UNIVERSIDADE FEDERAL DE RORAIMA
PRÓ-REITORIA DE GRADUAÇÃO
CENTRO DE CIÊNCIAS E TECNOLOGIA
DEPARTAMENTO DE MATEMÁTICA

Lucas Mateus de Oliveira Lima

Um estudo da construção dos números reais por meio das técnicas de Cantor

Boa Vista - RR
2022

LUCAS MATEUS DE OLIVEIRA LIMA

UM ESTUDO DA CONSTRUÇÃO DOS NÚMEROS REAIS POR MEIO DAS TÉCNICAS DE CANTOR

Trabalho de Conclusão de Curso apresentado como pré-requisito para a obtenção do título de Licenciatura Plena em Matemática da Universidade Federal de Roraima.

Orientador: Prof. Dr. Joselito de Oliveira.

Boa Vista - RR
2022

LUCAS MATEUS DE OLIVEIRA LIMA

UM ESTUDO DA CONSTRUÇÃO DOS NÚMEROS REAIS POR MEIO DAS TÉCNICAS DE CANTOR

Trabalho de Conclusão de Curso apresentado como pré-requisito para a obtenção do título de Licenciatura Plena em Matemática da Universidade Federal de Roraima. Defendida em 05 de Agosto de 2022 e avaliada pela seguinte banca examinadora:

Prof. Dr. Joselito de Oliveira
Orientador

Prof. Dr. Elzimar de Oliveira Rufino

Prof. Dr. Lindeval Fernandes de Lima

AGRADECIMENTOS

Agradeço a minha mãe, Maria Joseane de Oliveira Lima e ao meu tio Gilmar de Oliveira Lima, minhas maiores inspirações.

Ao meu orientador, Prof. Dr. Joselito de Oliveira, pelo empenho e companheirismo ao longo dessa caminhada.

E à minha companheira Ana Gabriele Carvalho, por todos os momentos juntos nessa caminhada.

RESUMO

O presente trabalho de conclusão de curso tem como principal objetivo estudar a construção dos números reais aplicando-se técnicas de álgebra e análise, precisamente, a construção se dá utilizando sequências de Cauchy e a teoria de anéis e corpos.
Palavras-chave: Anéis; Corpos; Sequências.

ABSTRACT

The main objective of this course conclusion work is to study the construction of real numbers by applying algebra and analysis techniques, more precisely, construction occurs using Cauchy sequences and theory of rings and fields.
Keywords: Rings; Fields; Sequences.

SUMÁRIO

Introdução

A utilização dos números acompanha o desenvolvimento da humanidade, e a ideia de contagem sempre esteve presente, destacando-se a correspondência biunívoca entre artefatos que precisavam ter suas quantidades controladas. Um exemplo disso, era a correspondência estabelecida por pastores que relacionavam gravetos e ovelhas, onde cada graveto correspondia a uma única ovelha, permitindo assim, um controle de seus rebanhos. Segundo (Ferreira, 2013), muitos anos ainda se passaram até que se iniciasse o desenvolvimento teórico do conceito de número que, embora hoje nos pareça natural, foi lento e complexo, envolvendo diversas civilizações.

Iniciamos o trabalho apresentando os fundamentos necessários para construção dos números reais, como os conceitos de anéis, corpos, e consequências de suas definições. Posteriormente, apresentamos a formalização dos números naturais, inteiros e racionais, baseado nas referências (MILIES, 2001) e (FERREIRA, 2013). Os naturais são construídos atráves dos Axiomas de Peano, tal conjunto serve de base para a contrução dos números inteiros, que é feita atráves de uma relação de equivalência de pares ordenados de números naturais no qual o conjunto das classes de equivalências é denotado por $\mathbb{Z}$, e chamado de conjunto dos números inteiros. A construção dos números racionais se dá de modo análogo, isto é, o conjunto das classes de equivalência estabelecida por uma relação de equivalência de pares ordenados de números inteiros é denotado por $\mathbb{Q}$ e chamado de conjunto dos números racionais.

Por fim, a preocupação de se construir o corpo dos números reais surgiu no século IX motivada pelo desenvolvimento da análise. Dois grandes matemáticos apresentaram, de modo independente, suas teorias de construção dos números reais, a saber: Cantor e Dedekind (HEFEZ, 2016). Dedekind se baseou no conceito de corte nos racionais, enquanto que Cantor optou pelo uso de sequências, também nos racionais. Neste trabalho, optamos pela abordagem de Cantor, em virtude da bela conexão entre as áreas da análise e de álgebra, uma vez que se trabalha com sequências e as estruturas algébricas de anéis e corpos.

Capítulo 1

PRELIMINARES

Neste capítulo, serão abordados os fundamentos necessários para a construção dos números reais por meio do método de Cantor. Inicialmente, abordaremos o conjunto dos números reais onde as propriedades das operações de adição e multiplicação são consideradas de um ponto de vista puramente axiomático. Os principiais resultados aqui elencados podem ser encontrados em (HEFEZ, 2016), (LIMA, 1995) e (GONÇALVES, 2001).

1.1 RELAÇÕES

Nesta seção, serão apresentadas duas definições que servirão de base para a construção dos conjuntos numéricos, as mesmas podem ser encontradas em (HEFEZ, 2016) e (FERREIRA, 2013).

Definição 1.1.1. *Uma relção binária $\mathcal{R}$ num conjunto $\mathcal{A}$ é qualquer subconjunto do produto cartesiano $\mathcal{A} \times \mathcal{A}$, isto é, $\mathcal{R} \subset \mathcal{A} \times \mathcal{A}$. E sendo $(a,b) \in \mathcal{R}$, é dito que $a\mathcal{R}b$, ou seja,*

$$(a,b) \in \mathcal{R} \Leftrightarrow a\mathcal{R}b.$$

Definição 1.1.2. *Uma relação binária $\mathcal{R}$ em $\mathcal{A}$ diz-se relação de equivalência se possuir as seguintes propriedades:*

1. *(Reflexiva)*

   $a\mathcal{R}a, \forall a \in \mathcal{A}.$

2. *(Simétrica)*

   Se $a, b \in \mathcal{A}$ e $a\mathcal{R}b$, então $b\mathcal{R}a$.

3. *(Transitiva)*

   Se $a\mathcal{R}b$ e $b\mathcal{R}c$, então $a\mathcal{R}c$. $\forall a, b, c \in \mathcal{A}$.

Observação 1.1.1. *Quando uma relação $\mathcal{R}$ em um conjunto $\mathcal{A}$ for de equivalência será utilizada a notação $\sim$ em vez de $\mathcal{R}$.*

Definição 1.1.3. *Sejam $\sim$ uma relação de equivalência num conjunto $\mathcal{A}$ e $a \in \mathcal{A}$ um elemento fixado arbitrariamente. O conjunto*

$$\overline{a} = \{x \in \mathcal{A} \ ; \ x \sim a\}$$

chama-se classe de equivalência de a pela relação $\sim$. Ou seja, $\overline{a}$ é o conjunto constituído por todos os elementos de $\mathcal{A}$ que são equivalentes a a.

Teorema 1.1.1. *Sejam $\sim$ uma relação de equivalência em um conjunto $\mathcal{A}$ e a e b elementos quaisquer de $\mathcal{A}$, então:*

1. $a \in \overline{a}$
2. $\overline{a} = \overline{b} \Leftrightarrow a \sim b$;

Demonstração. Veja em (FERREIRA, 2013, p.11). □

Definição 1.1.4. *Uma relação binária $\leq$ em um conjunto não vazio $\mathcal{A}$ é dita uma relação de ordem total, se possuir as seguintes propriedades:*

1. *(Reflexiva)*

   $a \leq a, \forall a \in \mathcal{A}$.

2. *(Antissimétrica)*

   Se $a \leq b$ *e* $b \leq a$, *então* $a = b, \ \forall a, b \in \mathcal{A}$.

3. *(Transitiva)*

   Se $a \leq b$ *e* $b \leq c$, *então* $a \leq c, \ \forall a, b, c \in \mathcal{A}$.

4. *(Totalidade)*

   $\forall a, b \in \mathcal{A}$, *tem-se que* $a \leq b$ *ou* $b \leq a$.

1.2 CORPOS

Nesta seção, estuda-se o conceito de corpos, cujas definições e propriedades foram encontradas em (LIMA, 1995).

Definição 1.2.1. *Um corpo $(\mathcal{K}, +, \cdot)$ é um conjunto não vazio onde estejam definidas duas operações, $+$ e $\cdot$, chamadas respectivamente de adição e multiplicação, que satisfazem os seguintes axiomas:*

Axiomas da adição:

A1) (Associatividade)

Para quaisquer $x, y, z \in \mathcal{K}$, *tem-se que*

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

A2) (Comtatividade)

Para quaisquer $x, y \in \mathcal{K}$, *tem-se que*

$$x + y = y + x.$$

A3) (Elemento neutro)

Existe $0 \in \mathcal{K}$ *tal que*

$$x + 0 = x,$$

para todo $x \in \mathcal{K}$.

A4) (Elemento simétrico)

Todo $x \in \mathcal{K}$ *possui um simétrico* $-x \in \mathcal{K}$ *tal que*

$$x + (-x) = 0.$$

Axiomas da multiplicação:

M1) (Associatividade)

Para quaisquer $x, y, z \in \mathcal{K}$, *tem-se que*

$$x \cdot (y \cdot z) = (x \cdot y) \cdot z.$$

M2) (Comtatividade)

Para quaisquer $x, y \in \mathcal{K}$, *tem-se que*

$$x \cdot y = y \cdot x.$$

M3) (Elemento neutro)

Existe $1 \in \mathcal{K}$ *com* $1 \neq 0$ *tal que*

$$x \cdot 1 = x,$$

para todo $x \in \mathcal{K}$. *O elemento* 1 *chama-se um.*

M4) (Inverso multiplicativo)

Todo $x \neq 0$ em $\mathcal{K}$ possui um inverso x^{-1} tal que

$$x \cdot x^{-1} = 1.$$

M5) (Distributividade)

Para quaisquer $x, y, z \in \mathcal{K}$, tem-se que

$$x \cdot (y + z) = x \cdot y + x \cdot z.$$

1.2.1 CORPO ORDENADO

Neste tópico estudam-se as propriedades fundamentais de um corpo, propriedades estas que garantem a existência de um corpo ordenado completo, que nos capítulos seguintes será denotado por $\mathbb{R}$. Os resultados aqui elencados podem ser encontrados em (LIMA, 1995).

Definição 1.2.2. *Um corpo ordenado é um corpo $\mathcal{K}$ no qual se destacou um subconjunto $\mathcal{P} \subset \mathcal{K}$, chamado o conjunto dos elementos positivos de $\mathcal{K}$, tal que as seguintes condições são satisfeitas:*

1. *Para quaisquer $x, y \in P$, tem-se que*

$$x + y \in P \quad e \quad x \cdot y \in P.$$

2. *Dado $x \in \mathcal{K}$, ocorre exatamente uma das três alternativas seguintes:*

$$x = 0 \quad ou \quad x \in \mathcal{P} \quad ou \quad -x \in \mathcal{P}.$$

Observação 1.2.1. *Sendo $-\mathcal{P}$ o conjunto dos elementos $-x$ onde $x \in \mathcal{P}$, temos $\mathcal{K} = \mathcal{P} \cup (-\mathcal{P}) \cup \{0\}$. Sendo os conjuntos $\mathcal{P}, -\mathcal{P}$ e $\{0\}$ dois a dois disjuntos. Os elementos de $-\mathcal{P}$ chamam-se negativos.*

Observação 1.2.2. *Em um corpo ordenado $\mathcal{K}$, escreve-se $x < y$ e diz que x é menor do que y quando $y - x \in \mathcal{P}$, ou seja, que $y = x + z$, onde $z \in \mathcal{P}$.*

Valem as seguintes propriedades da relação de ordem $x < y$ em $\mathcal{K}$:

1. (Transitividade)

$$\text{Se } x < y \text{ e } y < z \text{ então } x < z.$$

2. (Tricotomia)

   Dados $x, y \in \mathcal{K}$, ocorre exatamente uma das três alternativas:

$$x = y \text{ ou } x < y \text{ ou } y < x.$$

3. (Monotonicidade da adição)

   Se $x < y$ então, para todo $z \in \mathcal{K}$, tem-se

$$x + z < y + z.$$

4. (Monotonicidade da multiplicação)

   Se $x < y$ então, para todo $z > 0$ tem-se

$$xz < yz.$$

Definição 1.2.3. *Em um corpo ordenado $\mathcal{K}$ define-se o valor absoluto de um elemento $x \in \mathcal{K}$ como sendo,*

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

Os próximos dois teoremas nos mostram algumas propriedades do valor absoluto.

Teorema 1.2.1. *Sejam a e x elementos de um corpo ordenado $\mathcal{K}$. As seguintes afirmações são equivalentes*

1. $-a \leq x \leq a$;

2. $x \leq a$ *e* $-x \leq a$;

3. $\mid x \mid \leq a$.

Demonstração. Veja em (LIMA, 1995, p.72). □

Teorema 1.2.2. *Para os elementos arbitrários de um corpo ordenado $\mathcal{K}$, valem as relações:*

1. $\mid x + y \mid \leq \mid x \mid + \mid y \mid$;

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

3. $\mid x \mid - \mid y \mid \leq \mid\mid x \mid - \mid y \mid\mid \leq \mid x - y \mid$;

4. $\mid x - z \mid \leq \mid x - y \mid + \mid y - z \mid$

Demonstração. veja em (LIMA, 1995, p.73). □

Definição 1.2.4. *Um subconjunto $\mathcal{X}$ de um corpo ordenado $\mathcal{K}$ chama-se limitado superiormente quando existe $b \in \mathcal{K}$ tal que $b \geq x$ para todo $x \in \mathcal{X}$. Cada $b \in \mathcal{K}$ com esta propriedade chama-se uma cota superior de $\mathcal{X}$. De forma análoga, $\mathcal{X} \subset \mathcal{K}$ diz-se limitado inferiormente quando existe $a \in \mathcal{K}$ tal que $a \leq x$ para todo $x \in \mathcal{X}$. Um elemento $a \in \mathcal{K}$ com esta propriedade chama-se uma cota inferior de $\mathcal{X}$. Um subconjunto $\mathcal{X}$ de um corpo ordenado $\mathcal{K}$ chama-se limitado quando é limitado superiormente e inferiormente.*

Definição 1.2.5 (Supremo)**.** *Sejam $\mathcal{K}$ um corpo ordenado e $\mathcal{X} \subset \mathcal{K}$ um subconjunto limitado superiormente. Um elemento $b \in \mathcal{K}$ chama-se supremo de um conjunto $\mathcal{X} \subset \mathcal{K}$ se é a menor das cotas superiores, isto é,*

1. *Para todo $x \in \mathcal{X}$, tem-se $x \leq b$.*

2. *Se $c \in \mathcal{K}$ é tal que $x \leq c$ para todo $x \in \mathcal{X}$ então, $b \leq c$.*

Definição 1.2.6 (Ínfimo)**.** *Seja $\mathcal{K}$ um corpo ordenado e $\mathcal{X} \subset \mathcal{K}$ um subconjunto limitado inferiormente. Um elemento $a \in \mathcal{K}$ chama-se ínfimo de um conjunto $\mathcal{X} \subset \mathcal{K}$ se é a maior das cotas inferiores de $\mathcal{K}$.*

1. *Para todo $x \in$ tem-se $a \leq x$.*

2. *Se $c \in \mathcal{K}$ é tal que $c \leq x$ para todo $x \in \mathcal{X}$, então $c \leq a$.*

Definição 1.2.7. *Um corpo ordenado $\mathcal{K}$ chama-se completo quando todo subconjunto não-vazio, limitado superiormente, $\mathcal{X} \subset \mathcal{K}$, possui um supremo em $\mathcal{K}$.*

Axioma 1.2.1 (Axioma fundamental da análise)**.** *Existe um corpo ordenado completo, $\mathbb{R}$, chamado de corpo dos números reais.*

1.3 ANEL

Nesta seção, veremos a definição de anel, juntamente com suas propriedades. Os resultados aqui elencados podem ser encontrados em (HEFEZ, 2016), (HUNGERFORD, 1997) e (GONÇALVES, 2001).

Definição 1.3.1. *Um anel $(\mathcal{A}, +, \cdot)$ é um conjunto não vazio onde estejam definidas duas operações, $+$ e $\cdot$, chamadas respectivamente de adição e multiplicação, que satisfazem as seguintes propriedades:*

P1) (Assoiatividade da soma)

$\forall a, b, c \in \mathcal{A}$, tem-se que

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

P2) (Comutatividade da soma)

$\forall a, b \in \mathcal{A}$, *tem-se que*

$$a + b = b + a.$$

P3) (Existência de um elemento neutro aditivo)

$\exists\, \alpha \in \mathcal{A}$ *tal que*

$$\alpha + a = a + \alpha = a, \quad \forall a \in \mathcal{A}.$$

P4) (Existência de um inverso aditivo)

$\exists\, a' \in \mathcal{A}$ *tal que*

$$a + a' = \alpha, \quad \forall a \in \mathcal{A}.$$

P5) (Associatividade do produto)

$\forall a, b, c \in \mathcal{A}$, *tem-se que*

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

P6) (Distributividade)

$\forall a, b, c \in \mathcal{A}$, *tem-se que*

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

Se um anel $\mathcal{A}$ *cumpre a propriedade:*

P7) (Comutatividade do produto)

$\forall a, b \in \mathcal{A}$, *tem-se que*

$$a \cdot b = b \cdot a.$$

$(\mathcal{A}, +, \cdot)$ *é dito um anel comutativo.*

Se um anel $\mathcal{A}$ *cumpre a propriedade:*

P8) (Existência de um elemento neutro multiplicativo)

Existe um elemento pertencente a $\mathcal{A}$*, denotado por* 1 *e denominado de unidade, tal que*

$$a.1 = 1 \cdot a = a, \quad \forall a \in \mathcal{A}$$

$(\mathcal{A}, +, \cdot)$ é dito um anel com unidade.

Exemplo 1.3.1 (Anéis)**.**

1. *$(\mathbb{Z}, +, \cdot)$ é um anel.*

2. *$M_2(\mathbb{Z}) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} ; a, b, c, d \in \mathbb{Z} \right\}$, com as operações usuais de adição e multiplicação de matrizes é um anel não comutativo com unidade.*

Observação 1.3.1. *Note que o conjunto dos números naturais não é um anel, pois não cumpre a propriedade P4.*

Definição 1.3.2 (Anéis ordenados)**.** *Um anel $\mathcal{A}$ é dito ordenado, se existir uma relação de ordem total $\leq$ em $\mathcal{A}$ que possui as seguintes propriedades:*

1. *(Compatibilidade com a multiplicação)*

   $\forall a, b, c \in \mathcal{A}$, se $a \leq b$ e $c \geq 0$, então $a \cdot c \leq b \cdot c$.

2. *(Compatibilidade com a adição)*

   $\forall a, b, c \in \mathcal{A}$, se $a \leq b$, então $a + c \leq b + c$.

Definição 1.3.3. *Uma anel $(\mathcal{A}, +, \cdot)$ é um anel sem divisores de zero se satisfaz a seguinte propriedade:*

$$\textit{Se } a{\cdot}b = 0 \textit{ então } a = 0 \textit{ ou } b = 0.$$

Exemplo 1.3.2 (Divisores de zero)**.**

1. *O anel $(\mathbb{Z}, +, \cdot)$ é um anel sem divisores de zero.*

2. *O anel $(\mathbb{Z}_6, +, \cdot)$ é uma anel com divisores de zero. De fato, como $\mathbb{Z}_6 = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{4}, \overline{5}\}$ e $\overline{2}, \overline{3} \neq \overline{0}$, então $\overline{2} \cdot \overline{3} = \overline{6} = \overline{0}$. Portanto, $\overline{2}$ e $\overline{3}$ são divisores de zero em $(\mathbb{Z}_6, +, \cdot)$.*

Definição 1.3.4. *Se $(\mathcal{A}, +, \cdot)$ é um anel comutativo, com unidade e sem divisores de zero, então $(\mathcal{A}, +, \cdot)$ é denominado domínio de integridade.*

Definição 1.3.5. *Se um domínio de integridade satisfaz a propriedade*

$$\forall a \in \mathcal{A},\ a \neq 0, \exists\, a^{-1} \textit{ tal que } a \cdot a^{-1} = 1,$$

então $(\mathcal{A}, +, \cdot)$ é denominado corpo.

Exemplo 1.3.3 (Corpos)**.**

1. *O conjunto $\mathbb{Q}$ dos números racionais com as operações*

$$\frac{p}{q}+\frac{p'}{q'}=\frac{pq'+p'q}{qq'} \quad e \quad \frac{p}{q}\cdot\frac{p'}{q'}=\frac{pp'}{qq'},$$

é um corpo. O simétrico de $\frac{p}{q}$ *é* $\frac{-p}{q}$*, o elemento neutro da adição é* $0=\frac{0}{q}$*, seja qual for* $q\neq 0$ *e o inverso do número racional* $\frac{p}{q}\neq 0$ *é* $\frac{q}{p}$.

2. *O conjunto* $\mathbb{Z}_p=\{\overline{0},\overline{1},...,\overline{p-1}\}$*, onde* p *é um número primo, com as operações usuais de adição e multiplicação em classes de congruência é um corpo.*

Observação 1.3.2. *O conjunto dos números inteiros é um domínio de integridade que não é corpo.*

1.3.1 SUBANEL

Neste tópico, veremos o conceito de subanel, com o intuito de adquirirmos elementos suficientes para compreensão da próxima estrutura, a saber: um ideal. Os resultados aqui elencados podem ser encontrados em (HEFEZ, 2016), (HUNGERFORD, 1997) e (GONÇALVES, 2001).

Definição 1.3.6. *Um subconjunto* $\mathcal{B}$ *não vazio de um anel* $\mathcal{A}$ *será chamado de subanel de* $\mathcal{A}$ *se* $\mathcal{B}$*, juntamente com as restrições a ele das operações de adição e multiplicação de* $\mathcal{A}$ *for um anel.*

Proposição 1.3.1. *Sejam* $\mathcal{A}$ *um anel e* $\mathcal{B}$ *um subconjunto não vazio de* $\mathcal{A}$*. Temos que* $\mathcal{B}$ *é um subanel de* $\mathcal{A}$ *se, e somente se, são satisfeitas as seguintes condições:*

1. $0\in\mathcal{B}$*;*

2. *Quaisquer que sejam* $a,b\in\mathcal{B}$*, tem-se que* $a-b\in B$ *e* $a\cdot b\in\mathcal{B}$*.*

Demonstração.

($\Rightarrow$) Se $\mathcal{B}$ é um subanel de $\mathcal{A}$, então, por definição $0\in\mathcal{B}$. Além disso, para qualquer $a,b\in\mathcal{B}$ temos que $a+(-b)=a-b\in\mathcal{B}$ e $a\cdot b\in\mathcal{B}$, pois $\mathcal{B}$ é anel.

($\Leftarrow$) Suponha que as condições 1 e 2 sejam verificadas. Por 1, segue que $\mathcal{B}\neq\emptyset$. Sejam a e b elementos de $\mathcal{B}$, temos que $-b\in\mathcal{B}$ e consequentemente,

$$a+b=a-(-b)\in\mathcal{B}.$$

Como $a\cdot b\in\mathcal{B}$ e as demais condições que definem um anel são verificadas em $\mathcal{B}$, pois o são em $\mathcal{A}$, segue-se que $\mathcal{B}$ é um subanel de $\mathcal{A}$.

$\square$

Exemplo 1.3.4. *O conjunto* $S = \left\{ \begin{pmatrix} x & 0 \\ 0 & x \end{pmatrix} ; x \in \mathbb{Z} \right\}$ *é um subanel do anel* $M_2(\mathbb{Z})$.

Demonstração.

1. Seja $0 = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$, temos que $0 = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} \in S$. Portanto, S é um subconjunto de $M_2(\mathbb{Z})$ não vazio.

2. Sejam $A = \begin{pmatrix} x_1 & 0 \\ 0 & x_1 \end{pmatrix}$ e $B = \begin{pmatrix} x_2 & 0 \\ 0 & x_2 \end{pmatrix}$ matrizes pertencentes a S.

   (a) A - B $= \begin{pmatrix} x_1 & 0 \\ 0 & x_1 \end{pmatrix}$ - $\begin{pmatrix} x_2 & 0 \\ 0 & x_2 \end{pmatrix} = \begin{pmatrix} x_1 - x_2 & 0 \\ 0 & x_1 - x_2 \end{pmatrix} \in S$, pois $x_1 - x_2 \in \mathbb{Z}$.

   (b) A $\cdot$ B $= \begin{pmatrix} x_1 & 0 \\ 0 & x_1 \end{pmatrix} \cdot \begin{pmatrix} x_2 & 0 \\ 0 & x_2 \end{pmatrix} = \begin{pmatrix} x_1 \cdot x_2 & 0 \\ 0 & x_1 \cdot x_2 \end{pmatrix} \in S$, pois $x_1 \cdot x_2 \in \mathbb{Z}$.

Portanto, S é um subanel do anel $M_2(\mathbb{Z})$. □

Definição 1.3.7 (Subcorpo)**.** *Seja $\mathcal{A}$ um corpo e $\mathcal{B}$ um subanel comutativo com unidade de $\mathcal{A}$. O subanel $\mathcal{B}$ é chamado de subcorpo de $\mathcal{A}$ se todo elemento não nulo de $\mathcal{B}$ possui um inverso multiplicativo.*

Definição 1.3.8 (Extensão de corpos)**.** *Se $\mathcal{B}$ é um subcorpo de um corpo $\mathcal{A}$, $\mathcal{A}$ é dito uma extensão de $\mathcal{B}$.*

1.3.2 IDEAL

Nesta subseção, em decorrência da definição de subanel, será apresentado o conceito de ideal, estrutura bastante utilizada na construção do corpo dos números reais. Para esta definição utilizamos a referência (GONÇALVES, 2001).

Definição 1.3.9. *Um subanel $\mathcal{I}$ de um anel comutativo $\mathcal{A}$ é chamado de ideal de $\mathcal{A}$ se possuir a seguinte propriedade:*

$$\textit{Se } a \in \mathcal{A} \textit{ e } x \in \mathcal{I}, \textit{ então } a \cdot x \in \mathcal{I}.$$

Exemplo 1.3.5. *O anel dos inteiros pares, denotado por $A = 2\mathbb{Z}$ é um ideal de $\mathbb{Z}$.*

Demonstração.

1. $0 \in A$, portanto $A \neq \emptyset$.

2. Sejam $a, b \in A$, com $a = 2m$ e $b = 2n$, onde $m, n \in \mathbb{Z}$.

$$a - b = 2m - 2n = 2(m - n) \in A, \text{ pois } m - n \in \mathbb{Z}.$$

3. Sejam $a \in \mathbb{Z}$ e $b \in A$, com $b = 2n$, onde $n \in \mathbb{Z}$.

$$a \cdot b = a \cdot 2n = 2 \cdot (a \cdot n) \in A, \text{ pois } a, n \in \mathbb{Z}.$$

□

1.3.3 HOMOMORFISMO

Neste tópico, abordaremos a definição de homomorfismo e suas propriedades. Além disso, será apresentado o teorema do homomorfismo de anéis, um resultado conhecido, que pode ser encontrado juntamente com as propriedades aqui elencadas, nas referências (HEFEZ, 2016), (HUNGERFORD, 1997) e (GONÇALVES, 2001).

Definição 1.3.10. *Sejam $(\mathcal{A}, +, \cdot)$ e $(\mathcal{B}, +, \cdot)$ anéis. Uma aplicação $f : \mathcal{A} \to \mathcal{B}$ é um homomorfismo de $\mathcal{A}$ em $\mathcal{B}$, se satisfaz as seguintes condições:*

1. $f(a + b) = f(a) + f(b)$, $\forall a, b \in \mathcal{A}$.
2. $f(a \cdot b) = f(a) \cdot f(b)$, $\forall a, b \in \mathcal{A}$.

Proposição 1.3.2. *Se $\mathcal{A}$ e $\mathcal{B}$ são anéis com unidade e $f : \mathcal{A} \to \mathcal{B}$ um homomorfismo, então $f(1_{\mathcal{A}}) = 1_{\mathcal{B}}$.*

Demonstração.

Seja $a \in \mathcal{A}$, como f é um homomorfismo de anéis, temos que

$$f(a) \cdot f(1_{\mathcal{A}}) = f(a \cdot 1_{\mathcal{A}}) = f(a).$$

Como $f(a) \in \mathcal{B}$, pela unicidade da unidade, temos que, $f(1_{\mathcal{A}}) = 1_{\mathcal{B}}$ □

Exemplo 1.3.6. *A aplicação*

$$\begin{aligned} \rho : \mathbb{Z} &\to \mathcal{K} \\ n &\mapsto n1 \end{aligned}$$

é um homomorfismo de anéis, chamado de homomorfismo característico.

Demonstração.

