Universidade Estadual de Maringá - Departamento de Matemática
Cálculo Diferencial e Integral: um KIT de Sobrevivência
 http://www.dma.uem.br/kit

CONSTRUÇÃO DOS REAIS: UM ENFOQUE USANDO CORTES DE DEDEKIND

ADILANDRI MÉRCIO LOBEIRO

Sumário

Capítulo 1

NÚMEROS NATURAIS

Neste capítulo, propomo-nos a desenvolver o estudo do conjunto dos números naturais. A idéia de número natural está ligada ao problema de contar ou enumerar objetos de um conjunto dado. Nosso primeiro objetivo será então o de caracterizar os números naturais. Uma das maneiras de fazê-lo é elaborar um conjunto de axiomas e definições e daí desenvolver as propriedades do conjunto em forma de teoremas. Estes axiomas, conhecidos como Axiomas de Peano, em homenagem ao matemático italiano que, em 1899, inaugurou este processo, podem ser enuciada como segue.

1.1 OS AXIOMAS DE PEANO

AXIOMAS DE PEANO: Existe um conjunto $\mathbb{N}$ tal que os seguintes axiomas são verificados:

Axioma 1 $1 \in \mathbb{N}$

Axioma 2 *Para qualquer* $n \in \mathbb{N}$ *existe um único* $n^* \in \mathbb{N}$, *denominado o sucessor de* n

Axioma 3 *Para cada* $n \in \mathbb{N}$ *temos* $n^* \neq 1$

Axioma 4 *Se* m, $n \in \mathbb{N}$ *e* $m^* = n^*$, *então* $m = n$.

Axioma 5 *Se* M *é um subconjunto de* $\mathbb{N}$ *talque* $1 \in M$ *e* $n^* \in M$ *sempre que* $n \in M$, *então necessariamente* $M = \mathbb{N}$.

Observação 1.1.1 *O axioma* 1 *nos mostra que o conjunto* $\mathbb{N}$ *não é vazio, pois pelo menos o número* 1 *pertence a* $\mathbb{N}$. *O axioma 2 estabelece que para*

qualquer que seja, $n \in \mathbb{N}$ existe um único $n^* \in \mathbb{N}$. O axioma 3 diz que existe um elemento de $\mathbb{N}$ que não é sucessor de nenhum outro elemento de $\mathbb{N}$, ou seja, estabelece que existe um primeiro número natural 1. O axioma 4 diz que se dois elementos possuem o mesmo sucessor, então esses elementos são iguais. O axioma 5 conhecido como axioma de indução completa, estabelece essencialmente que qualquer número natural pode ser atingido começando com 1 e contando os sucessores consecutivos. Adotamos o símbolo 2 (dois) para indicar o sucessor de 1 (um), o símbolo 3 (três) para indicar o sucessor de 2 (dois) e assim por diante. Adotaremos também, indiferentemente, os símbolos n^* e $n+1$ para indicar o sucessor de n (adoção justificada pela definição de soma de dois números naturais).

Definição 1.1.2 *O conjunto $\mathbb{N}$ é chamado de o* ***conjunto dos números naturais*** *e seus elementos de números naturais.*

Vamos agora deduzir dos Axiomas de Peano as primeiras propriedades dos números naturais. A primeira delas diz que dados números naturais diferentes então seus sucessores também são diferentes; a segunda afirma que nenhum número natural é sucessor dele mesmo; a terceira garante que todo número natural, diferente de 1, é sucessor de algum outro número natural.

Teorema 1.1.3 *Para quaisquer números naturais m e n temos:*

(1) $m \neq n \Rightarrow m^* \neq n^*$

(2) $n \neq n^*$

(3) $n \neq 1 \Rightarrow \exists\, p, p \in \mathbb{N}$, tal que $p^* = n$

Demonstração. Parte (1) . Se tivermos $m^* = n^*$, pelo Axioma 4, teremos $m = n$,contrariando a hipótese.

Parte (2) . Seja

$$M = \{m \in \mathbb{N} \mid m \neq m^*\}$$

Então, pelo axioma 3 temos que $1 \in M$ e se $n \in M$, pela definição de M, temos $n^* \neq n$ e consequentemente por (1), segue $(n^*)^* \neq n^*$, logo $n^* \in M$ e pelo axioma 5 vamos ter $M = \mathbb{N}$

Parte (3) . Seja

$$M = \{1\} \cup \{n \in \mathbb{N} \ / \ \exists\ m, m \in \mathbb{N} \text{ tal que } n = m^*\}$$

Pela definição de M, temos $1 \in M$.Agora, se $n \in M$, com $n \neq 1$, vamos ter $n = m^*$, para algum m. Donde $n^* = (m^*)^*$ e n^* é o sucessor de m^*. Logo $n^* \in M$ e pelo axioma 5 segue que $M = \mathbb{N}$ ■

Do axioma 5 deduzimos imediatamente, o **Primeiro Princípio de Indução Completa:**

"Associemos a cada número natural n uma propriedade $P(n)$ (que pode ser verdadeira ou falsa). Suponhamos que

a) $P(1)$ é verdadeira;

b) para todo número natural k tal que $P(k)$ seja verdadeira, $P(k+1)$ também é verdadeira. Então, $P(n)$ é verdadeira para todo número natural n."

Com efeito, seja $S = \{n \in \mathbb{N} \mid P(n) \text{ é verdadeira}\}$. Conforme as hipóteses a) e b) acima temos $1 \in S$ e se $k \in S$, então, $k+1 \in S$, ou seja, as condições do axioma de indução completa estão satisfeitas, portanto, S coincide com o conjunto de todos os números naturais, isto é, $P(n)$ é verdadeira para todo número natural n.

1.2 ADIÇÃO DE NÚMEROS NATURAIS

Definição 1.2.1 *A **adição** em $\mathbb{N}$ é definida por:*

(1) $n + 1 = n^*$ para todo $n \in \mathbb{N}$

(2) $n + m^* = (n + m)^*$ sempre que $n + m$ está definido

A título de ilustração daremos um exemplo de como determinar a soma de 2 e 3.

$(2 + 1) = 2^* = 3$
$(2 + 2) = (2 + 1)^* = 3^* = 4$
$(2 + 3) = (2 + 2)^* = 4^* = 5$

Teorema 1.2.2 *Para quaisquer m, n e p pertencentes $\mathbb{N}$, tem-se:*

(1) $n + m \in \mathbb{N}$ ($\mathbb{N}$ *é fechado em relação à adição*)

(2) $m + (n + p) = (m + n) + p$ (*associatividade*)

Demonstração. Parte (1): Suponhamos que n é um número natural fixo mas arbitrário e consideremos a proposição

$$P(m) : n + m \in \mathbb{N}, \text{ para todo } m \in \mathbb{N}.$$

Assim

$$P(1) : n + 1 \in \mathbb{N}$$

é verdadeira, pois

$$n + 1 \overset{(1.2.1.(1))}{=} n^*$$

e $n^* \in \mathbb{N}$ (pelo axioma 2). Suponhamos agora, que para algum $k \in \mathbb{N}$

$$P(k) : n + k \in \mathbb{N}$$

seja verdadeira. Então, segue que

$$P(k^*) : n + k^* \in \mathbb{N}$$

é verdadeira, pois:

$$n + k^* \overset{(1.2.1.(2))}{=} (n + k)^*$$

e $(n + k)^* \in \mathbb{N}$ sempre que $n + k \in \mathbb{N}$ (pelo axioma 2). Portanto, por indução, $P(m)$ é verdadeira para todo $m \in \mathbb{N}$ e, como n era um número natural qualquer, fica demonstrado que $\mathbb{N}$ é fechado em relação à adição.

