathscr{U}} a \cdot (b \cdot c)$, ou seja, a multiplicação é associativa ${}^*\mathbb{R}$.

7. Existe o elemento neutro da multiplicação e ele é único. Esse elemento será a sequência constante $1 \in {}^*\mathbb{R}$. Como a multiplicação acontece ponto a ponto, teremos, para cada $j \in \mathbb{N},\ 1 \cdot a_j = a_j$. Assim, podemos escrever para todo $a \in {}^*\mathbb{R}$, $1 \cdot a =_{\mathscr{U}} a$, o que implica em $\{j \in \mathbb{N} / (1 \cdot a)_j = a_j\} \in \mathscr{U}$.

8. Existe em ${}^*\mathbb{R}$ o inverso multiplicativo de cada elemento e ele é único.
   Inicialmente vamos pensar nas entradas nulas de cada hiperreal $a \in {}^*\mathbb{R}$. Denotaremos por X o conjunto $\{j \in \mathbb{N} / a_j = 0\}$. Se $X \in \mathscr{U}$, então $a =_{\mathscr{U}} 0$ e aí, ele não tem inverso multiplicativo, assim como $0 \in \mathbb{R}$.
   Agora, se $X \notin \mathscr{U}$, então pela maximalidade do ultrafiltro $\mathscr{U}$ devemos ter $\mathbb{N} - X \in \mathscr{U}$. Assim, $a =_{\mathscr{U}} a'$, onde a' será uma sequência de valor real definida por

$$a'_n = \begin{cases} a_n \text{ se } n \in \mathbb{N} - X \\ 1 \text{ se } n \in X \text{ (ou seja, nas entradas nulas)} \end{cases}$$

   Desde que nenhum termo da sequência a'_n é 0, podemos definir o inverso multiplicativo ponto a ponto. Assim, a^{-1}(inverso multiplicativo de a) será $a^{-1} = (a'_n)^{-1}$.

9. Vale a distributiva da multiplicação em relação a adição. De fato, sejam $a, b, c, d \in {}^*\mathbb{R}$ e suponha que $a \cdot (b + c) =_{\mathscr{U}} d$. Assim, $\{j \in \mathbb{N} / a_j \cdot (b_j + c_j) = d_j\} \in \mathscr{U}$. Como cada um dos elementos $a_j,\ b_j,\ c_j,\ d_j \in \mathbb{R}$, vale a distributiva para cada valor de $j \in \mathbb{N}$, o que nos permite escrever $\{j \in \mathbb{N} / a_j \cdot (b_j + c_j) = a_j \cdot b_j + a_j \cdot c_j = d_j\} \in \mathscr{U}$. Portanto, $a_j \cdot b_j + a_j \cdot c_j =_{\mathscr{U}} d_j$, e vale a distributiva da multiplicação em relação à adição em $\mathscr{U}$.

Agora está demonstrado que ${}^*\mathbb{R}$ é um corpo. Vamos então definir uma relação de ordem em ${}^*\mathbb{R}$.

***Definição* 31.** (Ordem módulo ultrafiltro) Dados dois hiperreais $a = [(a_n)_{n\in\mathbb{N}}]$ e $b = [(b_n)_{n\in\mathbb{N}}]$, e um ultrafiltro $\mathscr{U}$ sobre $\mathbb{N}$, definimos a relação $\leq_{\mathscr{U}}$ por $a \leq_{\mathscr{U}} b$ se $\{j \in \mathbb{N}/a_j \leq b_j\} \in \mathscr{U}$.

Vamos mostrar abaixo que a relação $\leq_{\mathscr{U}}$ definida acima impõe uma ordem total no conjunto dos números hiperreais. Para isso vamos verificar que $\leq_{\mathscr{U}}$ é uma ordem parcial obedecendo as propriedades reflexividade, anti-simetria e transitividade.

- Reflexividade: Considere $a \in {}^*\mathbb{R}$.

  Assim, para cada $j \in \mathbb{N}$, é claro que $a_j \leq_{\mathscr{U}} a_j$ e, por isso, $\{j \in \mathbb{N}/a_j \leq_{\mathscr{U}} a_j\} = \mathbb{N}$. Como $\mathbb{N} \in \mathscr{U}$, temos $a \leq_{\mathscr{U}} a$ em ${}^*\mathbb{R}$;

- Anti-simetria: Suponha $a,\ b \in {}^*\mathbb{R}$ e $a \leq_{\mathscr{U}} b$ e $b \leq_{\mathscr{U}} a$. Assim, podemos escrever $\{j \in \mathbb{N}/a_j \leq_{\mathscr{U}} b_j\} \in \mathscr{U}$ e $\{j \in \mathbb{N}/b_j \leq_{\mathscr{U}} a_j\} \in \mathscr{U}$, o que implica em $\{j \in \mathbb{N}/a_j \leq_{\mathscr{U}} b_j \ \& \ b_j \leq_{\mathscr{U}} a_j\} \in \mathscr{U}$, isto é, $\{j \in \mathbb{N}/a_j =_{\mathscr{U}} b_j\} \in \mathscr{U}$. Portanto, $a =_{\mathscr{U}} b$;

- Transitividade. Para isso, considere os elementos $a, b, c \in {}^*\mathbb{R}$, de modo que $a \leq_{\mathscr{U}} b$ e $b \leq_{\mathscr{U}} c$. Assim, $\{j \in \mathbb{N}/a_j \leq_{\mathscr{U}} b_j\} \in \mathscr{U}$ e $\{j \in \mathbb{N}/b_j \leq_{\mathscr{U}} c_j\} \in \mathscr{U}$. Pela propriedade da intersecção finita temos $\{j \in \mathbb{N}/a_j \leq_{\mathscr{U}} b_j\} \cap \{j \in \mathbb{N}/b_j \leq_{\mathscr{U}} c_j\} \in \mathscr{U}$. Logo, temos $\{j \in \mathbb{N}/a_j \leq_{\mathscr{U}} b_j \ \& \ b_j \leq_{\mathscr{U}} c_j\} = \{j \in \mathbb{N}/a_j \leq_{\mathscr{U}} b_j \leq_U c_j\} \in \mathscr{U}$. Como a transitividade vale para os números reais, temos $\{j \in \mathbb{N}/a_j \leq_{\mathscr{U}} c_j\} \in \mathscr{U}$. Portanto, $a \leq_{\mathscr{U}} c$.

Agora mostraremos que $\leq_{\mathscr{U}}$ satisfaz a propriedade adicional: dados $a,\ b \in {}^*\mathbb{R}$, temos $a <_{\mathscr{U}} b$, $a =_{\mathscr{U}} b$ ou $a >_{\mathscr{U}} b$.

Para isso, considere $a,\ b \in {}^*\mathbb{R}$ e o conjunto $X = \{j \in \mathbb{N}/a_j \leq_{\mathscr{U}} b_j\}$. Pela maximalidade do ultrafiltro $\mathscr{U}$, temos que X ou $\mathbb{N} - X$ pertence a $\mathscr{U}$. Se $X \in \mathscr{U}$, então $a \leq_{\mathscr{U}} b$. Se $X \notin \mathscr{U}$, então $\mathbb{N} - X = \{j \in \mathbb{N}/a_j >_{\mathscr{U}} b_j\} \in \mathscr{U}$, o que implica em $b <_{\mathscr{U}} a$, como queríamos.

Temos agora um corpo totalmente ordenado, o qual chamaremos de conjunto dos números hiperreais e representaremos por ${}^*\mathbb{R}$. Falta mostrar a existência de números infinitos e números infinitesimais rigorosamente. Para isso, introduziremos a notação ${}^\sigma\mathbb{R}$ para o conjunto dos números hiperreais standard, que é o conjunto dos números reais propriamente dito, cujos elementos são representados por sequências constantes cujas entradas são o próprio número real. Similarmente ${}^\sigma\mathbb{N}$ denota o conjunto das sequências constantes com valores naturais. Definiremos abaixo o que são os números infinitos e infinitesimais.

***Definição* 32.** (Números infinitos e números infinitesimais) Um número hiperreal não negativo $a \in {}^*\mathbb{R}$ é dito infinitesimal se $a \leq_{\mathscr{U}} n$ para todo $n \in {}^\sigma\mathbb{N}$, e é dito infinito se $n \leq_{\mathscr{U}} a$ para todo $n \in {}^\sigma\mathbb{N}$.

Quanto à existência de números infinitos e números infinitesimais:

Seja ω um número hiperreal definido por $\omega_n = n$ e, seja j qualquer número natural standard $j \in {}^\sigma\mathbb{N}$. Então, $\omega_n \leq j$ para todo $n \leq j$ e, $\omega \geq j$ para todo $n > j$. Temos então que o conjunto

de índices no qual $n < j$ é finito. Porém, como já visto, qualquer ultrafiltro livre $\mathscr{U}$ precisa conter todos os subconjuntos cofinitos de $\mathbb{N}$, então, $\{n \in \mathbb{N} / \ \omega_n > j\} \in \mathscr{U}$. Portanto, para qualquer número natural standard j, $j \leq_{\mathscr{U}} \omega$, o que faz com que ω seja um número infinito.