Sejam $m, n \in \mathbb{Z}$. Então

$$\begin{aligned} \rho(m+n) = (m+n)1 &= \underbrace{1 + 1+, ..., +1}_{m+n-vezes} \\ &= \underbrace{(1 + 1+, ..., +1)}_{m-vezes} + \underbrace{(1 + 1+, ..., +1)}_{n-vezes} \\ &= m1 + n1 \\ &= \rho(m) + \rho(n). \end{aligned}$$

Como $\rho(m) = m1$ e $\rho(n) = n1$, então

$$\begin{aligned}
\rho(m) \cdot \rho(n) &= m1 \cdot n1 \\
&= m1 \cdot \underbrace{(1 + 1+, ..., +1)}_{n-vezes} \\
&= \underbrace{m1 + m1+, ..., +m1}_{n-vezes} \\
&= n \cdot m1 \\
&= \rho(n \cdot m) \\
&= \rho(m \cdot n)
\end{aligned}$$

Portanto, ρ é um homomorfismo. $\square$

Definição 1.3.11. *Se $\mathcal{A}$ e $\mathcal{B}$ são anéis ordenados e $f : \mathcal{A} \to \mathcal{B}$ é um homomorfismo, f é dito um homomorfismo ordenado se $a \leq b$, implica $f(a) \leq f(b)$.*

Proposição 1.3.3. *Sejam $(\mathcal{A}, +, \cdot)$ e $(\mathcal{B}, +, \cdot)$ anéis e $f : \mathcal{A} \to \mathcal{B}$ um homomorfismo de $\mathcal{A}$ em $\mathcal{B}$. Então,*

1. $f(0_{\mathcal{A}}) = 0_{\mathcal{B}}$;
2. $f(-a) = -f(a), \forall a \in \mathcal{A}$;

Demonstração.

1. Para qualquer $a \in \mathcal{A}$ tem-se que

$$f(a) = f(a + 0_{\mathcal{A}}) = f(a) + f(0_{\mathcal{A}}), \tag{1.1}$$

pois f é um homomorfismo de anéis. Como $f(a) \in \mathcal{B}$ e $\mathcal{B}$ é um anel, temos que

$$f(a) = f(a) + 0_{\mathcal{B}}. \tag{1.2}$$

De 1.1 e 1.2, obtemos

$$f(a) + 0_{\mathcal{B}} = f(a) + f(0_{\mathcal{A}}).$$

Adicionando o simétrico aditivo em ambos os membros da igualdade, obtemos:

$$(-f(a) + f(a)) + 0_{\mathcal{B}} = (-f(a) + f(a)) + f(0_{\mathcal{A}}).$$

Portanto, $0_{\mathcal{B}} = f(0_{\mathcal{A}})$.

2. Seja $a \in \mathcal{A}$, então $-a \in \mathcal{A}$, já que $\mathcal{A}$ é um anel. Portanto, $a + (-a) = 0_{\mathcal{A}}$. Pelo item 1, tem-se que

$$0_{\mathcal{B}} = f(a + (-a)) = f(a) + f(-a),$$

Adicionando o simétrico aditivo de $f(a)$ em ambos os membros da igualdade, obtemos:

$$\begin{aligned} -f(a) + 0_{\mathcal{B}} &= -f(a) + (f(a) + f(-a)) \\ -f(a) &= (-f(a) + f(a)) + f(-a) \\ -f(a) &= 0_{\mathcal{B}} + f(-a) \\ -f(a) &= f(-a). \end{aligned}$$

Logo, $-f(a) = f(-a)$.

□

Definição 1.3.12. *Seja $f : \mathcal{A} \to \mathcal{B}$ um homomorfismo de anéis. O núcleo de f, denotado por $N(f)$ é dado pelo seguinte subconjunto de $\mathcal{A}$,*

$$N(f) = \{a \in \mathcal{A}\,;\, f(a) = 0_{\mathcal{B}}\}.$$

Definição 1.3.13. *Se $f : \mathcal{A} \to \mathcal{B}$ é um homomorfismo bijetivo, é dito que f é um isomorfismo de $\mathcal{A}$ sobre $\mathcal{B}$.*

Teorema 1.3.1. *Sejam $\mathcal{A}$ e $\mathcal{B}$ anéis e $f : \mathcal{A} \to \mathcal{B}$ um homomorfismo. Então,*

1. *$Im(f)$ é um subanel de $\mathcal{B}$;*
2. *$N(f)$ é um ideal de $\mathcal{A}$;*
3. *f é injetiva se, e somente se, $N(f) = \{0_A\}$;*

Demonstração. Veja em (GONÇALVES, 2001, p.57). □

Proposição 1.3.4. *Seja $\mathcal{K}$ um corpo tal que o homomorfismo carcacterístico $\rho : \mathbb{Z} \to \mathcal{K}$ é injetor. Então existe um único homomorfismo $\widetilde{\rho} : \mathbb{Q} \to \mathcal{K}$ e este é tal que $\widetilde{\rho} \circ j = \rho$, onde $j : \mathbb{Z} \to \mathbb{Q}$ é o homomorfismo carcacterístico.*

Demonstração. Veja em (HEFEZ, 2016, p.52). □

Proposição 1.3.5. *Seja $\mathcal{K}$ um corpo ordenado. Existe um único homomorfismo $\widetilde{\rho} : \mathbb{Q} \to \mathcal{K}$. Além disso, $\widetilde{\rho}$ é um homomorfismo de anéis ordenados.*

Demonstração. Veja em (HEFEZ, 2016, p.53). □

Proposição 1.3.6. *Seja $f : \mathcal{K} \to \mathcal{B}$ um homomorfismo de anéis, onde $\mathcal{K}$ é um corpo. Então f é injetora e o subanel $f(\mathcal{K})$ de $\mathcal{B}$ é um corpo.*

Demonstração.

Inicialmente, mostraremos que f é injetora, isto é, $N(f) = \{0\}$. De fato, suponha que $N(f) \neq \{0\}$. Então existe $x \in N(f) \subset \mathcal{K}$ tal que $x \neq 0$. Logo, existe $x^{-1} \in \mathcal{K}$ tal que

$$x \cdot x^{-1} = 1.$$

Sendo $N(f)$ um ideal de $\mathcal{K}$, veja a Proposição 1.3.1, como $x \in N(f)$ e $x^{-1} \in \mathcal{K}$, então

$$1 = x \cdot x^{-1} \in N(f).$$

Então, $f(1) = 0$, o que é um absurdo pois f é um homomorfismo. Portanto, f e injetora. Resta provar que $f(\mathcal{K})$ é corpo. De fato, seja $f(a) \neq 0$ um elemento de $f(\mathcal{K})$, como f é injetora, temos que $a \neq 0$ e, portanto, a é invertível, sendo $f(a^{-1})$ o inverso de $f(a)$. $\square$

Observação 1.3.3. *Como $\mathbb{Q}$ é um corpo, pela proposição (1.3.6) $\widetilde{\rho}$ é um homomorfismo injetor. Sendo $\mathcal{K}'$ um subcorpo de $\mathcal{K}$, em decorrência das proposições (1.3.4), (1.3.5), temos que:*

$$\begin{aligned}
\widetilde{\rho} \circ j(n) &= \rho(n) \\
\widetilde{\rho}(j(n)) &= \rho(n) \\
\widetilde{\rho}\left(\frac{n}{1}\right) &= \rho(n) \in \mathcal{K}' \subset \mathcal{K}.
\end{aligned}$$

Além disso,

$$\begin{aligned}
\widetilde{\rho}\left(\frac{a}{b}\right) &= \widetilde{\rho}\left(\frac{a}{1} \cdot b^{-1}\right) \\
&= \widetilde{\rho}\left(\frac{a}{1}\right) \cdot \widetilde{\rho}(b^{-1}) \\
&= \widetilde{\rho}\left(\frac{a}{1}\right) \cdot \left(\widetilde{\rho}\left(\frac{b}{1}\right)\right)^{-1} \\
&= \widetilde{\rho} \circ j(a) \cdot (\widetilde{\rho} \circ j(b))^{-1} \\
&= \rho(a) \cdot (\rho(b))^{-1} \in \mathcal{K}'
\end{aligned}$$

Logo, $\widetilde{\rho}(\mathbb{Q}) \subset \mathcal{K}'$. Então o corpo $\widetilde{\rho}(\mathbb{Q})$ é o menor subcorpo de $\mathcal{K}$, e é denotado por $\mathcal{K}_0$, isto é, $\mathcal{K}_0 = \widetilde{\rho}(\mathbb{Q})$.

1.3.4 ANEL QUOCIENTE

Nesta subseção, veremos a construção de um anel quociente, juntamente com o teorema do isomorfismo de anéis. A construção aqui apresentada, além dos demais resultados, podem ser encontrados em (HEFEZ, 2016), (HUNGERFORD, 1997), (GONÇALVES, 2001) e (MILIES, 2001).

Seja $\mathcal{A}$ um anel qualquer e seja $\mathcal{I}$ um ideal de $\mathcal{A}$. Vamos definir a seguinte relação em $\mathcal{A}$:

$$\forall a, b \in \mathcal{A},\ a \equiv b\,(mod\,\mathcal{I}) \Leftrightarrow a - b \in \mathcal{I}.$$

Proposição 1.3.7. *A relação definida anteriormente é uma relação de equivalência.*

Demonstração.

Quaisquer que sejam $a, b, c \in \mathcal{A}$, tem-se que

1. Reflexiva.

   $a \equiv a\,(mod\,\mathcal{I})$, pois $a - a = 0 \in \mathcal{I}$, já que $\mathcal{I}$ é um ideal.

2. Simetria.

   Se $a \equiv b\,(mod\,\mathcal{I})$, $a - b \in \mathcal{I}$. Como $\mathcal{I}$ é um ideal, $b - a \in \mathcal{I}$. Portanto $b \equiv a\,(mod\,\mathcal{I})$.

3. Transitiva.

   Se $a \equiv b\,(mod\,\mathcal{I})$, e $b \equiv c\,(mod\,\mathcal{I})$, então $a - b \in \mathcal{I}$ e $b - c \in \mathcal{I}$. Sendo $\mathcal{I}$ um ideal, temos que $(a - b) + (b - c) = a - c \in \mathcal{I}$. Logo, $a \equiv c\,(mod\,\mathcal{I})$.

$\square$

A classe de equivalência do elemento $a \in \mathcal{A}$ relativamente a relação $\equiv$ $(mod\,\mathcal{I})$, será denotada por

$$\overline{a} = \{b \in \mathcal{A};\ b \equiv a\,(mod\,\mathcal{I})\}.$$

Note que $b \in \overline{a} \Leftrightarrow b - a \in \mathcal{I}$. Se $b - a = u$, para algum $u \in \mathcal{I}$, então $b = a + u$. Logo, podemos escrever $\overline{a} = a + \mathcal{I}$. O conjunto quociente de $\mathcal{A}$ pelo ideal $\mathcal{I}$, denotado por $\mathcal{A}/\mathcal{I}$, é dado por

$$\mathcal{A}/\mathcal{I} = \{\overline{a}\,; a \in \mathcal{A}\}.$$

A seguinte proposição nos permitirá definir operações de adição e multiplicação no conjunto quociente $\mathcal{A}/\mathcal{I}$.

Proposição 1.3.8. *Seja $\mathcal{A}$ um anel e $\mathcal{I}$ um ideal de $\mathcal{A}$. Se $a \equiv a'\,(mod\,\mathcal{I})$ e $b \equiv b'\,(mod\,\mathcal{I})$ então*

1. $a + b \equiv a' + b'\,(mod\,\mathcal{I})$;

2. $a \cdot b \equiv a' \cdot b'\,(mod\,\mathcal{I})$.

Demonstração.

1. $(a+b)-(a'+b') = a+b-a'-b' = (a-a')+(b-b') \in \mathcal{I}$, pois $a-a' \in \mathcal{I}$ e $b-b' \in \mathcal{I}$. Portanto $(a+b)-(a'+b') \in \mathcal{I}$.

2. Seja $a = a' + z, z \in \mathcal{I}$ e $b = b' + w, w \in \mathcal{I}$. Então,

$$a \cdot b - a' \cdot b' = (a'+z) \cdot (b'+w) - a' \cdot b' = a' \cdot b' + a' \cdot w + z \cdot b' + z \cdot w - a' \cdot b' = a' \cdot w + z \cdot b' + z \cdot w.$$

Como $z, w \in \mathcal{I}$ e sendo $\mathcal{I}$ um ideal de $\mathcal{A}$, segue que $a' \cdot w, z \cdot b', z \cdot w \in \mathcal{I}$. Portanto, $a \cdot b - a' \cdot b' = a' \cdot w + z \cdot b' + z \cdot w \in \mathcal{I}$.

□

Proposição 1.3.9. *Sejam $\mathcal{A}$ um anel, $\mathcal{I}$ um ideal de $\mathcal{A}$ e $a, b \in \mathcal{A}$. Então $a \equiv b\,(mod\,\mathcal{I})$ se, e somente se $\overline{a} = \overline{b}$.*

Demonstração.

$(\Rightarrow)$

1. $\overline{a} \subset \overline{b}$.
   Se $x \in \overline{a}$, então $x - a \in \mathcal{I}$, ou seja, existe $u \in \mathcal{I}$ tal que $x - a = u$. Como $a \equiv b\,(mod\,\mathcal{I})$, obtemos $y = a - b \in \mathcal{I}$.
   Segue que

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

Como $y + u \in \mathcal{I}$, resulta que $x \in \overline{b}$.

2. $\overline{b} \subset \overline{a}$.
   Dado $z \in \overline{b}$, então $z - b \in \mathcal{I}$, ou seja, existe $v \in \mathcal{I}$ tal que $z - b = v$. Como $a \equiv b\,(mod\,\mathcal{I})$ então $b \equiv a\,(mod\,\mathcal{I})$. Daí, $y = b - a \in \mathcal{I}$.
   Segue que:

$$z = v + b = v + y + a = a + (v + y).$$

Como $v + y \in \mathcal{I}$, então $z \in \overline{a}$. De 1. e 2. segue que $\overline{a} = \overline{b}$.

$(\Leftarrow)$ Observe que $a = a + 0 \in \overline{a} = \overline{b}$, então existe $x \in \mathcal{I}$, tal que $a = b + x$, portanto, temos que $a - b = x \in \mathcal{I}$, isto é, $a \equiv b\,(mod\,\mathcal{I})$.

□

Proposição 1.3.10. *Seja* $A/I = \{\overline{a}\,;a \in A\}$. *As operações de adição e multiplicação:*

$$\begin{aligned} + : A/I \times A/I &\to A/I \\ (\overline{a}, \overline{b}) &\mapsto \overline{a} + \overline{b} = \overline{a+b} \end{aligned} \qquad \begin{aligned} \cdot : A/I \times A/I &\to A/I \\ (\overline{a}, \overline{b}) &\mapsto \overline{a} \cdot \overline{b} = \overline{a \cdot b} \end{aligned}$$

estão bem definidas.

Demonstração.

Sejam $\overline{a}, \overline{b}, \overline{a'}, \overline{b'}$ elementos de A/I tais que $\overline{a} = \overline{a'}$ e $\overline{b} = \overline{b'}$. pela Proposição 1.3.9, temos que $a \equiv a'\,(mod\,I)$ e $b \equiv b'\,(mod\,I)$. Agora, a Proposição 1.3.8 nos permite que:

$$a + b \equiv a' + b'\,(mod\,I) \qquad \text{e} \qquad a \cdot b \equiv a' \cdot b'\,(mod\,I).$$

Daí, segue que

$$\overline{a+b} \equiv \overline{a'+b'} \qquad \text{e} \qquad \overline{a \cdot b} \equiv \overline{a' \cdot b'}.$$

□

Teorema 1.3.2. *Seja* $\mathcal{A}$ *um anel e* $\mathcal{I}$ *um ideal de* $\mathcal{A}$. *Então o conjunto* $\mathcal{A}/\mathcal{I}$ *em relação as operações soma e produto é um anel.*

Demonstração.

Sejam $\overline{a}, \overline{b}, \overline{c} \in \mathcal{A}/\mathcal{I}$. Faremos a verificação das seguintes propriedades.

P1) Associatividade da adição.

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

P2) Existência de um elemento neutro aditivo.

$$\begin{aligned} \overline{a} + \overline{0} &= \overline{a+0} \\ &= \overline{a}. \end{aligned}$$

P3) Existência de um inverso aditivo.

$$\begin{aligned} \overline{a} + \overline{(-a)} &= \overline{a + (-a)} \\ &= \overline{0}. \end{aligned}$$

P4) Comutatividade.

$$\begin{aligned}\overline{a}+\overline{b} &= \overline{a+b}\\ &= \overline{b+a}\\ &= \overline{b}+\overline{a}.\end{aligned}$$

P5) Associatividade da multiplicação.

$$\begin{aligned}\overline{a}\cdot(\overline{b}\cdot\overline{c}) &= \overline{a}\cdot(\overline{b\cdot c})\\ &= \overline{a\cdot(b\cdot c)}\\ &= \overline{(a\cdot b)\cdot c}\\ &= (\overline{a\cdot b})\cdot\overline{c}\\ &= (\overline{a}\cdot\overline{b})\cdot\overline{c}.\end{aligned}$$

P6) Distributividade.

$$\begin{aligned}\overline{a}\cdot(\overline{b}+\overline{c}) &= \overline{a}\cdot(\overline{b+c})\\ &= \overline{a\cdot(b+c)}\\ &= \overline{a\cdot b+a\cdot c}\\ &= \overline{a\cdot b}+\overline{a\cdot c}\\ &= \overline{a}\cdot\overline{b}+\overline{a}\cdot\overline{c}.\end{aligned}$$

Portanto, concluímos que $\mathcal{A}/\mathcal{I}$ é um anel. O anel $\mathcal{A}/\mathcal{I}$ é denominado de anel quociente. □

Proposição 1.3.11. *Se 1 é unidade de A, então $\overline{1}$ é unidade de $\mathcal{A}/\mathcal{I}$.*

Demonstração.
$1\cdot x = x\cdot 1 = x$, $\forall x\in A \Rightarrow \overline{1}\cdot\overline{x} = \overline{1\cdot x} = \overline{x\cdot 1} = \overline{x}\cdot\overline{1} = \overline{x}$, $\forall \overline{x}\in\mathcal{A}/\mathcal{I}$. □

Proposição 1.3.12. *Se $\mathcal{A}$ é comutativo, então $\mathcal{A}/\mathcal{I}$ é comutativo.*

Demonstração.
Se $x\cdot y = y\cdot x$, $\forall x,y\in A \Rightarrow \overline{x}\cdot\overline{y} = \overline{x\cdot y} = \overline{y\cdot x} = \overline{y}\cdot\overline{x}$, $\forall\, \overline{x},\overline{y}\in\mathcal{A}/\mathcal{I}$. □

Definição 1.3.14. *Se $f:\mathcal{A}\to\mathcal{B}$ é um homomorfismo bijetivo, então f é chamado isomorfismo, e $\mathcal{A}$ e $\mathcal{B}$ são ditos isomorfos, sendo denotado por $\mathcal{A}\simeq\mathcal{B}$.*

Teorema 1.3.3 (Teorema do homomorfismo de anéis)**.** *Sejam $\mathcal{A}$ e $\mathcal{B}$ anéis e $f:\mathcal{A}\to\mathcal{B}$ um homomorfismo, então os anéis $\mathcal{A}/N(f)$ e Im(f) são isomorfos.*

Demonstração.
Considere a seguinte aplicação:

$$\begin{aligned} \widetilde{f} : \mathcal{A}/N(f) &\to \mathcal{B} \\ \overline{a} &\mapsto \widetilde{f}(\overline{a}) := f(a). \end{aligned}$$

1. Vamos mostrar que $\widetilde{f}$ está bem definida. De fato, sejam $\overline{a_1}$, $\overline{a_2} \in \mathcal{A}/N(f)$ tais que $\overline{a_1} = \overline{a_2}$. Então,

$$a_1 \sim a_2 \Leftrightarrow a_1 \equiv a_2 \; mod \; N(f) \Leftrightarrow a_1 - a_2 \in N(f) \Leftrightarrow f(a_1 - a_2) = 0.$$

   Como f é um homomorfismo, tem-se que

$$f(a_1 - a_2) = f(a_1) - f(a_2) = 0.$$

   Então, $f(a_1) = f(a_2)$, e portanto $\widetilde{f}(\overline{a_1}) = \widetilde{f}(\overline{a_2})$.

2. $\widetilde{f}$ é um homomorfismo. De fato: sejam $\overline{a_1}$, $\overline{a_2} \in \mathcal{A}/N(f)$. Então,

   (a) $\widetilde{f}(\overline{a_1} + \overline{a_2}) = \widetilde{f}(\overline{a_1 + a_2}) = f(a_1 + a_2) = f(a_1) + f(a_2) = \widetilde{f}(\overline{a_1}) + \widetilde{f}(\overline{a_2})$, pois f é um homomorfismo.

   (b) $\widetilde{f}(\overline{a_1} \cdot \overline{a_2}) = \widetilde{f}(\overline{a_1 \cdot a_2}) = f(a_1 \cdot a_2) = f(a_1) \cdot f(a_2) = \widetilde{f}(\overline{a_1}) \cdot \widetilde{f}(\overline{a_2})$, já que f é um homomorfismo.

3. $\widetilde{f}$ é injetor. De fato: vamos mostrar que $N(\widetilde{f}) = \{\overline{0}\}$.

   (a) $N(\widetilde{f}) \subset \{\overline{0}\}$.
   Dado $\overline{a} \in N(\widetilde{f})$ então $\widetilde{f}(\overline{a}) = 0$, isto é, $f(a) = 0$. Portanto, $a \in N(f)$, o que implica $\overline{a} = \overline{0}$. Logo, $N(\widetilde{f}) \subset \{\overline{0}\}$.

   (b) $\{\overline{0}\} \subset N(\widetilde{f})$.
   Como $\widetilde{f}(\overline{0}) = f(0) = 0$, já que f é um homomorfismo, então $\overline{0} \in N(\widetilde{f})$.

   De (a) e (b) segue que $N(\widetilde{f}) = \{\overline{0}\}$. Concluímos então que $\widetilde{f}$ é injetor.

4. $\widetilde{f}$ é sobre sua imagem, isto é, $\widetilde{f}(A/N(f)) = Im(f)$.

□

Teorema 1.3.4 (Teorema do isomorfismo)**.** *Sejam $\mathcal{A}$ e $\mathcal{B}$ anéis e $f : \mathcal{A} \to \mathcal{B}$ um homomorfismo sobrejetor, então os aneis $\mathcal{A}/N(f)$ e $\mathcal{B}$ são isomorfos.*

Demonstração.

Como $f : \mathcal{A} \to \mathcal{B}$ é um homomorfismo de anéis, então pelo Teorema do homomorfismo, $\mathcal{A}/N(f)$ é isomorfo a $Im(f)$. Como f é sobrejetor, então $Im(f) = \mathcal{B}$. Portanto, $\mathcal{A}/N(f)$ é isomorfo a $\mathcal{B}$.

□

Capítulo 2

NÚMEROS NATURAIS

2.1 OS NÚMEROS NATURAIS

Iniciaremos a construção dos números reais a partir do estudo dos números naturais. Ademais, adotaremos como meio de formalização, o método axiomático de Peano. Esse método tem como princípio, três axiomas, que serão apresentados em seguida. Os principais resultados aqui elencados podem ser encontrados em (FERREIRA, 2013) e (MILIES, 2001).

2.1.1 AXIOMAS DE PEANO

Existe um conjunto $\mathbb{N}$ e uma função $s : \mathbb{N} \to \mathbb{N}$ que satisfaz as seguintes condições:

1. A função s é injetora;
2. Existe um elemento em $\mathbb{N}$, que denotaremos por 0, e chamaremos de zero, que não está na imagem de s, isto é, $0 \notin Im(s)$;
3. Seja A um subconjunto de $\mathbb{N}$ tal que:
   (a) $0 \in A$;
   (b) Se $n \in A$, então $s(n) \in A$.

   Nessas condições, $A = \mathbb{N}$.

O conjunto $\mathbb{N}$ é chamado de conjunto dos números naturais. Além disso, o Axioma (3), destacado acima é conhecido como Princípio da Indução Finita ou Princípio da Indução Matemática.

Proposição 2.1.1. *A função $s : \mathbb{N} \to \mathbb{N}$ denominada de sucessor, satisfaz:*

1. $s(n) \neq n$, para todo $n \in \mathbb{N}$;

2. $Im(s) = \mathbb{N} \setminus \{0\}$.

Demonstração.

1. Seja A um subconjunto de $\mathbb{N}$ constituído dos elementos $n \in \mathbb{N}$ tais que $s(n) \neq n$. Usaremos o Princípio da Indução Matemática para mostrarmos que $A = \mathbb{N}$, ou seja, $s(n) \neq n$, $\forall n \in \mathbb{N}$. Note que $0 \in A$, pois $s(0) \neq 0$ já que $0 \notin Im(s)$ pelo segundo axioma de Peano. Resta mostrar que, se $k \in A$ então $s(k) \in A$. De fato, como

$$k \in A \Leftrightarrow s(k) \neq k,$$

sendo a função s injetora, então $s(s(k)) \neq s(k)$. Logo $s(k) \in A$ e pelo Princípio da Indução Matemática, $A = \mathbb{N}$.

2. Seja $A = \{0\} \cup Im(s)$ um subconjunto de $\mathbb{N}$.

   (a) É óbvio que $0 \in A$;

   (b) Dado $k \in A \subset \mathbb{N}$, como $s(k) \in Im(s)$ então $s(k) \in A$. Portanto, pelo Princípio da Indução Matemática, temos que $A = \mathbb{N}$, isto é,

$$\mathbb{N} = \{0\} \cup Im(s).$$

Como $0 \notin Im(s)$, então $Im(s) = \mathbb{N} \setminus \{0\}$.

□

Observação 2.1.1. $\mathbb{N} \setminus \{0\}$ *é denotado por* $\mathbb{N}^*$*, isto é, o conjunto de todos os números naturais diferentes de zero.*

2.1.2 OPERAÇÕES COM NÚMEROS NATURAIS

Neste tópico, serão apresentadas duas operações sobre o conjunto dos números naturais, denominadas de adição $(+)$ e multiplicação $(\cdot)$.

Definição 2.1.1 (Operação de adição em $\mathbb{N}$)**.** *Define-se a operação de adição em* $\mathbb{N}$ *como sendo a aplicação* $+ : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ *que associa cada par* (m, n) *ao número* $m+n$ *pertencente a* $\mathbb{N}$*, satisfazendo as seguintes condições:*

1. $m + 0 = m$;

2. $m + s(n) = s(m + n)$*, onde* s *é a função sucessor.*

Proposição 2.1.2. *Dado* $m \in \mathbb{N}$ *a adição* $m + n$ *está bem definida para todo* $n \in \mathbb{N}$*.*

Demonstração.

Fixado um $m \in \mathbb{N}$ arbitrário, considere o conjunto $S = \{n \in \mathbb{N} : m + n \in \mathbb{N}\}$. Então:

1. $0 \in S$, pois da definição de adição do item 1 temos que $m + 0 = m$;

2. Dado $n \in \mathbb{N}$, então $m + n \in \mathbb{N}$. Logo, da definição, item 2, vale a igualdade $m + s(n) = s(m + n) \in \mathbb{N}$. Então $s(n) \in S$.
   Portanto, $S = \mathbb{N}$.

□

Proposição 2.1.3 (Associatividade)**.**

Para todos $m, n \in \mathbb{N}$ tem-se que,

$$m + (n + p) = (m + n) + p.$$

Demonstração.

Fixados os naturais m, n arbitrários, iremos considerar o conjuto $S = \{p \in \mathbb{N}\,;\, m + (n + p) = (m + n) + p\}$ e mostrar que $S = \mathbb{N}$.

1. $0 \in S$, pois

$$\begin{aligned} m + (n + 0) &= m + n \\ &= (m + n) + 0. \end{aligned}$$

2. Dado $p \in S$, isto é, $m + (n + p) = (m + n) + p$. Vamos provar que $s(p) \in S$.

$$\begin{aligned} m + (n + s(p)) &= m + s(n + p) \\ &= s(m + (n + p)) \\ &= s((m + n) + p) \\ &= (m + n) + s(p). \end{aligned}$$

   Portanto, $s(p) \in S$. Assim, pelo Princípio de Indução Matemática, $S = \mathbb{N}$.

□

Proposição 2.1.4 (Elemento Neutro aditivo)**.**

O zero é o único número natural, denominado elemento neutro aditivo, que satisfaz a seguinte igualdade:

$$m + 0 = m = 0 + m, \textit{ para todo } m \in \mathbb{N}.$$

Demonstração.

Dado $m \in \mathbb{N}$, por definição, temos que $m + 0 = m$, restando provar que $0 + m = m$. Para isso, consideremos o conjunto $S = \{m \in \mathbb{N}; 0 + m = m\}$.

1. Existência:

   (a) $0 \in S$, pois $0 + 0 = 0$;

   (b) Dado $n \in S$, então $0 + n = n$. Agora, $s(n) = s(0 + n) = 0 + s(n)$, isto é, $s(n) \in S$. Portanto, $S = \mathbb{N}$.