Parte (2): Vamos mostrar que $m + (n + p) = (m + n) + p$ para todo $m, n, p \in \mathbb{N}$. Sejam m, n números naturais fixos e consideremos a proposição

$$P(p) : m + (n + p) = (m + n) + p, \quad \text{para todo } p \in \mathbb{N}$$

Vamos mostrar que $P(p)$ é válido para $p = 1$, ou seja,

$$P(1) : m + (n + 1) = (m + n) + 1$$

Temos:

$$m + (n + 1) \overset{(1.2.1.(1))}{=} m + n^* \overset{(1.2.1.(2))}{=} (m + n)^* \overset{(1.2.1.(1))}{=} (m + n) + 1$$

logo $P(1)$ é verdadeira. Suponhamos que para $p = k \in \mathbb{N}$

$$P(k) : m + (n + k) = (m + n) + k$$

seja verdadeira. Vamos mostrar que

$$P(k^*) : m + (n + k^*) = (m + n) + k^*$$

é verdadeira.Temos:

$$\begin{aligned} m + (n + k^*) &\overset{(1.2.1.(2))}{=} m + (n + k)^* \overset{(1.2.1.(2))}{=} (m + (n + k))^* \\ &\overset{(\text{hipótese})}{=} ((m + n) + k)^* \overset{(1.2.1.(2))}{=} (m + n) + k^* \end{aligned}$$

Logo $P(k^*)$ é verdadeira e pelo Príncipio de Indução $P(p)$ está demonstrada $\forall m, n, p \in \mathbb{N}$. ■

Na demonstração do próxima Teorema será necessário o seguinte lema.

Lema 1.2.3 *Para todo $n \in \mathbb{N}$, tem-se $n+1 = 1+n$*

Demonstração. Vamos mostrar que $n+1 = 1+n$ para todo $n \in \mathbb{N}$. Considere a proposição:

$$P(n) : n+1 = 1+n, \text{ para todo } n \in \mathbb{N}$$

Claramente

$$P(1) : 1+1 = 1+1$$

é verdadeira. Suponhamos que para $n = k \in \mathbb{N}$

$$P(k) : k+1 = 1+k$$

seja verdadeira. Vamos mostrar que

$$P(k^*) : k^*+1 = 1+k^*$$

é verdadeira. Temos:

$$k^*+1 \overset{(1.2.1.(1))}{=} (k+1)+1 \overset{(\text{hipótese})}{=} (1+k)+1$$
$$\overset{(1.2.2.(2))}{=} 1+(k+1) \overset{(1.2.1.(1))}{=} 1+k^*$$

logo $P(k^*)$ é verdadeira e pelo Príncipio de Indução $P(n)$ está demonstrada. ■

Teorema 1.2.4 *Se m, n e p são números naturais, temos as seguintes propriedades:*

(1) $n+m = m+n$ (*comutatividade*)

(2) $m+r = n+r \Rightarrow m = n$ (*lei do corte*)

Demonstração. Parte (1): Suponhamos que n seja um número natural fixo mas arbitrário e consideremos a proposição

$$P(m) : n+m = m+n, \forall\ m \in \mathbb{N}$$

Pelo Lema(1.2.3), sabemos que $P(1)$ é verdadeira $\forall\ n \in \mathbb{N}$, ou seja,

$$P(1) : n+1 = 1+n, \forall\ n \in \mathbb{N}$$

Suponhamos que para $m = k \in \mathbb{N}$,

$$P(k) : n + k = k + n$$

seja verdadeira. Devemos mostrar que a proposição,

$$P(k^*) : n + k^* = k^* + n$$

é verdadeira. Temos:

$$n + k^* \overset{(1.2.1.(2))}{=} (n + k)^* \overset{\text{(hipótese)}}{=} (k + n)^* \overset{(1.2.1.(2))}{=} k + n^*$$
$$\overset{(1.2.1.(1))}{=} k + (n + 1) \overset{(1.2.3)}{=} k + (1 + n) \overset{(1.2.2.(2))}{=} (k + 1) + n \overset{(1.2.1.(1))}{=} k^* + n$$

logo $P(k^*)$ é verdadeira e pelo Príncipio de Indução $P(m)$ está demonstrada.

Parte (2): Suponhamos m, n números naturais fixos e consideremos a proposição

$$P(r) : m + r = n + r \Rightarrow m = n$$

Claramente $P(1)$ é verdadeira, pois.

$$m + 1 = n + 1 \overset{(1.2.1.(1))}{\Rightarrow} m^* = n^* \overset{\text{(axioma 4)}}{\Rightarrow} m = n$$

Suponhamos, que para $r = k \in \mathbb{N}$

$$P(k) : m + k = n + k \Rightarrow m = n$$

seja verdadeira. Devemos mostrar que a proposição

$$P(k^*) : m + k^* = n + k^* \Rightarrow m = n$$

é verdadeira. Se

$$\begin{aligned} m + k^* &= n + k^* \\ &\Rightarrow m + (k + 1) = n + (k + 1) \ \text{(Por (1.2.1. (1)))} \\ &\Rightarrow (m + k) + 1 = (n + k) + 1 \ \ \text{(Por (1.2.2. (2)))} \\ &\Rightarrow (m + k) = (n + k) \ \ \text{(Por (P(1))} \\ &\Rightarrow m = n \ \text{(Pela hipótese)} \end{aligned}$$

Logo $P(k^*)$ é verdadeira e pelo Príncipio de Indução $P(r)$ está demonstrada. ■

Teorema 1.2.5 *Dados $m, n \in \mathbb{N}$ tais que $m = n$, então $m + r = n + r$, para todo $r \in \mathbb{N}$.*

Demonstração. Suponhamos que m, n sejam números naturais fixo e consideremos a proposição

$$P(r) : m = n \Rightarrow m + r = n + r$$

Para $r = 1$, observamos claramente que

$$P(1) : m = n \Rightarrow m + 1 = n + 1$$

é verdadeira (axioma 2).

Suponhamos que para $r = k \in \mathbb{N}$,

$$P(k) : m = n \Rightarrow m + k = n + k$$

seja verdadeira. Vamos mostrar que $P(k^*)$,

$$P(k^*) : m = n \Rightarrow m + k^* = n + k^*$$

é verdadeira. De fato, temos que:

$$\begin{aligned} m &= n \Rightarrow m + k = n + k \ \ (\text{Por P(k)}) \\ &\Rightarrow (m + k) + 1 = (n + k) + 1 \ (\text{Por P}(1)) \\ &\Rightarrow m + (k + 1) = n + (k + 1) \ \ (\text{Por 1.2.2.}(2)) \\ &\Rightarrow m + k^* = n + k^* \ \ (\text{Por 1.2.1.}(1))) \end{aligned}$$

Logo $P(k^*)$ é verdadeira, e pelo Princípio de Indução $P(r)$ é válida para todo $m, n, r \in \mathbb{N}$. ■

Teorema 1.2.6 *Para todo $m, n \in \mathbb{N}$, tem-se $n + m \neq m$*

Demonstração. Suponhamos que n seja número natural fixo e consideremos a proposição

$$P(m) : n + m \neq m \ , \forall \ m \in \mathbb{N}$$

Observamos facilmente que

$$P(1) : n + 1 \neq 1$$

é verdadeira (axioma 3).