Similarmente, vamos considerar o número hiperreal $\dfrac{1}{\omega_n} = \dfrac{1}{n}$. Desta vez, para qualquer número natural standard j, nós sabemos que $\dfrac{1}{\omega_n}$ pode ser maior que j para um número finito de índices o que, como dito acima, significa $\dfrac{1}{\omega} \leq_{\mathscr{U}} j$ para qualquer número natural standard j. Assim, $\dfrac{1}{\omega}$ é um número infinitesimal.

Para finalizar, como o conjunto ${}^*\mathbb{R}$ dos números hiperreais contém números da forma $w > n, \ \forall n \in \mathbb{N}$, dizemos que $\mathbb{N}$ é limitado em ${}^*\mathbb{R}$. Sendo assim, ${}^*\mathbb{R}$ não é arquimediano e, como consequência ${}^*\mathbb{R}$ não é completo.

Existem outras extensões do conjunto dos números reais. Como exemplos temos os números complexos $\mathbb{C}$ e os quaternários $\mathbb{H}$.

Esses dois conjuntos citados não podem ser colocados na reta numérica, como acontece com os hiperreais.

Definimos $\mathbb{C} = \{a + bi; \ a, b \in \mathbb{R}; \ i^2 = -1\}$ uma extensão bidimensional de $\mathbb{R}$ e

$\mathbb{H} = \{a + bi + cj + dk; \ a, b, c, d \in \mathbb{R}; \ i^2 = j^2 = k^2 = ijk = -1\}$ uma extensão num espaço de dimensão 4.

Capítulo 5

Algumas considerações sobre Ensino de Matemática e a Teoria dos conjuntos

O ensino de matemática, hoje, possui características bem diferentes de outras épocas. O aluno que já teve uma posição passiva em relação à aprendizagem passa a protagonizar a construção do próprio conhecimento, e o professor inicia um papel de organizador dessa aprendizagem. Além disso, a construção do conhecimento deixa de ser linear. Essa linearidade, segundo Celia Maria Carolino Pires em seu livro "Currículos de Matemática: da Organização Linear à Ideia de Rede" p.9 - "...conduz a uma prática educativa excessivamente fechada, em que há pouco espaço para a criatividade, para a utilização de estratégias metodológicas como a resolução de problemas, para a abordagem interdisciplinar, para o estabelecimento de relações entre os diferentes campos matemáticos, enfim, para a consecução de metas colocadas para o ensino de Matemática pelas recentes propostas curriculares".

A partir de então essa construção de conhecimento passa a acontecer como em uma rede. Dessa maneira, é possível que haja vários assuntos ligados entre si dentro da própria matemática e interdisciplinarmente. Esse novo modelo de construir conhecimento pode ser "...comparável a uma espécie de tabuleiro de xadrez, em que peões possuem igual poder de direito, mas cujo verdadeiro poder varia segundo sua situação recíproca, num dado momento" (Celia Maria Carolino Pires em "Currículos de Matemática: da Organização Linear à Ideia de Rede" p.116).

Essas e outras mudanças tiveram início a partir dos anos 80, quando um novo paradigma de Educação começou a ser discutido em nível mundial. A Matemática Moderna até então vigente não satisfazia aos anseios de uma sociedade que "... parece começar a tomar consciência da iminência do desastre planetário, da explosão demográfica, da redução dos recursos naturais" (Pires C. M. C. - p. 35).

Nosso interesse nesse capítulo é analisar como inserir o assunto "Construção de conjunto numéricos" e assuntos ligados a esse tema em sala de aula de maneira interessante e valiosa. Para isso, devemos nos deixar guiar pelas tendências atuais da Educação e pelas sugestões de seus estudiosos.

É claro que não podemos, na escola básica, discutir na íntegra a construção dos reais ou a teoria dos hiperreais, porém, podemos fazer com que nossos alunos tenham uma ideia de como *Dedekind* pensou, do que é uma relação de equivalência ou de como mostrar que existem mais números além dos racionais. Além disso, é possível ligar esses assuntos a diversos outros, de modo que no final do processo de aprendizagem o aluno tenha conseguido fazer diversas conexões importantes e úteis.

Para chegarmos aos nossos objetivos, precisamos ter em mente o que dizem os PCN (Parâmetros Curriculares Nacionais). De acordo com eles, o conjunto dos números reais, na íntegra, só aparece no contexto escolar a partir do 9o ano, quando o aluno já conhece seus subconjuntos numéricos (números naturais, inteiros e racionais) e sabe operar com os elementos desses últimos. A partir de então a ideia do contínuo começa a ser discutida. Embora o aluno ainda não tenha noção da abrangência das informações às quais passa a ter acesso, começam a surgir indagações mais complexas com relação ao resultado de equações, localização de determinados números na reta, densidade do conjunto dos números racionais, a origem do número "pi" entre outras. Cada uma dessas perguntas pode ser o início de um caminho para o aprendizado, que vai se tornar mais sólido quando o aluno ingressa no Ensino Médio e necessita utilizar o novo conjunto numérico nos demais contextos matemáticos ou de outras disciplinas.

Nesse modelo de aprendizado, no contexto atual, onde o aluno se torna protagonista da aprendizagem, o trabalho do professor tem extrema relevância, segundo o texto que segue dos Parâmetros Curriculares Nacionais: "Numa perspectiva de trabalho em que se considere a criança como protagonista da construção de sua aprendizagem, o papel do professor ganha novas dimensões. Uma faceta desse papel é a de organizador da aprendizagem; para desempenhá-la, além de conhecer as condições socioculturais, expectativas e competência cognitiva dos alunos, precisará escolher o(s) problema(s) que possibilita(m) a construção de conceitos/procedimentos e alimentar o processo de resolução, sempre tendo em vista os objetivos a que se propõe atingir." (PCN – Ensino Fundamental).

Ao focar o ensino dos números reais, o professor deverá, inicialmente, ter em mente os principais objetivos a serem atingidos. Segundo o PCN do quarto ciclo do Ensino Fundamental (no qual está inserido o 9o ano) esses objetivos são: "Neste ciclo, o ensino de Matemática deve visar ao desenvolvimento: Do pensamento numérico, por meio da exploração de situações de aprendizagem que levem o aluno a:

- ampliar e consolidar os significados dos números racionais a partir dos diferentes usos em contextos sociais e matemáticos e reconhecer que existem números que não são racionais;
- resolver situações-problema envolvendo números naturais, inteiros, racionais e irracionais, ampliando e consolidando os significados da adição, subtração, multiplicação, divisão, potenciação e radiciação;
- selecionar e utilizar diferentes procedimentos de cálculo com números naturais, inteiros, racionais e irracionais."

Já no Ensino Médio podemos destacar uma certa diferença dos objetivos vimos acima (vide PCN – Ensino Médio – p. 42):

As finalidades do ensino de Matemática no nível médio indicam como objetivos levar o aluno a:

- compreender os conceitos, procedimentos e estratégias matemáticas que permitam a ele desenvolver estudos posteriores e adquirir uma formação científica geral;
- aplicar seus conhecimentos matemáticos a situações diversas, utilizando-os na interpretação da ciência, na atividade tecnológica e nas atividades cotidianas;
- analisar e valorizar informações provenientes de diferentes fontes, utilizando ferramentas matemáticas para formar uma opinião própria que lhe permita expressar-se criticamente sobre problemas da Matemática, das outras áreas do conhecimento e da atualidade;
- desenvolver as capacidades de raciocínio e resolução de problemas, de comunicação, bem como o espírito crítico e criativo;
- utilizar com confiança procedimentos de resolução de problemas para desenvolver a compreensão dos conceitos matemáticos;
- expressar-se oral, escrita e graficamente em situações matemáticas e valorizar a precisão da linguagem e as demonstrações em Matemática;
- estabelecer conexões entre diferentes temas matemáticos e entre esses temas e o conhecimento de outras áreas do currículo;
- reconhecer representações equivalentes de um mesmo conceito, relacionando procedimentos associados às diferentes representações;
- promover a realização pessoal mediante o sentimento de segurança em relação às suas capacidades matemáticas, o desenvolvimento de atitudes de autonomia e cooperação.

A partir desses objetivos é possível traçar um caminho para a aprendizagem dos números, utilizando estratégias para instigar a curiosidade dos alunos e a pesquisa. Nesse sentido, o recurso à História da Matemática e às Tecnologias da Comunicação como indicados no PCN podem tornar os objetivos mais facilmente conquistados.

No caso do apelo à História da Matemática não é suficiente apenas preencher as aulas com fragmentos da mesma. À luz do PCN, vemos que "...essa abordagem não deve ser entendida simplesmente que o professor deva situar no tempo e no espaço cada item do programa de Matemática ou contar sempre em suas aulas trechos da história da Matemática, mas que a encare como um recurso didático com muitas possibilidades para desenvolver diversos conceitos, sem reduzi-la a fatos, data e

nomes a serem memorizados" (PCN, 1998 – p.43). Sendo assim, torna-se interessante posicionar a História da Matemática como motivadora para o estudo da Matemática. No caso da introdução aos números reais, pode-se utilizar como motivação à pergunta inicial que deu origem à construção dos números reais.

Além disso, de acordo com o PCN, "A História da Matemática pode oferecer uma importante contribuição ao processo ensino e aprendizagem dessa área do conhecimento. Ao revelar a Matemática como uma criação humana, ao mostrar necessidades e preocupações de diferentes culturas, em diferentes momentos históricos, ao estabelecer comparações entre os conceitos e processos matemáticos do passado e do presente, o professor cria condições para que o aluno desenvolva atitudes e valores mais favoráveis diante desse conhecimento" (PCN – Ensino Fundamental, 1998 – p.42).