2. Unicidade:

   Suponha que exista um número natural n tal que $m + n = m = n + m$ para todo $m \in \mathbb{N}$. Em particular, temos que $0 + n = 0$. Mas zero é o elemento neutro aditivo, isto é, $0 + n = n$. Então $n = 0$.

$\square$

Definição 2.1.2. *Indicaremos por 1 o número natural que é sucessor de 0, ou seja,* $1 = s(0)$.

Proposição 2.1.5. *O sucessor de um número natural n é dado pela seguinte igualdade:*

$$s(n) = 1 + n$$

Demonstração.
Considere o seguinte conjunto: $S = \{n \in \mathbb{N}; s(n) = 1 + n\}$.

1. $0 \in S$, pois $s(0) := 1 = 1 + 0$;

2. Seja $n \in S$. Vamos mostrar que $s(n) \in S$. De fato, como $s(n) = 1 + n$, temos que,

   $$s(s(n)) = s(1 + n) = 1 + s(n),$$

   isto é, $s(n) \in S$. Assim, pelo Princípio de Indução Matemática, temos $S = \mathbb{N}$.

$\square$

Observação 2.1.2. *Note que a definição de sucessor pode ser entendida da seguinte forma: somar o número 1 a um número natural n é tomar o seu sucessor.*

Como já temos os símbolos 0 e $1 = s(0)$, a continuação é definida como:

$$s(1) = 2 \text{ (lê-se dois)},\ s(2) = 3 \text{ (lê-se três)},\ s(3) = 4 \text{ (lê-se quatro)},$$

e assim por diante. Dessa forma, vemos então que $\mathbb{N}$ contém o conjunto:

$$\{0, s(0), s(s(0)), s(s(s(0)), ...\} = \{0, 1, 2, 3, ...\}.$$

O teorema a seguir mostra que os axiomas de Peano formalizam a ideia intuitiva de conjunto dos números naturais, ou seja, $\mathbb{N} = \{0, 1, 2, 3, ...\}$, não contém outros elementos além desses.

Teorema 2.1.1. *O conjunto dos números naturais é dado por* $\mathbb{N} = \{0, 1, 2, 3, ...\}$.

Demonstração.
Seja $S = \{0, 1, 2, 3, ...\}$ um subconjunto de $\mathbb{N}$. Então:

1. É óbvio que $0 \in S$;
2. Como S contém o sucessor de qualquer elemento nele contido, isto é, se $n \in S$ então, $s(n) \in S$.

Logo, pelo Princípio de Indução Matemática, temos $S = \mathbb{N}$. □

Proposição 2.1.6 (Comutatividade)**.**
Para todo $m, n \in \mathbb{N}$ *tem-se que*

$$m + n = n + m.$$

Demonstração.
Consideremos o seguinte conjunto:

$$S = \{n \in \mathbb{N} \ ; \ m + n = n + m, \ \forall m \in \mathbb{N}.\}$$

1. $0 \in S$, pois $m + 0 = 0 + m$, para todo $m \in \mathbb{N}$;
2. Dado $n \in \mathbb{N}$, isto é, $m+n = n+m$, para todo $m \in \mathbb{N}$. Vamos mostrar que $s(n) \in S$. De fato,

$$\begin{aligned} m + s(n) &= s(m + n) \\ &= s(n + m) \\ &= 1 + (n + m) \\ &= (1 + n) + m \\ &= s(n) + m. \end{aligned}$$

   Daí, temos que $s(n) \in S$.

Portanto, pelo Princípio de Indução Matemática, temos $S = \mathbb{N}$. □

Proposição 2.1.7 (Lei do corte da adição)**.**
Para todo $m, n, p \in \mathbb{N}$ *tem-se que*

$$n + m = n + p \Rightarrow m = p.$$

Demonstração.
Consideremos o seguinte conjunto:

$$S = \{n \in \mathbb{N} \ ; \ n + m = n + p \Rightarrow m = p, \ \forall m, p \in \mathbb{N}\}.$$

1. $0 \in S$, pois $0 + m = 0 + p \Rightarrow m = p$;

2. Dado $n \in S$, isto é, $n + m = n + p \Rightarrow m = p$. Vamos mostrar que $s(n) \in S$. De fato, pela injetividade de s e pela hipótese, temos que,

$$s(n) + m = s(n) + p \Rightarrow s(n + m) = s(n + p) \Rightarrow n + m = n + p \Rightarrow m = p.$$

Portanto, $s(n) \in S$. Assim, pelo Princípio de Indução Matemática, $S = \mathbb{N}$.

□

Definição 2.1.3 (Operação de multiplicação em $\mathbb{N}$)**.** *Define-se a operação multiplicação em* $\mathbb{N}$ *como sendo a aplicação* $\cdot : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ *que cada par* $(m, n) \in \mathbb{N} \times \mathbb{N}$ *é associado o número* $m \cdot n$ *pertencente a* $\mathbb{N}$*, satisfazendo as seguintes condições:*

1. $m \cdot 0 = 0$;

2. $m \cdot s(n) = m \cdot n + m$, *onde* s *é a função sucessor.*

Proposição 2.1.8. *Dado* $m \in \mathbb{N}$*, a multiplicação* $m \cdot n$ *está definida para todo número* $n \in \mathbb{N}$.

Demonstração.
Fixado $m \in \mathbb{N}$ arbitrário, considere o seguinte conjunto:

$$S = \{n \in \mathbb{N} \ : \ m \cdot n \in \mathbb{N}\}.$$

1. $0 \in S$, pois da definição de multiplicação, item 1, temos que, $m \cdot 0 = 0$;

2. Dado $n \in S$, isto é, $m \cdot n \in \mathbb{N}$. Vamos mostrar que $s(n) \in S$. De fato, pelo item 2 da definição de multiplicação, vale a igualdade $m \cdot s(n) = m \cdot n + m \in \mathbb{N}$. Então, $s(n) \in S$.

Portanto, pelo princípio de Indução Matemática, $S = \mathbb{N}$. □

Proposição 2.1.9 (Elemento neutro multiplicativo)**.**
Existe um único número natural, denominado elemento neutro multiplicativo, que satisfaz a seguinte igualdade:

$$1 \cdot m = m = m \cdot 1, \textit{ para todo } m \in \mathbb{N}.$$

Demonstração.

1. Existência:
Considere o seguinte conjunto: $S = \{n \in \mathbb{N} \ ; \ 1 \cdot n = n\}$.

(a) $0 \in S$, pois, por definição, $1 \cdot 0 = 0$;

(b) Dado $n \in S$, isto é, $1 \cdot n = n$. Vamos mostrar que $s(n) \in S$. De fato,

$$\begin{aligned} 1 \cdot s(n) &:= 1 \cdot n + 1 \\ &= n + 1 \\ &:= s(n) \end{aligned}$$

Logo, $s(n) \in S$. Assim, pelo Princípio de Indução Matemática, temos $S = \mathbb{N}$. Resta provar que $n \cdot 1 = n$. Note que,

$$n \cdot 1 = n \cdot s(0) = n \cdot 0 + n = 0 + n = n$$

Portanto, $n \cdot 1 = n$.

2. Unicidade:
Suponha que exista $1' \in \mathbb{N}$ tal que $1' \cdot n = n$ para todo $n \in \mathbb{N}$. Em particular,

$$1' \cdot 1 = 1. \tag{2.1}$$

Agora, sendo 1 o elemento neutro multiplicativo, então

$$1 \cdot 1' = 1'. \tag{2.2}$$

Como $1' \cdot 1 = 1 \cdot 1'$, de (2.1) e (2.2), temos que $1' = 1$.

□

Proposição 2.1.10 (Distributiva)**.**
Para todo $m, n, p \in \mathbb{N}$ tem-se que

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

Demonstração.
Fixados os naturais m, n arbitrários, considere o seguinte conjunto:

$$S = \{p \in \mathbb{N} \ ; \ m \cdot (n + p) = m \cdot n + m \cdot p\}$$

1. $0 \in S$, pois

$$\begin{aligned} m \cdot (n + 0) &= m \cdot n \\ &= m \cdot n + 0 \\ &= m \cdot n + m \cdot 0. \end{aligned}$$

2. Dado $p \in S$, isto é, $m \cdot (n + p) = m \cdot n + m \cdot p$. Vamos mostrar que $s(p) \in S$. De fato,

$$\begin{aligned} m \cdot (n + s(p)) &= m \cdot s(n + p) \\ &= m \cdot (n + p) + m \\ &= m \cdot n + m \cdot p + m \\ &= m \cdot n + m \cdot s(p). \end{aligned}$$

Portanto, $s(p) \in S$.

Logo, pelo princípio de Indução Matemática, $S = \mathbb{N}$. □

Proposição 2.1.11 (Associativa)**.**
Para todo $m, n, p \in \mathbb{N}$ *tem-se que*

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

Demonstração.
Fixados os naturais m, n arbitrários, considere o seguinte conjunto:

$$S = \{p \in \mathbb{N} \;;\; m \cdot (n \cdot p) = (m \cdot n) \cdot p\}$$

1. $0 \in S$, pois

$$\begin{aligned} m \cdot (n \cdot 0) &= m \cdot 0 \\ &= 0 \\ &= (m \cdot n) \cdot 0. \end{aligned}$$

2. Dado $p \in S$, isto é, $m \cdot (n \cdot p) = (m \cdot n) \cdot p$. Vamos mostrar que $s(p) \in S$. De fato,

$$\begin{aligned} m \cdot (n \cdot s(p)) &= m \cdot (n \cdot p + n) \\ &= m \cdot (n \cdot p) + m \cdot n \\ &= (m \cdot n) \cdot p + m \cdot n \\ &= (m \cdot n) \cdot s(p). \end{aligned}$$

Portanto, $s(p) \in S$

Logo, pelo Princípio de Indução Matemática, temos que $S = \mathbb{N}$. □

Proposição 2.1.12 (Comutativa)**.**
Para todo $m, n \in \mathbb{N}$ *tem-se que*

$$m \cdot n = n \cdot m.$$

Demonstração.

Consideremos o seguinte conjunto:

$$S = \{n \in \mathbb{N}\ ;\ m \cdot n = n \cdot m,\ \ \forall m \in \mathbb{N}\}$$

1. $0 \in S$, pois $m \cdot 0 = 0 = 0 \cdot m$;

2. Dado $n \in S$ isto é, $m \cdot n = n \cdot m$. Vamos provar que $s(n) \in S$. De fato,

$$\begin{aligned} m \cdot s(n) &= m \cdot n + m \\ &= n \cdot m + m \\ &= s(n) \cdot m. \end{aligned}$$

   Logo, $s(n) \in S$.

Portanto, pelo Princípio de Indução Matemática, temos $S = \mathbb{N}$. □

Proposição 2.1.13. *Sejam $m, n \in \mathbb{N}$ tais que $m + n = 0$. Então $m = n = 0$.*

Demonstração.

Suponha que $n \neq 0$. Então $n = s(k)$ para algum $k \in \mathbb{N}$.
Agora,

$$0 = m + n = m + s(k) = s(m + k),$$

o que é um absurdo, pois $0 \notin Im(s)$. Portanto, $n = 0$, isto é, $m = m + 0 = m + n = 0$. □

Proposição 2.1.14. *Sejam $m, n \in \mathbb{N}$, se $m \cdot n = 0$, então $m = 0$ ou $n = 0$*

Demonstração.

Por hipótese, temos que $m \cdot n = 0$. Suponha que $n \neq 0$, então $n = s(k)$, para algum $k \in \mathbb{N}$. Assim,

$$m \cdot n = m \cdot s(k) = 0 \Rightarrow m \cdot k + m = 0.$$

Logo, pela Propoposição 2.1.13, segue que $m \cdot k = m = 0$. De modo análogo, supondo que $m \neq 0$, conclui-se que $n = 0$. □

2.1.3 RELAÇÃO DE ORDEM EM $\mathbb{N}$

Em $\mathbb{N}$ existe uma relação de ordem que nos permitirá comparar os números naturais.

Definição 2.1.4. *Dados $m, n \in \mathbb{N}$, diz-se que m é menor do que ou igual a n, denotando-se por $m \leq n$, se existe $p \in \mathbb{N}$ tal que*

$$n = m + p.$$

No caso em que $n \leq m$, diz-se que m é maior ou igual a n. Além disso, dizemos que um número natural m é menor do que o número natural n, denotando-se por $m < n$, se $m \leq n$ e $m \neq n$.

Os seguintes resultados provam que a relação $\leq$ em $\mathbb{N}$, é uma relação de ordem, ou seja, valem as propriedades reflexiva, anti-simétrica e transitiva.

Proposição 2.1.15 (Reflexiva)**.**
Dado $m \in \mathbb{N}$, se $m \leq m$, então $m = m$

Demonstração.
Por hipótese, temos que $m \leq m$, com $m \in \mathbb{N}$, ou seja, $m = m + p$. Portanto, para $p = 0$, obtemos $m = m$ □

Proposição 2.1.16 (Antissimétrica)**.**
Dados $m, n \in \mathbb{N}$, se $m \leq n$ e $n \leq m$, então $m = n$.

Demonstração.
Por hipótese, $m \leq n$ e $n \leq m$, então existem $p, q \in \mathbb{N}$ tais que

$$n = m + p \tag{2.3}$$

e

$$m = n + q. \tag{2.4}$$

Substituindo 2.3 em 2.4, obtemos:

$$m = n + q = (m + p) + q = m + (p + q),$$

ou seja, $p + q = 0$ e pela Proposição 2.1.13 temos que $p = q = 0$. Portanto, $m = n$. □

Proposição 2.1.17 (Transitividade)**.**
Dados $m, n, p \in \mathbb{N}$. Se $m \leq n$ e $n \leq p$, então $m \leq p$.

Demonstração.

Por hipótese $m \leq n$ e $n \leq p$. Então existem $r, s \in \mathbb{N}$ tais que

$$n = m + r \tag{2.5}$$

e

$$p = n + s. \tag{2.6}$$

De 2.5 e 2.6 temos que,

$$\begin{aligned} p &= (m + r) + s \\ &= m + (r + s). \end{aligned}$$

Portanto, $m \leq p$. □

Proposição 2.1.18 (Tricotomia)**.**

Para quaisquer $m, n \in \mathbb{N}$, temos que uma, e apenas uma, das seguintes relações ocorre:

1. $m < n$;

2. $m = n$;

3. $m > n$.

Demonstração.

Inicialmente vamos mostrar que duas dessas relações não podem ocorrer simultaneamente. Posteriormente, mostraremos que uma delas necessariamente ocorre.

1. Note que 1 e 2 não podem ocorrer simultaneamente, pois, por definição, temos que $n = m + p$ com $p \in \mathbb{N}^*$ e $m = n$. Substituindo a segunda igualdade na primeira, obtemos $m = m + p$ e pela lei do corte, $p = 0$, o que é uma contradição, já que $p \in \mathbb{N}^*$. De modo análogo, concluimos que 2 e 3 não podem ocorrer juntas. Suponha que 1 e 3 ocorram simultaneamente, nesse caso, teríamos:

$$n = m + p \tag{2.7}$$

$$m = n + p', \tag{2.8}$$

com $p, p' \in \mathbb{N}^*$. Então,

$$n + 0 = n = (n + p') + p = n + (p + p'),$$

e pela lei do corte, temos que $p + p' = 0$. Pela Proprosição 2.1.13, segue que $p = p' = 0$, o que é uma contradição, pois $p, p' \in \mathbb{N}^*$.

2. Mostraremos agora que uma das três relações acontece. Seja m um natural arbitrário, considere o seguinte conjunto:

$$S = \{x \in \mathbb{N} \ ; \ x = m \ \ ou \ \ x > m \ \ ou \ \ x < m\}.$$

   (a) $0 \in S$, pois $0 = m$ ou $0 \neq m$.

   (b) Dado $k \in S$, mostraremos que $k + 1 \in S$. Para isso, devemos considerar três situações:

      i. $k = m$. Neste caso, $k + 1 = m + 1$, o que implica $k + 1 > m$. Portanto, $k + 1 \in S$.

      ii. $k > m$. Neste caso, existe $p \in \mathbb{N}^*$ tal que $k = m + p$. Então, $k + 1 = (m + p) + 1 = m + (p + 1)$, o que implica $k + 1 > m$. Logo, $k + 1 \in S$.

      iii. $k < m$. Neste caso, existe $p \in \mathbb{N}^*$ tal que $m = k + p$. Como $p \neq 0$, então $p = p' + 1$, $p' \in \mathbb{N}$. Agora,

      $$m = k + (p' + 1) = k + (1 + p') = (k + 1) + p'.$$

      Se $p' = 0$ então $m = k + 1$ e $k + 1 \in S$. Se $p' \neq 0$, então $m > k + 1$ e $k + 1 \in S$.

   Portanto, pelo Princípio de Indução Matemática, temos $S = \mathbb{N}$.

□

Proposição 2.1.19 (Monotonicidade da adição)**.**
Para quaisquer $m, n \in \mathbb{N}$, se $m \leq n$, então $m + p \leq n + p$, para todo $p \in \mathbb{N}$.

Demonstração.
Consideremos o seguinte conjunto:

$$S = \{p \in \mathbb{N} \ ; \ m + p \leq n + p\}.$$

1. $0 \in S$, pois $m + 0 = m \leq n = n + 0$;

2. Dado $p \in S$. Vamos mostrar que $s(p) \in S$. Como $p \in S$, então $m + p \leq n + p$. Por definição, existe $r \in \mathbb{N}$ tal que $n + p = r + (m + p)$.

Agora,

$$\begin{aligned} n + s(p) &= s(n+p) \\ &= 1 + (n+p) \\ &= 1 + (r + (m+p)) \\ &= s(r + (m+p)) \\ &= r + s(m+p) \\ &= r + (m + s(p)). \end{aligned}$$

Portanto, $m + s(p) \leq n + s(p)$. Então, $s(p) \in S$.

Logo, pelo Princípio de Indução Matemática, temos $S = \mathbb{N}$. □

Proposição 2.1.20 (Monotonicidade da multiplicação)**.**

Para quaisquer $m, n \in \mathbb{N}$, se $m \leq n$, então $m \cdot p \leq n \cdot p$, para todo $p \in \mathbb{N}^*$.

Demonstração.

Por hipótese, $m \leq n$, isto é, existe $q \in \mathbb{N}$ tal que $n = m + q$. Suponha que $m \cdot p > n \cdot p$, ou seja, $m \cdot p = n \cdot p + q'$, com $q' \in \mathbb{N}^*$. Substituindo a primeira igualdade nesta ultima, obtemos,

$$m \cdot p = (m+q) \cdot p + q' \Rightarrow m \cdot p = m \cdot p + q \cdot p + q' \Rightarrow q \cdot p + q' = 0,$$

pela Proposição 2.1.14, segue que, $p \cdot q = q' = 0$, o que é uma contradição, pois $q' \in \mathbb{N}^*$. Logo, $m \cdot p \leq n \cdot p$. □

Capítulo 3

NÚMEROS INTEIROS

3.1 OS NÚMEROS INTEIROS

No ensino básico, os números inteiros e suas propriedades são introduzidas para dar significado as operações do tipo $a - b$, onde a é menor que b. O conjunto que possui os referidos números é denominado conjunto dos números inteiros e é constituído de números naturais e seus simétricos, ou seja,

$$\mathbb{Z} = \mathbb{N} \cup \{-1, -2, ..., -n, ...\}.$$

Caso $\mathbb{N}$ seja considerado sem o zero, tem-se que o conjunto dos números inteiros pode ser apresentado da seguinte forma:

$$\mathbb{Z} = \mathbb{N} \cup \{0\} \cup \{-1, -2, ..., -n, ...\}.$$

Os resultados aqui apresentados podem ser encontrados em (FERREIRA, 2013) e (MILIES, 2001).

3.1.1 CONSTRUÇÃO DOS NÚMEROS INTEIROS

O conjunto dos números inteiros será construído a partir do conjunto dos números naturais, considerando uma relação de equivalência.

Considere inicialmente o conjunto $\mathbb{N} \times \mathbb{N} = \{(a, b)\ ;\ a, b \in \mathbb{N}\}$. Nele é definido a seguinte relação:

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

Proposição 3.1.1. *A relação definida anteriormente é uma relação de equivalência.*

Demonstração.

1. Reflexiva.

   Dados $(a,b) \in \mathbb{N} \times \mathbb{N}$, como $a+b = b+a$, segue que $(a,b) \sim (a,b)$.

2. Simétrica.

   Dados $(a,b),(c,d) \in \mathbb{N} \times \mathbb{N}$ com $(a,b) \sim (c,d)$, temos que

$$\begin{aligned} a+d &= b+c \\ b+c &= a+d \\ c+b &= d+a. \end{aligned} \tag{3.1}$$

   De 3.1 temos que $(c,d) \sim (a,b)$.

3. Transitiva.

   Sejam $(a,b),(c,d),(e,f) \in \mathbb{N} \times \mathbb{N}$ tais que

$$(a,b) \sim (c,d) \tag{3.2}$$
$$(c,d) \sim (e,f). \tag{3.3}$$

   De 3.2 temos que $a+d = b+c$ e de 3.3 tem-se que $c+f = d+e$. Daí,

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

   pela lei do corte, obtemos

$$a+f = b+e.$$

   Logo, $(a,b) \sim (e,f)$.

$\square$

Obetemos então a seguinte classe de equivalência:

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

Definição 3.1.1. *O conjuto $\mathbb{N} \times \mathbb{N}/\sim$, constituído pelas classes de equivalências $\overline{(a,b)}$ é denotado por $\mathbb{Z}$ e será chamado de conjunto dos números inteiros, ou seja,*

$$\mathbb{Z} = \mathbb{N} \times \mathbb{N}/\sim \; = \{\overline{(a,b)} \ ; \ (a,b) \in \mathbb{N} \times \mathbb{N}\}.$$

3.1.2 OPERAÇÕES COM NÚMEROS INTEIROS

Neste tópico, serão apresentadas duas operações em $\mathbb{Z}$, denominadas de adição $(+)$ e multiplicação $(\cdot)$ de números inteiros.

Definição 3.1.2 (Operação de adição em $\mathbb{Z}$)**.** *Define-se a operação de adição em $\mathbb{Z}$ como sendo a aplicação $+ : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$ que a cada par $(\alpha, \beta) \in \mathbb{Z} \times \mathbb{Z}$ é associado o número $\alpha + \beta$ pertencente a $\mathbb{Z}$, onde $\alpha = \overline{(a,b)}$, $\beta = \overline{(c,d)}$ e*

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

Proposição 3.1.2. *A operação de adição em $\mathbb{Z}$ está bem definida.*

Demonstração.
Sejam $(\alpha, \beta), (\alpha', \beta') \in \mathbb{Z} \times \mathbb{Z}$ tais que $(\alpha, \beta) = (\alpha', \beta')$, onde $\alpha = \overline{(a,b)}$, $\beta = \overline{(c,d)}$, $\alpha' = \overline{(a',b')}$ e $\beta' = \overline{(c',d')}$. Segue da igualdade de pares ordenados que,

$$\alpha = \alpha' \text{ e } \beta = \beta',$$

ou seja,

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

Daí, $(a,b) \sim (a',b')$, isto é,

$$a + b' = b + a'. \tag{3.4}$$

De modo análogo, concluímos que

$$c + d' = d + c'. \tag{3.5}$$

De 3.4 e 3.5 temos que,

$$(a + b') + (c + d') = (b + a') + (d + c') \tag{3.6}$$
$$(a + c) + (b' + d') = (b + d) + (a' + c'). \tag{3.7}$$

De 3.7 obtemos

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

ou seja,

$$\begin{aligned} \overline{(a+c, b+d)} &= \overline{(a'+c', b'+d')} \\ \alpha + \beta &= \alpha' + \beta'. \end{aligned}$$

$\square$

Proposição 3.1.3 (Associatividade)**.**

Para quaisquer $\alpha, \beta, \gamma \in \mathbb{Z}$*, tem-se que*

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

Demonstração.

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

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

□

Proposição 3.1.4 (Comutatividade)**.**

Para quaisquer $\alpha, \beta \in \mathbb{Z}$*, tem-se que*

$$\alpha + \beta = \beta + \alpha.$$

Demonstração.

Dados $\alpha = \overline{(a,b)}$, $\beta = \overline{(c,d)}$ em $\mathbb{Z}$. Então,

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

□

Proposição 3.1.5 (Elemento neutro aditivo)**.**

$$\alpha + 0 = \alpha, \textit{ para todo } \alpha \in \mathbb{Z}, \textit{ onde } 0 = \overline{(0,0)}$$

Demonstração.

Dado $\alpha = \overline{(a,b)} \in \mathbb{Z}$, então

$$\begin{aligned} \alpha + 0 &= \overline{(a,b)} + \overline{(0,0)} \\ &= \overline{(a+0, b+0)} \\ &= \overline{(a,b)} \\ &= \alpha. \end{aligned}$$

□

Proposição 3.1.6 (Elemento simétrico)**.**

Para cada $\alpha \in \mathbb{Z}$ existe um único elemento, chamado de elemento simético a α, denotado por $-\alpha$ tal que

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

Demonstração.

1. Existência:

   Sejam $\alpha = \overline{(a,b)}$ e $-\alpha = (x,y)$ em $\mathbb{Z}$ tais que $\alpha + (-\alpha) = 0$. Então,

   $$\begin{aligned} \overline{(a,b)} + \overline{(x,y)} &= \overline{(0,0)} \\ \overline{(a+x, b+y)} &= \overline{(0,0)}. \end{aligned}$$

   Então $(a+x, b+y) \sim (0,0)$, isto é, $(a+x)+0 = (b+y)+0$. Daí, obtemos a seguinte equação linear:

   $$a + x = b + y.$$

   Logo, temos que $x = b$ e $y = a$ é uma das soluções da equação linear. Portanto, $-\alpha = \overline{(b,a)}$.

2. Unicidade:

   Seja $\alpha = \overline{(a,b)}$. Suponhamos que existam dois elementos distintos simétrios a α, isto é, $-\alpha = \overline{(b,a)}$ e $-\alpha' = \overline{(b', a')}$ em $\mathbb{Z}$. Como α e $-\alpha'$ são simétricos a α, segue que

   $$\begin{aligned} \alpha + (-\alpha) = \overline{(a,b)} + \overline{(b,a)} = \overline{(0,0)} \quad &\Rightarrow \quad \overline{(a+b, b+a)} = \overline{(0,0)} \qquad (3.8) \\ &\Rightarrow \quad a + b = b + a. \qquad (3.9) \end{aligned}$$

e

$$\alpha + (-\alpha') = \overline{(a,b)} + \overline{(b',a')} = \overline{(0,0)} \;\Rightarrow\; \overline{(a+b', b+a')} = \overline{(0,0)} \tag{3.10}$$
$$\Rightarrow\; a + b' = b + a'. \tag{3.11}$$

De 3.9 e 3.11, obtemos

$$\begin{aligned}(a+b) + (b+a') &= (b+a) + (a+b')\\ (a+b) + (b+a') &= (a+b) + (a+b').\end{aligned}$$

Pela lei do corte em $\mathbb{N}$, temos que

$$b + a' = a + b'.$$

Portanto,

$$(b,a) \sim (b',a),$$

isto é,

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

$\square$

Proposição 3.1.7 (Lei do corte da adição)**.**

Para todo α, β, $\gamma \in \mathbb{Z}$ tem-se que

$$\alpha + \beta = \gamma + \beta \Rightarrow \alpha = \gamma.$$

Demonstração.

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

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

$\square$

Definição 3.1.3 (Operação de multiplicação em $\mathbb{Z}$). *Define-se a operação de multiplicação em $\mathbb{Z}$ como sendo a aplicação $\cdot : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$ que a cada par $(\alpha, \beta) \in \mathbb{Z} \times \mathbb{Z}$ é associado o número $\alpha \cdot \beta$ pertencente a $\mathbb{Z}$, onde $\alpha = \overline{(a,b)}$, $\beta = \overline{(c,d)}$ e*

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

Proposição 3.1.8. *A operação de multiplicação em $\mathbb{Z}$ está bem definida.*

Demonstração.