Suponhamos que $P(m)$ seja verdadeira para $m = k \in \mathbb{N}$,

$$P(k) : n + k \neq k$$

e vamos mostrar que $P(k^*)$ é válida, ou seja:

$$P(k^*) : n + k^* \neq k^*$$

Observe que $(n+k)^* \neq k^*$, pois pelo (axioma(4)) se $(n+k)^* = k^*$ então $n + k = k$, o que contraria a hipótese. Como

$$(n+k)^* \neq (k)^* \overset{(1.2.1.(2))}{\Rightarrow} n + k^* \neq k^*,$$

logo $P(k^*)$ é verdadeira

Portanto pelo Princípio de Indução $P(m)$ é válida $\forall\ m, n \in \mathbb{N}$. ■

1.3 RELAÇÃO DE ORDEM EM $\mathbb{N}$

Agora que as propriedades usuais da adição estão disponíveis podemos introduzir uma relação de ordem entre os números naturais.

Definição 1.3.1 *Dados os números naturais m e n, diremos que m* ***é menor que*** *n, e escrevemos $m < n$, se existir $p \in \mathbb{N}$ tal que $n = m + p$. Diremos que m* ***é maior que*** *n, e escrevemos $m > n$, se $n < m$.*

Teorema 1.3.2 *Sejam m, n e p números naturais. Então:*

(1) $m < n$ e $n < p \Rightarrow m < p$ (*transitividade*)

(2) $m < n \Leftrightarrow m + p < n + p$ (*monotonicidade*)

Demonstração. Parte (1). Existem números naturais r e t, tais que $n = m + r$ e $p = n + t$. Logo:

$$p \overset{\text{(hipótese)}}{=} n + t \overset{\text{(hipótese)}}{=} (m + r) + t \overset{(1.2.2.(2))}{=} m + (r + t)$$

e, portanto $m < p$.

Parte (2).

($\Rightarrow$) Se $m < n$, então existe $r \in \mathbb{N}$, tal que $n = m + r$, logo

$$n + p \overset{\text{(hipótese)}}{=} (m + r) + p \overset{(1.2.2.(2))}{=} m + (r + p) \overset{(1.2.4.(1))}{=} m + (p + r) \overset{(1.2.2.(2))}{=} (m + p) + r$$

e, portanto $m + p < n + p$.

($\Leftarrow$)Se $m + p < n + p$, então existe $t \in \mathbb{N}$, tal que

$$n + p = (m + p) + t \overset{(1.2.2.(2))}{=} m + (p + t) \overset{(1.2.4.(1))}{=} m + (t + p) \overset{(1.2.2.(2))}{=} (m + t) + p$$

logo por (1.2.4. (2)) $n = m + t$, donde segue $m < n$. ■

Observação 1.3.3 *A relação $<$ é transitiva, porém não é reflexiva e nem simétrica. Pois, dados $m, n \in \mathbb{N}$, com $m < n$ e $n < m$, pela transitividade $m < m$, o que é absurdo. Assim a relação $<$ não é simétrica. Além disso, $n \in \mathbb{N}$ com $n < n$ é falsa, pois se fosse verdadeira, haveria algum $k \in \mathbb{N}$, tal que $n + k = n$, contrariando o teorema*(1.2.6)*, logo a relação $<$ não é reflexiva.*

Teorema 1.3.4 *(Lei Da Tricotomia). Se m e n são números naturais uma e apenas uma das seguintes alternativas é verdadeira:*

(1) $m = n$

ou

(2) $m < n$

ou

(3) $m > n$

Demonstração. É claro que apenas uma das alternativas pode ser válida, pois:

Parte (2) : Se $m < n$, então existe $r \in \mathbb{N}$, tal que $n = m + r$, logo $n \neq m$ (1.2.6). Suponhamos que $n < m$, logo existe $t \in \mathbb{N}$, tal que:

$$m = n + t \overset{\text{(hipótese)}}{=} (m + r) + t \overset{(1.2.2.(2))}{=} m + (r + t)$$

e portanto $m > m$, o que é absurdo.

Parte (3): Se $n < m$, então existe $r \in \mathbb{N}$, tal que $m = n + r$, logo $m \neq n$ (1.2.6).Suponhamos que $m < n$, logo existe $t \in \mathbb{N}$, tal que:

$$n = m + t \overset{\text{(hipótese)}}{=} (n + r) + t \overset{(1.2.2.(2))}{=} n + (r + t)$$

e portanto $n > n$, o que é absurdo.

Parte (1): Se $m = n$, é óbvio que não é válida as outras duas alternativas.

Devemos então demonstrar que uma delas é válida. Fixemos n em $\mathbb{N}$ e façamos

$$M = \{m \in \mathbb{N} \mid m = n \text{ ou } m < n \text{ ou } n < m\}$$

Vamos provar a proposição acima por indução.

Temos que $1 \in M$; de fato, se $n = 1$ não há o que demonstrar e se $n \neq 1$, existe $p \in \mathbb{N}$ tal que

$$n = p^* \overset{(1.2.1.(1))}{=} p + 1$$

e portanto $1 < n$ e pela definição de M , temos $1 \in M$. Agora, suponhamos que $m \in M$ e vamos mostrar que $m^* \in M$, temos três casos a considerar:

Parte $(2) : m < n$. Neste caso, existe $p \in \mathbb{N}$ tal que $n = m + p$. Se $p = 1$, então

$$n = m + 1 \overset{(1.2.1.(1))}{=} m^*$$

e $m^* \in M$; por outro lado se $p \neq 1$ existe $r \in \mathbb{N}$ tal que

$$p \overset{(1.1.3.(3))}{=} r^*$$

e então

$$m^* + r \overset{(1.2.1.(1))}{=} (m + 1) + r \overset{(1.2.2.(2))}{=} m + (1 + r)$$
$$\overset{(1.2.1.(1))}{=} m + r^* \overset{(1.1.3.(3))}{=} m + p \overset{(\text{hipótese})}{=} n$$

logo $m^* < n$ e portanto $m^* \in M$.

Parte $(1) : m = n$. Neste caso temos

$$m^* \overset{(\text{axioma 4})}{=} n^* \overset{(1.2.1.(1))}{=} n + 1$$

ou seja, $n < m^*$ e $m^* \in M$.

Parte $(3) : n < m$. Neste caso temos $m = n + p$ e portanto

$$m^* = (n + p)^* \overset{(1.2.1.(2))}{=} n + p^*$$

ou seja, $n < m^*$ e $m^* \in M$.

Portanto nos três casos $m^* \in M$ e consequentemente pelo Princípio de Indução $M = \mathbb{N}$. ■

Definição 1.3.5 *Dados m e n em $\mathbb{N}$, diremos que m* ***é menor que ou igual à*** *n e escrevemos $m \leq n$ se $m < n$ ou $m = n$. Analogamente, definimos a relação $m \geq n$.*

Vamos agora estabelecer o **Princípio de Indução Generalizada.**

Teorema 1.3.6 *Seja M um subconjunto de números naturais tal que $k \in M$ e $m^* \in M$, para todo $m \geqslant k$ em M. Então, M contém todos os números naturais $n \geq k$.*

Demonstração. Seja $N = \{1; 2; 3; \cdots ; l\} \cup M$, onde l é tal que $l^* = k$. Temos que $1 \in N$, suponhamos que $n \in N$, então $n^* \in N$; logo pelo Princípio de Indução, temos $N = \mathbb{N}$. ■

Definição 1.3.7 *Seja A um subconjunto de $\mathbb{N}$. Diremos que $m \in N$* ***é o menor elemento de*** *A, se:*

(1) $m \in A$

(2) $m \leq n$, para todo n em A

O teorema seguinte, conhecido como o Princípio do Menor Elemento, é um dos resultados mais importantes envolvendo a relação de ordem.