Na próxima seção foram reunidas 3 atividades que utilizam, de forma básica, alguns dos assuntos estudados nesta dissertação. A 1ª atividade permite que o aluno reveja como são os números racionais e suas representações e conclua que o número $\sqrt{2}$ não pertence a esse conjunto. Além disso, é possível visualizar esse número geometricamente como a diagonal de um quadrado de lado 1 e localizá-lo na reta real.

A 2ª atividade trabalha o conceito de números decimais e permite que aluno entenda a ideia de densidade de um conjunto numérico. Além disso, ele relembra o conceito de média e seu significado. A identificação de número irracional com algumas raízes, logaritmos e funções trigonométricas que não tem resolução fácil e com as quais o aluno passa a identificar um número irracional, deixa de ser a fonte mais importante de obtenção de um número que não pertence a $\mathbb{Q}$, possibilitando a associação de I com um conjunto infinito e que, comparado ao conjunto dos números racionais pode ser até maior.

A 3ª atividade aborda polígonos inscritos e circunscritos e os cálculos de área e perímetro. É uma atividade com muitas contas, o que pode causar algum embaraço no Ensino Médio, porém, ela introduz a ideia básica de limite. Nessa atividade são necessários bons conhecimentos de geometria plana e trigonometria para uma boa visualização dos resultados.

5.1 Atividades

Atividade 1: Alguns exemplos de números irracionais.

A primeira atividade proposta está vinculada à ideia de existência de números não racionais, e poderá ser aplicada a estudantes do 9º ano do Ensino Fundamental, momento em que os alunos estarão prontos para descobrir o conjunto dos números reais e sua representação através da reta numérica. A proposta dessa atividade começa com o lançamento da seguinte pergunta:

"Existe um número racional cujo quadrado seja igual a 2?"

Para responder a essa pergunta, primeiro precisamos lembrar como é um número racional e quais são as representações desse tipo de número. Os elementos do conjunto dos números racionais são números que podem ser representados na forma de fração, e isso inclui: os números inteiros, os números decimais finitos e os decimais infinitos e periódicos (também chamados de dízimas periódicas).

- Os números inteiros podem ser representados como frações de denominador 1.

  ***Exemplo* 31.**

  $2 = \frac{2}{1}$;

  $-5 = \frac{-5}{1}$;

  $30 = \frac{30}{1}$

- Os decimais finitos podem ser representados como frações decimais, considerando-se o número de casas depois da vírgula.

  ***Exemplo* 32.**

  $3,7 = \frac{37}{10}$;

  $15,67 = \frac{1567}{100}$;

  $0,003 = \frac{3}{1000}$

- As dízimas periódicas podem ser representadas como frações da seguinte forma:

  ***Exemplo* 33.**

  $1,444\cdots = \frac{13}{9}$;

  $0,002323\cdots = \frac{23}{9900}$;

  $3,1222\cdots = \frac{281}{90}$

Obs.: Para encontrarmos a fração que gera a dízima periódica (fração geratriz) podemos proceder da seguinte forma:

Considere

$$1,444\cdots = x \qquad (1)$$

Multiplicando ambos os lados da equação por 10 ficamos com:

$$10 \cdot 1,444\cdots = 10 \cdot x$$
$$\Rightarrow\ 14,444\cdots = 10 \cdot x \qquad (2)$$

Subtraindo a equação (1) da equação (2), ficamos com:

$$14,444\cdots - 1,444\cdots = 10 \cdot x - x$$
$$\Rightarrow 13 = 9 \cdot x$$
$$= x = \frac{13}{9}$$

Para encontrar outras frações geratrizes utiliza-se um raciocínio análogo.

Tendo uma boa noção de como representar um número racional, podemos então voltar à nossa pergunta inicial: **"Existe um número racional cujo quadrado seja igual a 2?"**

Para chegar a uma resposta adequada a essa pergunta podemos inicialmente sugerir os cálculos de alguns números ao quadrado que poderiam ter respostas próximas de 2. Para isso precisamos de um intervalo no qual tal número se encaixe. Se x representa nosso número, $1 < x < 2$ pois, nesse caso, $1^2 < x^2 < 2^2$:

$$1,0^2 = 1,0$$
$$1,1^2 = 1,21$$
$$1,2^2 = 1,44$$
$$1,3^2 = 1,69$$
$$1,4^2 = 1,96$$
$$1,5^2 = 2,25$$

Neste ponto, não conseguimos chegar a uma resposta, porém, conseguimos identificar um intervalo menor onde tal número pode ser encontrado: $1,4 < x < 1,5$. Tentando melhorar a estimativa de x, podemos calcular:

$$1,41^2 = 1,9881$$
$$1,42^2 = 2,0164$$

É claro que podemos continuar aumentando o número de casas decimais a fim de chegarmos tão próximo quanto queiramos do número 2, mas o valor exato, de fato, nunca será atingido, independente do número de casas decimais que x possa ter.

Por meio de uma demonstração simples podemos chegar à conclusão de que não existe uma fração que represente tal valor de x, o que implica na irracionalidade do número em questão. Como todo número racional pode ser escrito na forma de uma fração $\frac{p}{q}$ com p um número inteiro e q um natural não nulo, considere então que exista um número dessa forma cujo quadrado seja igual a 2. Assim, mostraremos através de um absurdo que o número cujo quadrado é 2 não é racional, sendo

portanto um número irracional:

Seja $\frac{p}{q}$ o número tal que $\left(\frac{p}{q}\right)^2 = 2$.

Assim, temos $\left(\frac{p}{q}\right)^2 = 2 \Rightarrow \frac{p^2}{q^2} = 2 \Rightarrow p^2 = 2 \cdot q^2$.

Observemos que, no 1^o membro temos o quadrado de um número natural. Assim, no segundo membro deveríamos ter um número cujos fatores primos aparecessem um número par de vezes. Porém, o número $2 \cdot q^2$ tem o fator 2 aparecendo um número ímpar de vezes, o que torna a igualdade absurda e, consequentemente a nossa suposição também absurda, o que implica na não racionalidade de x.

Pelas possíveis representações de um número racional que envolvem fração, decimal exato e dízimas periódicas, podemos concluir que os números não racionais na forma decimal são números com a representação decimal infinita e não periódica.

Mas, mesmo o número apresentado não sendo racional, é possível visualizar sua dimensão comparando-o com outros números ou localizá-lo numa reta numérica?

Para responder a essas perguntas entraremos no domínio da geometria, calculando a diagonal de um quadrado de lado 1.

Considere uma linha graduada (que não precisa necessariamente utilizar alguma unidade de comprimento conhecida), como a linha dada abaixo:

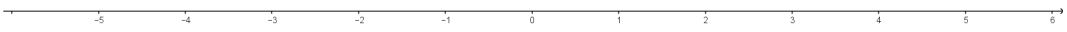

Figura 5.1: Régua graduada

Repousemos sobre essa linha o lado de um quadrado de lado 1 unidade, posicionando-o entre os pontos 0 e 1 da reta, como abaixo:

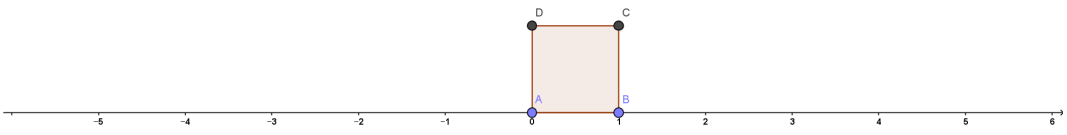

Figura 5.2: Quadrado de lado 1

Agora, com um compasso com a ponta seca em A, medimos o comprimento da diagonal $\overline{AC}$, e transportamos essa medida para o eixo x anotando o ponto E:

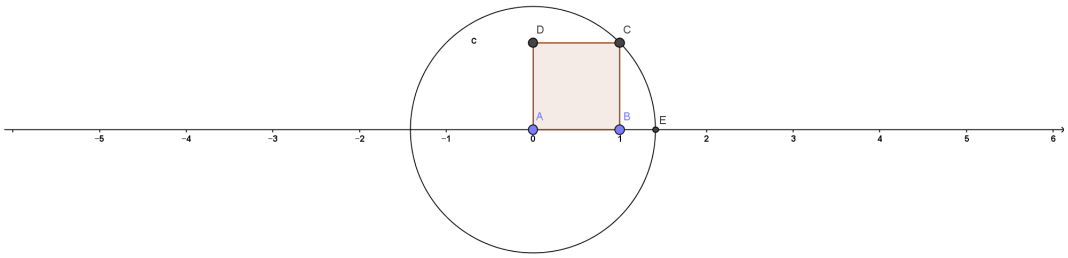

Figura 5.3: Diagonal do quadrado

A diagonal do quadrado é também a distância entre os pontos A e E. Pelo Teorema de Pitágoras calculamos a diagonal d do quadrado de lado 1:

$$d^2 = 1^2 + 1^2$$
$$d^2 = 2$$
$$d = \sqrt{2}$$

Assim, chegamos a um resultado numérico que tem uma representação geométrica na reta, porém ainda não sabemos quanto é, exatamente $\sqrt{2}$, apesar de conseguirmos um segmento de reta com a sua medida exata.

Essa atividade pode ser proposta com outras raízes havendo a necessidade de adaptação das figuras escolhidas na representação geométrica.