Sejam $(\alpha, \beta), (\alpha', \beta') \in \mathbb{Z} \times \mathbb{Z}$ tais que $(\alpha, \beta) = (\alpha', \beta')$, onde $\alpha = \overline{(a,b)}$, $\beta = \overline{(c,d)}$, $\alpha' = \overline{(a',b')}$ e $\beta' = \overline{(c',d')}$. Então

$$\alpha = \alpha' \quad \text{e} \quad \beta = \beta'.$$

1. De $\alpha = \alpha'$ temos que

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

Daí, $(a,b) \sim (a',b')$ e portanto

$$a + b' = b + a'. \tag{3.12}$$

Multiplicando 3.12 por c, obtemos:

$$ca + cb' = cb + ca'. \tag{3.13}$$

De modo análogo, multiplicando 3.12 por d, tem-se que

$$da + db' = db + da'. \tag{3.14}$$

Somando membro a membro as equações 3.13 e 3.14 obetemos

$$\begin{aligned}
(ca + cb') + (db + da') &= (cb + ca') + (da + db') \\
ac + bd + a'd + b'c &= ad + bc + a'c + b'd \\
(ac + bd, ad + bc) &\sim (a'c + b'd, a'd + b'c) \\
\overline{(ac + bd, ad + bc)} &= \overline{(a'c + b'd, a'd + b'c)} \\
\overline{(a,b)} \cdot \overline{(c,d)} &= \overline{(a',b')} \cdot \overline{(c,d)}. \qquad (3.15)
\end{aligned}$$

2. De $\beta = \beta'$ temos que

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

Daí, $(c,d) \sim (c',d')$ e assim

$$c + d' = d + c'. \tag{3.16}$$

Multiplicando a equação 3.16 por a' obtemos

$$a'c + a'd' = a'd + a'c'. \tag{3.17}$$

De modo análogo, multiplicando a equação 3.16 por b' tem-se que

$$b'c + b'd' = b'd + b'c'. \tag{3.18}$$

Somando membro a membro as equações 3.17 e 3.18 obtemos as seguintes igualdades

$$\begin{aligned}
(a'c + a'd') + (b'd + b'c') &= (a'd + a'c') + (b'c + b'd') \\
a'c + b'd + a'd' + b'c' &= a'd + b'c + a'c' + b'd' \\
(a'c + b'd, a'd, b'c) &\sim (a'c' + b'd', a'd', b'c') \\
\overline{(a'c + b'd, a'd, b'c)} &= \overline{(a'c' + b'd', a'd', b'c')} \\
\overline{(a',b')} \cdot \overline{(c,d)} &= \overline{(a',b')} \cdot \overline{(c',d')}. \qquad (3.19)
\end{aligned}$$

Portanto, das equações 3.15 e 3.19 segue-se que

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

isto é,

$$\begin{aligned}
\overline{(a,b)} \cdot \overline{(c,d)} &= \overline{(a',b')} \cdot \overline{(c',d')} \\
\alpha \cdot \beta &= \alpha' \cdot \beta'.
\end{aligned}$$

□

Proposição 3.1.9 (Associatividade)**.**

Para quaisquer $\alpha, \beta, \gamma \in \mathbb{Z}$, tem-se que

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

Demonstração.

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

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

$\square$

Proposição 3.1.10 (Comutatividade)**.**
Para quaisquer $\alpha, \beta \in \mathbb{Z}$, tem-se que

$$\alpha \cdot \beta = \beta \cdot \alpha.$$

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

$$\begin{aligned}
\alpha \cdot \beta &= \overline{(a,b)} \cdot \overline{(c,d)} \\
&= \overline{(ac+bd, ad+bc)} \\
&= \overline{(ca+db, cb+da)} \\
&= \overline{(c,d)} \cdot \overline{(a,b)} \\
&= \beta \cdot \alpha.
\end{aligned}$$

$\square$

Proposição 3.1.11 (Elemento neutro)**.**

$$\alpha \cdot 1 = \alpha, \textit{ para todo } \alpha \textit{ em } \mathbb{Z}, \textit{ onde } 1 = \overline{(1,0)}.$$

Demonstração.
Sejam $\alpha = \overline{(a,b)}$, $1 = \overline{(1.0)}$ em $\mathbb{Z}$. Então

$$\begin{aligned}
\alpha \cdot 1 &= \overline{(a,b)} \cdot \overline{(1,0)} \\
&= \overline{(a \cdot 1 + b \cdot 0,\ a \cdot 0 + b \cdot 1)} \\
&= \overline{(a+0, 0+b)} \\
&= \overline{(a,b)} \\
&= \alpha.
\end{aligned}$$

□

Proposição 3.1.12 (Distributiva)**.**
Para quaisquer $\alpha, \beta, \gamma \in \mathbb{Z}$*, tem-se que*

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

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

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

□

3.1.3 RELAÇÃO DE ORDEM EM $\mathbb{Z}$

Assim como no conjunto dos números naturais, existe uma relação de ordem em $\mathbb{Z}$, que nos permitirá comparar os números inteiros. Os resultados aqui apresentados podem ser encontrados em (FERREIRA, 2013) e (MILIES, 2001)

Definição 3.1.4. *Dados* $\alpha = \overline{(a,b)}$, $\beta = \overline{(c,d)} \in \mathbb{Z}$*,* α *é dito menor o igual a* β*, denotando-se por* $\alpha \leq \beta$*, se*

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

Os seguintes resultados provam que $\leq$ em $\mathbb{Z}$ é uma relação de ordem, ou seja, valem as propriedades reflexiva, antissimétrica e transitiva.

Proposição 3.1.13. *A desigualdade* $\leq$ *define uma relação de ordem em* $\mathbb{Z}$*.*

Demonstração.

1. (Reflexiva)

   Se $\alpha = \overline{(a,b)} \in \mathbb{Z}$, então $\alpha \leq \alpha$, pois $a + b = b + a$.

2. (Antissimétrica)

   Sejam $\alpha = \overline{(a,b)}$, $\beta = \overline{(c,d)} \in \mathbb{Z}$. Vamos mostrar que se $\alpha \leq \beta$ e $\beta \leq \alpha$, então $\alpha = \beta$.

   (a) Se $\alpha \leq \beta$, tem-se que

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

   (b) Se $\beta \leq \alpha$, tem-se que

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

   Então, pela tricotomia dos números naturais, temos que

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

3. (Transitiva)

   Sejam $\alpha = \overline{(a,b)}$, $\beta = \overline{(c,d)}$ e $\gamma = \overline{(e,f)}$ em $\mathbb{Z}$. Vamos mostrar que se $\alpha \leq \beta$ e $\beta \leq \gamma$, então $\alpha \leq \gamma$.

   (a) Se $\alpha \leq \beta$, tem-se que

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

   (b) Se $\beta \leq \gamma$, tem-se que

   $$\begin{aligned} \overline{(c,d)} &\leq \overline{(e,f)} \\ c+f &\leq d+e. \end{aligned}$$

   Então, existem $p, q \in \mathbb{N}$ tais que

   $$b+c = (a+d)+p. \tag{3.20}$$

   e

   $$d+e = (c+f)+q. \tag{3.21}$$

Somando membro a membro das Equações 3.20 e 3.21, obtemos

$$\begin{aligned} b+c+d+e &= (a+d)+p+(c+f)+q \\ b+e+(c+d) &= a+f+p+q+(c+d). \end{aligned}$$

Pela lei do corte em $\mathbb{N}$, temos que

$$b+e = a+f+(p+q).$$

Como $p+q \in \mathbb{N}$, então

$$\begin{aligned} a+f &\leq b+e \\ \overline{(a,b)} &\leq \overline{(e,f)} \\ \alpha &\leq \gamma. \end{aligned}$$

□

Proposição 3.1.14 (Tricotomia)**.**

Para quaisquer $\alpha, \beta, \gamma \in \mathbb{Z}$, temos que uma, e apenas uma, das seguintes relações ocorre:

1. $\alpha < \beta$;

2. $\alpha = \beta$;

3. $\alpha > \beta$.

Demonstração.

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

1. Suponha que $\alpha < \beta$ e $\beta < \alpha$ simultaneamente, então

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

e

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

o que é um absurdo, pela a Proposição 2.1.18.

2. Suponha que $\alpha < \beta$ e $\alpha = \beta$ simultaneamente, então

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

e

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

o que é um absurdo, pela Proposição 2.1.18.

3. Suponha que $\beta < \alpha$ e $\alpha = \beta$ simultaneamente, então

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

e

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

o que é um absurdo, pela Proposição 2.1.18.

Portanto, pela tricotomia dos números naturais, necessariamente um dos seguintes casos ocorre:

$$\alpha < \beta, \quad \alpha = \beta, \quad \alpha > \beta.$$

□

Proposição 3.1.15. *Para quaisquer $\alpha, \beta, \gamma \in \mathbb{Z}$, se $\alpha \leq \beta$, tem-se que*

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

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

$$\begin{array}{rcl}
\alpha & \leq & \beta \\
\overline{(a,b)} & \leq & \overline{(c,d)} \\
a + d & \leq & b + c \\
a + d + (e + f) & \leq & b + c + (e + f) \\
a + e + d + f & \leq & b + f + c + e \\
\overline{(a + e, b + f)} & \leq & \overline{(c + e, d + f)} \\
\overline{(a,b)} + \overline{(e,f)} & \leq & \overline{(c,d)} + \overline{(e,f)} \\
\alpha + \gamma & \leq & \beta + \gamma.
\end{array}$$

□

Proposição 3.1.16. *Para quaisquer $\alpha, \beta, \gamma \in \mathbb{Z}$, se $\alpha \leq \beta$, e $\gamma \geq 0$ então*

$$\alpha \cdot \gamma \leq \beta \cdot \gamma.$$

Demonstração.

Dados $\alpha = \overline{(a,b)}$, $\beta = \overline{(c,d)}$, $\gamma = \overline{(e,f)}$ em $\mathbb{Z}$. Como $\alpha \leq \beta$, e $\gamma \geq \overline{(0,0)}$, então

$$\begin{aligned} \overline{(a,b)} &\leq \overline{(c,d)} \\ a+d &\leq b+c, \end{aligned} \tag{3.22}$$

e

$$\begin{aligned} \overline{(0,0)} &\leq \overline{(e,f)} \\ 0+f &\leq 0+e \\ f &\leq e. \end{aligned} \tag{3.23}$$

Pela relação de ordem no conjunto dos números naturais, existem $p, q \in \mathbb{N}$ tais que

$$b + c = (a+d) + p \tag{3.24}$$

e

$$e = f + q. \tag{3.25}$$

Multiplicando a Equação 3.24 por e, temos que

$$\begin{aligned} be + ce &= (a+d)e + pe \\ be + ce &= ae + de + pe. \end{aligned} \tag{3.26}$$

De modo análogo, multiplicando a Equação 3.24 por f, tem-se que

$$\begin{aligned} bf + cf &= (a+d)f + pf \\ bf + cf &= af + df + pf. \end{aligned} \tag{3.27}$$

Por fim, multiplicando a equação 3.25 por p, temos que

$$pe = pf + pq. \tag{3.28}$$

Somando o segundo membro da equação 3.26 com o primeiro membro da equação 3.27 e o primeiro membro da equação 3.26 com o segundo membro da equação 3.27, obtemos

$$(ae + de + pe) + (bf + cf) = (be + ce) + (af + df + pf). \tag{3.29}$$

Substituindo (3.28) na igualdade acima, temos as seguintes equivalências

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

□

Definição 3.1.5. *Um número inteiro α é dito positivo se $\alpha > 0$ e negativo, se $\alpha < 0$.*

Definição 3.1.6. *Um número inteiro α é dito não negativo se $\alpha \leq 0$ e não positivo, se $\alpha \geq 0$.*

O conjunto dos números inteiros não negativos é dado por

$$\mathbb{Z}^+ = \{\alpha \in \mathbb{Z} \ ; \ \alpha \geq 0\},$$

enquanto o conjunto dos números inteiros não positivos é dado por:

$$\mathbb{Z}^- = \{\alpha \in \mathbb{Z} \ ; \ \alpha \leq 0\}.$$

Proposição 3.1.17. *Os números inteiros não negativos e não positivos têm a forma $\overline{(m, 0)}$ e $\overline{(0, m)}$, onde $m \in \mathbb{N}$, respectivamente.*

Demonstração.

Dado $\alpha = \overline{(a, b)} \in \mathbb{Z}^+$, então

$$\begin{aligned}
\overline{(a, b)} &\geq \overline{(0, 0)} \\
a + 0 &\geq b + 0 \\
a &\geq b.
\end{aligned}$$

Pela Definição 2.1.4, existe $m \in \mathbb{N}$ tal que

$$a = b + m.$$

Agora, substituindo a em $\overline{(a, b)}$, obtemos:

$$\begin{aligned}
\overline{(a, b)} &= \overline{(b + m, b)} \\
&= \overline{(b, b)} + \overline{(m, 0)} \\
&= \overline{(0, 0)} + \overline{(m, 0)} \\
&= \overline{(m, 0)}.
\end{aligned}$$

De maneira análoga, prova-se que os números inteiros não positivos têm a forma $\overline{(0,m)}$.

$\square$

Observação 3.1.1. *Note que* $b+0=b+0$, *então* $(b,b)\sim(0,0)$. *Portanto,* $\overline{(b,b)}=\overline{(0,0)}$.

3.1.4 IMERSÃO DOS NATURAIS NOS INTEIROS

Neste tópico, será visto que o conjunto dos números naturais pode ser imerso no conjunto dos números inteiros. Portanto, teremos, na realidade, uma cópia dos naturais nos inteiros com todas as propriedades preservadas.

Proposição 3.1.18. *O conjunto dos números inteiros não negativos* $\mathbb{Z}^+$ *é uma cópia do conjunto dos números naturais.*

Demonstração.

Considere a seguinte aplicação:

$$\begin{array}{rcl} \phi:\mathbb{N} & \to & \mathbb{Z}^+ \\ a & \mapsto & \phi(a)=\overline{(a,0)}, \end{array}$$

onde $a\in\mathbb{N}$. Vamos provar que ϕ é uma aplicação bijetora que preserva as operações de adição, multiplicação, e operação de ordem em $\mathbb{N}$.

1. ϕ está bem definida:

   Dados $a,b\in\mathbb{N}$ tais que $a=b$, então

   $$\begin{array}{rcl} \phi(a) & = & \overline{(a,0)} \\ & = & \overline{(b,0)} \\ & = & \phi(b). \end{array}$$

2. ϕ é uma aplicação injetora:

   Dados $a,b\in\mathbb{N}$ tais que $\phi(a)=\phi(b)$, ou seja $\overline{(a,0)}=\overline{(b,0)}$. Então,

   $$(a,b)\sim(b,0),$$

   isto é,

   $$\begin{array}{rcl} a+0 & = & 0+b \\ a & = & b. \end{array}$$

3. ϕ é uma aplicação sobrejetora:

   Dado $\alpha\in\mathbb{Z}^+$, existe $a\in\mathbb{N}$ tal que $\alpha=\overline{(a,0)}:=\phi(a)$.

4. A aplicação ϕ preserva a operação adição:

   Dados $a, b \in \mathbb{N}$, então

$$\begin{aligned} \phi(a+b) &= \overline{(a+b,0)} \\ &= \overline{(a,0)} + \overline{(b,0)} \\ &= \phi(a) + \phi(b). \end{aligned}$$

5. A aplicação ϕ preserva a operação multiplicalção:

   Dados $a, b \in \mathbb{N}$, então

$$\begin{aligned} \phi(a \cdot b) &= \overline{(a \cdot b, 0)} \\ &= \overline{(ab + 0 \cdot 0, a \cdot 0 + 0 \cdot b)} \\ &= \overline{(a,0) \cdot (b,0)} \\ &= \overline{(a,0)} \cdot \overline{(b,0)} \\ &= \phi(a) \cdot \phi(b). \end{aligned}$$

6. A aplicação ϕ preserva a ordem:

   Dados $a \leq b$, então $a + 0 \leq 0 + b$. Daí,

$$\begin{aligned} \overline{(a,0)} &\leq \overline{(b,0)} \\ \phi(a) &\leq \phi(b). \end{aligned}$$

$\square$

Capítulo 4

NÚMEROS RACIONAIS

4.1 OS NÚMEROS RACIONAIS

Ao tentarmos encontrar uma solucão para a equacão $2x = 1$, observamos que em $\mathbb{Z}$ não existe solucão, já que neste conjunto numérico não há inverso multiplicativo de qualquer número não nulo. Para que se torne possível a existência de solucão da referida equação, se faz necessário a construcão de um novo conjunto, de tal modo que ele contenha uma cópia do conjunto dos números inteiros e suas propriedades. Os principais resultados citados neste capítulo podem ser encontrados em (FERREIRA, 2013) e (MILIES, 2001).

4.1.1 A CONSTRUÇÃO DOS NÚMEROS RACIONAIS

O conjunto dos números racionais será construído a partir do conjunto dos números inteiros, considerando uma relação de equivalência.
Considere inicialmente o seguinte conjunto:

$$\mathbb{Z} \times \mathbb{Z}^* = \{(a, b) \ ; \ a \in \mathbb{Z}, b \in \mathbb{Z}^*\}, \text{ onde } \mathbb{Z}^* = \{a \in \mathbb{Z} \ ; \ a \neq 0\}.$$

Em $\mathbb{Z} \times \mathbb{Z}^*$ é definida a seguinte relação:
Dados $(a, b), (c, d) \in \mathbb{Z} \times \mathbb{Z}^*$,

$$(a, b) \sim (c, d) \Leftrightarrow ad = bc.$$

Proposição 4.1.1. *A relação $\sim$ definida anteriormente é uma relação de equivalência.*

Demonstração.

1. (Reflexiva)

   Dado $(a, b) \in \mathbb{Z} \times \mathbb{Z}^*$, como $ab = ba$, segue que $(a, b) \sim (a, b)$.

2. (Simétrica)

Sejam $(a,b),(c,d) \in \mathbb{Z} \times \mathbb{Z}^*$, com $(a,b) \sim (c,d)$. Então

$$\begin{aligned} ad &= bc \\ bc &= ad \\ cb &= da. \end{aligned} \tag{4.1}$$

Portanto, da Equação 4.1 temos que $(c,d) \sim (a,b)$.

3. (Transitiva)

   Sejam $(a,b),(c,d),(e,f) \in \mathbb{Z} \times \mathbb{Z}^*$, tais que

$$\begin{aligned} (a,b) &\sim (c,d) \\ (c,d) &\sim (e,f), \end{aligned}$$

   ou seja,

$$ad = bc \tag{4.2}$$

$$cf = de. \tag{4.3}$$

   Múltiplicando a Equação 4.2 por f e a Equação 4.3 por b, obtemos

$$adf = bcf \tag{4.4}$$

$$cfb = deb. \tag{4.5}$$

   Das Equações 4.4 e 4.5 obtemos

$$adf = deb.$$

   Pela comutatividade em $\mathbb{Z}$, tem-se que

$$afd = bed.$$

   Como $d \neq 0$, então pela lei do corte em $\mathbb{N}$, obtemos

$$af = be.$$

   Portanto, $(a,b) \sim (e,f)$.

$\square$

Obtemos então a seguinte classe de equivalência:

$$\overline{(a,b)} = \{(x,y) \in \mathbb{Z} \times \mathbb{Z}^* \ ; \ (x,y) \sim (a,b)\}.$$

Definição 4.1.1. *O conjunto $\mathbb{Z} \times \mathbb{Z}^*/\sim$ constituído pelas classes de equivalência $\overline{(a,b)}$, é denotado por $\mathbb{Q}$ e é chamado de conjunto dos números racionais, ou seja,*

$$\mathbb{Q} = \{\overline{(a,b)}\ ;\ (a,b) \in \mathbb{Z} \times \mathbb{Z}^*\}.$$

Observação 4.1.1. *O símbolo $\dfrac{a}{b} := \overline{(a,b)}$ é denominado de fração, onde a é o numerador e b o denominador. Além disso, $\dfrac{a}{b}$ é denominado número racional.*

4.1.2 OPERAÇÕES COM NÚMEROS RACIONAIS

Neste tópico, serão apresentadas duas operacões em $\mathbb{Q}$, denominadas de adicão e multiplicação de números racionais.

Definição 4.1.2 (Operação de adição em $\mathbb{Q}$)**.** *Define-se a operação de adição em $\mathbb{Q}$, como sendo a aplicação $+ : \mathbb{Q} \times \mathbb{Q} \to \mathbb{Q}$, que a cada par $(\alpha, \beta) \in \mathbb{Q} \times \mathbb{Q}$ é associado o número $\alpha + \beta$ pertencente a $\mathbb{Q}$, onde $\alpha = \dfrac{a}{b}$ e $\beta = \dfrac{c}{d}$, com $b, d \neq 0$.*

Proposição 4.1.2. *A operação de adição em $\mathbb{Q}$ esta bem definida.*

Demonstração.

Sejam $(\alpha, \beta), (\alpha', \beta') \in \mathbb{Q} \times \mathbb{Q}$, tais que $(\alpha, \beta) = (\alpha', \beta')$, onde $\alpha = \dfrac{a}{b}$, $\beta = \dfrac{c}{d}$, $\alpha' = \dfrac{a'}{b'}$, $\beta' = \dfrac{c'}{d'}$. Então

$$\alpha = \alpha' \quad e \quad \beta = \beta',$$

ou seja,

$$\begin{aligned} ab' &= ba' && (4.6)\\ cd' &= dc'. && (4.7) \end{aligned}$$

Multiplicando as Equações 4.6 e 4.7 por dd' e bb', respectivamente, obtemos

$$\begin{aligned} ab'dd' &= ba'dd' && (4.8)\\ cd'bb' &= dc'bb'. && (4.9) \end{aligned}$$

Somando membro a membro as Equações 4.8 e 4.9, temos que

$$ab'dd' + cd'bb' = ba'dd' + dc'bb'.$$

Fazendo o uso da comutatividade e da distributividade em $\mathbb{Z}$, segue que

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

Isto é,

$$\begin{array}{rcl} \dfrac{ad+bc}{bd} & = & \dfrac{a'd'+b'c'}{b'd'} \\ \dfrac{a}{b}+\dfrac{c}{d} & = & \dfrac{a'}{b'}+\dfrac{c'}{d'} \\ \alpha+\beta & = & \alpha'+\beta'. \end{array}$$

$\square$

Proposição 4.1.3 (Associatividade)**.**

Para quaisquer $\alpha, \beta, \gamma \in \mathbb{Q}$, tem-se que

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

Demonstração.

Dados $\alpha, \beta, \gamma \in \mathbb{Q}$, com $\alpha = \dfrac{a}{b}$, $\beta = \dfrac{c}{d}$ e $\gamma = \dfrac{e}{f}$. Então

$$\begin{array}{rcl} \alpha+(\beta+\gamma) & = & \dfrac{a}{b}+\left(\dfrac{c}{d}+\dfrac{e}{f}\right) \\ & = & \dfrac{a}{b}+\dfrac{cf+de}{df} \\ & = & \dfrac{adf+bcf+bde}{bdf} \\ & = & \dfrac{ad+bc}{bd}+\dfrac{e}{f} \\ & = & \left(\dfrac{a}{b}+\dfrac{c}{d}\right)+\dfrac{e}{f} \\ & = & (\alpha+\beta)+\gamma. \end{array}$$

$\square$

Proposição 4.1.4 (Comutatividade)**.**

Para quaisquer $\alpha, \beta \in \mathbb{Q}$, tem-se que

$$\alpha + \beta = \beta + \alpha.$$

Demonstração.

Dados $\alpha, \beta \in \mathbb{Q}$, com $\alpha = \dfrac{a}{b}$ e $\beta = \dfrac{c}{d}$. Então

$$\begin{array}{rcl} \alpha+\beta & = & \dfrac{a}{b}+\dfrac{c}{d} \\ & = & \dfrac{ad+bc}{bd} \\ & = & \dfrac{bc+ad}{db} \\ & = & \dfrac{c}{d}+\dfrac{a}{b} \\ & = & \beta+\alpha. \end{array}$$

$\square$

Proposição 4.1.5 (Existência de elemento neutro)**.**

Existe um único elemento de $\mathbb{Q}$, denotado por 0, tal que

$$\alpha + 0 = \alpha, \textit{ para todo } \alpha \in \mathbb{Q}.$$

Demonstração.

1. Existência:

   Dado $\alpha = \dfrac{a}{b} \in \mathbb{Q}$ e seja $0 = \dfrac{x}{y} \in \mathbb{Q}$ tal que

   $$\alpha + 0 = \alpha.$$

   Então,

   $$\frac{a}{b} + \frac{x}{y} = \frac{a}{b},$$

   ou seja,

   $$\frac{ay + bx}{by} = \frac{a}{b}$$

   Assim, obtemos a equação linear $(ay + bx)b = bya$, ou seja,

   $$(ay + bx)b = (ay)b.$$

   Pela lei do corte em $\mathbb{Z}$, temos que

   $$ay + bx = ay,$$

   isto é,

   $$ay + bx = ay + 0,$$

   e novamente pela lei do corte em $\mathbb{Z}$, temos que $bx = 0$. Sendo $b \neq 0$, então $x = 0$. Logo, $0 = \dfrac{0}{y}$, onde $y \in \mathbb{Z}^*$

2. Unicidade

   Pelo item anterior, se existir um elemento neutro, ele será da forma $\dfrac{0}{y'}$. Mas,

   $$0' \cdot y = y \cdot 0 \Leftrightarrow \frac{0}{y} = \frac{0}{y'}.$$

   Portanto, o elemento neutro aditivo é único.

$\square$

Proposição 4.1.6 (Elemento simétrico).

Para cada $\alpha \in \mathbb{Q}$ existe um único elemento, chamado de elemento simétrico a α, denotado por $-\alpha$ tal que

$$\alpha + (-\alpha) = 0$$

Demonstração.

1. Existência:

   Sejam $\alpha = \dfrac{a}{b}$ e $-\alpha = \dfrac{x}{y}$, então

$$\begin{aligned} \alpha + (-\alpha) &= 0 \\ \frac{a}{b} + \frac{x}{y} &= \frac{0}{1} \\ \frac{ay + bx}{by} &= \frac{0}{1}. \end{aligned} \tag{4.10}$$

   Da Equação 4.10, temos que

$$\begin{aligned} (ay + bx) \cdot 1 &= by \cdot 0 \\ ay + bx &= 0. \end{aligned} \tag{4.11}$$

   Sendo $x = -a$ e $y = b$, uma das soluções da Equação 4.11, então $-\alpha = \dfrac{-a}{b}$.

2. Unicidade:

   Suponha que exista $\beta \in \mathbb{Q}$ tal que

$$\alpha + \beta = 0.$$

   Observe que,

$$\begin{aligned} \beta &= \beta + 0 \\ &= \beta + (\alpha + (-\alpha)) \\ &= (\beta + \alpha) + (-\alpha) \\ &= 0 + (-\alpha) \\ &= -\alpha. \end{aligned}$$

$\square$

Definição 4.1.3 (Operação de multiplicação em $\mathbb{Q}$). *Define-se a operação produto em $\mathbb{Q}$ como sendo a aplicação $\cdot : \mathbb{Q} \times \mathbb{Q} \to \mathbb{Q}$ que a cada par $(\alpha, \beta) \in \mathbb{Q} \times \mathbb{Q}$ é associado o número $\alpha \cdot \beta$ pertencente a $\mathbb{Q}$, onde $\alpha = \dfrac{a}{b}$ e $\beta = \dfrac{c}{d}$, com $b, d \neq 0$, ou seja,*

$$\alpha \cdot \beta = \frac{ac}{bd}.$$

Proposição 4.1.7. *A operação multiplicação em $\mathbb{Q}$ está bem definida.*

Demonstração.

Dados $(\alpha, \beta), (\alpha', \beta') \in \mathbb{Q} \times \mathbb{Q}$, tais que $(\alpha, \beta) = (\alpha', \beta')$, onde $\alpha = \dfrac{a}{b}$, $\beta = \dfrac{c}{d}$, $\alpha' = \dfrac{a'}{b'}$ e $\beta' = \dfrac{c'}{d'}$. Então

$$\alpha = \alpha' \quad \text{e} \quad \beta = \beta',$$

ou seja,

$$\begin{aligned} ab' &= ba' && (4.12) \\ cd' &= dc' && (4.13) \end{aligned}$$

Multiplicando membro a membro as Equações 4.12 e 4.13, temos que

$$\begin{aligned} ab'cd' &= ba'dc' \\ (ac)b'd' &= (a'c')bd. \end{aligned}$$

Isto é,

$$\begin{aligned} \frac{ac}{bd} &= \frac{a'c'}{b'd'} \\ \frac{a}{b} \cdot \frac{c}{d} &= \frac{a'}{b'} \cdot \frac{c'}{d'} \\ \alpha \cdot \beta &= \alpha' \cdot \beta'. \end{aligned}$$

$\square$

Proposição 4.1.8 (Associatividade)**.**

Para quaisquer $\alpha, \beta, \gamma \in \mathbb{Q}$, tem-se que

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

Demonstração.

Dados $\alpha, \beta, \gamma \in \mathbb{Q}$, com $\alpha = \frac{a}{b}$, $\beta = \frac{c}{d}$ e $\gamma = \frac{e}{f}$. Então

$$\begin{aligned}
\alpha \cdot (\beta \cdot \gamma) &= \frac{a}{b} \cdot \left(\frac{c}{d} \cdot \frac{e}{f} \right) \\
&= \frac{a}{b} \cdot \left(\frac{ce}{df} \right) \\
&= \frac{ace}{bdf} \\
&= \left(\frac{ac}{bd} \right) \cdot \frac{e}{f} \\
&= \left(\frac{a}{b} \cdot \frac{c}{d} \right) \cdot \frac{e}{f} \\
&= (\alpha \cdot \beta) \cdot \gamma.
\end{aligned}$$

□

Proposição 4.1.9 (Comutatividade)**.**

Para quaisquer $\alpha, \beta \in \mathbb{Q}$, tem-se que

$$\alpha \cdot \beta = \beta \cdot \alpha.$$

Demonstração.