Teorema 1.3.8 *Todo subconjunto não vazio de $\mathbb{N}$ tem um menor elemento.*

Demonstração. Seja $A \subset \mathbb{N}$, $A \neq \emptyset$. Se $1 \in A$ então 1 é o menor elemento de A. Suponhamos então que $1 \notin A$ e que A não tenha menor elemento; isto vai levar á uma contradição. Seja

$$B = \{n \in \mathbb{N} \,|m \leq n \Rightarrow m \notin A\}$$

É claro que $A \cap B = \emptyset$, pois se $n \in B$ então $n \leq n$ e $n \notin A$. Agora, temos que $1 \in B$, pois $1 \leq 1$ e $1 \notin A$. Suponhamos então que $n \in B$. Como $m \notin A$, se $m \leq n$ então $n^* \notin A$, pois senão n^* seria um menor elemento para A. Logo se $m \leq n^*$, vamos ter $m \notin A$ e então $n^* \in B$.

Pelo Princípio de Indução vamos ter $B = \mathbb{N}$. Mas $A \cap B = \emptyset$ e como $B = \mathbb{N}$ segue que $A = \emptyset$, contrariando a hipótese, logo todo subconjunto não vazio de $\mathbb{N}$ tem um menor elemento. ■

Observação 1.3.9 *O Princípio do Menor Elemento é num certo sentido equivalente ao Princípio de Indução. De fato assumindo o Princípio do Menor Elemento como axioma, seja N um subconjunto de $\mathbb{N}$ tal que $1 \in N$ e se $n \in N$ então $n + 1 \in N$; suponhamos que $N \neq \mathbb{N}$. Então $N^c \neq \emptyset$ (complementar de N) e portanto tem um menor elemento k (Teorema*(1.3.8)*). Como $k \neq 1$ (pois $1 \in N$, logo $1 \notin N^c$), existe $h \in \mathbb{N}$ tal que $k = h^*$. Logo $h < k$ e portanto $h \notin N^c$ e então $h \in N$. Mas pela definição de N segue que $k = h^* \in N$, o que é absurdo. Logo $N = \mathbb{N}$.*

1.4 MÚLTIPLICAÇÃO DE NÚMEROS NATURAIS

Definição 1.4.1 *A **multiplicação** em* $\mathbb{N}$ *é definida por:*

(1) $n \cdot 1 = n, \forall\ n \in \mathbb{N}$

(2) $n \cdot m^* = n \cdot m + n$, sempre que $n \cdot m$ está definido

Lema 1.4.2 *Para todo* $n \in \mathbb{N}$*, tem-se* $n \cdot 1 = 1 \cdot n$*.*

Demonstração. Consideremos a proposição

$$P(n) : n \cdot 1 = 1 \cdot n \ , \text{ para todo } n \in \mathbb{N}$$

Claramente

$$P(1) : 1 \cdot 1 = 1 \cdot 1$$

é verdadeira. Suponhamos que para $n = k \in \mathbb{N}$

$$P(k) : k \cdot 1 = 1 \cdot k$$

seja verdadeira. Vamos mostrar que

$$P(k^*) : k^* \cdot 1 = 1 \cdot k^*$$

é verdadeira. Temos:

$$1 \cdot k^* \overset{(1.4.1.(2))}{=} (1 \cdot k) + 1 \overset{\text{(hipótese)}}{=} (k \cdot 1) + 1 \overset{(1.4.1.(1))}{=} k + 1$$
$$\overset{(1.4.1.(1))}{=} (k+1) \cdot 1 \overset{(1.2.1.(1))}{=} k^* \cdot 1$$

logo $P(k^*)$ é verdadeira e pelo Príncipio de Indução $P(n)$ está demonstrada. ■

Teorema 1.4.3 *Para todo* m, n *e* $p \in \mathbb{N}$ *, temos as seguintes propriedades:*

(1) $n \cdot m \in \mathbb{N}$ ($\mathbb{N}$ *é fechado em relação à multiplicação*)

(2) $m \cdot (n + p) = m \cdot n + m \cdot p$ (*distributiva á esquerda*)

(3) $m \cdot (n \cdot p) = (m \cdot n) \cdot p$ (*associatividade*)

(4) $(n+p)\cdot m = n\cdot m + p\cdot m$ (*distributiva á direita*)

(5) $1 \cdot n = n$

(6) $m\cdot n = n\cdot m$ (*comutatividade*)

Demonstração. Parte (1): Suponhamos que n seja um número natural fixo mas arbitrário e consideremos a proposição

$$P(m) : n \cdot m \in \mathbb{N}, \text{ para todo } m \in \mathbb{N}.$$

Assim

$$P(1) : n \cdot 1 \in \mathbb{N}$$

é verdadeira, pois

$$n \cdot 1 \overset{(1.4.1.(1))}{=} n$$

e $n \in \mathbb{N}$. Suponhamos agora, que para algum $k \in \mathbb{N}$

$$P(k) : n \cdot k \in \mathbb{N}$$

seja verdadeira. Então, segue que

$$P(k^*) : n \cdot k^* \in \mathbb{N}$$

é verdadeira, pois

$$n \cdot k^* \overset{(1.4.1.(2))}{=} n \cdot k + n$$

e $n \cdot k \in \mathbb{N}$ (hipótese), logo $(n \cdot k + n) \in \mathbb{N}$ (Por $(1.2.2.(1))$). Portanto, por indução, $P(m)$ é verdadeira para todo $m \in \mathbb{N}$ e, como n era um número natural qualquer, fica demonstrado que $\mathbb{N}$ é fechado em relação à multiplicação.

Parte (2): Sejam m, n números naturais fixos e consideremos a proposição

$$P(p) : m \cdot (n+p) = m \cdot n + m \cdot p, \forall\ p \in \mathbb{N}$$

Vamos mostrar que $P(p)$ é válido para $p = 1$, ou seja,

$$P(1) : m \cdot (n+1) = m \cdot n + m \cdot 1$$

Temos:

$$m \cdot (n+1) \overset{(1.2.1.(1))}{=} m \cdot n^* \overset{(1.4.1.(2))}{=} m \cdot n + m \overset{(1.4.1.(1))}{=} m \cdot n + m \cdot 1$$

logo $P(1)$ é verdadeira. Suponhamos que para $p = k \in \mathbb{N}$

$$P(k) : m \cdot (n + k) = m \cdot n + m \cdot k$$

seja verdadeira. Vamos mostrar que

$$P(k^*) : m \cdot (n + k^*) = m \cdot n + m \cdot k^*$$

é verdadeira. Temos:

$$\begin{aligned} m \cdot (n + k^*) &\overset{(1.2.1.(1))}{=} m \cdot [n + (k + 1)] \\ &\overset{(1.2.2.(2))}{=} m \cdot [(n + k) + 1] \\ &\overset{(P(1))}{=} m \cdot (n + k) + m \cdot 1 \\ &\overset{(\text{hipótese})}{=} m \cdot n + m \cdot k + m \cdot 1 \\ &\overset{(P(1))}{=} m \cdot n + m \cdot (k + 1) \\ &\overset{(1.2.1.(1))}{=} m \cdot n + m \cdot k^* \end{aligned}$$

Logo $P(k^*)$ é verdadeira e pelo Príncipio de Indução $P(p)$ está demonstrada.