Observemos que a construção de outras raízes quadradas de números inteiros pode ser feita observando-se os passos da construção a seguir. Para isso, considere a construção do número $\sqrt{a}$, com $a \in \mathbb{Z}$.

1º passo: Considere um segmento AB de comprimento a.

2º passo: Prolongue o segmento AB até o ponto C de modo que BC seja um segmento unitário $(u = 1)$.

3º passo: Trace a circunferência de diâmetro AC.

4º passo: Trace um segmento de reta perpendicular ao diâmetro AC, pelo ponto B encontrando a circunferência no ponto E.

5º passo: O segmento BE tem medida $\sqrt{a}$.

6º passo: Transportar o segmento de reta de medida $\sqrt{a}$ para uma reta graduada com segmento unitário igual a u.

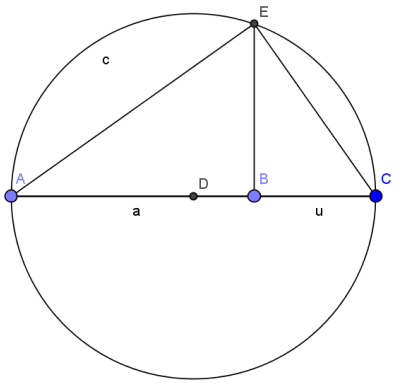

Figura 5.4: Representação de $\sqrt{a}$

Esqueleto da atividade 1:

- Iniciar com a pergunta: Existe um número racional cujo quadrado seja igual a 2?
- Relembrar o que é um número racional e quais são as suas representações. Relembrar como passar de uma representação para outra;
- Calcular alguns números ao quadrado que podem se aproximar do número que se quer encontrar;
- Admitir a inexistência de algum número x que ao quadrado dê 2;
- Provar, que é impossível encontrar uma fração cujo quadrado seja 2 e concluir que esse número não pode ser racional;
- Mostrar que apesar de não sabermos exatamente que número é esse, é possível representa-lo numa reta graduada, localizando-o entre 1 e 2;
- Encontrar outros números que tenham a mesma propriedade (não podem ser representados por frações, mas podem ser representados numa reta graduada numa posição exata).

Atividade 2: Verificação de que o conjunto dos números racionais é denso em $\mathbb{R}$.

A ideia da densidade do conjunto dos números racionais no conjunto dos números reais pode ser explicada simplificadamente pelo fato de encontrarmos números racionais em qualquer intervalo de números reais, por menor que ele seja. Para facilitar, tomemos o intervalo $(0, 1)$ da reta real. A densidade dos números racionais será feita em etapas.

- 1ª etapa: Existem infinitos números racionais entre dois números racionais.

  Num primeiro momento tomemos dois números racionais, por exemplo, os números $\frac{1}{4}$ e $\frac{1}{2}$.

  Ambos os números escolhidos pertencem ao intervalo $(0, 1)$ e, claramente $\frac{1}{4} < \frac{1}{2} = \frac{2}{4}$.

  O número gerado pela média aritmética de $\frac{1}{4}$ e $\frac{1}{2}$ é o número $\frac{\frac{1}{4} + \frac{1}{2}}{2} = \frac{\frac{3}{4}}{2} = \frac{3}{8}$, que também pertence ao intervalo $(0, 1)$ e está entre $\frac{1}{4}$ e $\frac{1}{2}$. De fato, $\frac{1}{4} = \frac{2}{8} < \frac{3}{8} < \frac{1}{2} = \frac{4}{8}$. Ampliando este primeiro item, podemos pegar os números $\frac{1}{4}$ e $\frac{3}{8}$ e e calcular a média aritmética entre eles.

  Obteremos o número $\frac{\frac{1}{4} + \frac{3}{8}}{2} = \frac{\frac{5}{8}}{2} = \frac{5}{16}$. Que está entre $\frac{1}{4}$ e $\frac{3}{8}$ $\left(\frac{1}{4} = \frac{4}{16} < \frac{5}{16} < \frac{3}{8} = \frac{6}{16}\right)$.

  Podemos encontrar a média aritmética de dois números no intervalo em questão quantas vezes forem necessárias. O resultado encontrado será sempre um número racional do intervalo. Constatamos então que existem infinitos números racionais entre dois números racionais quaisquer.

- 2ª etapa: Existem infinitos números racionais entre dois números irracionais.

  Mas como são os números irracionais? Na escola básica os estudantes estão muito acostumados a classificar como números irracionais algumas raízes, alguns logaritmos e algumas funções trigonométricas. Como exemplos, temos: $\sqrt{5}$, $\sqrt[3]{2}$, $\sqrt[3]{15}$, $\log_2 3$ e $sen\ 60^0$, o que sugere que o conjunto dos números irracionais pode ser um conjunto menor que o conjunto dos números racionais. Como os números citados são um pouco difíceis de dimensionar, vamos procurar números irracionais na forma decimal. Que "cara" esses números possuem? Como observado na atividade 1, os números decimais irracionais tem uma representação decimal infinita e não periódica. Assim, não existe um período de repetição de números nos números irracionais. Alguns exemplos de irracionais são: $0,123456789101112\cdots$ ou $0,122333444455555\cdots$, entre infinitos outros.

  Para nossa verificação de que entre dois números irracionais podemos encontrar infinitos números racionais, tomemos os irracionais $0,1234567891011\cdots$ e $0,1234577891011\cdots$.

  Temos $0,1234567891011\cdots < 0,1234577891011\cdots$ e, ambos pertencem ao intervalo $(0, 1)$.

Para encontrarmos um número entre esses dois observemos:

a) a mudança na parte decimal que leva um dos números a ser maior que o outro ocorre na 6ª casa decimal, e

b) na atividade 1 vimos que as dízimas periódicas são também exemplos de números racionais.

Assim, a construção de um número racional entre $0,1234567891011\cdots$ e $0,1234577891011\cdots$ pode ser feita considerando-se as duas observações acima e pode ser dado por $0,1234568888888\cdots$ Outros exemplos de números racionais entre $0,1234567891011\cdots$ e $0,1234577891011\cdots$ são $0,12345689999999\cdots$, $0,12345691111111\cdots$, $0,1234569121212\cdots$, entre outros. Se escolhermos outros dois números irracionais podemos utilizar a mesma ideia e encontrar outros números racionais, o que nos leva a concluir que entre dois números irracionais existem infinitos números racionais.

Concluímos, então, que entre quaisquer números reais podemos encontrar infinitos números racionais. O que fizemos nesta atividade não foi uma demonstração, mas uma verificação de que, em cada espaço muito pequeno da reta real é possível encontrar números racionais, o que é o princípio da densidade deste último conjunto em $\mathbb{R}$.

Para finalizar e fixar as ideias, vamos buscar mais números racionais em intervalos de números da reta numérica, considerando novamente o intervalo $(0,1)$. Por exemplo, considerando o trio de números $0,1234$ (decimal finito), $0,123444444\cdots$ (decimal infinito e periódico) e $0,12345678910\cdots$ (decimal infinito e não periódico). Temos nessa sequência de três números a seguinte ordem: $0,1234 < 0,123444\cdots < 0,12345678910\cdots$. Será possível encontrar dois números racionais x e y tais que $0,123 < x < 0,123444\cdots$ e $0,123444\cdots < y < 0,12345678910\cdots$?

Vimos nesta atividade que entre quaisquer dois números reais podemos encontrar infinitos números racionais. De fato, x pode ser o número $0,1234111\cdots$ e y pode ser o número $0,1234555\cdots$, pois, nesse caso $0,1234 < 0,1234111\cdots < 0,123444\cdots$ e, $0,123444\cdots < 0,1234555\cdots < 0,12345678910\cdots$.

Concluímos então que o conjunto dos números racionais é denso em $\mathbb{R}$, ou seja, os números racionais estão por toda a parte. Quanto aos números irracionais, será que isso também acontece?

Esqueleto da atividade 2:

- Explicar o que é um conjunto denso em matemática;
- Estimular os alunos a encontrarem dois números racionais (nesse momento representados por decimais exatos) e calcular a média entre esses números;
- Recalcular mais duas médias, entre cada número do intervalo principal e a média calculada acima;
- Ajudar os alunos a raciocinarem que é possível fazer isso infinitamente, obtendo números com a parte decimal cada vez mais extensa;

- Pedir aos alunos que pensem como seria um número irracional representado por um número decimal;
- Estimulá-los a dar mais de um exemplo de irracionais e propor encontrar um número racional entre eles lembrando-se de como é um número racional;
- Propor encontrar outros números racionais entre os limites irracionais do intervalo dado acima e o número racional encontrado;
- Concluir a proposta inicial da densidade de $\mathbb{Q}$ em $\mathbb{R}$.

Atividade 3: Calculando com infinito e infinitesimais.

A ideia desta atividade é calcular a área de um círculo sem utilizar as fórmulas usuais, aproximando-a das áreas de polígonos inscritos e circunscritos cujos números de lados são sucessivamente duplicados. Arquimedes utilizou um processo semelhante para aproximar a razão entre o comprimento da circunferência e o diâmetro do círculo, razão conhecida como π.

Para facilitar, trabalharemos em duas etapas: a 1ª etapa corresponde ao cálculo das áreas de polígonos inscritos e a 2ª etapa corresponde aos cálculos das áreas e dos perímetros de polígonos circunscritos.