Dados $\alpha, \beta \in \mathbb{Q}$, com $\alpha = \frac{a}{b}$ e $\beta = \frac{c}{d}$. Então

$$\begin{aligned}
\alpha \cdot \beta &= \frac{a}{b} \cdot \frac{c}{d} \\
&= \frac{ac}{bd} \\
&= \frac{ca}{db} \\
&= \frac{c}{d} \cdot \frac{a}{b} \\
&= \beta \cdot \alpha.
\end{aligned}$$

□

Proposição 4.1.10 (Elemento neutro)**.**

Existe um único número racional, denotado por 1, tal que

$$\alpha \cdot 1 = \alpha,$$

para todo $\alpha \in \mathbb{Q}$, onde $1 = \frac{1}{1}$.

Demonstração.

1. Existência:

   Seja $\alpha = \frac{a}{b} \in \mathbb{Q}$, então

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

2. Unicidade

   Suponha que exista $1' \in \mathbb{Q}$ tal que $\alpha \cdot 1' = \alpha$, para todo $\alpha \in \mathbb{Q}$. Então

$$1 \cdot 1' \;=\; 1. \tag{4.14}$$

   Por outro lado,

$$1' \cdot 1 \;=\; 1' \tag{4.15}$$

   De 4.14 e 4.15, temos que $1 = 1'$.

□

Proposição 4.1.11 (Elemento inverso)**.**

Para cada $\alpha \neq 0$, existe um único elemento, chamado elemento inverso de α, denotado por α^{-1} tal que

$$\alpha \cdot \alpha^{-1} = 1.$$

Demonstração.

1. Existência:

   Dado $\alpha = \dfrac{a}{b} \neq 0$ em $\mathbb{Q}$, então $a \neq 0$. Logo, $\dfrac{b}{a} \in \mathbb{Q}$. Agora,

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

   Já que $ba \in \mathbb{Z}$ e em $\mathbb{Z}$ vale a comutatividade. Temos então que $\alpha^{-1} = \dfrac{b}{a}$.

2. Unicidade:

   Seja β um elemento em $\mathbb{Q}$ tal que $\alpha \cdot \beta = 1$.
   Agora,

$$\beta = \beta \cdot 1 = \beta \cdot \frac{ab}{ab} = \beta \cdot \frac{a}{b} \cdot \frac{b}{a} = \beta \cdot \alpha \cdot \frac{b}{a} = 1 \cdot \frac{b}{a} = \frac{b}{a} = \alpha^{-1}$$

Denota-se também α^{-1} por $\dfrac{1}{\alpha}$. □

Proposição 4.1.12 (Distributividade)**.**

Para quaisquer $\alpha, \beta, \gamma \in \mathbb{Q}$, tem-se que

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

Demonstração.

Dados $\alpha, \beta, \gamma \in \mathbb{Q}$, com $\alpha = \frac{a}{b}$, $\beta = \frac{c}{d}$ e $\gamma = \frac{e}{f}$. Então

$$\begin{aligned}
\alpha \cdot (\beta + \gamma) &= \frac{a}{b} \cdot \left(\frac{c}{d} + \frac{e}{f}\right) \\
&= \frac{a}{b} \cdot \left(\frac{cf + de}{df}\right) \\
&= \frac{a(cf + de)}{bdf} \\
&= \frac{acf + ade}{bdf} \\
&= \frac{b}{b} \cdot \frac{(acf + ade)}{bdf} \\
&= \frac{(bacf + bade)}{b(bdf)} \\
&= \frac{bfac + bdae}{bdbf} \\
&= \frac{ac}{bd} + \frac{ae}{bf} \\
&= \frac{a}{b} \cdot \frac{c}{d} + \frac{a}{b} \cdot \frac{e}{f} \\
&= \alpha \cdot \beta + \alpha \cdot \gamma.
\end{aligned}$$

□

4.1.3 RELAÇÃO DE ORDEM EM $\mathbb{Q}$

Assim como nos números inteiros, existe uma relação de ordem em $\mathbb{Q}$, que permitirá comparar os números racionais.

Definição 4.1.4. *Dados dois números racionais α, β em $\mathbb{Q}$, é dito que α é menor do que ou igual a β, e escrito $\alpha \leq \beta$ se, tomando como representantes $\frac{a}{b}$ e $\frac{c}{d}$, de α e β, respectivamente, tivermos $ad \leq bc$, onde $b > 0$ e $d > 0$. Resumindo, temos que:*

$$\frac{a}{b} \leq \frac{c}{d} \Leftrightarrow ad \leq bc.$$

Proposição 4.1.13. *A desigualdade $\leq$ define uma relação de ordem em $\mathbb{Q}$.*

Demonstração.

1. (Reflexiva)

   Para todo $\alpha \in \mathbb{Q}$, tem-se que $\alpha \leq \alpha$. De fato: seja $\alpha = \overline{(a, b)} \in \mathbb{Q}$, com $b > 0$. Sendo $a \in \mathbb{Z}$, então $a \leq a$, pois em $\mathbb{Z}$ vale a propriedade reflexiva. Sendo $b > 0$, então $ab \leq ab$. Da comutatividade em $\mathbb{Z}$, obtemos $ab \leq ba$. Portanto, $\alpha \leq \alpha$.

2. (Antissimétrica)

   Sejam $\alpha, \beta \in \mathbb{Q}$. Se $\alpha \leq \beta$ e $\beta \leq \alpha$, então $\alpha = \beta$. De fato: como $\alpha \leq \beta$, então $ad \leq bc$, e sendo $\beta \leq \alpha$, temos que $cb \leq da$, isto é, $bc \leq ad$. Portanto, $ad = bc$, ou seja, $\alpha = \beta$.

3. (Transitiva)

   Sejam $\alpha, \beta, \gamma \in \mathbb{Q}$. Se $\alpha \leq \beta$ e $\beta \leq \gamma$, então $\alpha \leq \gamma$. De fato: Sejam $\alpha = \overline{(a, b)}$, $\beta = \overline{(c, d)}$ e $\gamma = \overline{(e, f)}$, tais que $b, d, f > 0$. Como $\alpha \leq \beta$ e $\beta \leq \gamma$, então

$$ad \leq bc \tag{4.16}$$

   e

$$cf \leq de, \tag{4.17}$$

   Multiplicando a Inequação 4.16 por $f > 0$ e a Inequação 4.17 por $b > 0$, temos que

$$adf \leq bcf \tag{4.18}$$

   e

$$bcf \leq bde. \tag{4.19}$$

   Logo, das Inequações 4.18 e 4.19, da transitividade da relação $\leq$ em $\mathbb{Z}$ e da comutatividade, obtemos

$$afd \leq bed.$$

   Como $d \neq 0$, então pela lei do corte, temos que

$$af \leq be,$$

   ou seja, $\alpha \leq \gamma$.

$\square$

Proposição 4.1.14 (Tricotomia)**.**

Para quaisquer $\alpha, \beta \in \mathbb{Q}$, temos que uma, e apenas uma, das seguintes relações ocorre:

1. $\alpha < \beta$;

2. $\alpha = \beta$;

3. $\alpha > \beta$.

Demonstração.

Dados $\alpha, \beta \in \mathbb{Q}$, onde $\alpha = \dfrac{a}{b}$ e $\beta = \dfrac{c}{d}$, com $b, d > 0$. Note que, se $\alpha = \beta$, então $ad = bc$, ou, se $\alpha < \beta$, então $ad < bc$. E por fim, se $\alpha > \beta$, então $ad > bc$, e apenas uma delas pode ocorrer, devido a tricotomia em $\mathbb{Z}$. $\square$

Proposição 4.1.15. *Dados $\alpha, \beta, \gamma \in \mathbb{Q}$, se $\alpha \leq \beta$, então $\alpha + \gamma \leq \beta + \gamma$.*

Demonstração.

Sejam $\alpha, \beta, \gamma \in \mathbb{Q}$, com $\alpha = \dfrac{a}{b}$, $\beta = \dfrac{c}{d}$ e $\gamma = \dfrac{e}{f}$, onde $b, d, f > 0$. Então

$$\alpha + \gamma = \frac{a}{b} + \frac{e}{f} = \frac{af + be}{bf} \tag{4.20}$$

e

$$\beta + \alpha = \frac{c}{d} + \frac{a}{b} = \frac{cf + de}{df} \tag{4.21}$$

Dá hipótese temos que $ad \leq bc$. E multiplicando-se esta desigualdade por $f > 0$, obtemos consecutivamente as seguintes desigualdades

$$\begin{aligned} adf &\leq bcf \\ (af)d &\leq (bf)c \\ (af)d + (be)d &\leq (bf)c + (be)d \\ (af + be)d &\leq b(fc + ed) \end{aligned} \tag{4.22}$$

Multiplicando a Inequação 4.22 por $f > 0$ temos que

$$\begin{aligned} (af + be)df &\leq b(fc + ed)f \\ (af + be)df &\leq bf(fc + ed) \\ \frac{af + be}{bf} &\leq \frac{fc + ed}{df} \\ \alpha + \gamma &\leq \beta + \gamma. \end{aligned}$$

$\square$

Proposição 4.1.16. *Dados $\alpha, \beta, \gamma \in \mathbb{Q}$, se $\alpha \leq \beta$ e $\gamma \geq 0$, então $\alpha\gamma \leq \beta\gamma$.*

Demonstração.

Sejam $\alpha, \beta, \gamma \in \mathbb{Q}$, com $\alpha = \dfrac{a}{b}$, $\beta = \dfrac{c}{d}$ e $\gamma = \dfrac{e}{f}$, onde $b, d, f > 0$. Como $\alpha \leq \beta$, então

$$ad \leq bc. \tag{4.23}$$

Além disso, $\dfrac{e}{f} \geq 0 = \dfrac{0}{f}$, ou seja, $ef \geq f \cdot 0$. Sendo $f > 0$, então $e \geq 0$.

Multiplicando a Desigualdade 4.23 por e e em seguida por f, obtemos

$$\begin{array}{rcl} (ad)e & \leq & (bc)e \\ (ae)d & \leq & b(ce) \\ (ae)df & \leq & bf(ce) \\ \dfrac{ae}{bf} & \leq & \dfrac{ce}{df} \\ \dfrac{a}{b}\cdot\dfrac{e}{f} & \leq & \dfrac{c}{d}\cdot\dfrac{e}{f} \\ \alpha\cdot\gamma & \leq & \beta\cdot\gamma. \end{array}$$

□

4.1.4 IMERSÃO DOS INTEIROS NOS RACIONAIS

De modo análogo a imersão dos naturais nos inteiros, será apresentado aqui a imersão do conjunto dos números inteiros no conjunto dos números racionais. Portanto, teremos uma cópia dos inteiros nos racionais, com todas as propriedades preservadas. Os resultados aqui elencados podem ser encontrados em (MILIES, 2001).

Proposição 4.1.17. *O conjunto dos números inteiros $\mathbb{Z}$ é imerso no conjunto dos números racionais $\mathbb{Q}$.*

Demonstração.

Considere a seguinte aplicação:

$$\begin{array}{rcl} \phi:\mathbb{Z} & \to & \mathbb{Q} \\ a & \mapsto & \phi(a)=\dfrac{a}{1}, \end{array}$$

onde $a \in \mathbb{Z}$. Vamos provar que ϕ é uma aplicação injetora que preserva as operações de adição, multiplicação e relação de ordem em $\mathbb{Q}$.

1. ϕ está bem definida:

   Dados $a, b \in \mathbb{Z}$ tais que $a = b$, então

$$\begin{array}{rcl} \phi(a) & = & \dfrac{a}{1} \\ & = & a \\ & = & b \\ & = & \dfrac{b}{1} \\ & = & \phi(b). \end{array}$$

2. ϕ é uma aplicação injetiva:

Dados $a, b \in \mathbb{Z}$ tais que $\phi(a) = \phi(b)$, ou seja, $\frac{a}{1} = \frac{b}{1}$. Então

$$a \cdot 1 = 1 \cdot b,$$

isto é,

$$a = b.$$

3. a aplicação ϕ preserva a adição:

   Dados $a, b \in \mathbb{Z}$, então

$$\begin{aligned} \phi(a+b) &= \frac{a+b}{1} \\ &= \frac{a \cdot 1 + 1 \cdot b}{1 \cdot 1} \\ &= \frac{a}{1} + \frac{b}{1} \\ &= \phi(a) + \phi(b). \end{aligned}$$

4. a aplicação ϕ preserva a multiplicação:

   Dados $a, b \in \mathbb{Z}$, então

$$\begin{aligned} \phi(a \cdot b) &= \frac{a \cdot b}{1} \\ &= \frac{a \cdot b}{1 \cdot 1} \\ &= \frac{a}{1} \cdot \frac{b}{1} \\ &= \phi(a) + \phi(b). \end{aligned}$$

5. A aplicação ϕ preserva a ordem:

   Dados $a, b \in \mathbb{Z}$ com $a \leq b$, então $a \cdot 1 \leq 1 \cdot b$. Daí

$$\begin{aligned} \frac{a}{1} &\leq \frac{b}{1} \\ \phi(a) &\leq \phi(b). \end{aligned}$$

Portanto, temos que ϕ é uma imersão de $\mathbb{Z}$ em $\mathbb{Q}$. $\square$

Capítulo 5

NÚMEROS REAIS

Ao tentarmos encontrar a solução para a equação $x^2 = 2$, observamos que em $\mathbb{Q}$ não existe solução. Logo, para que exista solução para a equação mencionada acima, faz-se necessário a construção de um novo conjunto. Segundo Hefez (2016, p.145), na primeira metade do século XIX, Cantor e Dedekind apresentaram duas construções diferentes dos números reais. Neste capítulo, tomando como base a referência (HEFEZ, 2016), apresentaremos a construção desenvolvida por Cantor.

5.1 O ANEL DAS SEQUÊNCIAS

Neste tópico, será abordado alguns resultados sobre sequências convergentes em um corpo ordenado $\mathcal{K}$, afim de obter elementos suficientes para a construção dos números reais.

5.1.1 SEQUÊNCIAS EM $S(\mathcal{K})$

Definição 5.1.1. *Uma sequência em um corpo $\mathcal{K}$ é uma aplicação $x : \mathbb{N} \longrightarrow \mathcal{K}$ que associa cada $n \in \mathbb{N}$ um elemento $x(n) := x_n$.*

Definição 5.1.2. *O conjunto das sequências em um corpo $\mathcal{K}$ é denotado por $S(\mathcal{K})$, onde as operações de adição e multiplicação são dadas por*

$$(x_n) + (y_n) = (x_n + y_n) \qquad e \qquad (x_n) \cdot (y_n) = (x_n \cdot y_n),$$

para quaisquer (x_n), $(y_n) \in \mathcal{S}(\mathcal{K})$.

Observação 5.1.1. *Será utilizada a seguinte notação:*

$$\mathcal{K}_+^* = \{x \in \mathcal{K} \ ; \ x > 0\}.$$

Proposição 5.1.1. *O conjunto das sequências em um corpo $\mathcal{K}$, denotado por $S(\mathcal{K})$ é um anel comutativo com unidade.*

Demonstração.

Sejam $(x_n), (y_n), (z_n) \in S(\mathcal{K})$. Para mostrar que $S(\mathcal{K})$ é um anel, faremos a verificação das seguintes propriedades:

P1) (Associatividade da adição)

$$\begin{aligned} (x_n) + [(y_n) + (z_n)] &= (x_n) + (y_n + z_n) \\ &= (x_n + y_n + z_n) \\ &= (x_n + y_n) + (z_n) \\ &= [(x_n) + (y_n)] + (z_n). \end{aligned}$$

P2) (Existência de um elemento neutro aditivo)

$$\begin{aligned} (x_n) + 0 &= (x_n + 0) \\ &= (0 + x_n) \\ &= 0 + (x_n) \\ &= (x_n). \end{aligned}$$

P3) (Existência de um inverso aditivo)

$$\begin{aligned} (x_n) + (-x_n) &= (x_n + (-x_n)) \\ &= 0. \end{aligned}$$

P4) (Comutatividade da adição)

$$\begin{aligned} (x_n) + (y_n) &= (x_n + y_n) \\ &= (y_n + x_n) \\ &= (y_n) + (x_n). \end{aligned}$$

P5) (Associatividade da multiplicação)

$$\begin{aligned} (x_n) \cdot [(y_n \cdot z_n)] &= (x_n) \cdot (y_n \cdot z_n) \\ &= (x_n \cdot y_n \cdot z_n) \\ &= (x_n \cdot y_n) \cdot (z_n) \\ &= [(x_n) \cdot (y_n)] \cdot (z_n). \end{aligned}$$

P6) (Comutatividade da multiplicação)

$$\begin{aligned}(x_n)\cdot(y_n) &= (x_n\cdot y_n)\\ &= (y_n\cdot x_n)\\ &= (y_n)\cdot(x_n).\end{aligned}$$

P7) (Distributividade)

$$\begin{aligned}(x_n)\cdot[(y_n)+(z_n)] &= (x_n)\cdot(y_n+z_n)\\ &= (x_n\cdot(y_n+z_n))\\ &= (x_n\cdot y_n + x_n\cdot z_n)\\ &= (x_n\cdot y_n)+(x_n\cdot z_n)\\ &= (x_n)\cdot(y_n)+(x_n)\cdot(z_n).\end{aligned}$$

P8) (Existência de um elemento neutro multiplicativo)

$$\begin{aligned}(x_n)\cdot 1 &= (x_n\cdot 1)\\ &= (x_n).\end{aligned}$$

Portanto concluímos que $S(\mathcal{K})$ é um anel comutativo com unidade. □

5.1.2 ANEL DAS SEQUÊNCIAS CONVERGENTES $S_c(\mathcal{K})$

Neste tópico, faremos o uso dos resultados elencados no Capitulo 1. Mais precisamente, veremos que existe um ideal de $S_c(\mathcal{K})$ que possibilitará a construção de um anel quociente, que atráves do teorema do isomorfismo, será isomorfo a $\mathcal{K}$, obtendo assim um importante resultado na construção do corpo dos números reais. Esta subseção tem como referência (HEFEZ, 2016).

Definição 5.1.3. *Uma sequência $(x_n)\in S(\mathcal{K})$ será dita convergente em $\mathcal{K}$ quando existir um elemento $x\in\mathcal{K}$ tal que, para todo $\varepsilon\in\mathcal{K}^*_+$, existe $N\in\mathbb{N}$ com a seguinte propriedade:*

$$\mid x_n - x \mid < \varepsilon, \quad \forall n > N.$$

Um elemento x como acima, se existir, será chamado de limite da sequência (x_n). Neste caso, é dito também que a sequência (x_n) converge para x.

Proposição 5.1.2. *Uma sequência convergente possui um único limite.*

Demonstração.

Suponha por absurdo, que x e y sejam dois limites distintos de uma sequência (x_n). Logo, dado $\varepsilon = \frac{1}{2} \mid y - x \mid > 0$, pela definição de convergência, existem N_1 e N_2 em $\mathbb{N}$ tais que

$$\mid x_n - x \mid < \varepsilon, \ \forall n > N_1 \qquad e \qquad \mid x_n - y \mid < \varepsilon, \ \forall n > N_2.$$

Tomando $N > max\{N_1, N_2\}$, temos que
$\mid y - x \mid = \mid x_n - x + y - x_n \mid \leq \ \mid x_n - x \mid + \mid x_n - y \mid < 2\varepsilon \ = \mid y - x \mid$, o que é um absurdo. □

No caso em que (x_n) é uma sequência cujo limite é x, escrevemos:

$$lim \ x_n = x.$$

Será denotado por $S_c(\mathcal{K})$ o subconjunto de $S(\mathcal{K})$ das sequências convergentes. A proposição anterior garante que a aplicação a seguir está bem definida.

$$\begin{aligned} lim : S_c(\mathcal{K}) &\to \mathcal{K} \\ (x_n) &\mapsto lim(x_n) := lim \ x_n. \end{aligned}$$

Uma sequência que não é convergente será dita divergente.

Definição 5.1.4. *Se $x \in \mathcal{K}$, uma sequência (x_n) é dita constante se $x_n = x$, para todo $n \in \mathbb{N}$. É claro que*

$$lim \ x_n = x.$$

Definição 5.1.5. *Uma sequência $(x_n) \in S(\mathcal{K})$ será dita limitada superiormente (respectivamente, limitada inferiormente) se existir $L \in \mathcal{K}$ tal que para todo $n \in \mathbb{N}$ se tenha $x_n \leq L$ (respectivamente $x_n \geq L$). Uma sequência limitada superiormente e inferiormente será dita limitada.*
Decorre da definição que (x_n) é limitada se, e somente se, existe $B \in \mathcal{K}_+^*$ tal que

$$\mid x_n \mid \leq B \quad \forall n \in \mathbb{N}.$$

O subconjunto de $S(\mathcal{K})$ das sequências limitadas, é denotado por $S_l(\mathcal{K})$.

Proposição 5.1.3. *Toda sequência convergente é limitada.*

Demonstração.
Suponha que $lim \ x_n = x$. Dado $\varepsilon = 1$, existe um número natural N tal que se $n > N$, então $\mid x_n - x \mid < 1$. Como $\mid x_n \mid - \mid x \mid \leq \mid x_n - x \mid$, temos que se $n > N$, então $\mid x_n - x \mid < 1$, consequentemente $\mid x_n \mid < 1 + \mid x \mid$. Pondo

$$B = max\{\mid x_0 \mid, \ldots, \mid x_n \mid, \ 1+ \mid x \mid\},$$

temos, para todo n $\in \mathbb{N}$, que $\mid x_n \mid \leq B$. Portanto, (x_n) é limitada. □

Proposição 5.1.4. *Sejam* $(x_n), (y_n) \in S_c(\mathcal{K})$. *Então* $(x_n)+(y_n)$ *e* $(x_n)-(y_n)$ *pertencem a* $S_c(\mathcal{K})$ *e*

$$lim\ (x_n \pm y_n) = lim\ (x_n) \pm lim\ (y_n).$$

Demonstração.

Suponha que $lim\ (x_n) = x$ e $lim\ (y_n) = y$. Dado $\varepsilon \in \mathcal{K}_+^*$, existem N_1 e $N_2 \in \mathbb{N}$ tais que

$$| x_n - x | < \frac{\varepsilon}{2}, \qquad \forall n > N_1$$

e

$$| y_n - y | < \frac{\varepsilon}{2}, \qquad \forall n > N_2.$$

Seja $N = max\{N_1, N_2\}$. Logo, se $n > N$, temos que

$$| x_n \pm y_n - (x \pm y) | = | (x_n - x) \pm (y_n - y) | \leq | x_n - x | + | y_n - y | < \frac{\varepsilon}{2} + \frac{\varepsilon}{2} = \varepsilon.$$

Portanto,

$$lim\ (x_n \pm y_n) = x \pm y = lim\ x_n \pm \lim\ y_n = lim\ (x_n) \pm \lim\ (y_n).$$

□

Definição 5.1.6. *Uma sequência* $(x_n) \in S_c(\mathcal{K})$ *é dita nula, se*

$$lim\ x_n = 0,$$

isto é, se ela converge para zero.

Corolário 5.1.1. *Se* $(x_n), (y_n) \in S_c(\mathcal{K})$ *e* $lim\ x_n = lim\ y_n$, *então* $(x_n - y_n)$ *é uma sequência nula.*

Denota-se por $S_0(\mathcal{K})$ o subconjunto de $S_c(\mathcal{K})$ das sequências nulas, isto é, das sequências que convergem para zero.

Proposição 5.1.5. *Sejam* $(x_n), (y_n) \in S(\mathcal{K})$. *Se* (x_n) *é limitada e* (y_n) *é uma sequência nula, então* $(x_n \cdot y_n)$ *é uma sequência nula.*

Demonstração.

Como (x_n) é limitada, existe $B \in \mathcal{K}_+^*$ tal que $| x_n | \leq B$, para todo $n \in \mathbb{N}$. Como $lim\ y_n = 0$, temos que dado $\varepsilon \in \mathcal{K}_+^*$, existe $N \in \mathbb{N}$ tal que

$$| y_n | = | y_n - 0 | < \frac{\varepsilon}{B}, \qquad \forall n > N.$$

Portanto, para $n > N$, temos que

$$| x_n \cdot y_n - 0 | = | x_n | \cdot | y_n | < B \cdot \frac{\varepsilon}{B} = \varepsilon,$$

provando assim o resultado. □

Proposição 5.1.6. *Sejam $(x_n), (y_n) \in S(\mathcal{K})$. Se (x_n) e (y_n) são convergentes, então $(x_n) \cdot (y_n)$ é convergente e*

$$lim\ (x_n \cdot y_n) = lim\ (x_n) \cdot lim\ (y_n).$$

Demonstração.

Suponha que $lim\ x_n = x$ e $lim\ y_n = y$. Vamos mostrar que a sequência $(x_n \cdot y_n) - (x \cdot y)$ converge para zero. De fato, como (y_n) é convergente, pela Proposição 5.1.3 ela é limitada. Por outro lado, a sequência $(x_n - x)$ converge para zero. Portanto, pela Proposição 5.1.5 tem-se que

$$lim\ (x_n - x) \cdot (y_n) = 0$$

De modo análogo, conclui-se que

$$lim\ x \cdot (y_n - y) = 0$$

Utilizando as duas igualdades acima e a Proposição 5.1.4, obtemos

$$\begin{aligned} 0 &= lim\ (x_n - x) \cdot (y_n) + lim\ x \cdot (y_n - y) \\ &= lim\ [(x_n - x) \cdot (y_n) + x \cdot (y_n - y)] \\ &= lim\ [(x_n) \cdot (y_n) - x \cdot (y_n) + x \cdot (y_n) - x \cdot y] \\ &= lim\ [(x_n) \cdot (y_n) - x \cdot y]. \end{aligned}$$

Portanto, segue que

$$lim\ [(x_n) \cdot (y_n) - x \cdot y] = 0.$$

□

Teorema 5.1.1. *O conjunto $S_c(\mathcal{K})$ é um subanel de $S(\mathcal{K})$.*

Demonstração.

1. Sejam $x_n = 0$ e $y_n = 1$, $\forall n \in \mathbb{N}$. Então, $(x_n), (y_n) \in S_c(\mathcal{K})$, pois $lim\ x_n = 0$ e $lim\ y_n = 1$. Portanto, $S_c(\mathcal{K}) \neq \emptyset$.

2. Sejam $(x_n), (y_n) \in S_c(\mathcal{K})$, então existem $a \in \mathcal{K}$ e $b \in \mathcal{K}$ tais que $lim\ x_n = a$ e $lim\ y_n = b$. Pelas Proposições 5.1.4 e 5.1.6 tem-se que

   (a) $lim\ (x_n - y_n) = lim\ x_n - lim\ y_n = a - b \in \mathcal{K}$. Portanto, $(x_n - y_n) \in S_c(\mathcal{K})$.

   (b) $lim\ (x_n \cdot y_n) = lim\ x_n \cdot lim\ y_n = a \cdot b \in \mathcal{K}$. Logo, $(x_n \cdot y_n) \in S_c(\mathcal{K})$.

De 1 e 2, segue que $S_c(\mathcal{K})$ é um subanel de $S(\mathcal{K})$. Além disso, $S_c(\mathcal{K})$ é um anel comutativo com unidade. □

Proposição 5.1.7. *A aplicação $lim : S_c(\mathcal{K}) \to \mathcal{K}$:*

1. *É um homomorfismo sobrejetor de anéis;*

2. $N(lim) = S_0(\mathcal{K})$.

Demonstração.

1. Dados $(x_n), (y_n) \in S_c(\mathcal{K})$ temos que

   (a) $lim\ ((x_n)) + lim\ ((y_n)) = lim\ x_n + lim\ y_n = lim\ (x_n + y_n) = lim\ ((x_n + y_n)) = lim\ ((x_n) + (y_n))$.

   (b) $lim\ ((x_n)) \cdot lim\ ((y_n)) = lim\ x_n \cdot lim\ y_n = lim\ (x_n \cdot y_n) = lim\ ((x_n \cdot y_n)) = lim\ ((x_n) \cdot (y_n))$.

   (c) Dado $a \in \mathcal{K}$, considere a sequência $x_n = a$, $\forall n \in \mathbb{N}$. Então,

   $$lim\ ((x_n)) = lim\ x_n = lim\ a = a.$$

2. $N(lim) = S_0(\mathcal{K})$.
   Como $N(lim) = \{(x_n) \in S_c(\mathcal{K})\ ;\ lim\ (x_n) = 0\}$, segue que

   $$\forall (x_n) \in N(lim) \Leftrightarrow lim\ x_n = lim\,(x_n) = 0 \Leftrightarrow (x_n) \in S_0(\mathcal{K}).$$

□

Proposição 5.1.8. *O conjunto $S_0(\mathcal{K})$ das sequências nulas é um ideal do anel $S_c(\mathcal{K})$, das sequências convergentes.*

Demonstração.