Parte (3): Sejam m, n números naturais fixos e consideremos a proposição

$$P(p) : m \cdot (n \cdot p) = (m \cdot n) \cdot p, \forall\ p \in \mathbb{N}$$

Vamos mostrar que $P(p)$ é válido para $p = 1$, ou seja,

$$P(1) : m \cdot (n \cdot 1) = (m \cdot n) \cdot 1$$

Temos:

$$m \cdot (n \cdot 1) \overset{(1.4.1.(1))}{=} m \cdot n \overset{(1.4.1.(1))}{=} (m \cdot n) \cdot 1$$

logo $P(1)$ é verdadeira. Suponhamos que para $p = k \in \mathbb{N}$

$$P(k) : m \cdot (n \cdot k) = (m \cdot n) \cdot k$$

seja verdadeira. Vamos mostrar que

$$P(k^*) : m \cdot (n \cdot k^*) = (m \cdot n) \cdot k^*$$

é verdadeira. Temos:

$$\begin{aligned} m \cdot (n \cdot k^*) &\overset{(1.4.1.(2))}{=} m \cdot (n \cdot k + n) \\ &\overset{(1.4.3.(2))}{=} m \cdot (n \cdot k) + m \cdot n \overset{(\text{hipótese})}{=} (m \cdot n) \cdot k + m \cdot n \\ &\overset{(1.4.1.(2))}{=} (m \cdot n) \cdot k^* \end{aligned}$$

Logo $P(k^*)$ é verdadeira e pelo Príncipio de Indução $P(p)$ está demonstrada.

Parte (4): Sejam n, p números naturais fixos e consideremos a proposição

$$P(m) : (n+p) \cdot m = n \cdot m + p \cdot m, \forall\ m \in \mathbb{N}$$

Vamos mostrar que $P(m)$ é válido para $m = 1$, ou seja,

$$P(1) : (n+p) \cdot 1 = n \cdot 1 + p \cdot 1$$

Temos:

$$(n+p) \cdot 1 \overset{(1.4.1.(1))}{=} n + p \overset{(1.4.1.(1))}{=} n \cdot 1 + p \cdot 1$$

logo $P(1)$ é verdadeira. Suponhamos, em seguida, que para $m = k \in \mathbb{N}$

$$P(k) : (n+p) \cdot k = n \cdot k + p \cdot k$$

seja verdadeira. Vamos mostrar que

$$P(k^*) : (n+p) \cdot k^* = n \cdot k^* + p \cdot k^*$$

é verdadeira. Temos:

$$\begin{aligned}
&(n+p) \cdot k^* \overset{(1.4.1.(2))}{=} (n+p) \cdot k + (n+p) \\
&\overset{(\text{hipótese})}{=} n \cdot k + p \cdot k + (n+p) \\
&\overset{(1.2.2.(2))}{=} n \cdot k + (p \cdot k + n) + p \overset{(1.2.4.(1))}{=} n \cdot k + (n + p \cdot k) + p \\
&\overset{(1.2.2.(2))}{=} (n \cdot k + n) + (p \cdot k + p) \overset{(1.4.3.(2))}{=} n \cdot (k+1) + p \cdot (k+1) \\
&\overset{(1.2.1.(1))}{=} n \cdot k^* + p \cdot k^*
\end{aligned}$$

Logo $P(k^*)$ é verdadeira e pelo Príncipio de Indução $P(m)$ está demonstrada.

Parte (5): Consideremos a proposição

$$P(n) : 1 \cdot n = n, \forall\ n \in \mathbb{N}$$

Vamos mostrar que $P(n)$ é válido para $n = 1$.

Claramente $P(1) : 1 \cdot 1 = 1$ é verdadeira. Suponhamos que para $n = k \in \mathbb{N}$

$$P(k) : 1 \cdot k = k$$

seja verdadeira. Devemos mostrar que

$$P(k^*) : 1 \cdot k^* = k^*$$

é verdadeira. Temos:

$$1 \cdot k^* \overset{(1.4.1.(2))}{=} 1 \cdot k + 1 \overset{(\text{hipótese})}{=} k + 1 \overset{(1.2.1.(1))}{=} k^*$$

logo $P(k^*)$ é verdadeira e pelo Príncipio de Indução $P(n)$ está demonstrada.

Parte (6): Suponhamos que n é um número natural fixo mas arbitrário e consideremos a proposição

$$P(m) : n \cdot m = m \cdot n, \forall\ m \in \mathbb{N}$$

Segue do Lema(1.4.2) que $P(m)$ é válida para $m = 1$, ou seja

$$P(1) : n \cdot 1 = 1 \cdot n, \forall\ n \in \mathbb{N}$$

Suponhamos agora que $P(m)$ é válido para $m = k \in \mathbb{N}$, ou seja,

$$P(k) : n \cdot k = k \cdot n$$

Vamos mostrar que $P(m)$ é válido para $m = k^*$, ou seja,

$$P(k^*) : n \cdot k^* = k^* \cdot n$$

Temos:

$$n \cdot k^* \overset{(1.4.1.(2))}{=} n \cdot k + n \overset{(\text{hipótese})}{=} \dot{k} \cdot n + n \overset{(1.4.3.(5))}{=} \dot{k} \cdot n + 1 \cdot n$$
$$\overset{(1.4.3.(4))}{=} (k+1) \cdot n \overset{(1.2.1.(1))}{=} k^* \cdot n$$

logo $P(k^*)$ é verdadeira e pelo Príncipio de Indução $P(m)$ está demonstrada. ■

Teorema 1.4.4 *Sejam m, n, p e q números naturais quaisquer. Então, as seguintes propriedades são válidas:*

(1) $m < n + 1 \Rightarrow m \leq n$

(2) $m + p \leq n + p \Leftrightarrow m \leq n$ (*monotonicidade da adição*)

(3) $m < n$ e $p < q \Rightarrow m + p < n + q$ (*princípio* da soma de igualdade)

(4) $m < n \Rightarrow m \cdot p < n \cdot p$ (*monotonicidade da* multiplicação)

(5) $m \cdot p = n \cdot p \Rightarrow m = n$ (*lei* do corte)

(6) $1 \leq n$

(7) $m < n \Rightarrow m + 1 \leq n$

(8) $m \leq n$ e $n \leq m \Rightarrow m = n$ (anti-simétrica)

Demonstração. Parte (1): Se $m < n + 1$, resulta que existe $p \in \mathbb{N}$, tal que $n + 1 = m + p$.

Se $p = 1$, significa que

$$n + 1 = m + 1 \overset{(1.2.4.(2))}{\Rightarrow} n = m$$

logo, a igualdade ocorre.

Se $p \neq 1$, existe $q \in \mathbb{N}$ tal que $p = q^*$, logo

$$\begin{aligned} n + 1 &= m + q^* \overset{(1.2.1.(1))}{=} m + (q + 1) \overset{(1.2.2.(2))}{=} (m + q) + 1 \\ \overset{(1.2.4.(2))}{\Rightarrow} n &= m + q \end{aligned}$$

portanto $n = m + q$, donde segue $m < n$ e a desigualdade ocorre.