- 1ª etapa: Inscrição de polígonos numa circunferência de raio r.

  Considere a circunferência C de centro A e raio r dada abaixo:

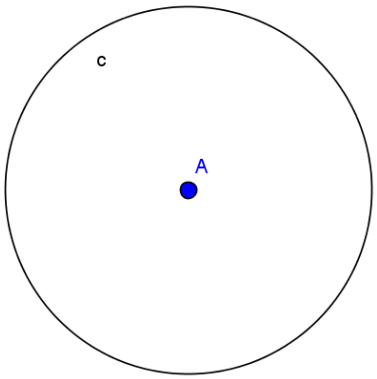

Figura 5.5: Círculo de raio r

Agora vamos inscrever um quadrado nessa circunferência:

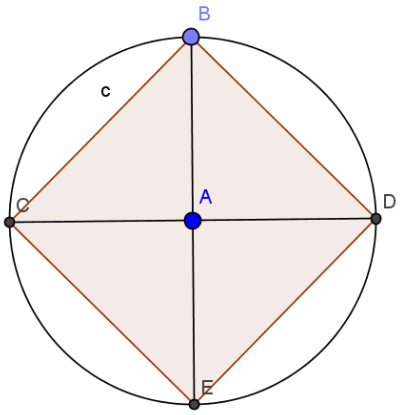

Figura 5.6: Quadrado inscrito

Para calcular a área do quadrado inscrito A_4 primeiramente devemos observar que, sendo o raio do círculo r, temos que a diagonal do quadrado tem valor 2r e, considerando o lado desse quadrado como l_4, temos, pelo teorema de Pitágoras:

$$(l_4)^2 + (l_4)^2 = (2 \cdot r)^2 \Rightarrow\ 2 \cdot (l_4)^2 = 4 \cdot r^2 \Rightarrow\ (l_4)^2 = 2 \cdot r^2$$

Assim, $A_4 = (l_4)^2 = 2 \cdot r^2$ e $l_4 = r\sqrt{2}$.

O próximo polígono a ser inscrito na circunferência será o octógono (8 lados):

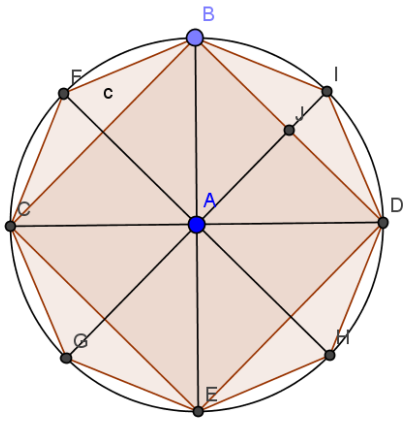

Figura 5.7: Octógono inscrito

Para calcular a área desse polígono e o comprimento de seu lado l_8, consideremos a figura abaixo:

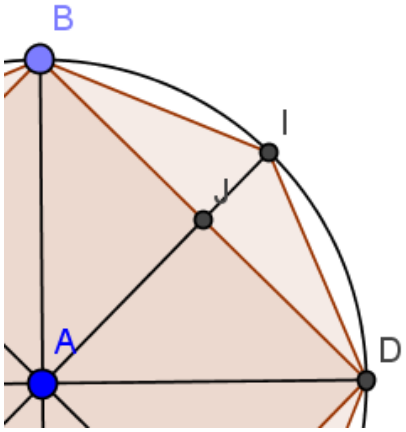

Figura 5.8: Zoom no octógono inscrito

Observe que o lado do octógono será o comprimento do segmento BI e será representado por l_8. Para calculá-lo utilizaremos a lei dos cossenos no triângulo AIB, já que o ângulo A nesse triângulo corresponde a $\frac{1}{8}$ de uma volta completa, isto é, 45º:

$$(\overline{BI})^2 = r^2 + r^2 - 2 \cdot r^2 \cdot \cos 45^o \Rightarrow (\overline{BI})^2 = 2 \cdot r^2 - 2 \cdot r^2 \cdot \frac{\sqrt{2}}{2}$$

$$\Rightarrow \overline{BI}^2 = 2 \cdot r^2 - r^2\sqrt{2} \Rightarrow l_8 = r \cdot \sqrt{2 - \sqrt{2}}$$

Para o cálculo da área do octógono observe que a área do triângulo ABI corresponde a $\frac{1}{8}$ da área do octógono, que será denotada por A_8. Temos então $A_8 = 8 \cdot \frac{r^2}{2} \cdot \frac{\sqrt{2}}{2} = 2 \cdot r^2\sqrt{2}$.

Temos então $A_8 = 2 \cdot r^2 \cdot \sqrt{2}$ e $l_8 = r \cdot \sqrt{2 - \sqrt{2}}$.

Para finalizar a 1ª etapa vamos dobrar o número de lados do octógono, obtendo um hexadecágono inscrito, isto é, um polígono de 16 lados:

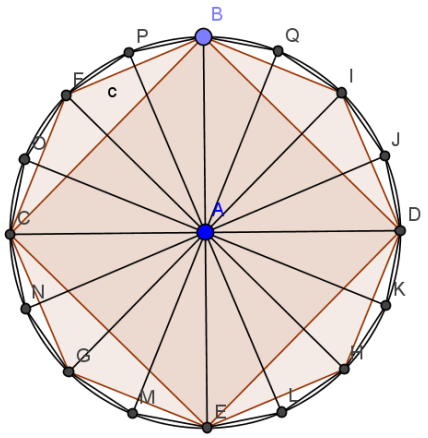

Figura 5.9: Hexadecágono inscrito

Calcularemos para o polígono de 16 lados novamente o comprimento de seu lado l_{16} e o valor de sua área A_{16}. Para isso, considere a figura abaixo com o triângulo BAQ destacado:

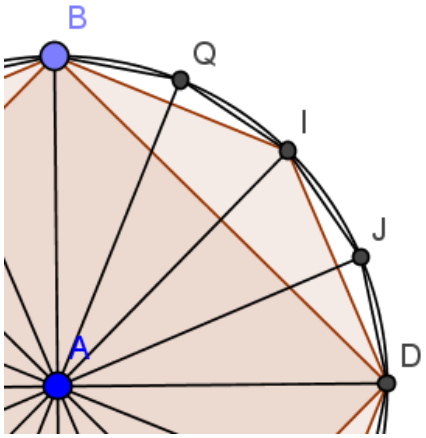

Figura 5.10: Zoom no hexadecágono inscrito

O comprimento do lado o hexadecágono será calculado pela lei dos cossenos aplicada ao triângulo BAQ. Nesse caso o ângulo a ser considerado terá valor $\frac{1}{16} \cdot 360^o = 22,5^o$. Temos então:

$$(l_{16})^2 = r^2 + r^2 - 2 \cdot r^2 \cdot \cos 22,5^o = 2 \cdot r^2 - 2 \cdot r^2 \cdot \frac{\sqrt{2+\sqrt{2}}}{2}$$

$$l_{16} = r \cdot \sqrt{2 - \sqrt{2+\sqrt{2}}}$$

A área do hexadecágono A_{16} é equivalente a 16 vezes a área do triângulo BAQ. Assim, temos: $A_{16} = 16 \cdot \dfrac{r^2 \cdot \ sen\ 22,5^o}{2} = 8 \cdot r^2 \cdot \dfrac{\sqrt{2-\sqrt{2}}}{2} = 4 \cdot r^2\sqrt{2-\sqrt{2}}.$

Comparando os lados das figuras obtidas e suas áreas, temos:

	Número de lados n	Lado l	Área A
Quadrado	4	$l_4 = r \cdot \sqrt{2}$	$A_4 = 2 \cdot r^2$
Octógono	8	$l_8 = r \cdot \sqrt{2-\sqrt{2}}$	$A_8 = 2 \cdot r^2\sqrt{2}$
Hexadecágono	16	$l_{16} = r \cdot \sqrt{2-\sqrt{2+\sqrt{2}}}$	$A_{16} = 4 \cdot r^2\sqrt{2-\sqrt{2}}$

Pode-se observar que, com o aumento do número de lados do polígono inscrito há uma diminuição do tamanho do lado de cada polígono e um aumento do tamanho da área do polígono, que se aproxima cada vez mais do valor da área do círculo, por valores menores do que o valor real. A partir dessa constatação, podemos responder à seguinte pergunta: O que acontecerá se aumentarmos *infinitamente* o número de lados do polígono? Nesse caso, o tamanho do lado diminuirá *infinitamente* tendendo a um *infinitésimo* e o valor da área do polígono estará *infinitamente* próximo da área real do círculo. Vejamos um exemplo numérico, com $r = 1$ para os casos estudados acima:

	Número de lados n	Lado l	Área A
Quadrado	4	$l_4 = \sqrt{2}$	$A_4 = 2$
Octógono	8	$l_8 = \sqrt{2 - \sqrt{2}}$	$A_8 = 2 \cdot \sqrt{2}$
Hexadecágono	16	$l_{16} = \sqrt{2 - \sqrt{2 + \sqrt{2}}}$	$A_{16} = 4 \cdot \sqrt{2 - \sqrt{2}}$

Lembrando que o cálculo da área do círculo pode ser feito através da fórmula $A_o = \pi \cdot r^2$, para o caso $r = 1$ temos $A_o = \pi$. O número π é um número irracional cujo valor pode ser aproximado por 3,14. Aproximando $\sqrt{2}$ pelo número $1,41$, temos que as áreas do quadrado, octógono e hexadecágono são, respectivamente, $2;\ 2,83;\ 3,06$; o que confirma uma aproximação que tende para o número 3,14 por falta. No caso do comprimento da circunferência, que pode ser calculada pela fórmula $C = 2 \cdot \pi \cdot r$, caso $r = 1$ teremos $C = 2 \cdot \pi$ que se aproxima muito do número $6,28$. Utilizando as fórmulas encontradas acima para os comprimentos dos lados dos polígonos de 4, 8 e 16 lados, formamos uma sequência de perímetros que se aproxima do comprimento da circunferência também por falta, já que os perímetros são: $5,66;\ 6,12;\ 6,24$, confirmando uma sequência que tende para valor real de $2 \cdot \pi$.