1. $S_0(\mathcal{K})$ é um subanel de $S_c(\mathcal{K})$.

   (a) Seja $x_n = 0, \forall n \in \mathbb{N}$, então $lim\ x_n = 0$. Portanto, $(x_n) \in S_0(\mathcal{K})$, ou seja, $0 \in S_0(\mathcal{K})$.

   (b) Sejam $(x_n), (y_n) \in S_0(\mathcal{K})$, então $lim\ x_n = lim\ y_n = 0$. Daí,

      i. $0 = lim\ x_n - lim\ y_n = lim\ (x_n - y_n)$. Logo, $(x_n - y_n) \in S_0(\mathcal{K})$.

      ii. $0 = lim\ x_n \cdot lim\ y_n = lim\ (x_n \cdot y_n)$. Portanto, $(x_n \cdot y_n) \in S_0(\mathcal{K})$.

2. Sejam $(x_n) \in S_0(\mathcal{K})$ e $(y_n) \in S_c(\mathcal{K})$, então $(x_n) \cdot (y_n) \in S_0(\mathcal{K})$.

   (a) Como $(x_n) \in S_0(\mathcal{K})$, então $lim\ x_n = 0$. Por outro lado, $(y_n) \in S_c(\mathcal{K})$, então pela Proposição 5.1.3, (y_n) é limitada. Logo, pela Proposição 5.1.5, temos que

   $$0 = lim\ x_n \cdot lim\ y_n = lim\ (x_n \cdot y_n).$$

   Logo, $(x_n \cdot y_n) \in S_0(\mathcal{K})$, isto é, $(x_n) \cdot (y_n) \in S_0(\mathcal{K})$.

Portanto, de 1 e 2, segue que $S_0(\mathcal{K})$ é um ideal do anel $S_c(\mathcal{K})$ das sequências convergentes. $\square$

Proposição 5.1.9. *Os anéis $S_c(\mathcal{K})/S_0(\mathcal{K})$ e $\mathcal{K}$ são isomorfos.*

Demonstração.
Pela Proposição 5.1.8 temos que $S_c(\mathcal{K})/S_0(\mathcal{K})$ é um anel, e pela Proposição 5.1.7 a aplicação $lim : S_c(\mathcal{K}) \to \mathcal{K}$ é um homomorfismo sobrejetor de anéis cujo núcleo é $S_0(\mathcal{K})$. Portanto, pelo Teorema do isomorfismo temos que $S_c(\mathcal{K})/S_0(\mathcal{K})$ e $\mathcal{K}$ são isomorfos. $\square$

5.1.3 CORPOS ARQUIMEDIANOS

Nesta subseção, serão apresentados algumas definições e propriedades que serão utilizadas posteriormente. Os resultados aqui apresentados encontram-se em (HEFEZ, 2016).

Definição 5.1.7. *Um corpo ordenado $\mathcal{K}$ é arquimediano, se para quaisquer $a, b \in \mathcal{K}$, com $a > 0$, existe $n \in \mathbb{N}$ tal que $n \cdot a > b$.*

Exemplo 5.1.1. *O corpo $\mathbb{Q}$ dos números racionais é arquimediano.*

Demonstração.
Suponha que existam $a, b \in \mathbb{Q}$ com $a > 0$ tal que para todo $n \in \mathbb{N}$ tem-se que

$$n \cdot a \leq b.$$

Ou seja,

$$b - n \cdot a \geq 0.$$

Seja $S = \{b - n \cdot a \ ; \ n \in \mathbb{N}, n > 0\}$. É claro que $S \neq \emptyset$. Como S é limitado inferiormente, pelo príncipio da boa ordenação existe $m = minS$, e como $m \in S$, existe $r > 0$, $r \in \mathbb{N}$ tal que $m = b - r \cdot a$. Seja $m' = b - (r+1) \cdot a \in S$, então

$$m' = b - (r+1) \cdot a = b - r \cdot a - a = (b - r \cdot a) - a = m - a < m,$$

pois $a > 0$, o que é um absurdo, pois $m = minS$. Portanto, $\mathbb{Q}$ é um corpo arquimediano. $\square$

Definição 5.1.8. *Um subcorpo primo de um corpo $\mathcal{K}$ é a interseção de todos os subcorpos de $\mathcal{K}$.*

Proposição 5.1.10. *Sejam $\mathcal{K}$ um corpo ordenado e $\mathcal{K}_0$ o seu corpo primo. As asserções abaixo são equivalentes.*

1. *$\mathcal{K}$ é arquimediano;*

2. *Dados $a, b \in \mathcal{K}$, quaisquer, com $a < b$, existe $r \in \mathcal{K}_0$ tal que*

$$a < r < b;$$

3. *Todo elemento de $\mathcal{K}$ é limite de uma sequência em $\mathcal{K}_0$.*

Demonstração.

1. $(1 \Rightarrow 2)$. Sejam $a, b \in \mathcal{K}$ com $a < b$, ou seja $b - a > 0$. Pela definição de corpo arquimediano, existe $n \in \mathbb{N}$, tal que $n \cdot (b - a) > 1$. Daí,

$$b - a > \frac{1}{n \cdot 1} \cdot$$

Por outro lado, seja $S = \{x \in \mathbb{N}\, ; x \cdot 1 > n \cdot a\}$. Como S é limitado inferiormente, pelo princípio da boa ordenação existe $m \in S$ tal que $m = min\ S$. Então $m - 1 \notin S$, ou seja, $(m - 1) \cdot 1 \leqslant n \cdot a$, isto é,

$$\frac{(m-1) \cdot 1}{n \cdot 1} \leqslant a.$$

Como $m \in S$, segue que

$$a < \frac{m \cdot 1}{n \cdot 1} = \frac{(m-1) \cdot 1}{n \cdot 1} + \frac{1}{n \cdot 1} < a + (b - a) = b.$$

Tomando $r = \dfrac{m \cdot 1}{n \cdot 1}$, temos que $a < r < b$. E como $\dfrac{m}{n} \in \mathbb{Q}$ que é isomorfo a $\mathcal{K}_0$, então $\dfrac{m \cdot 1}{n \cdot 1} \in \mathcal{K}_0$, ou seja, $r \in \mathcal{K}_0$.

2. $(2 \Rightarrow 3)$. Seja $a \in \mathcal{K}$. Para cada $n \in \mathbb{N} \setminus \{0\}$, pela hipótese 2 existe $(r_n) \in \mathcal{K}_0$ tal que

$$a - \frac{1}{n \cdot 1} < r_n < a + \frac{1}{n \cdot 1} \cdot$$

Aplicando o limite na desigualdade acima, obtemos

$$lim \left(a - \frac{1}{n \cdot 1}\right) \leq\ lim\ r_n\ \leq lim\ \left(a + \frac{1}{n \cdot 1}\right).$$

Como $lim \left(a - \dfrac{1}{n \cdot 1}\right) = a$ e $lim \left(a + \dfrac{1}{n \cdot 1}\right) = a$, resulta que, $lim\ r_n = a$.

3. $(3 \Rightarrow 1)$ Dado $a \in \mathcal{K}$, devemos mostrar que existe $m \in \mathbb{N}$, tal que $m \cdot 1 > a$. Como $a \in \mathcal{K}$, pela hipótese 3, existe uma sequência (r_n) em $\mathcal{K}_0$ tal que

$$lim\ r_n = a.$$

Seja $S_n = r_n + 1 \in \mathcal{K}_0$. Então,

$$lim\ S_n = lim\ (r_n + 1) = lim\ r_n + lim\ 1 = a + 1.$$

Tomando $\varepsilon = \dfrac{1}{2}$, existe $N \in \mathbb{N}$ tal que,

$$\mid S_n - (a+1) \mid < \frac{1}{2}, \quad \forall n > N,$$

isto é,

$$(a+1) - \frac{1}{2} < S_n < (a+1) + \frac{1}{2},$$

ou seja,

$$S_n > (a+1) - \frac{1}{2} = a + \frac{1}{2} > a.$$

Em particular, a desiguldade vale para N+1, ou seja,

$$S_N + 1 > a.$$

Como $\mathcal{K}_0$ é arquimediano, pois $\mathcal{K}_0$ é isomorfo a $\mathbb{Q}$, e $S_N + 1, 1 \in \mathcal{K}_0$, então existe $m \in \mathbb{N}$ tal que

$$m \cdot 1 > S_N + 1 > a.$$

Portanto $m \cdot 1 > a$.

□

5.1.4 ANEL DAS SEQUÊNCIAS DE CAUCHY $S_f(\mathcal{K})$

Neste tópico, veremos como se dá a extensão do corpo $S_c(\mathcal{K})/S_0(\mathcal{K})$. Para isso, utilizaremos os resultados aqui elencados sobre sequências de Cauchy, juntamente com as propriedades elementares sobre anéis abordadas no Capítulo 1. Esta subseção está baseada na referência (HEFEZ, 2016).

Definição 5.1.9. *Seja $\mathcal{K}$ um corpo ordenado. Uma sequência (x_n) será chamada de sequência de Cauchy ou sequência fundamental em $\mathcal{K}$, se para todo $\varepsilon \in \mathcal{K}_+^*$ existe $N \in \mathbb{N}$ tal que para todo $m, n \in \mathbb{N}$, com $m, n > N$, se tenha*

$$\mid x_m - x_n \mid < \varepsilon.$$

Proposição 5.1.11. *Toda sequência convergente é de Cauchy.*

Demonstração.

Seja $(x_n) \in S(\mathcal{K})$ e suponha que $lim\ x_n = x$. Dado $\varepsilon \in \mathcal{K}_+^*$, existe $N \in \mathbb{N}$, tal que se $n > N$ então

$$\mid x_n - x \mid < \frac{\varepsilon}{2}.$$

Segue-se que, se $m, n > N$, então

$$\mid x_m - x_n \mid = \mid x_m - x - (x_n - x) \mid \leqslant \mid x_m - x \mid + \mid x_n - x \mid < \frac{\varepsilon}{2} + \frac{\varepsilon}{2} = \varepsilon.$$

Portanto, (x_n) é uma sequência de Cauchy. $\square$

Proposição 5.1.12. *Toda sequência monótona crescente e limitada em um corpo arquimediano é de Cauchy.*

Demonstração.

Seja $(x_n) \in S(\mathcal{K})$ uma sequência monótona crescente e limitada superiormente, onde $\mathcal{K}$ é arquimediano. Seja $c \in \mathcal{K}$ tal que,

$$x_n \leqslant c, \ \ \forall n \in \mathbb{N}.$$

Seja $\varepsilon \in \mathcal{K}_+^*$, considere o seguinte conjunto:

$$\text{S} = \{z \in \mathbb{N} \ ; \ z \cdot 1 \leqslant \frac{c - x_n}{\varepsilon}, \ \forall n \in \mathbb{N}\}.$$

S é limitado superiormente. De fato, considere o elemento $\dfrac{c - x_1}{\varepsilon}$, como $1 \in \mathcal{K}$ e $\mathcal{K}$ é arquimediano, existe $l \in \mathbb{N}$ tal que $l \cdot 1 > \dfrac{c - x_1}{\varepsilon}$. Daí resulta que para todo $k \geq l$ tem-se que k $\notin$ S, pois

$$k \geq l = l \cdot 1 > \frac{c - x_1}{\varepsilon}.$$

Como $x_n \leqslant c$, então

$$\begin{aligned} 0 &\leq c - x_n \\ 0 \cdot \varepsilon &\leq c - x_n. \end{aligned}$$

Como $\varepsilon \in \mathcal{K}_+^*$, existe $\varepsilon^{-1} \in \mathcal{K}_+^*$ tal que $\varepsilon^{-1} \cdot \varepsilon = \varepsilon \cdot \varepsilon^{-1} = 1$. Então

$$\begin{aligned} (0 \cdot \varepsilon) \cdot \varepsilon^{-1} &\leq (c - x_n) \cdot \varepsilon^{-1} \\ 0 \cdot (\varepsilon \cdot \varepsilon^{-1}) &\leq (c - x_n) \cdot \frac{1}{\varepsilon} \\ 0 \cdot 1 &\leq \frac{c - x_n}{\varepsilon} \cdot \end{aligned}$$

Portanto, $0 \in S$. Como $0 \in S$, obtemos que $S \neq \emptyset$ e, sendo S limitado superiormente, temos pelo principio da boa ordenação que S possui um maior elemento que denotaremos por r. Como $r \in \mathrm{S}$ e $r+1 \notin S$ temos que

$$r \cdot \varepsilon \ \leq \ c - x_n, \ \ \forall n \in \mathbb{N}, \tag{5.1}$$

e existe $N \in \mathbb{N}$ tal que

$$c - x_N \ < \ (r+1) \cdot \varepsilon. \tag{5.2}$$

De 5.1 e 5.2, segue que

$$c - x_N < (r+1) \cdot \varepsilon = r \cdot \varepsilon + \varepsilon \ \leq \ c - x_n + \varepsilon, \quad \forall n \in \mathbb{N}.$$

Dados $m, n \in \mathbb{N}$ tais que $n \geq m > N$. Como (x_n) é uma sequência crescente, então $x_n \geq x_m > x_N$. Observe que:

$$\begin{aligned}
x_n &\geq x_m \\
x_n + (-x_n) &\geq x_m + (-x_n) \\
0 &\geq x_m + (-x_n) \\
-x_m + 0 &\geq x_m + (-x_m) + (-x_n) \\
-x_m &\geq 0 + (-x_n) \\
-x_m &\geq -x_n.
\end{aligned}$$

De modo análogo, $-x_N > -x_m$, portanto $-x_N > -x_m \geq -x_n$, isto é,

$$\begin{aligned}
-x_N > -x_m &\geq -x_n \\
-x_N + c > -x_m + c &\geq -x_n + c \\
c - x_N > c - x_m &\geq c - x_n.
\end{aligned}$$

Como $r \cdot \varepsilon \leq c - x_n$, então $\varepsilon \cdot (r+1) \leq c - x_n + \varepsilon$, daí

$$\begin{aligned}
c - x_m < c - x_N &< c - x_n + \varepsilon \\
c - x_m &< c - x_n + \varepsilon \\
x_n - x_m &< \varepsilon.
\end{aligned}$$

Logo,

$$|\, x_n - x_m \,| = |\, x_m - x_n \,| = \ x_m - x_n < \varepsilon.$$

Portanto, a sequência (x_n) é uma sequência de Cauchy em $\mathcal{K}$. $\square$

Exemplo 5.1.2. *A sequências (r_n), definida recorrentemente como,*

$$r_1 = 1, \qquad r_{n+1} = \frac{4 \cdot r_n}{2 + r_n^2}, \qquad \forall n \geq 1.$$

é um exemplo de sequência de Cauchy em um corpo arquimediano $\mathcal{K}$.

Lema 5.1.1. *Para todo $n \in \mathbb{N} \setminus \{0\}$, temos que $r_n^2 < 2$ e $r_n \geq 1$.*

Demonstração.

Vamos usar indução sobre n. Para $n = 1$, tem-se que $r_1 = 1$ e

$$r_1^2 = r_1 \cdot r_1 = 1 \cdot 1 = 1 < 2.$$

Portanto o resultado vale para n=1. Agora, suponha que o resultado vale para $n = k \in \mathbb{N}$, ou seja,

$$r_k^2 < 2 \text{ e } r_k \geq 1.$$

Queremos mostrar que vale para $n = k + 1$, ou seja,

$$r_{k+1}^2 = \frac{16 \cdot r_k^2}{(2 + r_k^2)^2} = \frac{16 \cdot r_k^2}{(2 - r_k^2) + 8 \cdot r_k^2} < \frac{16 \cdot r_k^2}{8 \cdot r_k^2} = 2, \quad \text{pois } (2 - r_k^2) > 0,$$

e

$$r_{k+1} = \frac{4 \cdot r_k}{(2 + r_k^2)} \geq \frac{4}{2 + 2} = 1, \text{ pois } r_k \geq 1 \text{ e } r_k^2 < 2.$$

□

Proposição 5.1.13. *A sequência (r_n) é de Cauchy.*

Demonstração.

1. (r_n) é limitada superiormente. De fato, pelo Lema 5.1.1 temos que

   $$r_n^2 < 2 < 4,$$

   ou seja,

   $$1 \leq r_n < 2.$$

   Portanto, (r_n) é limitada.

2. (r_n) é uma sequência monótona crescente. De fato, note que

   $$r_{n+1} - r_n = \frac{4 \cdot r_n}{2 + r_n^2} - r_n = \frac{4 \cdot r_n - r_n \cdot (2 + r_n^2)}{2 + r_n^2} = \frac{2 \cdot r_n - r_n^3}{2 + r_n^2} = \frac{r_n \cdot (2 - r_n^2)}{2 + r_n^2} > 0,$$

   pois $r_n^2 < 2$ e $r_n \geq 1, \forall n \geq 1$. Portanto, (r_n) é uma sequência monótona crescente.

Logo, pela Proposição 5.1.12, temos que (r_n) é uma sequência de Cauchy. □

Proposição 5.1.14. *A sequência (r_n) não é convergente em $\mathbb{Q}$.*

Demonstração.

Suponha que (r_n) seja convergente em $\mathbb{Q}$, então

$$lim\ r_n = \alpha \in \mathbb{Q}.$$

Segue que

$$\begin{aligned} lim\ 4 \cdot r_n &= lim\ [r_{n+1} \cdot (2 + r_n^2)] \\ &= lim\ r_{n+1} \cdot lim\ (2 + r_n^2) \\ &= \alpha \cdot (2 + \alpha^2), \end{aligned}$$

ou seja,

$$4 \cdot \alpha = \alpha \cdot (2 + \alpha^2). \tag{5.3}$$

Como $r_n \geq 1$, então $\alpha = lim\ r_n \geq 1$, ou seja, $\alpha \neq 0$. Logo, existe $\alpha^{-1} \in \mathbb{Q}$ tal que $\alpha \cdot \alpha^{-1} = 1$. Portanto, de (5.3), obtemos:

$$\begin{aligned} 2 + \alpha^2 &= 4 \\ \alpha^2 &= 2. \end{aligned}$$

Absurdo, pois não existe $\alpha \in \mathbb{Q}$ tal que $\alpha^2 = 2$ □

O objetivo é ampliar o corpo $\mathbb{Q}$ de modo que a sequência (r_n) passe a ter limite, obtendo assim um corpo contendo $\sqrt{2}$.

Proposição 5.1.15. *Toda sequência de Cauchy é limitada.*

Demonstração.

Seja (x_n) uma sequência de Cauchy. Dado $\varepsilon = 1$, existe $N \in \mathbb{N}$ tal que, para todo $n > N$, tem-se que

$$\mid x_n \mid - \mid x_{N+1} \mid \leq \mid x_n - x_{N+1} \mid < 1.$$

Logo,

$$\mid x_n \mid < \ 1 + \mid x_{N+1} \mid, \quad \forall n > N.$$

Tomando $B = max\,\{\mid x_0 \mid, ..., \mid x_N \mid, 1 + \mid x_{N+1} \mid\}$, segue-se que

$$\mid x_n \mid \leq B, \quad \forall n \in \mathbb{N}.$$

Portanto, (x_n) é limitada. □

O conjunto das sequências de Cauchy em um corpo $\mathcal{K}$ será denotado por $S_f(\mathcal{K})$.

Proposição 5.1.16. *O conjunto $S_f(\mathcal{K})$ é um subanel comutativo com unidade de $S(\mathcal{K})$.*

Demonstração.

1. Sejam $x_n = 1$ e $y_n = 0$, $\forall n \in \mathbb{N}$. Como $lim\ x_n = 1$ e $lim\ y_n = 0$, tem-se que $(x_n), (y_n) \in S_c(\mathcal{K})$, e pela Proposição 5.1.11, $(x_n), (y_n) \in S_f(\mathcal{K})$, ou seja, $0, 1 \in S_f(\mathcal{K})$.

2. Sejam $(x_n), (y_n) \in S_f(\mathcal{K})$. Dado $\varepsilon \in \mathcal{K}_+^*$, existe $N \in \mathbb{N}$ tal que se $m, n > N$, então
$$| x_m - x_n | < \frac{\varepsilon}{2} \quad \text{e} \quad | y_m - y_n | < \frac{\varepsilon}{2}.$$
Logo, se $m, n > N$ tem-se que
$$\begin{aligned} | x_m - y_m - (x_n - y_n) | &= | (x_m - x_n) + (y_n - y_m) | \\ &\leq | x_m - x_n | + | y_m - y_n | \\ &< \frac{\varepsilon}{2} + \frac{\varepsilon}{2} = \varepsilon. \end{aligned}$$
Portanto, $(x_n - y_n) \in S_f(\mathcal{K})$.

3. Sejam $(x_n), (y_n) \in S_f(\mathcal{K})$. Pela Proposição 5.1.15, as sequências (x_n) e (y_n) são limitadas, então existe $B \in \mathcal{K}_+^*$ tal que
$$| x_n | \leq B \quad \text{e} \quad | y_n | \leq B, \ \forall n \in \mathbb{N}.$$
Dado $\varepsilon \in \mathcal{K}_+^*$, existe $N \in \mathbb{N}$ tal que se $m, n > N$, então
$$| x_m - x_n | < \frac{\varepsilon}{2\,B} \quad \text{e} \quad | y_m - y_n | < \frac{\varepsilon}{2\,B}.$$
Segue-se que se $m, n > N$, então
$$\begin{aligned} | x_m \cdot y_m - x_n \cdot y_n | &= | x_m \cdot (y_m - y_n) + y_n \cdot (x_m - x_n) | \\ &\leq | x_m | \cdot | y_m - y_n | + | y_n | \cdot | x_m - x_n | \\ &< B \cdot \frac{\varepsilon}{2\,B} + B \cdot \frac{\varepsilon}{2\,B} = \varepsilon. \end{aligned}$$
Portanto, $(x_n \cdot y_n) \in S_f(\mathcal{K})$.

4. Como $S(\mathcal{K})$ é um anel comutativo, $S_f(\mathcal{K}) \subset S(\mathcal{K})$ e a operação produto é fechada em $S_f(\mathcal{K})$, então $S_f(\mathcal{K})$ é comutativo.

Portanto, de 1, 2, 3 e 4, segue que $S_f(\mathcal{K})$ é um sabanel comutativo com unidade de $S(\mathcal{K})$. $\square$

Proposição 5.1.17. *O anel das sequências nulas $S_0(\mathcal{K})$ é um ideal do anel das sequências de Cauchy $S_f(\mathcal{K})$.*

Demonstração.

1. Pelas Proposições 5.1.8 e 5.1.11, $S_0(\mathcal{K})$ é um sabanel de $S_f(\mathcal{K})$.

2. Sejam $(x_n) \in S_0(\mathcal{K})$ e $(y_n) \in S_f(\mathcal{K})$. Então, $lim\ x_n = 0$ e pela Proposição 5.1.15, (y_n) é limitada. Logo, pela Proposição 5.1.5 temos que

$$lim\ (x_n \cdot y_n) = 0.$$

Portanto, $(x_n \cdot y_n) \in S_0(\mathcal{K})$.

De (1) e (2), segue que $S_0(\mathcal{K})$ é um ideal de $S_f(\mathcal{K})$. □

Proposição 5.1.18. *Seja $(x_n) \in S_f(\mathcal{K}) \backslash S_0(\mathcal{K})$. Então existem $c \in \mathcal{K}_+^*$ e $N \in \mathbb{N}$ tais que*

$$\mid x_n \mid > c,\ \forall n > N.$$

Demonstração.

Seja $(x_n) \in S_f(\mathcal{K}) \backslash S_0(\mathcal{K})$, isto é, $(x_n) \in S_f(\mathcal{K})$ e $(x_n) \notin S_0(\mathcal{K})$. Como $(x_n) \notin S_0(\mathcal{K})$, então $lim\ x_n\ \neq 0$. Logo, existe $\varepsilon \in \mathcal{K}_+^*$ tal que para cada $N \in \mathbb{N}$, existe um $S \in \mathbb{N}$, com $S > N$ tal que

$$\mid x_S \mid \geq \varepsilon. \tag{5.4}$$

Como $(x_n) \in S_f(\mathcal{K})$, para este $\varepsilon \in \mathcal{K}_+^*$, existe $N_0 \in \mathbb{N}$ tal que para todo $m, n > N_0$ tem-se que

$$\mid x_n \mid - \mid x_m \mid \leq\ \mid\mid x_n \mid - \mid x_m \mid\mid\ \leq \mid x_n - x_m \mid <\ \varepsilon,$$

ou seja,

$$\mid x_n \mid -\varepsilon\ < \mid x_m \mid \tag{5.5}$$

Seja $\varepsilon' \in \mathcal{K}_+^*$ tal que $\varepsilon' < \varepsilon$. Considere $c = \varepsilon - \varepsilon'$, então $c \in \mathcal{K}_+^*$. Seja $N \in \mathbb{N}$, com $N > N_0$, então para todo $m, n > N$ a desigualdade (5.5) ocorre. Para este N, existe $l > N$, $l \in \mathbb{N}$, tal que $\mid x_l \mid \geq\ \varepsilon$. De (5.5), para todo $n > N$, temos que

$$\mid x_n \mid > \mid x_l \mid -\varepsilon' \geq \varepsilon - \varepsilon' = c.$$

□

Lema 5.1.2. *Se $\mathcal{K}$ é corpo e $x_m, x_n \in \mathcal{K}^*$, então*

$$\frac{1}{x_n \cdot x_m} \cdot (x_m - x_n) = \frac{1}{x_n} - \frac{1}{x_m}.$$

Demonstração.

Sejam $x_n, x_m \in \mathcal{K}^*$. Então existem x_n^{-1} e x_m^{-1} tal que

$$x_n \cdot x_n^{-1} = 1 \quad \text{e} \quad x_m \cdot x_m^{-1} = 1.$$

Como $x_n \cdot x_m \in \mathcal{K}^*$, temos as seguintes igualdades

$$\begin{aligned}
(x_n \cdot x_m)^{-1} \cdot (x_n \cdot x_m) &= 1 \\
(x_n \cdot x_m)^{-1} \cdot x_n \cdot x_m \cdot x_m^{-1} &= 1 \cdot x_m^{-1} \\
(x_n \cdot x_m)^{-1} \cdot x_n \cdot 1 &= x_m^{-1} \\
(x_n \cdot x_m)^{-1} \cdot x_n &= x_m^{-1} \\
(x_n \cdot x_m)^{-1} \cdot x_n \cdot x_n^{-1} &= x_m^{-1} \cdot x_n^{-1} \\
(x_n \cdot x_m)^{-1} \cdot 1 &= x_m^{-1} \cdot x_n^{-1} \\
(x_n \cdot x_m)^{-1} &= x_m^{-1} \cdot x_n^{-1} \\
\frac{1}{x_n \cdot x_m} &= x_m^{-1} \cdot x_n^{-1}.
\end{aligned}$$

Note que

$$\begin{aligned}
\frac{1}{x_n \cdot x_m} \cdot (x_m - x_n) &= x_m^{-1} \cdot x_n^{-1} \cdot (x_m - x_n) \\
&= x_n^{-1} \cdot x_m^{-1} \cdot (x_m - x_n) \\
&= x_n^{-1} \cdot x_m^{-1} \cdot x_m - x_n^{-1} \cdot x_m^{-1} \cdot x_n \\
&= x_n^{-1} \cdot 1 - x_n^{-1} \cdot x_n \cdot x_m^{-1} \\
&= x_n^{-1} - 1 \cdot x_m^{-1} \\
&= x_n^{-1} - x_m^{-1} \\
&= \frac{1}{x_n} - \frac{1}{x_m}.
\end{aligned}$$

□

Teorema 5.1.2. *O anel quociente $S_f(\mathcal{K})/S_0(\mathcal{K})$ é um corpo.*

Demonstração.