Parte (2):

($\Rightarrow$) Se $m + p \leq n + p$, então $m + p = n + p$ ou $m + p < n + p$.

Se

$$m + p = n + p \overset{(1.2.4.(2))}{\Rightarrow} m = n$$

logo, a igualdade ocorre.

Se

$$m + p < n + p$$

existe $r \in \mathbb{N}$, tal que

$$n + p \overset{(\text{hipótese})}{=} (m + p) + r \overset{(1.2.2.(2))}{=} m + (p + r) \overset{(1.2.4.(1))}{=} m + (r + p) \overset{(1.2.2.(2))}{=} (m + r) + p$$

portanto $n = m + r$, donde segue $m < n$ e a desigualdade ocorre.

($\Leftarrow$) Se $m \leq n$, então $m = n$ ou $m < n$.

Se

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

logo, a igualdade ocorre.

Se $m < n$ existe $r \in \mathbb{N}$, tal que $n = m + p$, logo:

$$n + p \overset{\text{(hipótese)}}{=} (m + p) + r \overset{(1.3.1)}{\Rightarrow} m + p < n + p$$

logo, a desigualdade ocorre.

Parte (3): Temos que:

Se $m < n$, então existe $t \in \mathbb{N}$, tal que $n = m + t$ **.**

Se $p < q$, então existe $r \in \mathbb{N}$, tal que $q = p + r$.

Logo

$$\begin{aligned} n + q &\overset{\text{(hipótese)}}{=} (m + t) + (p + r) \overset{(1.2.2.(2))}{=} m + (t + p) + r \\ &\overset{(1.2.4.(1))}{=} m + (p + t) + r \overset{(1.2.2.(2))}{=} (m + p) + t + r \end{aligned}$$

logo $m + p < n + q$

Parte (4): Suponhamos que m, n são números naturais fixos mas arbitrários e consideremos a proposição

$$P(p) : m < n \Rightarrow m \cdot p < n \cdot p \ , \forall \ p \in \mathbb{N}$$

Por $(1.4.1.\,(1))$ segue que $P(p)$ é válida para $p = 1$, ou seja,

$$P(1) : m < n \Rightarrow m \cdot 1 < n \cdot 1$$

Suponhamos agora que $P(p)$ é válida para $p = k \in \mathbb{N}$, ou seja,

$$P(k) : m < n \Rightarrow m \cdot k < n \cdot k$$

devemos mostrar que

$$P(k^*) : m < n \Rightarrow m \cdot k^* < n \cdot k^*$$

é verdadeira. Temos que

$$\begin{aligned} m &< n \overset{\text{(hipótese)}}{\Rightarrow} m \cdot k < n \cdot k \\ \overset{(1.4.4.(3))}{\Rightarrow} m \cdot k + m &< n \cdot k + n \\ \overset{(1.4.1.(2))}{\Rightarrow} m \cdot k^* &< n \cdot k^* \end{aligned}$$

logo $P(k^*)$ é verdadeira e pelo Príncipio de Indução $P(p)$ é verdadeira para todo $n, m, p \in \mathbb{N}$.

Parte (5): Vamos mostrar que $m \cdot p = n \cdot p \Rightarrow m = n$ para todo n, m e $p \in \mathbb{N}$. Suponhamos por absurdo que $m \neq n$. Então pela Lei da Tricotomia, $m < n$ ou $n < m$. Por (1.4.4. (4)), se $m < n$ temos $m \cdot p < n \cdot p$ e se $n < m$ temos $n \cdot p < m \cdot p$. Consequentemente, em ambos os casos temos $m \cdot p \neq n \cdot p$, o que contraria à hipótese.

Parte (6): Vamos mostrar que $1 \leq n$, $\forall\ n \in \mathbb{N}$.

Se $n = 1$, a igualdade ocorre, pois $1 = 1$.

Se $n \neq 1$, temos por (1.1.3. (3)) que existe $m \in \mathbb{N}$, tal que $n = m^* = m+1$, logo $n > 1$ e a desigualdade ocorre.

Parte (7): Vamos mostrar que se $m < n$, então, $m + 1 \leq n, \forall\ m, n \in \mathbb{N}$.

Se $m < n$, resulta que existe $q \in \mathbb{N}$ tal que $n = m + q$.

Se $q = 1$, ocorre a igualdade, pois $m + 1 = n$

Se $q \neq 1$, existe $r \in \mathbb{N}$ tal que $q = r^*$, logo

$$n \overset{\text{(hipótese)}}{=} m + q \overset{\text{(hipótese)}}{=} m + r^* \overset{(1.2.1.(1))}{=} m + (r + 1)$$
$$\overset{(1.2.4.(1))}{=} m + (1 + r) \overset{(1.2.2.(2))}{=} (m + 1) + r$$

logo, a desigualdade ocorre.

Parte (8): Vamos mostrar que,

$$m \leq n \text{ e } n \leq m \Rightarrow m = n$$

Suponhamos por absurdo que $m \neq n$. Por hipótese, temos

$$m < n \text{ e } n < m \Rightarrow m < m$$

absurdo. Portanto, se

$$m \leq n \text{ e } n \leq m \Rightarrow m = n$$

■

Teorema 1.4.5 *Mostre que o conjunto* $\mathbb{N}$ *é bem ordenado.*

Consideremos qualquer subconjunto $S \neq \emptyset$ de $\mathbb{N}$. Devemos mostrar que S tem um mínimo. Isto certamente é verdade se $1 \in S$ (Por (1.4.4. (6))). Suponhamos $1 \notin S$, então, $1 < s$ para todo $s \in S$. Denotemos por K o conjunto

$$K = \{k \in \mathbb{N}, k \leq s \text{ para todo } s \in S\}$$

Como $1 \in K$, temos que $K \neq \emptyset$. Além disso $K \neq \mathbb{N}$; portanto, deve existir um $r \in K$ tal que $r^* \notin K$. Este $r \in S$, pois, caso contrário, $r < s$ e, assim $r^* \leq s$, $\forall\, s \in S$ (Por (1.4.4.7)) . Mas, então, $r^* \in K$, uma contradição. Portanto r é o elemento mínimo de S. Como S é qualquer subconjunto não vazio de $\mathbb{N}$, cada conjunto não vazio de $\mathbb{N}$ tem um mínimo e $\mathbb{N}$ é bem ordenado.

1.5 POTÊNCIAS DE NÚMEROS NATURAIS

Definição 1.5.1 *Seja $a \in \mathbb{N}$, onde operações binárias $+$ e $\cdot$ estão definidas, e defina*

(1) $a^1 = a$

(2) $a^{n+1} = a^n \cdot a$

sempre que a^n, para $n \in \mathbb{N}$, está definido.