- 2ª etapa: Circunscrição de polígonos numa circunferência de raio r.

  Considerando a mesma circunferência utilizada na 1ª etapa, observe o quadrado circunscrito:

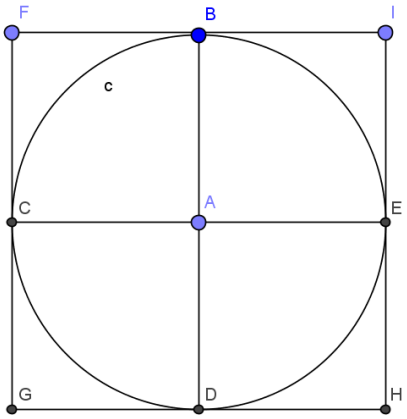

Figura 5.11: Quadrado circunscrito

O lado L_4 do quadrado circunscrito tem medida $L_4 = 2 \cdot r$. A sua área será dada por $S_4 = (2 \cdot r)^2 = 4 \cdot r^2$. Dobrando o número de lados do polígono ficamos com o octógono, com 8 lados:

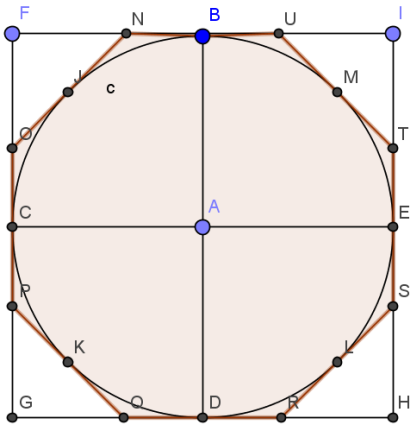

Figura 5.12: Octógono circunscrito

Observemos na figura abaixo, o cálculo do lado e da área do octógono:

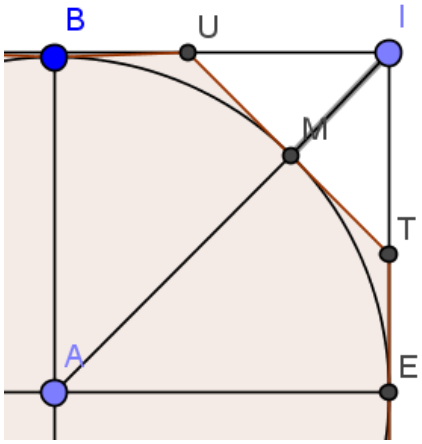

Figura 5.13: Zoom no octógono circunscrito

O lado do octógono L_8 pode ser identificado pelo segmento de reta $\overline{NU}$. Assim, $\overline{BU} = \dfrac{L_8}{2}$. O segmento $\overline{MU}$ tem a mesma medida de $\overline{BU}$ pois U é um ponto externo pelo qual passam duas retas tangentes à circunferência. Além disso, analisando o triângulo IMU vemos que o ângulo $M\hat{U}I$ tem medida $45°$ pois $\overline{IA}$ divide o ângulo I de $90°$ ao meio e $U\hat{M}I$ é $90°$. Podemos então dizer que $\dfrac{L_8}{2}$ = metade da diagonal do quadrado $-r$, isto é, $\dfrac{L_8}{2} = r \cdot \sqrt{2} - r$, o que implica em $L_8 = 2 \cdot r \cdot (\sqrt{2} - 1)$. Já a área S_8 do octógono poderá ser calculada multiplicando-se por 8 a área do triângulo AUT. Concluímos então que $S_8 = 8 \cdot \dfrac{r \cdot 2 \cdot r \cdot (\sqrt{2} - 1)}{2} = 8 \cdot r^2 \cdot (\sqrt{2} - 1)$. Temos então, $L_8 = 2 \cdot r \cdot (\sqrt{2} - 1)$ e $S_8 = 8 \cdot r^2 \cdot (\sqrt{2} - 1)$.

Para finalizar os cálculos desta 2ª etapa, observe o hexadecágono circunscrito:

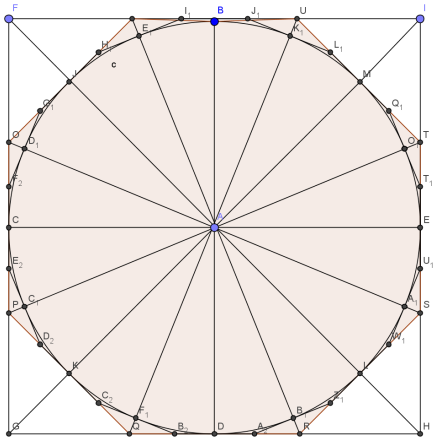

Figura 5.14: Hexadecágono circunscrito

Vamos ampliar um pedaço do desenho acima:

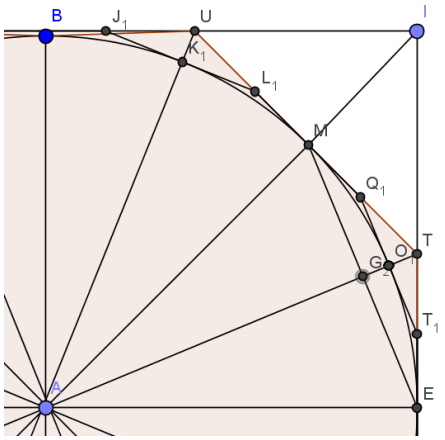

Figura 5.15: Zoom no hexadecágono circunscrito

No triângulo AML_1, temos $M\hat{A}L_1 = 11,25°$ (pois $M\hat{A}L_1 = \dfrac{1}{32}$ de $360°$).

Como $tg\ 11,25° = (2+\sqrt{2}) \cdot \sqrt{2-\sqrt{2}} - (1+\sqrt{2})$ e $tg\ 11,25° = \dfrac{\frac{L_{16}}{2}}{r}$, temos

$$\frac{L_{16}}{2 \cdot r} = (2+\sqrt{2}) \cdot \sqrt{2-\sqrt{2}} - (1+\sqrt{2}) \Rightarrow L_{16} = 2 \cdot r \cdot ((2+\sqrt{2}) \cdot \sqrt{2-\sqrt{2}} - (1+\sqrt{2})).$$

Já o cálculo da área do hexadecágono circunscrito pode ser feito multiplicando-se a área do triângulo L_1AQ_1, por 16.

$$S_{16} = 16 \cdot \frac{L_{16} \cdot r}{2} = 8 \cdot L_{16} \cdot r = 8r \cdot 2r((2+\sqrt{2}) \cdot \sqrt{2-\sqrt{2}} - (1+\sqrt{2}))$$
$$\Rightarrow S_{16} = 16r^2[(2+\sqrt{2})] \cdot \sqrt{2-\sqrt{2}} - (1+\sqrt{2})].$$

Comparando os lados dos polígonos circunscritos e suas áreas ficamos com:

	n	Lado l	Área S
Quadrado	4	$L_4 = 2 \cdot r$	$S_4 = 4 \cdot r^2$
Octógono	8	$L_8 = 2 \cdot r \cdot (\sqrt{2} - 1)$	$S_8 = 8 \cdot r^2(\sqrt{2} - 1)$
Hexadecágono	16	$L_{16} = 2 \cdot r \cdot [(2 + \sqrt{2}) \cdot \sqrt{2 - \sqrt{2}} - (1 + \sqrt{2})]$	$S_{16} = 16 \cdot r^2 \cdot [(2 + \sqrt{2}) \cdot \sqrt{2 - \sqrt{2}} - (1 + \sqrt{2})]$

Novamente com o aumento do número de lados do polígono, a área se aproxima cada vez mais da área do círculo e o perímetro se aproxima cada vez mais do comprimento da circunferência, agora por excesso.

Pensando numa circunferência de raio $r = 1$ ficamos com a tabela:

	n	Lado l	Área A
Quadrado	4	2	4
Octógono	8	$2 \cdot (\sqrt{2} - 1)$	$8 \cdot (\sqrt{2} - 1)$
Hexadecágono	16	$2 \cdot [(2 + \sqrt{2}) \cdot \sqrt{2 - \sqrt{2}} - (1 + \sqrt{2})]$	$16 \cdot [(2 + \sqrt{2}) \cdot \sqrt{2 - \sqrt{2}} - (1 + \sqrt{2})]$

Calculando os perímetros para L_4, L_8 e L_6 temos, respectivamente 8; 6,63; 6,37; a sequência que se aproxima, por excesso, do número 6,28.

Já com relação às áreas, temos, respectivamente para os polígonos de 4,8 e 16 lados a sequência 4; 3,31; 3,18, que se aproxima por excesso do valor 3,14 que é uma boa aproximação para a área do círculo de raio 1.