Inicialmente provaremos que $S_f(\mathcal{K})/S_0(\mathcal{K})$ é um corpo. De fato, sabemos que $S_f(\mathcal{K})/S_0(\mathcal{K})$ é um anel, já que $S_0(\mathcal{K})$ é um ideal de $S_f(\mathcal{K})$, veja a Proposição 5.1.17. Resta provar que todo elemento não nulo do anel $S_f(\mathcal{K})/S_0(\mathcal{K})$ é invertível, ou seja, para cada $\overline{(x_n)} \in S_f(\mathcal{K})/S_0(\mathcal{K})$, existe $\overline{(y_n)} \in S_f(\mathcal{K})/S_0(\mathcal{K})$ tal que

$$\overline{(x_n \cdot y_n)} = \overline{(1)}.$$

Seja $(x_n) \in S_f(\mathcal{K}) \backslash S_0(\mathcal{K})$, pela Proposição 5.1.18, existe $c \in \mathcal{K}_+^*$ e $N \in \mathbb{N}$ tais que

$$|\, x_n \,| > c, \ \ \forall n > N.$$

Portanto, $x_n \neq 0$. Agora, definindo $(y_n) \in S(\mathcal{K})$ tal que $y_n = 1$, se $x_n = 0$, para $n \leq N$ e $y_n = x_n^{-1}$, se $x_n \neq 0$. Note que $x_n \cdot y_n = 1$, para todo $n > N$, e $x_n \cdot y_n = 0$, se $x \leq N$, que é um número finito de índices. Portanto, $lim\ x_n \cdot y_n = 1$, ou seja, $(x_n \cdot y_n - 1) \in S_0(\mathcal{K})$. Agora, mostraremos que $(y_n) \in S_f(\mathcal{K})$. De fato, como $(x_n) \in S_f(\mathcal{K})$, dado $\varepsilon \in \mathcal{K}_+^*$, existe $N' \in \mathbb{N}$ tal que se $m, n > N'$ então:

$$\mid x_n - x_m \mid < \varepsilon \cdot c^2.$$

Tomando $N_0 = max\{N, N'\}$, tem-se que, $\forall n > N_0$

$$\mid x_n \mid > \ c \quad \text{e} \quad \mid x_n - x_m \mid < \ \varepsilon \cdot c^2.$$

Daí, pelo Lema 5.1.2, segue que:

$$\mid y_n - y_m \mid = \left| \frac{1}{x_n} - \frac{1}{x_m} \right| = \left| \frac{x_m - x_n}{x_n \cdot x_m} \right| = \frac{\mid x_m - x_n \mid}{\mid x_n \cdot x_m \mid} = \frac{\mid x_m - x_n \mid}{\mid x_n \mid \cdot \mid x_m \mid} \ < \ \frac{\varepsilon \cdot c^2}{c^2} = \varepsilon.$$

Logo, $(y_n) \in S_f(\mathcal{K})$. Agora,

$$\begin{aligned} \overline{(x_n \cdot y_n)} = \overline{(1)} \ &\Leftrightarrow \ (x_n \cdot y_n) \sim (1) \\ &\Leftrightarrow \ (x_n \cdot y_n) - (1) \in S_0(\mathcal{K}) \\ &\Leftrightarrow \ (x_n \cdot y_n - 1) \in S_0(\mathcal{K}). \end{aligned}$$

Portanto, $\overline{(x_n)} \cdot \overline{(y_n)} = \overline{(x_n \cdot y_n)} = \overline{(1)}$. □

O corpo $S_f(\mathcal{K})/S_0(\mathcal{K})$ é denotado por $\widehat{\mathcal{K}}$ e chamado de o completamento de $\mathcal{K}$.

Considere a seguinte aplicação:

$$\begin{aligned} \varphi : S_c(\mathcal{K}) &\to \widehat{\mathcal{K}} \\ (x_n) &\mapsto \varphi((x_n)) := \overline{(x_n)} = (x_n) + S_0(\mathcal{K}). \end{aligned}$$

,

Proposição 5.1.19. *A aplicação φ está bem definida.*

Demonstração.

Dados $(x_n), (y_n) \in S_c(\mathcal{K})$ tais que $(x_n) = (y_n)$, temos que

$$\begin{aligned} \varphi((x_n)) &= \overline{(x_n)} \\ &= (x_n) + S_0(\mathcal{K}) \\ &= (y_n) + S_0(\mathcal{K}) \\ &= \overline{(y_n)} \\ &= \varphi((y_n)). \end{aligned}$$

□

Na proposição a seguir será provado que $\varphi : S_c(\mathcal{K}) \to \widehat{\mathcal{K}}$ é um homomorfismo cujo núcleo é $S_0(\mathcal{K})$ e que o corpo $S_f(\mathcal{K})/S_0(\mathcal{K})$ é uma extensão do corpo $S_c(\mathcal{K})/S_0(\mathcal{K})$.

Proposição 5.1.20. *A aplicação $\varphi : S_c(\mathcal{K}) \to \widehat{\mathcal{K}}$:*

1. *É um homomorfismo de anéis;*

2. $N(\varphi) = S_0(\mathcal{K})$.

Demonstração.

1. Sejam $(x_n), (y_n) \in S_c(\mathcal{K})$. Então,

   (a) $\varphi((x_n) + (y_n)) = \varphi((x_n + y_n)) = \overline{(x_n + y_n)} = \overline{(x_n)} + \overline{(y_n)} = \varphi((x_n)) + \varphi((y_n))$.

   (b) $\varphi((x_n) \cdot (y_n)) = \varphi((x_n \cdot y_n)) = \overline{(x_n \cdot y_n)} = \overline{(x_n)} \cdot \overline{(y_n)} = \varphi((x_n)) \cdot \varphi((y_n))$.

   Portanto, a aplicação φ é um homomorfismo.

2. $N(\varphi) = S_0(\mathcal{K})$.

   (a) $N(\varphi) \subset (\mathcal{K})$. De fato: seja $(x_n) \in N(\varphi)$, então

   $$\varphi((x_n)) = \overline{(x_n)} = (x_n) + S_0(\mathcal{K}) = S_0(\mathcal{K}).$$

   Logo, $(x_n) \in S_0(\mathcal{K})$.

   (b) $S_0(\mathcal{K}) \subset N(\varphi)$. De fato: dado $(y_n) \in S_0(\mathcal{K})$, temos que

   $$\varphi((y_n)) = \overline{(y_n)} = (y_n) + S_0(\mathcal{K}) = S_0(\mathcal{K}).$$

   Portanto, $(y_n) \in N(\varphi)$.

Pelo Teorema 1.3.1, temos que

$$S_c(\mathcal{K})/S_0(\mathcal{K}) \simeq Im(\varphi) \subset \widehat{\mathcal{K}}.$$

Como $\mathcal{K} \simeq S_c(\mathcal{K})/S_0(\mathcal{K})$, segue que $\mathcal{K} \simeq Im(\varphi)$. Portanto, temos uma cópia de $\mathcal{K}$ em $\widehat{\mathcal{K}}$, ou seja, $\mathcal{K} \subset \widehat{\mathcal{K}}$. Logo, podemos ver $\widehat{\mathcal{K}}$ como uma extensão do corpo $\mathcal{K}$. $\square$

5.1.5 ORDENAÇÃO DO COMPLETAMENTO

Neste tópico, veremos com se dá a extensão da ordenação de $\mathcal{K}$ para $\widehat{\mathcal{K}}$. Os resultados aqui elencados podem ser encontrados em (HEFEZ, 2016).

Proposição 5.1.21. *Seja $(x_n) \in S_f(\mathcal{K})$. Então uma, e somente uma, das seguintes condições é satisfeita:*

1. $(x_n) \in S_0(\mathcal{K})$;

2. *Existem $c \in \mathcal{K}_+^*$ e $N \in \mathbb{N}$ tais que $x_n \geq c$, $\forall n > N$.*

3. *Existem $c \in \mathcal{K}_+^*$ e $N \in \mathbb{N}$ tais que $x_n \leq -c$, $\forall n > N$.*

Demonstração.

Suponha que $(x_n) \notin S_0(\mathcal{K})$, então temos que $(x_n) \in S_f(\mathcal{K}) \setminus S_0(\mathcal{K})$. Logo, pela Proposição 5.1.18, existem $c \in \mathcal{K}_+^*$ e $N \in \mathbb{N}$ tais que

$$| x_n | > \ c, \ \ \forall n > N.$$

Assim, se $n > N$, temos que $x_n \geq c$, se $x_n > 0$. Além disso, se $x_n < 0$, então $-x_n \geq c$, ou seja, $x_n \geq -c$. Agora, vamos provar que o sinal de x_n é o mesmo para n grande. Suponha que para todo $N \in \mathbb{N}$ existam n, m naturais com $n, m > N$ tais que

$$x_n \geq c \qquad e \quad -x_m \geq c,$$

ou seja, x_n e x_m têm sinais contrários. Logo,

$$x_n - x_m = x_n + (-x_m) \geq c + c = 2c > 0.$$

Isto é,

$$| x_n - x_m | \geq 2c.$$

Portanto, $(x_n) \notin S_f(\mathcal{K})$, contradizendo a hipótese. □

Definição 5.1.10. *É definido o seguinte subconjunto de* $S_f(\mathcal{K})$*:*

$$S_f(\mathcal{K})^+ = \{(x_n) \in S_f(\mathcal{K})\,;\ \textit{existem } c \in \mathcal{K}_+^* \textit{ e } N \in \mathbb{N} \textit{ tais que } x_n \geq c, \forall n > N\} \cup S_0(\mathcal{K})$$

Lema 5.1.3. *Valem as seguintes afirmações:*

1. *Se* $(x_n) \in S_f(\mathcal{K})^+$ *e* $(-x_n) \in S_f(\mathcal{K})^+$, *então* $(x_n) \in S_0(\mathcal{K})$.

2. $(x_n), (y_n) \in S_f(\mathcal{K})^+$, *então* $(x_n + y_n), (x_n \cdot y_n) \in S_f(\mathcal{K})^+$.

Demonstração.

1. Sejam $(x_n), (-x_n) \in S_f(\mathcal{K})^+$. Suponha que $(x_n) \notin S_0(\mathcal{K})$, então pela Proposição 5.1.21, podemos supor sem perda de generalidade que existem $c \in \mathcal{K}_+^*$ e $N \in \mathbb{N}$ tais que $x_n \geq c$, $\forall n > N$, e para todo $c' \in \mathcal{K}_+^*$ e $N' \in \mathbb{N}$ tem-se que $-x_n < c$, para algum $n > N'$.

2. Sejam $(x_n), (y_x) \in S_f(\mathcal{K})^+$.

   (a) Se $(x_n), (y_x) \in S_0(\mathcal{K})$, então $(x_n + y_x), (x_n \cdot y_x) \in S_0(\mathcal{K})$, pois $S_0(\mathcal{K})$ é um anel. Como $S_0(\mathcal{K}) \subset S_f(\mathcal{K})^+$, resulta que $(x_n + y_x), (x_n \cdot y_x) \in S_f(\mathcal{K})^+$.

   (b) Se $(x_n) \in S_f(\mathcal{K})^+ \setminus S_0(\mathcal{K})$ e $(y_n) \in S_0(\mathcal{K})$, então existem $c \in \mathcal{K}_+^*$ e $N \in \mathbb{N}$ tais que $x_n \geq c, \forall n > N$ e $lim\ y_n = 0$. Para este $c \in \mathcal{K}_+^*$, existe $N_0 \in \mathbb{N}$ tal que

   $$| y_n - 0 | < \frac{c}{2}, \ \ \forall n > N_0.$$

   Segue que

$$\frac{-c}{2} < y_n < \frac{c}{2} \quad \forall n > N_0.$$

Se $N' = max\{N_0, N\}$, então para todo $n > N'$ temos que

$$x_n + y_n > c + \left(\frac{-c}{2}\right) = \frac{c}{2} > 0.$$

Portanto, $(x_n + y_n) \in S_f(\mathcal{K})^+$.
Agora, como em particular $(x_n) \in S_f(\mathcal{K})$, segue da Proposição 5.1.15 que (x_n) é limitada, e como $lim\ y_n = 0$, temos pela Proposição 5.1.5 que

$$lim\ (x_n \cdot y_n) = 0,$$

ou seja, $(x_n \cdot y_n) \in S_0(\mathcal{K}) \subset S_f(\mathcal{K})^+$.

□

Observação 5.1.2. *Note que* $(0) \in S_0(\mathcal{K}) \subset S_f(\mathcal{K})^+$ *e pelo item 2(b), temos que* $S_f(\mathcal{K})^+$ *é um subanel de* $S_f(\mathcal{K})$ *e portanto um anel.*

Definição 5.1.11. *Sejam* $\overline{(x_n)}, \overline{(y_n)} \in \widehat{\mathcal{K}}$*, é definida a seguinte relação em* $\widehat{\mathcal{K}}$*:*

$$\overline{(x_n)} \leq \overline{(y_n)} \Leftrightarrow (y_n) - (x_n) \in S_f(\mathcal{K})^+.$$

Proposição 5.1.22. *A relação definida em* $\widehat{\mathcal{K}}$ *independe dos representantes das classes.*

Demonstração.

Lembremos que $\widehat{\mathcal{K}} = S_f(K)/S_0(K)$. Vamos mostrar que se $(x_n)' - (x_n)$, $(y_n)' - (y_n) \in S_0(\mathcal{K})$ e se $(y_n) - (x_n) \in S_f(\mathcal{K})^+$, então $(y_n)' - (x_n)' \in S_f(\mathcal{K})^+$.
Seja $(x_n)'$ um representante de $\overline{(x_n)}$ e $(y_n)'$ um representante de $\overline{(y_n)}$, vamos provar que $(x_n)' - (y_n)' \in S_f(\mathcal{K})^+$. Como $(x_n)'$ é um representante de $\overline{(x_n)}$, então $(x_n)' - (x_n) \in S_0(\mathcal{K})$. De modo análogo, temos que $(y_n)' - (y_n) \in S_0(\mathcal{K})$, então existem $(x_n)'', (y_n)'' \in S_0(\mathcal{K})$ tais que

$$(x_n)' - (x_n) = (x_n)'' \qquad \text{e} \qquad (y_n)' - (y_n) = (y_n)'',$$

ou seja,

$$(x_n)' = (x_n) + (x_n)'' \qquad \text{e} \qquad (y_n)' = (y_n) + (y_n)''.$$

Como $S_0(\mathcal{K})$ é um anel, então $(x_n)'' - (y_n)'' \in S_0(\mathcal{K}) \subset S_f(\mathcal{K})^+$. Agora, se $(y_n) - (x_n) \in S_f(\mathcal{K})^+$, então pelo Lema 5.1.3, segue que $(x_n) - (y_n) + ((x_n)'' - (y_n)'') \in S_f(\mathcal{K})^+$.

Observe que,

$$\begin{aligned} (y_n)' - (x_n)' &= (y_n) + (y_n)'' - ((x_n) + (x_n)'') \\ &= (y_n) - (x_n) + ((y_n)'' - (x_n)''). \end{aligned}$$

Portanto, $(y_n)' - (x_n)' \in S_f(\mathcal{K})^+$. □

Proposição 5.1.23. *A relação $\leq$ definida anteriormente é uma relação de ordem em $\widehat{\mathcal{K}}$.*

Demonstração.

Vamos provar que as propriedades, reflexiva, antissimétrica e transitiva são verificadas. Lembremos que:

$$\overline{(x_n)} \leq \overline{(y_n)} \Leftrightarrow (y_n) - (x_n) \in S_f(\mathcal{K})^+.$$

1. (Reflexiva)

   Para todo $\overline{(x_n)} \in \widehat{\mathcal{K}}$, temos que $\overline{(x_n)} \leq \overline{(x_n)}$, pois $(x_n) - (x_n) = (x_n - x_n) = (0) \in S_0(\mathcal{K}) \subset S_f(\mathcal{K})^+$

2. (Antissimétrica)

   Se $\overline{(x_n)} \leq \overline{(y_n)}$ e $\overline{(y_n)} \leq \overline{(x_n)}$, então $\overline{(x_n)} = \overline{(y_n)}$. De fato, como $\overline{(x_n)} \leq \overline{(y_n)}$, então $(y_n) - (x_n) \in S_f(\mathcal{K})^+$ e sendo $\overline{(y_n)} \leq \overline{(x_n)}$, temos que $(x_n) - (y_n) \in S_f(\mathcal{K})^+$.
   Note que,

   $$-((y_n) - (x_n)) = (x_n) - (y_n) \in S_f(\mathcal{K})^+.$$

   Logo, pelo Lema 5.1.3, tem-se que $(y_n) - (x_n) \in S_0(\mathcal{K})$, ou seja, $(y_n) \sim (x_n)$. Portanto, $\overline{(x_n)} = \overline{(y_n)}$.

3. (Transitiva)

   Se $\overline{(x_n)} \leq \overline{(y_n)}$ e $\overline{(y_n)} \leq \overline{(z_n)}$, então $\overline{(x_n)} \leq \overline{(z_n)}$. De fato, como $\overline{(x_n)} \leq \overline{(y_n)}$, então $(y_n) - (x_n) \in S_f(\mathcal{K})^+$ e sendo $\overline{(y_n)} \leq \overline{(z_n)}$, temos que $(z_n) - (y_n) \in S_f(\mathcal{K})^+$. Pelo Lema 5.1.3, segue que

   $$\begin{aligned} (z_n) - (x_n) &= ((z_n) - (x_n)) + ((y_n) - (y_n)) \\ &= ((y_n) - (x_n)) + ((z_n) - (y_n)) \in S_f(\mathcal{K})^+. \end{aligned}$$

   Logo, como $(z_n) - (x_n) \in S_f(\mathcal{K})^+$, segue que $\overline{(x_n)} \leq \overline{(z_n)}$.

□

Teorema 5.1.3. *$(\widehat{\mathcal{K}}, +, \cdot, \leq)$ é um corpo ordenado e além disso, a relação $\leq$ de $\widehat{\mathcal{K}}$ é uma extensão da relação $\leq$ de $\mathcal{K}$.*

Demonstração.

Inicialmente iremos mostrar que $(\widehat{\mathcal{K}}, +, \cdot, \leq)$ é um anel ordenado, ou seja, que as propriedades compatibilidade da soma, compatibilidade da multiplicação e totalidade são verificadas.

1. (Compatibilidade da multiplicação)

   Sejam $\overline{(x_n)}, \overline{(y_n)}, \overline{(z_n)} \in \widehat{\mathcal{K}}$. Se $\overline{(x_n)} \leq \overline{(y_n)}$ então $\overline{(x_n)} + \overline{(z_n)} \leq \overline{(y_n)} + \overline{(z_n)}$. De fato, como $\overline{(x_n)} \leq \overline{(y_n)}$, então $(y_n) - (x_n) \in S_f(\mathcal{K})^+$.
   Observe que,

$$\begin{aligned} ((y_n) + (z_n)) - ((x_n) + (z_n)) &= ((y_n) - (x_n)) + ((z_n) - (z_n)) \\ &= (y_n) - (x_n) \in S_f(\mathcal{K})^+. \end{aligned}$$

   Portanto, $\overline{((x_n) + (z_n))} \leq \overline{((y_n) + (z_n))}$, ou seja, $\overline{(x_n)} + \overline{(z_n)} \leq \overline{(y_n)} + \overline{(z_n)}$.

2. (Compatibilidade da adição)

   Sejam $\overline{(x_n)}, \overline{(y_n)}, \overline{(z_n)} \in \widehat{\mathcal{K}}$, com $\overline{(z_n)} \geq \overline{(0)}$ e $\overline{(x_n)} \leq \overline{(y_n)}$, então

$$\overline{(x_n)} \cdot \overline{(z_n)} \leq \overline{(y_n)} \cdot \overline{(z_n)}.$$

   De fato, como $\overline{(x_n)} \leq \overline{(y_n)}$ então $(y_n) - (x_n) \in S_f(\mathcal{K})^+$. Sendo $\overline{(z_n)} \geq \overline{(0)}$, temos que $(z_n) - (0) = (z_n - 0) = (z_n) \in S_f(\mathcal{K})^+$. Pelo Lema 5.1.3, segue que

$$((y_n) - (x_n)) \cdot (z_n) \in S_f(\mathcal{K})^+.$$

   Note que

$$((y_n) - (x_n)) \cdot (z_n) \quad = \quad (y_n) \cdot (z_n) - (x_n) \cdot (z_n) \in S_f(\mathcal{K})^+,$$

   ou seja,

$$(y_n \cdot z_n) - (x_n \cdot z_n) \in S_f(\mathcal{K})^+.$$

   Portanto,

$$\begin{aligned} \overline{(x_n \cdot z_n)} &\leq \overline{(y_n \cdot z_n)} \\ \overline{(x_n) \cdot (z_n)} &\leq \overline{(y_n) \cdot (z_n)} \\ \overline{(x_n)} \cdot \overline{(z_n)} &\leq \overline{(y_n)} \cdot \overline{(z_n)}. \end{aligned}$$

3. (Totalidade)

   Dados $\overline{(x_n)}, \overline{(y_n)} \in \widehat{\mathcal{K}}$, então $\overline{(x_n)} \leq \overline{(y_n)}$ ou $\overline{(y_n)} \leq \overline{(x_n)}$. De fato: seja $\overline{(x_n)}, \overline{(y_n)} \in \widehat{\mathcal{K}} = S_f(\mathcal{K})/S_0(\mathcal{K})$, então $(x_n), (y_n) \in S_f(\mathcal{K})$. Como $S_f(\mathcal{K})$ é um anel, temos que

$$(x_n - y_n) = (x_n) - (y_n) \in S_f(\mathcal{K}).$$

Se $(x_n - y_n) \in S_0(\mathcal{K}) \subset S_f(\mathcal{K})^+$, isto é $(x_n) - (y_n) \in S_f(\mathcal{K})^+$, então $\overline{(y_n)} \leq \overline{(x_n)}$. De modo análogo, temos que $(y_n) - (x_n) \in S_f(\mathcal{K})^+$, e portanto $\overline{(x_n)} \leq \overline{(y_n)}$. Por outro lado, se $(x_n - y_n) \notin S_0(\mathcal{K})$, Pela Proposição 5.1.21, vale apenas uma das seguintes afirmações:

(a) Existem $c \in \mathcal{K}_+^*$ e $N \in \mathbb{N}$ tais que $(x_n - y_n) \geq c, \ \forall n > N$.

(b) Existem $c' \in \mathcal{K}_+^*$ e $N' \in \mathbb{N}$ tais que $-(x_n - y_n) \geq c, \ \forall n > N$.

Portanto, $(x_n - y_n) \in S_f(\mathcal{K})^+$ ou $(y_n - x_n) = -(x_n - y_n) \in S_f(\mathcal{K})^+$, isto é, $\overline{(y_n)} \geq \overline{(x_n)}$ ou $\overline{(x_n)} \geq \overline{(y_n)}$, respectivamente.

Vamos agora provar que a relação $\leq$ de $\widehat{\mathcal{K}}$ é uma extensão da relação $\leq$ de $\mathcal{K}$.
Dados $a, b \in \mathcal{K}$ com $a \leq b$, defina as seguintes sequências constantes:

$$a_n = a \quad \text{e} \quad b_n = b, \quad \forall n \in \mathbb{N}.$$

Como $b \geq a$, então $b - a \geq 0$. Logo, $b - a > 0$ ou $b - a = 0$. Se $b - a = 0$, então $lim\ (b_n - a_n) = lim\ (b - a) = 0$. Portanto, $(b) - (a) = (b_n) - (a_n) = (b_n - a_n) \in S_0(\mathcal{K}) \subset S_f(\mathcal{K})^+$, isto é, $\overline{(a)} \leq \overline{(b)}$. Agora, se $b - a > 0$, tome $c = b - a$, então $c \in \mathcal{K}^*$. Daí,

$$b_n - a_n = b - a = c, \quad \forall n \in \mathbb{N}.$$

Portanto, $(b_n) - (a_n) = (b_n - a_n) \in S_f(\mathcal{K})^+$, ou seja, $\overline{(a_n)} \leq \overline{(b_n)}$, isto é, $\overline{a} \leq \overline{b}$. □

Proposição 5.1.24. *Se $\mathcal{K}$ é arquimediano, então $\widehat{\mathcal{K}}$ é arquimediano.*

Demonstração.
Seja $\overline{(x_n)} \in \widehat{\mathcal{K}} = S_f(\mathcal{K})/S_0(\mathcal{K})$, então $(x_n) \in S_f(\mathcal{K})$. Pela Proposição 5.1.15, temos que (x_n) é limitada, ou seja, existe $r \in \mathcal{K}_+^*$ tal que

$$|\ x_n\ | \leq r, \ \forall n \in \mathbb{N}$$

e portanto,

$$x_n \leq r, \ \forall n \in \mathbb{N}.$$

Como $1 \in \mathcal{K}_+^* \subset \mathcal{K}$, e sendo $\mathcal{K}$ arquimediano, então existe $m \in \mathcal{K}$ tal que

$$m \cdot 1 > r + 1 \geq x_n + 1,$$

ou seja,

$$m \cdot 1 - x_n > 1 \ \forall n \in \mathbb{N}.$$

Portanto, segue que

$$m \cdot (1) - (x_n) = (m \cdot 1 - x_n) \in S_f(\mathcal{K})^+.$$

Logo,

$$\overline{(x_n)} \leq m \cdot \overline{(1)}.$$

□

Proposição 5.1.25. *Sejam* $(x_n), (y_n) \in S_f(\mathcal{K})$*. Se existir* $N \in \mathbb{N}$ *tal que*

$$x_n \geq y_n, \ \ \forall n > N,$$

então $\overline{(x_n)} \geq \overline{(y_n)}$*.*

Demonstração.

Como $(x_n), (y_n) \in S_f(\mathcal{K})$, suponha que exista $N \in \mathbb{N}$ tal que

$$x_n \geq y_n, \ \ \forall n > N.$$

Daí, $x_n - y_n \geq 0$, $\forall n > N$

Se $(x_n - y_n) \in S_0(\mathcal{K}) \subset S_f(\mathcal{K})^+$, então $(x_n) - (y_n) \in S_f(\mathcal{K})^+$. Portanto,

$$\overline{(y_n)} \leq \overline{(x_n)}.$$

Por outro lado, se $(x_n - y_n) \notin S_0(\mathcal{K})$, pela Proposição 5.1.21: existem $c \in \mathcal{K}_+^*$ e $N_0 \in \mathbb{N}$ tais que

$$x_n - y_n \geq c, \ \forall n > N_0, \tag{5.6}$$

ou existem $c' \in \mathcal{K}_+^*$ e $N' \in \mathbb{N}$ tais que

$$x_n - y_n \leq -c, \ \forall n > N'. \tag{5.7}$$

O item 5.7 não pode acorrer, pois tomando o $M = max\{N_0, N'\}$, então para todo $n > M$, tem-se que

$$x_n - y_n \geq 0 \qquad e \qquad x_n - y_n < 0.$$

Chegando assim a uma contradição. Daí, segue que o item 5.6 vale, ou seja,

$$x_n - y_n \geq c, \quad \forall n > N_0.$$

Então,

$$(x_n) - (y_n) = (x_n - y_n) \in S_f(\mathcal{K})^+.$$

Portanto, $\overline{(y_n)} \leq \overline{(x_n)}$. □

Lema 5.1.4. *Seja* $\mathcal{K}$ *um corpo arquimediano e seja* $(x_n) \in S_f(\mathcal{K})$*. Considerando a sequência* $(\overline{x}_m)$ *em* $\widehat{\mathcal{K}}$*, temos que*

$$lim \ \overline{x}_m = \overline{(x_n)}.$$

Demonstração.

Pela Proposição 5.1.24, temos que $\widehat{\mathcal{K}}$ é arquimediano. Logo, dado $\overline{\varepsilon} \in \widehat{\mathcal{K}}_+^*$, isto é, $\overline{\varepsilon} > \overline{0}$, então $(\varepsilon) = (\varepsilon) - (0) \in S_f(\mathcal{K})^+$. Como $(\varepsilon) \notin S_0(\mathcal{K})$, existe $c \in \mathcal{K}_+^*$ tal que $\varepsilon \geq c > 0$, para todo $n > N$. Sendo $\mathcal{K}$ arquimediano, pela Proposição 5.1.10, existe $\varepsilon' \in \mathcal{K}_0$ tal que

$$0 < \varepsilon' < \varepsilon.$$

Pelo Lema 5.1.25, temos que

$$(\overline{0}) < (\overline{\varepsilon'}) < (\overline{\varepsilon}).$$

Agora, para este $\varepsilon' \in \mathcal{K}_0$, dado que $(x_n) \in S_f(\mathcal{K})$, existe $N_0 \in \mathbb{N}$ tal que

$$\mid x_n - x_m \mid < \varepsilon', \quad \forall m, n > N_0.$$

Para cada $m > N$ fixo, temos que

$$x_m - \varepsilon' < x_n < x_m + \varepsilon', \quad \forall n > N.$$

Pelo Lema 5.1.25, temos que

$$\begin{aligned}
\overline{(x_m - \varepsilon')} < \overline{(x_m)} &< \overline{(x_m + \varepsilon')} \\
\overline{(x_m)} - \overline{(\varepsilon')} < \overline{(x_m)} &< \overline{(x_m)} + \overline{(\varepsilon')} \\
\overline{x}_m - \overline{\varepsilon'} < \overline{(x_m)} &< \overline{x}_m + \overline{\varepsilon'}
\end{aligned}$$

Então, para todo $m > N$, temos que

$$\mid \overline{x}_m - \overline{(x_n)} \mid < \overline{\varepsilon'} < \overline{\varepsilon}.$$

Portanto,

$$lim\ \overline{x}_m = \overline{x},$$

onde $\overline{x} = \overline{(x_n)}$. □

O teorema a seguir fornecerá uma propriedade fundamental do completamento $\widehat{\mathcal{K}}$ de um corpo arquimedino $\mathcal{K}$.

Teorema 5.1.4. *Sejam $\mathcal{K}$ um corpo arquimediano e seja $\widehat{\mathcal{K}}$ o seu completamento. Temos que toda sequência de Cauchy em $\widehat{\mathcal{K}}$ é convergente em $\widehat{\mathcal{K}}$, isto é,*

$$S_f(\widehat{\mathcal{K}}) = S_c(\widehat{\mathcal{K}}).$$

Demonstração.