Exemplo 1.5.2 *Como $a^1 = a$, temos:*

$$\begin{aligned} a^2 &= a^{1+1} \overset{(1.5.1.(2))}{=} a^1 \cdot a \overset{(1.5.1.(1))}{=} a \cdot a \\ a^3 &= a^{2+1} \overset{(1.5.1.(2))}{=} a^2 \cdot a = a \cdot a \cdot a \end{aligned}$$

Teorema 1.5.3 *Para todo n em $\mathbb{N}$ temos, $1^n = 1$*

Demonstração. Consideremos a proposição

$$P(n) : 1^n = 1 \ , \forall\ n \in \mathbb{N}$$

Por $(1.5.1.\,(1))$, $P(n)$ é verdadeira para $n = 1$.
Suponhamos que para $n = k \in \mathbb{N}$

$$P(k) : 1^k = 1$$

seja verdadeira. Devemos mostrar que

$$P(k^*) : 1^{k^*} = 1$$

é verdadeira. Temos que

$$1^{k^*} \overset{(1.2.1.(1))}{=} 1^{k+1} \overset{(1.5.1.(2))}{=} 1^k \cdot 1 \overset{(\text{hipótese})}{=} 1 \cdot 1 \overset{(1.4.3.(5))}{=} 1$$

logo $P(k^*)$ é verdadeira e pelo Príncipio de Indução $P(n)$ está demonstrada.
■

Teorema 1.5.4 *Quaisquer que sejam os números naturais m, n, a e $b \in \mathbb{N}$, tem-se:*

(1) $a^{m+n} = a^m \cdot a^n$

(2) $a^{m \cdot n} = (a^m)^n = (a^n)^m$

(3) $(a \cdot b)^n = a^n \cdot b^n$

Demonstração. Parte (1): Vamos mostrar que $a^{m+n} = a^m \cdot a^n$ para todo m, n e $a \in \mathbb{N}$. Seja m um número natural fixo mas arbitrário e consideremos a proposição

$$P(n) : a^{m+n} = a^m \cdot a^n \ , \forall \ n \in \mathbb{N}$$

Para $n = 1$, temos:

$$P(1) : a^{m+1} = a^m \cdot a^1$$

a qual é verdadeira, pois:

$$a^{m+1} \overset{(1.5.1.(2))}{=} a^m \cdot a^1$$

Suponhamos que para $n = k \in \mathbb{N}$

$$P(k) : a^{m+k} = a^m \cdot a^k$$

seja verdadeira. Devemos mostrar que

$$P(k^*) : a^{m+k^*} = a^m \cdot a^{k^*}$$

é verdadeira. Temos que

$$\begin{aligned} a^{m+k^*} &\overset{(1.2.1.(1))}{=} a^{m+(k+1)} \overset{(1.2.2.(2))}{=} a^{(m+k)+1} \overset{(1.5.1.(2))}{=} a^{(m+k)} \cdot a \\ &\overset{\text{(hipótese)}}{=} \left(a^m \cdot a^k\right) \cdot a \overset{(1.4.3.(3))}{=} a^m \cdot \left(a^k \cdot a\right) \\ &\overset{(1.5.1.(2))}{=} a^m \cdot a^{k+1} \overset{(1.2.1.(1))}{=} a^m \cdot a^{k^*} \end{aligned}$$

Logo $P(k^*)$ é verdadeira e pelo Príncipio de Indução $P(n)$ está demonstrada.

Parte (2): Vamos mostrar que $a^{m \cdot n} = (a^m)^n$ para todo m, n e $a \in \mathbb{N}$. Seja m um número natural fixo porém arbitrário e consideremos a proposição

$$P(n) : a^{m \cdot n} = (a^m)^n \ , \forall \ n \in \mathbb{N}$$

Para $n = 1$, temos:

$$P(1) : a^{m\cdot 1} = (a^m)^1$$

a qual é verdadeira, pois:

$$a^{m\cdot 1} \overset{(1.4.1.(1))}{=} a^m \overset{(1.5.1.(1))}{=} (a^m)^1$$

Suponhamos que para $n = k \in \mathbb{N}$

$$P(k) : a^{m\cdot k} = (a^m)^k$$

seja verdadeira. Devemos mostrar que

$$P(k^*) : a^{m\cdot k^*} = (a^m)^{k^*}$$

é verdadeira. Temos que

$$\begin{aligned} a^{m\cdot k^*} &\overset{(1.2.1.(1))}{=} a^{m\cdot(k+1)} \overset{(1.4.3.(2))}{=} a^{m\cdot k+m} \overset{(1.5.4.(1))}{=} a^{m\cdot k}\cdot a^m \\ &\overset{(\text{hipótese})}{=} (a^m)^k \cdot a^m \overset{(1.5.1.(1))}{=} (a^m)^k \cdot (a^m)^1 \\ &\overset{(1.5.4.(1))}{=} (a^m)^{k+1} \overset{(1.2.1.(1))}{=} (a^m)^{k^*} \end{aligned}$$

Logo $P(k^*)$ é verdadeira e pelo Príncipio de Indução $P(n)$ está demonstrada.

Observamos que a segunda parte de (1.5.4. (2)) é uma consequência imediata do fato que a multiplicação sobre $\mathbb{N}$ é comutativa, logo:

$$a^{m\cdot n} = (a^m)^n = (a^n)^m$$

é verdadeira $\forall$ a, m e $n \in \mathbb{N}$

Parte (3): Vamos mostrar que $(a\cdot b)^n = a^n \cdot b^n$ para todo a, b e $n \in \mathbb{N}$. Consideremos a proposição

$$P(n) : (a\cdot b)^n = a^n \cdot b^n, \ \forall\ n \in \mathbb{N}$$

$P(1)$ é verdadeira, pois:

$$(a\cdot b)^1 \overset{(1.5.1.(1))}{=} a\cdot b \overset{(1.5.1.(1))}{=} a^1 \cdot b^1$$

Suponhamos que para $n = k \in \mathbb{N}$

$$P(k) : (a\cdot b)^k = a^k \cdot b^k$$

seja verdadeira. Devemos mostrar que

$$P\left(k^*\right) : \left(a \cdot b\right)^{k^*} = a^{k^*} \cdot b^{k^*}$$

é verdadeira. Temos que

$$\begin{aligned}
&\left(a \cdot b\right)^{k^*} \overset{(1.2.1.(1))}{=} \left(a \cdot b\right)^{k+1} \overset{(1.5.1.(2))}{=} \left(a \cdot b\right)^{k} \cdot \left(a \cdot b\right) \\
&\overset{\text{(hipótese)}}{=} \left(a^k \cdot b^k\right) \cdot \left(a \cdot b\right) \overset{(1.4.3.(3))}{=} a^k \cdot \left(b^k \cdot a\right) \cdot b \\
&\overset{(1.4.3.(6))}{=} a^k \cdot \left(a \cdot b^k\right) \cdot b \overset{(1.4.3.(3))}{=} \left(a^k \cdot a\right) \cdot \left(b^k \cdot b\right) \\
&\overset{(1.5.1.(2))}{=} a^{k+1} \cdot b^{k+1} \overset{(1.2.1.(1))}{=} a^{k^*} \cdot b^{k^*}
\end{aligned}$$

Logo $P\left(k^*\right)$ é verdadeira e pelo Príncipio de Indução $P\left(n\right)$ está demonstrada. ■

Capítulo 2

NÚMEROS INTEIROS

Como motivação deste capítulo consideremos o seguinte problema, análogo a outros que surgirão em capítulos posteriores: dados dois números naturais a e b, determinar um número natural x tal que $a+x=b$. Com o conhecimento que já possuimos do conjunto dos números naturais ($\mathbb{N}$) é possível afirmar que tal problema nem sempre tem solução (mais precisamente, só admite solução quando $a<b$). Entretanto (usando uma linguagem não rigorosa) é possível "ampliar" o conjunto $\mathbb{N}$, introduzindo novos elementos, de modo a se obter um conjunto onde o problema acima tenha sempre solução. Realmente, o que faremos é determinar um certo conjunto $\mathbb{Z}$ (conjunto dos número inteiros) e aí definir uma operação de adição e outra de multiplicação e identificar depois, num certo sentido, o conjunto $\mathbb{N}$ como um subconjunto de $\mathbb{Z}$ e, finalmente, mostrar que no conjunto $\mathbb{Z}$ o problema acima tem sempre solução.