Assim, se S é a área do círculo de raio 1, $S = \pi$ e

$$A_4 < A_8 < A_{16} < \cdots < S < \cdots < S_{16} < S_8 < S_4$$
$$2 < 2,83 < 3,06 < \cdots < S < \cdots < 3,18 < 3,31 < 4$$

Temos então $3,06 < S = \pi < 3,18$ (essa é a nossa melhor aproximação).

Se C é o comprimento da circunferência de raio 1, $C = 2 \cdot \pi$ e

$$p_4 < p_8 < p_{16} < \cdots < C < \cdots < P_{16} < P_8 < P_4$$
$$5,66 < 6,12 < 6,24 < \cdots < C < \cdots < 6,37 < 6,63 < 8$$

Assim, para o comprimento da circunferência nossa melhor aproximação é $6,24 < C = 2 \cdot \pi < 6,37$.

Observemos também que podemos concluir que $3,06 < \pi < 3,18$, já que π é a área do círculo de raio 1.

Essa 3ª atividade é mais complexa pois para realizá-la é necessário ter bons conhecimentos de geometria plana e trigonometria. Em geral, na escola básica temos poucos alunos que se debruçariam sobre essa atividade.

Esqueleto da atividade 3:

- Falar brevemente sobre polígonos inscritos e circunscritos;
- Estimular os alunos a desenharem os polígonos de 4 e 8 lados inscritos e circunscritos;
- Relembrar conceitos de trigonometria;
- Pedir que os alunos calculem área e lado do quadrado e octógono inscrito e circunscrito;
- Pedir que computem os valores calculados para $r = 1$;
- Incentivá-los a comparar os resultados;
- Fornecer os valores prontos para área e lado do polígono de 16 lados (inscrito e circunscrito) para efeito de comparação;
- Falar sobre a ideia de pegar uma quantidade cada vez maior de lados nos polígonos inscritos e circunscritos e incentivar os alunos a tirarem as próprias conclusões;
- Encerrar a atividade com a aproximação de π.

Referências Bibliográficas

[1] Aguilar, I. e Dias, M. S. *A Construção dos Números Reais e suas Extensões*, apresentado no 4º Colóquio da Região Centro-Oeste em Novembro de 2015

[2] Aragona, J., *Números Reais*, Editora Livraria da Física, São Paulo, 2010.

[3] Berlinghoff, W. P., and Gouvêa, F. Q., *A Matemática através dos tempos: um guia fácil e prático para professores e entusiastas*, Blucher, São Paulo, 2nd edition, 2010.

[4] Boyer, C. B., *História da Matemática*, Editora Edgard Blucher *and* Editora da Universidade de São Paulo, 1974.

[5] Carvalho, T. F. and D'Ottaviano, I. M. L., *Sobre Leibniz, Newton e infinitésimos, das origens do cálculo infinitesimal aos fundamentos do cálculo diferencial paraconsistente*, Educação Matemática Pesquisa, V.08, n.01, 2006, pp. 13-43.

[6] Davis, I., *An Introduction to Non-Standard Analysis*, aug/2009. homepage: http://www.math.uchicago.edu/ may/VIGRE/VIGRE2009/REUPapers/Davis.pdf

[7] Eves, H., *Introdução à História da Matemática*, Campinas: Editora UNICAMP, 4th edition, 2004.

[8] Felizardo, S. B., *Aplicação da Análise Não-Standard à Teoria da Medida: uma Representação Hiperfinita da Medida de Lebesgue*, Dissertação de Mestrado,Universidade Federal do Paraná, 2005.

[9] Gonçalves, A., *Introdução à Álgebra*. Projeto Euclides, Rio de Janeiro: IMPA, 5th edition, 2003.

[10] Hefez, A., *Elementos de Aritmética*, SBM, Rio de Janeiro, 2nd edition, 2011.

[11] Ifrah, G., *Os Números: história de uma grande invenção*, Editora Globo, São Paulo, 4th edition, 1992.

[12] Junior, O. S. *Calculo no Ensino Medio: Numeros Reais*, Mestrado Profissional em Matematica em Rede Nacional, Rio de Janeiro: IMPA, 2014.

[13] O'Neill, K., *An Introduction to Non-Standard Analysis and its Aplplications*, mar, mar/2014. homepage: https://math.berkeley.edu/ jhicks/links/SOTS/koneill030514.pdf

[14] Tatiana, R. and Carvalho, J. B. P., *Tópicos de História da Matemática*, SBM, Rio de Janeiro, 2012.

[15] Rudin, W., *Principles of Mathematical Analysis*, EUA: McGraw-Hill, Inc., 3rd edition, 1976.

[16] Silvia, E. M., *Companion Notes: A Working Excursion to Accompany Baby Rudin*, Berkeley: University of California Press, apr/1999. homepage: https://www.math.ucdavis.edu/ emsilvia/math127/companionnotes.pdf

[17] Parâmetros curriculares nacionais : Matemática *Secretaria de Educação Fundamental*. Brasília: MEC / SEF, 1998. 148 p.

[18] Pires, C.C. *Currículos de Matemática: da organização linear da ideia de rede*, São Paulo: FTD, 2000.

Apêndice A

A construção dos números reais feitas por Cantor.

Nosso objetivo com esta explanação é dar uma ideia básica, sem muitos detalhes de como *Cantor* fez a construção dos números reais trabalhando com sequências de *Cauchy*. Para mais detalhes leia [1].

A ideia de *Cantor* foi pegar sequências de *Cauchy* de números racionais e construir os números reais a partir de seus limites.

Temos nesse caso, por exemplo, sequências como $\left(\frac{1}{1},\ \frac{1}{2},\ \frac{1}{3},\ \frac{1}{4},\ \cdots\right)$ e $(2,\ 2,\ 2,\ \cdots)$ que convergem para os números racionais 0 e 2 respectivamente, mas temos também sequências como $x_n = \left(1+\frac{1}{n}\right)^n$ com termos $\left(2,\ \frac{9}{4},\ \frac{64}{27},\ \cdots\right)$ e $(1;\ 1,4;\ 1,41;\ 1,414;\ 1,4142;\ \cdots)$ que não convergem para os números racionais, mas para os números *e* e $\sqrt{2}$ respectivamente.

Além disso, podemos encontrar mais de uma sequência que converge para o mesmo número. Por exemplo, as sequências $(0,\ 0,\ 0,\ \cdots)$ e $\left(\frac{1}{1},\ \frac{1}{2},\ \frac{1}{3},\ \frac{1}{4},\ \cdots\right)$ convergem para 0.

Para resolver esse problema, *Cantor* criou uma relação de equivalência onde cada elemento do conjunto dos números reais será identificado com uma classe de sequências que possuem o mesmo limite.

Definamos então a relação de equivalência desejada:

***Definição* 33.** Sejam as sequências de Cauchy de números racionais $x = (x_n)$ e $y = (y_n)$. No conjunto das sequências de Cauchy de números racionais, definimos a relação $\sim$ como $x \sim y \Leftrightarrow (x_n - y_n) \to 0$.

***Teorema* 7.** A relação $\sim$ definida acima no conjunto de sequências de Cauchy de números racionais é uma relação de equivalência.

Para demonstrar esse teorema devemos verificar que as propriedades reflexiva, simétrica e transitiva são válidas para a relação $\sim$.

Os elementos de $\mathbb{R}$ serão classes de equivalência de sequências de Cauchy. Cada número racional r será a classe de equivalência da sequência constante $(r,\ r,\ r,\ \cdots)$.

Já os números irracionais não podem ser representados por classes de sequências que tenham a sequência constante como representante. Se isso acontecesse, sendo $[i]$ a classe de equiva-

lência das sequências que tendem a um número irracional e $(r,\ r,\ r,\ \cdots)$ uma sequência constante em $[i]$, deveríamos ter, $i_n - r \to 0$, isto é, $i_n \to r$ o que seria absurdo pois a sequência i_n tende para um número irracional.

Vamos agora definir duas operações no conjunto das classes de equivalência de sequências de Cauchy. Essas duas operações com suas propriedades definirão a estrutura algébrica do conjunto dos números reais. As operações serão:

- adição: $[x] + [y] := [x + y]$ e,
- multiplicação: $[x] \cdot [y] := [x \cdot y]$

Tomando representantes das classes $[x]$ e $[y]$, as operações definidas são feitas ponto a ponto.

O teorema a seguir garante que $+$ e $\cdot$ estão bem definidas.

***Teorema* 8.** Se (x_n) e (x'_n) são sequências de Cauchy equivalentes, da mesma forma que (y_n) e (y'_n), então $(x_n) + (y_n)$ e $(x'_n) + (y'_n)$ são equivalentes, do mesmo modo que $(x_n) \cdot (y_n)$ e $(x'_n) \cdot (y'_n)$ são equivalentes.

A demonstração deste teorema se encontra em [1].

A próxima etapa é demonstrar que $\mathbb{R}$ é um corpo com as operações definidas.

Nesta etapa é necessário definir elementos como: elemento neutro da adição e da multiplicação, inverso aditivo e inverso multiplicativo.