1. Pela Proposição 5.1.11 toda sequência convergente é de Cauchy, portanto, $S_c(\widehat{\mathcal{K}}) \subset S_f(\widehat{\mathcal{K}})$.

2. Resta provar que toda sequência de Cauchy é convergente em $\widehat{\mathcal{K}}$, ou seja, $S_f(\widehat{\mathcal{K}}) \subset S_c(\widehat{\mathcal{K}})$.

   Seja $(\overline{x}_n) \in S_f(\widehat{\mathcal{K}})$. Como para cada $n \in \mathbb{N}$, temos que

$$\overline{x}_n - \frac{1}{n1} < \overline{x}_n < \overline{x}_n + \frac{1}{n1},$$

   e $\widehat{\mathcal{K}}$ é arquimediano, então pela Proprosição 5.1.10, existe $\overline{a}_n \in \widehat{\mathcal{K}}_0$ (corpo primo), tal que

$$\overline{x}_n - \frac{1}{\overline{n1}} < \overline{a}_n < \overline{x}_n + \frac{1}{\overline{n1}},$$

   isto é,

$$\mid \overline{a}_n - \overline{x}_n \mid \leq \frac{1}{\overline{n1}}, \quad \forall n \in \mathbb{N}.$$

   Como $(\overline{x}_n) \in S_f(\widehat{\mathcal{K}})$, dado $\overline{\varepsilon} \in \widehat{\mathcal{K}}^*_+$, existe $N \in \mathbb{N}$, tal que

$$\mid \overline{x}_n - \overline{x}_m \mid < \frac{\overline{\varepsilon}}{3}, \quad \forall m, n > N.$$

   Seja $N_1 \in \mathbb{N}$ tal que $N_1 > N$ e $\overline{N_1 \cdot 1} > \frac{3}{\overline{\varepsilon}}$. Temos então, para todo $m, n \geq N_1$ que

$$\begin{aligned}
\mid \overline{a}_n - \overline{a}_m \mid &= \mid \overline{a}_n - \overline{x}_n + \overline{x}_n - \overline{x}_m + \overline{x}_m - \overline{a}_m \mid \\
&\leq \mid \overline{a}_n - \overline{x}_n \mid + \mid \overline{x}_n - \overline{x}_m \mid + \mid \overline{x}_m - \overline{a}_m \mid \\
&< \frac{1}{\overline{n \cdot 1}} + \frac{\overline{\varepsilon}}{3} + \frac{1}{\overline{m \cdot 1}} \\
&< \frac{\overline{\varepsilon}}{3} + \frac{\overline{\varepsilon}}{3} + \frac{\overline{\varepsilon}}{3} = \overline{\varepsilon},
\end{aligned}$$

   pois,

$$m \geq N_1 \Rightarrow \overline{m \cdot 1} \geq \overline{N_1 \cdot 1} > \frac{3}{\overline{\varepsilon}} \Rightarrow \frac{\overline{\varepsilon}}{3} > \frac{1}{\overline{m \cdot 1}}.$$

   De modo análogo, conclui-se que

$$\frac{\overline{\varepsilon}}{3} > \frac{1}{\overline{n \cdot 1}}.$$

   Isso prova que $(\overline{a}_n) \in S_f(\widehat{\mathcal{K}})$. Logo, pelo Lema 5.1.4, temos que

$$lim\ \overline{a}_n = \overline{(a_n)}.$$

   Então, dado $\overline{\varepsilon} \in \widehat{\mathcal{K}}^*_+$, existe $N \in \mathbb{N}$ tal que

$$|\,\overline{a}_n - \overline{(a_n)}\,| < \frac{\overline{\varepsilon}}{2} \quad e \quad |\,\overline{x}_n - \overline{a}_n\,| < \frac{\overline{\varepsilon}}{3} < \frac{\overline{\varepsilon}}{2}, \quad \forall n > N.$$

Logo, para $n > N$, temos que

$$\begin{aligned} |\,\overline{x}_n - \overline{(a_n)}\,| &= |\,\overline{x}_n - \overline{a}_n + \overline{a}_n - \overline{(a_n)}\,| \\ &\leq |\,\overline{x}_n - \overline{a}_n\,| + |\,\overline{a}_n - \overline{(a_n)}\,| \\ &< \frac{\overline{\varepsilon}}{2} + \frac{\overline{\varepsilon}}{2} = \overline{\varepsilon}. \end{aligned}$$

Portanto,

$$lim\ \overline{x}_n = \overline{(a_n)}$$

□

Definição 5.1.12. *Um corpo $\mathcal{L}$ tal que $S_f(\mathcal{L}) = S_c(\mathcal{L})$ é dito completo.*

Proposição 5.1.26. *Sejam $a, b \in \mathbb{R}$, se $a \geq 0$ e $b > 0$, então $a < b$ se, e somente se, $a^2 < b^2$.*

Demonstração. Veja em [Apêndice A]. □

Proposição 5.1.27. *Seja $a \geq 0$, então existe $b \in \mathbb{R}$ tal que $b^2 = a$.*

Demonstração. Veja em [Apêndice A]. □

Observação 5.1.3. *Observe que o Teorema 5.1.4 afirma que o completamento $\widehat{\mathcal{K}}$ de um corpo arquimediano $\mathcal{K}$ é completo, já que*

$$S_f(\widehat{\mathcal{K}}) = S_c(\widehat{\mathcal{K}}).$$

Observação 5.1.4. *Sabemos que $\mathbb{Q}$ é um corpo arquimediano, denota-se o completamento $\widehat{\mathbb{Q}}$ de $\mathbb{Q}$ por $\mathbb{R}$, que é chamado de corpo dos números reais, isto é,*

$$\mathbb{R} := \widehat{\mathbb{Q}} = S_f(\mathbb{Q})/S_0(\mathbb{Q}).$$

Observação 5.1.5. *Note que, sendo $\mathbb{Q}$ um corpo arquimediano, pela proposição (5.1.24), $\mathbb{R}$ é também arquimediano.*

O próximo resultado mostra que o corpo dos números reais é único a menos de isomorfismo.

Teorema 5.1.5. *Seja $\mathcal{K}$ um corpo arquimediano completo. Então existe um único homomorfismo de anéis de $\mathbb{R}$ em $\mathcal{K}$. Além disso, este homomorfismo é um isomorfismo de anéis ordenados.*

Demonstração.

Seja $\mathcal{K}$ um corpo arquimediano completo.

1. Inicialmente iremos provar que qualquer homomorfismo $f : \mathbb{R} \to \mathcal{K}$ é ordenado. Dados $a, b \in \mathbb{R}$, com $a \leq b$, ou seja, $b - a \geq 0$, então pela Proposição 5.1.27 existe $c \in \mathbb{R}$ tal que $c^2 = b - a$. Temos que

$$\begin{aligned} 0 &\leq \mid f(c) \mid^2 \\ &= (f(c))^2 \\ &= f(c) \cdot f(c) \\ &= f(c \cdot c) \\ &= f(c^2) \\ &= f(b - a) \\ &= f(b + (-a)) \\ &= f(b) + f(-a) \\ &= f(b) - f(a). \end{aligned}$$

   Portanto, $f(b) \geq f(a)$.

2. Unicidade do homomorfismo de $\mathbb{R}$ em $\mathcal{K}$.
   Dados f, g homomorfismos de anéis de $\mathbb{R}$ no corpo arquimediano $\mathcal{K}$.
   Considere o seguinte conjunto:

$$M = \{x \in \mathbb{R} \ ; \ f(x) = g(x)\}.$$

   Vamos provar que M é um subcorpo de $\mathbb{R}$.

   (a) M é um subanel de $\mathbb{R}$.

      i. $0 \in M$, pois $f(0) = 0 = g(0)$.

      ii. Dados $x, y \in M$, vamos provar que $x - y, x \cdot y \in M$.

$$\begin{aligned} f(x - y) &= f(x + (-y)) \\ &= f(x) + f(-y) \\ &= f(x) - f(y) \\ &= g(x) - g(y) \\ &= g(x) + g(-y) \\ &= g(x + (-y)) \\ &= g(x - y). \end{aligned}$$

De modo análogo tem-se que

$$\begin{aligned} f(x \cdot y) &= f(x) \cdot f(y) \\ &= g(x) \cdot g(y) \\ &= g(x \cdot y). \end{aligned}$$

(b) Vamos provar que para todo $x \in M^*$ existe $x^{-1} \in M$ tal que

$$x \cdot x^{-1} = 1.$$

Se $x \in M^*$, então $x \in \mathbb{R}^*$ tal que $f(x) = g(x)$. Como $x \in \mathbb{R}^*$, existe $x^{-1} \in \mathbb{R}$ tal que

$$\begin{aligned} x \cdot x^{-1} &= 1 && (5.8) \\ f(x \cdot x^{-1}) &= f(1) \\ f(x) \cdot f(x^{-1}) &= 1. && (5.9) \end{aligned}$$

Portanto, $f(x) \neq 0$ e como $\mathcal{K}$ é corpo, existe $(f(x))^{-1} \in \mathcal{K}$ tal que

$$f(x) \cdot (f(x))^{-1} = 1.$$

Multiplicando a Equação 5.9 por $(f(x))^{-1}$, temos que

$$\begin{aligned} (f(x))^{-1} \cdot (f(x) \cdot f(x^{-1})) &= (f(x))^{-1} \cdot 1 \\ ((f(x))^{-1} \cdot f(x)) \cdot f(x^{-1}) &= (f(x))^{-1} \\ 1 \cdot f(x^{-1}) &= (f(x))^{-1} \\ f(x^{-1}) &= (f(x))^{-1}. && (5.10) \end{aligned}$$

De modo análogo, prova-se que

$$g(x^{-1}) = (g(x))^{-1}. \quad (5.11)$$

Assim, de 5.10 e 5.11 tem-se que

$$f(x^{-1}) = (f(x))^{-1} = (g(x))^{-1} = g(x^{-1}).$$

Portanto, $x^{-1} \in M$. Logo M é um corpo.
Resta provar que $M = \mathbb{R}$.
Suponha que $M \neq \mathbb{R}$. Seja $a \in \mathbb{R} \backslash M$, então $f(a) \neq g(a)$. Sem perda de generalidade, podemos supor $a > 0$ tal que $f(a) < g(a)$. Como $\mathcal{K}$ é um corpo arquimediano, existe $r \in \mathcal{K}_0$ (corpo primo) tal que

$$f(a) < r < g(a).$$

Como $\mathcal{K}_0 = \widetilde{\rho}(\mathbb{Q})$, (veja a Observação 1.3.3) e $\widetilde{\rho}$ é o único homomorfismo de $\mathbb{Q}$ em $\mathcal{K}$. Sendo f e g homomorfismo de $\mathbb{R}$ em $\mathcal{K}$, então $f|_{\mathbb{Q}}$ e $g|_{\mathbb{Q}}$ são homomorfismos, e portanto, $f|_{\mathbb{Q}} = g|_{\mathbb{Q}} = \widetilde{\rho}$. Como $r \in \mathcal{K}_0$, existe $s \in \mathbb{Q}$ tal que $r = \widetilde{\rho}(s) = f(s) = g(s)$. Agora:
Se $a \leq s$, sendo g homomorfismo, então

$$g(a) \leq g(s) = r,$$

o que é uma contradição.
Se $a \geq s$, sendo f um homomorfismo então

$$f(a) \geq f(s) = r,$$

o que é um absurdo.
Portanto, $M = \mathbb{R}$.

3. Existência do homomorfismo de $\mathbb{R}$ em $\mathcal{K}$.

Considere a aplicação $\psi : S_f(\mathbb{Q}) \to \mathcal{K}$, definida por:

$$\psi((x_n)) = lim\ \widetilde{\rho}(x_n).$$

(a) A aplicação ψ está bem definida.

i. Existência do limite.
Dado $(x_n) \in S_f(\mathbb{Q})$, como $\mathcal{K}$ é completo, isto é, $S_f(\mathcal{K}) = S_c(\mathcal{K})$, basta mostrar que a sequência $(\widetilde{\rho}(x_n))$ é de Cauchy.
Dado $\varepsilon \in \mathcal{K}_+^*$, como $\mathcal{K}$ é arquimediano, pela Proposição 5.1.10, existe $r \in \mathcal{K}_0 = \widetilde{\rho}(\mathbb{Q})$ tal que

$$0 < r < \varepsilon.$$

Como $r \in \widetilde{\rho}(\mathbb{Q})$, existe $t \in \mathbb{Q}_+^* \subset \mathbb{Q}$, em virtude de $\widetilde{\rho}$ ser um homomorfismo ordenado, tal que $r = \widetilde{\rho}(t)$.
Logo,

$$0 < \widetilde{\rho}(t) < \varepsilon.$$

Como $(x_n) \in S_f(\mathbb{Q})$, para este t, existe $N \in \mathbb{N}$ tal que

$$\mid x_n - x_m \mid < \ t, \quad \forall m, n > N.$$

Ou seja,

$$-t < x_n - x_m < t, \quad \forall m, n > N.$$

Sendo $\widetilde{\rho}$ um homomorfismo ordenado, temos que

$$\mid \widetilde{\rho}(x_n) - \widetilde{\rho}(x_m) \mid = \mid \widetilde{\rho}(x_n - x_m) \mid < \mid \widetilde{\rho}(t) \mid = \ \widetilde{\rho}(t) \ < \ \varepsilon, \quad \forall m, n > N.$$

Portanto, $(\widetilde{\rho}(x_n)) \in S_f(\mathcal{K})$.

ii. Dados $(x_n), (y_n) \in S_f(\mathbb{Q})$, tais que $(x_n) = (y_n)$. Vamos provar que

$$\psi((x_n)) = \psi((y_n)).$$

Dá unicidade do limite temos que

$$\psi((x_n)) = lim\ \widetilde{\rho}(x_n) = lim\ \widetilde{\rho}(y_n) = \psi((y_n)).$$

(b) ψ é um homomorfismo de anéis.

Vamos provar que se $(x_n), (y_n) \in S_f(\mathbb{Q})$, então

i. $\psi((x_n) + (y_n)) = \psi((x_n)) + \psi((y_n))$;

ii. $\psi((x_n) \cdot (y_n)) = \psi((x_n)) \cdot \psi((y_n))$.

Note que:

$$\begin{aligned}
\psi((x_n) + (y_n)) &= \psi((x_n + y_n)) \\
&= lim\ \widetilde{\rho}(x_n + y_n) \\
&= lim\ [\widetilde{\rho}(x_n) + \widetilde{\rho}(y_n)] \\
&= lim\ \widetilde{\rho}(x_n) + lim\ \widetilde{\rho}(y_n) \\
&= \psi((x_n)) + \psi((y_n)).
\end{aligned}$$

e

$$\begin{aligned}
\psi((x_n) \cdot (y_n)) &= \psi((x_n \cdot y_n)) \\
&= lim\ \widetilde{\rho}(x_n \cdot y_n) \\
&= lim\ [\widetilde{\rho}(x_n) \cdot \widetilde{\rho}(y_n)] \\
&= lim\ \widetilde{\rho}(x_n) \cdot lim\ \widetilde{\rho}(y_n) \\
&= \psi((x_n)) \cdot \psi((y_n)).
\end{aligned}$$

E pelas Proposições 1.3.2 e 1.3.3, temos que

$$\psi((0)) = 0 \quad e \quad \psi((1)) = 1.$$

(c) ψ é sobrejetor.

Vamos provar que, dado $\alpha \in \mathcal{K}$, existe uma sequência $(s_n) \in S_f(\mathbb{Q})$ tal que $\psi((s_n)) = \alpha$, ou seja,

$$lim\ \widetilde{\rho}(s_n) = \alpha.$$

Como $\alpha \in \mathcal{K}$, e $\mathcal{K}$ é arquimediano, pela Proposição 5.1.10, existe uma sequência $(t_n) \in \mathcal{K}_0 \subset \mathcal{K}$, tal que

$$lim\ t_n = \alpha.$$

Como cada $t_n \in \mathcal{K}_0 = \widetilde{\rho}(\mathbb{Q})$, existe $S_n \in \mathbb{Q}$ tal que

$$t_n = \widetilde{\rho}(s_n).$$

Então,

$$lim\ \widetilde{\rho}(s_n) = lim\ t_n = \alpha.$$

Resta provar que $(s_n) \in S_f(\mathbb{Q})$.
Como para cada n, $t_n = \widetilde{\rho}(s_n)$, e sendo $\widetilde{\rho} : \mathbb{Q} \to \mathcal{K}_0$ um isomorfismo ordenado de anéis, segue que

$$s_n = \widetilde{\rho}^{-1}(t_n).$$

Dado $\varepsilon \in \mathbb{Q}_+^*$, então $\widetilde{\rho}(\varepsilon) > \widetilde{\rho}(0) = 0$. Logo, $\widetilde{\rho}(\varepsilon) \in \mathcal{K}_+^*$. Como $(t_n) \in S_c(\mathcal{K}_0) \subset S_f(\mathcal{K}_0)$, então existe $N \in \mathbb{N}$ tal que para quaisquer $m, n \in \mathbb{N}$, com $m, n > N$, tem-se que

$$\mid t_m - t_n \mid < \ \widetilde{\rho}(\varepsilon),$$

ou seja,

$$-\widetilde{\rho}(\varepsilon) < t_m - t_n < \widetilde{\rho}(\varepsilon).$$

Como $\widetilde{\rho}^{-1}$ é um homomorfismo ordenado, então

$$\begin{aligned}
\widetilde{\rho}^{-1}(-\widetilde{\rho}(\varepsilon)) &< \widetilde{\rho}^{-1}(t_m - t_n) &< \quad & \widetilde{\rho}^{-1}(\widetilde{\rho}(\varepsilon)) = \varepsilon. \\
-\widetilde{\rho}^{-1}(\widetilde{\rho}(\varepsilon)) &< \widetilde{\rho}^{-1}(t_m - t_n) &< \quad & \varepsilon. \\
-\varepsilon &< \widetilde{\rho}^{-1}(t_m - t_n) &< \quad & \varepsilon.
\end{aligned}$$

Ou seja,

$$\mid \widetilde{\rho}^{-1}(t_m - t_n) \mid < \ \varepsilon, \quad \forall m, n > N.$$

Agora,

$$\mid s_m - s_n \mid = \mid \widetilde{\rho}^{-1}(t_m) - \widetilde{\rho}^{-1}(t_n) \mid = \mid \widetilde{\rho}^{-1}(t_m - t_n) \mid < \ \varepsilon, \quad \forall m, n > N.$$

Portanto, $(s_n) \in S_f(\mathbb{Q})$.

4. $N(\psi) = S_0(\mathbb{Q})$.

   (a) $N(\psi) \subset S_0(\mathbb{Q})$.
   Seja $(x_n) \in N(\psi) \subset S_f(\mathbb{Q})$, então

$$lim\ \widetilde{\rho}(x_n) = \psi((x_n)) = 0.$$

Dado $\varepsilon \in \mathbb{Q}_+^*$, isto é, $\varepsilon > 0$, então $\widetilde{\rho}(\varepsilon) > \widetilde{\rho}(0) = 0$. Logo, $\widetilde{\rho}(\varepsilon) \in \mathcal{K}_+^*$. Então, existe um $N \in \mathbb{N}$ tal que

$$\mid \widetilde{\rho}(x_n) \mid < \ \widetilde{\rho}(\varepsilon), \quad \forall n > N.$$

Ou seja,

$$-\widetilde{\rho}(\varepsilon) \ < \ \widetilde{\rho}(x_n) \ < \ \widetilde{\rho}(\varepsilon), \quad \forall n > N.$$

Como $\widetilde{\rho}^{-1} : \mathcal{K}_0 \to \mathbb{Q}$ é um homomorfismo ordenado, então

$$\begin{aligned} \widetilde{\rho}^{-1}(-\widetilde{\rho}(\varepsilon)) \ < \ \widetilde{\rho}^{-1}(\widetilde{\rho}(x_n)) \ &< \ \widetilde{\rho}^{-1}(\widetilde{\rho}(\varepsilon)) \\ -\widetilde{\rho}^{-1}(\widetilde{\rho}(\varepsilon)) \ < \ x_n \ &< \ \varepsilon \\ -\varepsilon \ < \ x_n \ &< \ \varepsilon. \end{aligned}$$

Isto é,

$$| \, x_n \, | < \ \varepsilon, \quad \forall n > N.$$

Então, $lim \ x_n = 0$. Portanto, $(x_n) \in S_0(\mathbb{Q})$.

(b) $S_0(\mathbb{Q}) \subset N(\psi)$.
Seja $(x_n) \in S_0(\mathbb{Q})$, então $lim \ x_n = 0$. Logo, dado $\varepsilon \in \mathbb{Q}_+^*$, existe $N \in \mathbb{N}$ tal que

$$| \, x_n \, | < \varepsilon, \quad \forall n > N.$$

Ou seja,

$$-\varepsilon < x_n < \varepsilon, \quad \forall n > N.$$

Sendo $\widetilde{\rho} : \mathbb{Q} \to \mathcal{K}_0 \subset \mathcal{K}$ um homomorfismo ordenado, então

$$\widetilde{\rho}(-\varepsilon) < \widetilde{\rho}(x_n) < \widetilde{\rho}(\varepsilon), \quad \forall n > N.$$

Isto é,

$$-\widetilde{\rho}(\varepsilon) < \widetilde{\rho}(x_n) < \widetilde{\rho}(\varepsilon), \quad \forall n > N.$$

Como $\varepsilon > 0$, então $\widetilde{\rho}(\varepsilon) > \widetilde{\rho}(0) = 0$, ou seja, $\widetilde{\rho}(\varepsilon) \in \mathcal{K}_+^*$.

Logo,

$$| \, \widetilde{\rho}(x_n) \, | < \widetilde{\rho}(\varepsilon), \quad \forall n > N.$$

Portanto, $lim \ \widetilde{\rho}(x_n) = 0$, ou seja,

$$\psi((x_n)) = lim \ \widetilde{\rho}(x_n) = 0.$$

Com base nas afirmações anteriores, pelo teorema do isomorfismo, temos que

$$\mathbb{R} = S_f(\mathbb{Q})/S_0(\mathbb{Q}) \simeq \mathcal{K}.$$

$\square$

CONSIDERAÇÕES FINAIS

A produção deste Trabalho de Conclusão de Curso, nos mostra a importância do conhecimento das áreas de álgebra e Análise. A partir dessa percepção, concluímos que a junção da álgebra com a análise é de extrema importância, pois essas duas áreas proporcionaram a construção do corpo dos números reais, considerando a técnica de construção proposta por Cantor. A álgebra com suas estruturas de anéis e corpos, e a análise com o conceito de sequências e suas propriedades.

REFERÊNCIAS

[1] BARTLE, R.G; SHERBERT, D.R. **Introduction to real analysis**. 3. ed. New York: John Wiley e Sons, Inc 2000.

[2] FERREIRA, J. F. **A construção dos números**. 3. ed. Rio de Janeiro: SBM, 2013.

[3] GONÇALVES, A. G. **Introdução à álgebra**. 5. ed. Rio de Janeiro: IMPA, 2001.

[4] HEFEZ, A. H. **Curso de álgebra**, vol 1. 5. ed. Rio de Janeiro: IMPA, 2016.

[5] HUNGERFORD, T W. **Abstract algebra: An introduction**. 2. ed. Boston: Thomson Learning, 1997.

[6] LIMA, E. L. **Curso de análise**, vol 1. 13. ed. Rio de Janeiro: IMPA, 1995.

[7] MILIES, C.P; COELHO, S.P. **Números uma introdução a matemática**. 3. ed. São Paulo: EDUSP, 2001.

Apêndice A

As provas dos seguintes resultados foram baseadas nas demonstrações apresentadas nas referências (LIMA, 1995) e (BARTLE, 2000).

Lema A.0.1. *Se $a \geq 0$ e $b > 0$, então $a < b$ se, e somente se, $a^2 < b^2$.*

Demonstração.

($\Rightarrow$) Suponha que $a < b$, isto é, $b - a > 0$. Então

$$b^2 - a^2 = (b - a) \cdot (b + a) > 0,$$

ou seja, $b^2 > a^2$, isto é, $a^2 < b^2$.

($\Leftarrow$) Se $a^2 < b^2$, então $b^2 - a^2 > 0$. Como $a + b > 0$ e $(b + a) \cdot (b - a) = b^2 - a^2 > 0$, então $b - a > 0$, ou seja, $b > a$

$\square$

Proposição A.0.1. *Seja $a \geq 0$, então existe $b \in \mathbb{R}$ tal que $b^2 = a$.*

Demonstração.

Se $a = 0$, basta tomar $b = 0$.
Considere $a > 0$. Seja $S = \{x \in \mathbb{R}\ ;\ x \geq 0 \text{ e } x^2 < a\}$, temos que $S \neq \emptyset$, pois $0 \in S$.

1. O conjunto S é limitado superiormente, pois se $a > 1$, S é limitado superiormente por a.
   Suponha que isto não ocorra, então exite $t \in S$, tal que $a < t$. Logo, $t^2 = t \cdot t > a \cdot a > a$, pois $a > 1$. Mas isto é um absurdo, já que $t \in S$. Por outro lado, se $0 < a < 1$, então 1 é cota superior de S, pois dado $t \in S$, temos que $t^2 < a < 1$, isto é, $t^2 - 1 < 0$. Portanto, $t < 1$. Concluimos então que, em qualqer caso S é limitado superiormente. Portanto, S tem supremo $b = SupS \in \mathbb{R}$.

2. Vamos provar que não podemos ter as desigualdades $b^2 < a$ e $b^2 > a$.

(a) O conjunto S não possui elemento máximo.

Dado $x \in S$, vamos provar que existe $0 < \varepsilon < 1$ tal que $(x+\varepsilon)^2 < a$, isto é, $x + \varepsilon \in S$.

Note que para todo $0 < \varepsilon < 1$, tem-se que

$$(x+\varepsilon)^2 = x^2 + 2x\varepsilon + \varepsilon^2 = x^2 + \varepsilon(2x+\varepsilon). \tag{A.1}$$

Como $x \in S$, isto é, $x \geq 0$ e $x^2 < a$. Logo,

$$a - x^2 > 0 \quad \text{e} \quad 2x + \varepsilon > 0.$$

Então,

$$\frac{a-x^2}{2x+\varepsilon} > 0,$$

para todo $0 < \varepsilon < 1$. Logo, existe $0 < \varepsilon' < 1$, tal que

$$\frac{a-x^2}{2x+\varepsilon'} > \varepsilon' > 0.$$

Ou seja, $\varepsilon'(2x+\varepsilon') < a - x^2$. De (A.1), temos que

$$(x+\varepsilon')^2 = x^2 + \varepsilon'(2x+\varepsilon') < x^2 + (a - x^2) = a.$$

Sendo $x \geq 0$, então $(x + \varepsilon') > 0$. Logo $x + \varepsilon' \in S$ e protanto, S não contém máximo.

(b) Seja $W = \{y \in \mathbb{R}\ ;\ y > 0 \text{ e } y^2 > a\}$. Como $a > 0$, tome $y = a + 1 > 0$. Agora,

$y^2 = (a+1)^2 = a^2 + 2a + 1 > a$. Logo, $a + 1 \in W$ e portanto, $W \neq \emptyset$.

Vamos provar que W não tem elemento mínimo.

Seja $y \in W$, escolha $0 < \varepsilon < 1$ tal que $(y - \varepsilon)^2 > a$, isto é, $y - \varepsilon \in W$. Agora,

$$(y-\varepsilon)^2 = y^2 - 2y\varepsilon + \varepsilon^2 > y^2 - 2y\varepsilon,$$

para todo $0 < \varepsilon < 1$. Como $y \in W$, então $y > 0$ e $y^2 > a$, isto é, $y^2 - a > 0$. Logo,

$$\frac{y^2 - a}{2y} > 0.$$

Existe $\varepsilon' > 0$, tal que

$$0 < \varepsilon' < \frac{y^2-a}{2y}.$$

Ou seja,

$$\begin{aligned} y^2 - a &> 2y\varepsilon' \\ y^2 &> 2y\varepsilon' + a \\ y^2 - 2y\varepsilon' &> a. \end{aligned}$$

Então,

$$(y - \varepsilon')^2 > y^2 - 2y\varepsilon' > a.$$

Logo, $y - \varepsilon' \in W$, e portanto W não tem elemento mínimo.

3. Se $x \in S$ e $y \in W$, então $x \geq 0$, $x^2 < a$ e $y > 0$, $y^2 > a$. Logo, $x^2 < a < y^2$, isto é, $x^2 < y^2$. Pelo lema (A.0.1), temos que $x < y$. Agora, se $b^2 < a$, então $b \in S$, e sendo $b = SupS$, b seria o máximo de S, o que contradiz o fato de S não ter máximo. Por outro lado, se $b^2 > a$, então $b \in W$ e como W não elemento mínimo, existe $c \in W$, tal que $c < b$. Pelo item (3), para $x \in S$, tem-se que $x < c < b$. Logo, c seria uma cota superior para S, mas isto é um absurdo, pois $b = SupS$. Logo, não se pode ter $b^2 > a$.
Portanto, $b^2 = a$.

□