Nesse caso temos:

- $[(1,\ 1,\ 1,\ \cdots)]$ é a classe de equivalência do elemento neutro multiplicativo;
- $[(0,\ 0,\ 0,\ \cdots)]$ é a classe de equivalência do elemento neutro aditivo;
- O inverso aditivo de cada elemento $(a_1,\ a_2,\ a_3,\ \cdots)$ será o elemento $(-a_1,\ -a_2,\ -a_3,\ \cdots)$ e;
- O inverso multiplicativo existirá para sequências que não estão na classe da sequência nula, ou seja, se existe n_0 tal que para $n > n_0,\ x_n \neq 0$.

Assim, o inverso será definido como 0 nos termos anteriores a n_0 e $\dfrac{1}{x_n}$ nos termos a partir de $n_0 + 1$. Assim, $x_n^{-1} = (0,\ 0,\ 0,\ \cdots,\ \dfrac{1}{x_{n_0+1}},\ \dfrac{1}{x_{n_0+2}},\ \cdots)$.

A demonstração fica como exercício. Sobre a ordem:

***Definição* 34.** Uma sequência de Cauchy de números racionais (x_n) é chamada positiva se existem inteiros positivos M e n_0 tais que, se $n > n_0$ então $x_n > \dfrac{1}{M}$. Se $s \in \mathbb{R}$, dizemos que s é positiva se uma das sequências em s é positiva. Dados dois números reais $s,\ t$ dizemos que $s > t$ se $s - t$ é positiva.

A boa definição dessas relações de ordem é garantida pelo teorema abaixo:

***Teorema* 9.** Se uma sequência de Cauchy na classe de equivalência de s no final tem apenas termos positivos então qualquer sequência de Cauchy na mesma classe de equivalência no final tem apenas termos positivos.

Com a demonstração do teorema anterior, que fica a cargo do leitor, $\mathbb{R}$ fica caracterizado como um corpo ordenado.

Para chegar à conclusão de que $\mathbb{R}$ é completo deve-se ainda mostrar que $\mathbb{R}$ tem a propriedade do supremo e que $\mathbb{R}$ é arquimediano, verificando-se que $\mathbb{N}$ é ilimitado superiormente em $\mathbb{R}$, o que é feito em [1].

Observemos que as construções dos conjuntos numéricos são muito semelhantes entre si mudando-se apenas o tipo de elemento com o qual se decide trabalhar.

No caso dos números reais temos como exemplos *Richard Dedekind* que trabalhou com conjuntos (cortes) e *George Cantor* que se baseou na teoria das sequências. O importante é construir o conjunto reafirmando suas características, as quais são conhecidas e utilizadas amplamente.

Apêndice B

A ideia desse apêndice é mostrar os cálculos de $sen\ 22,5°$, $cos\ 22,5°$, $tg\ 22,5°$ e $tg\ 11,25°$, usados na atividade 3 do capítulo 5, com base nos valores de $sen\ 45°$, $cos\ 45°$ e $tg\ 45°$ conhecidos no Ensino Médio.

Lembramos que o cosseno de uma soma de dois arcos a e b pode ser calculada por:

$$cos\ (a+b) = cos\ a \cdot cos\ b - sen\ a \cdot sen\ b.$$

Se $a = b$, temos:

$$cos\ (2 \cdot a) = cos^2\ a - sen^2\ a.$$

Para o cálculo de $cos\ 22,5°$, consideramos $a = 22,5°$ e $2 \cdot a = 45°$.
Assim, escrevemos:

$$cos\ 45° = cos^2 22,5° - sen^2\ 22,5°$$

mas $cos^2\ 22,5° + sen^2\ 22,5° = 1$, o que implica em $sen^2\ 22,5° = 1 - cos^2\ 22,5°$.
Então $cos\ 45° = cos^2\ 22,5° - (1 - cos^2\ 22,5°)$ e aí, $\dfrac{\sqrt{2}}{2} = 2 \cdot cos^2\ 22,5 - 1$

$$\Rightarrow \frac{\sqrt{2}+2}{2} = cos^2\ 22,5°$$

$$\Rightarrow cos^2\ 22,5° = \frac{\sqrt{2}+2}{4}$$

$$\Rightarrow cos\ 22,5° = \frac{\sqrt{\sqrt{2}+2}}{2}$$

Temos também $sen^2 22,5° = 1 - cos^2\ 22,5°$ o que nos leva a $sen^2\ 22,5° = 1 - \left(\dfrac{\sqrt{2}+2}{4}\right)$ e aí, $sen^2\ 22,5° = \dfrac{4-\sqrt{2}-2}{4}$ o que implica em $sen\ 22,5° = \dfrac{\sqrt{2-\sqrt{2}}}{2}$.
Quanto a $tg\ 22,5°$, temos:

$$tg\ 22,5° = \frac{sen\ 22,5°}{cos\ 22,5°} = \frac{\frac{\sqrt{2-\sqrt{2}}}{2}}{\frac{\sqrt{\sqrt{2}+2}}{2}} = \frac{\sqrt{2-\sqrt{2}}}{\sqrt{2+\sqrt{2}}}$$

Multiplicando a última fração por $\frac{\sqrt{2+\sqrt{2}}}{\sqrt{2+\sqrt{2}}}$ temos:

$$tg\ 22,5^\circ = \frac{2-\sqrt{2}}{\sqrt{2+\sqrt{2}}} \cdot \frac{\sqrt{2+\sqrt{2}}}{\sqrt{2+\sqrt{2}}} = \frac{\sqrt{(2-\sqrt{2})\cdot(2+\sqrt{2})}}{2+\sqrt{2}} = \frac{\sqrt{2}}{2+\sqrt{2}}$$
$$= \frac{\sqrt{2}\cdot(2-\sqrt{2})}{(2+\sqrt{2})\cdot(2-\sqrt{2})} = \frac{2\cdot\sqrt{2}-2}{4-2} = \sqrt{2}-1.$$

Calcularemos, finalmente $tg\ 11,25^\circ$ com base na fórmula da tangente do arco dobro.

Como $tg\ (a+b) = \frac{tg\ a + tg\ b}{1 - tg\ a \cdot tg\ b}$, temos $tg\ (2\cdot a) = \frac{2\cdot tg\ a}{1 - tg^2\ a}$.

Se $a = 11,25^\circ;\ 2\cdot a = 22,5^\circ$, podemos escrever:

$$tg\ 22,5^\circ = \frac{2\cdot tg\ 11,25^\circ}{1 - tg^2\ 11,25^\circ} \Rightarrow \sqrt{2} - 1 = \frac{2\cdot tg\ 11,25^\circ}{1 - tg^2\ 11,25^\circ}$$
$$\Rightarrow (\sqrt{2}-1) - (\sqrt{2}-1)\cdot tg^2 11,25^\circ - 2\cdot tg\ 11,25^\circ = 0,$$

isto é, $(1-\sqrt{2})\cdot tg^2\ 11,25^\circ - 2\cdot tg\ 11,25^\circ + (\sqrt{2}-1) = 0$ (1).

Para determinarmos o valor de $tg\ 11,25^\circ$, devemos resolver a equação do segundo grau (1):

Os coeficientes dessa equação são:

$$a = 1-\sqrt{2} \qquad b = -2$$
$$c = \sqrt{2}-1$$
$$\Delta = b^2 - 4\cdot a\cdot c$$
$$\Delta = (-2)^2 - 4\cdot(1-\sqrt{2})\cdot(\sqrt{2}-1)$$
$$\Delta = 4 + 4\cdot(1 - 2\cdot\sqrt{2} + 2)$$
$$\Delta = 16 - 8\cdot\sqrt{2}$$

Assim,

$$tg\ 11,25^\circ = \frac{-b \pm \sqrt{\Delta}}{2\cdot a}$$
$$\Rightarrow tg\ 11,25^\circ = \frac{2 \pm \sqrt{16 - 8\cdot\sqrt{2}}}{2\cdot(1-\sqrt{2})}$$
$$\Rightarrow tg\ 11,25^\circ = \frac{2 \pm 2\cdot\sqrt{4 - 2\cdot\sqrt{2}}}{2\cdot(1-\sqrt{2})}$$
$$\Rightarrow tg\ 11,25^\circ = \frac{1 \pm \sqrt{4 - 2\cdot\sqrt{2}}}{1-\sqrt{2}}$$

Como $1-\sqrt{2} < 0$ e $11,25^\circ$ pertence ao primeiro quadrante do círculo trigonométrico, devemos ter $1 \pm \sqrt{4-2\cdot\sqrt{2}}$ com sinal negativo, o que implica em $tg\ 11,25^\circ = \frac{1-\sqrt{4-2\cdot\sqrt{2}}}{1-\sqrt{2}}$.

Racionalizando o denominador da fração temos:

$$tg\ 11,25^\circ = \frac{(1-\sqrt{4-2\cdot\sqrt{2}})\cdot(1+\sqrt{2})}{(1-\sqrt{2})\cdot(1+\sqrt{2})}$$

$$\Rightarrow tg\ 11,25^\circ = \frac{1+\sqrt{2}-\sqrt{4-2\sqrt{2}}-\sqrt{8-4\cdot\sqrt{2}}}{1-2}$$

$$\Rightarrow tg\ 11,25^\circ = -(1+\sqrt{2})+\sqrt{2}\cdot(\sqrt{2-\sqrt{2}})+2\cdot\sqrt{2-\sqrt{2}}$$

$$\Rightarrow tg\ 11,25^\circ = (2+\sqrt{2})\cdot\sqrt{2-\sqrt{2}}-(1+\sqrt{2}).$$