2.1 RELAÇÕES DE EQUIVALÊNCIA E CONJUNTOS QUOCIENTE.

Para conveniencia do leitor vamos lembrar aqui as noções de relação de equivalência e de conjunto quociente.

Definição 2.1.1 *Uma* ***relação*** *R num conjunto A é qualquer subconjunto do produto cartesiano $A\times A$: $R\subset A\times A$.*

Se R é uma relação em A, e se $(x,y)\in R$, escrevemos também xRy :

$$(x,y)\in R \Leftrightarrow xRy$$

Definição 2.1.2 *Uma* ***relação de equivalênica*** *num conjunto A é uma relação tal que, para $a,b,c\in A$, as seguintes propriedades são verificadas:*

(1) $aRa, \forall a, a \in A$ $(reflexiva)$

(2) $aRb \Rightarrow bRa$ $(simétrica)$

(3) $aRb \text{ e } bRc \Rightarrow aRc$ $(transitiva)$

Definição 2.1.3 *Seja R uma relação de equivalência num conjunto A e $a \in A$ um elemento fixado. O conjunto*

$$\overline{a} = \{x \in A \mid xRa\}$$

denomina-se ***a classe de equivalência*** *de a pela relação R.*

Teorema 2.1.4 *Seja R uma relação de equivalência. Então, se a e b são elementos de A, temos:*

(1) $a \in \overline{a}, \forall a, a \in A$

(2) $\overline{a} = \overline{b} \Leftrightarrow aRb$

(3) $\overline{a} \neq \overline{b} \Rightarrow \overline{a} \cap \overline{b} = \emptyset$

Demonstração. Parte (1)**:** Como R é uma relação de equivalência segue que aRa, para todo $a \in A$. Logo, pela definição de $\overline{a}, a \in \overline{a}$.

Parte (2)**:** Como $\overline{a} = \overline{b}$ segue, pela Parte (1), que $b \in \overline{a}$. Pela definição de $\overline{a}$, segue então que aRb. Recíprocamente, se aRb e $x \in \overline{a}$ então, por transitividade, xRb e portanto $x \in \overline{b}$; ou seja $\overline{a} \subset \overline{b}$. Trocando-se os papéis de a por b tem-se $\overline{b} \subset \overline{a}$, logo $\overline{a} = \overline{b}$

Parte (3)**:** Suponhamos que $\overline{a} \cap \overline{b} \neq \emptyset$ e seja $c \in \overline{a} \cap \overline{b}$. Então, aRc e cRb. Logo, aRb e consequentemente, pela Parte (2), segue que $\overline{a} = \overline{b}$, contrariando a hipótese. ■

Definição 2.1.5 *Seja R uma relação de equivalência num conjunto A. A família das classes de equivalência em A, pela relação R, denotada por A/R, denomina-se o* ***conjunto quociente de*** *A* ***por*** *R:*

$$A/R = \{\overline{a} \mid a \in A\}$$

Definição 2.1.6 *Seja A um conjunto e P uma família de subconjuntos de A. Dizemos que P* ***é uma partição de*** *A se:*

(1) os elementos de P forem disjuntos dois à dois;

(2) a união dos elementos de P for igual à A.

Teorema 2.1.7 *Seja R uma relação de equivalência num conjunto A. Então, o conjunto quociente A/R é uma partição de A.*

Demonstração. Como as classes de equivalência de A/R são disjuntas, resta demonstrar que sua união contém A. Mas, se $a \in A$ segue que $a \in \overline{a} \subset \cup \{\overline{a} \mid a \in A\}$.

A recíproca deste teorema é também verdadeira. ■

Teorema 2.1.8 *Seja P uma partição de um conjunto A. Então, existe uma relação de equivalência R tal que $A/R = P$.*

Demonstração. Vamos definir uma relação R em A da seguinte maneira:

$$aRb \Leftrightarrow \exists P, P \in \mathcal{P}, \text{tal que } a \in P \text{ e } b \in P$$

A relação R é uma relação de equivalência. De fato, como $\mathcal{P}$ é uma partição de A, dado $a \in A$, existe $P \in \mathcal{P}$ tal que $a \in P$. Óbviamente $a \in P$ e $a \in \mathcal{P}$, e pela definição de R temos a reflexividade: aRa. A simetria da relação R é clara, agora, se aRb e bRc é porque existem conjuntos P_1 e P_2 da partição tais que $a, b \in P_1$ e $b, c \in P_2$. Mas como os elementos da partição são disjuntos e no caso $P_1 \cap P_2 \neq \emptyset$, segue necessariamente que $P_1 = P_2$. Portanto $a, c \in P_1 = P_2$ e aRc.

Por outro lado, é fácil ver que se $a \in P$ então $\overline{a} = P$. Portanto, $A/R = P$

■

2.2 CONSTRUÇÃO DO CONJUNTO $\mathbb{Z}$ DOS NÚMEROS INTEIROS

Teorema 2.2.1 *A relação R no conjunto $\mathbb{N} \times \mathbb{N}$ definida por*

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

é uma relação de equivalência

Demonstração. Parte (1)**:** $\forall\ (a, b) \in \mathbb{N} \times \mathbb{N}$, tem-se $(a, b)\, R\, (a, b)$, pois $a + b = b + a$

Parte (2)**:** Quaisquer que sejam (a, b) e (c, d) em $\mathbb{N} \times \mathbb{N}$, se $(a, b)\, R\, (c, d)$, então, $(c, d)\, R\, (a, b)$. Pois, se

$$\begin{aligned} (a, b)\, R\, (c, d) &\overset{(2.2.1)}{\Rightarrow} a + d = b + c \Rightarrow b + c = a + d \\ &\overset{(1.2.4.(1))}{\Rightarrow} c + b = d + a \overset{(2.2.1)}{\Rightarrow} (c, d)\, R\, (a, b) \end{aligned}$$

Parte(3)**:** Quaisquer que sejam (a,b), (c,d) e (e,f) em $\mathbb{N}\times\mathbb{N}$, se $(a,b)\,R\,(c,d)$ e se $(c,d)\,R\,(e,f)$, então, $(a,b)\,R\,(e,f)$

Se $(a,b)\,R\,(c,d)$ e $(c,d)\,R\,(e,f)$ segue que $a+d=b+c$, $c+f=d+e$, e

$$\begin{aligned} a+d+c+f &= b+c+d+e \\ \overset{(1.2.2.(2))}{\Rightarrow} a+(d+c)+f &= b+(c+d)+e \\ \overset{(1.2.4.(1))}{\Rightarrow} a+f+(d+c) &= b+e+(c+d) \\ \overset{(1.2.4.(1))}{\Rightarrow} a+f+(d+c) &= b+e+(d+c) \\ \overset{(1.2.4.(2))}{\Rightarrow} a+f &= b+e \overset{(2.2.1)}{\Rightarrow} (a,b)\,R\,(e,f) \end{aligned}$$

■

Notação 2.2.2 *Se (a,b) é um elemento qualquer de $\mathbb{N}\times\mathbb{N}$, denotaremos por $\overline{(a,b)}$ a classe de equivalência de (a,b) pela relação R, isto é,*

$$\overline{(a,b)} = \{(x,y)\in\mathbb{N}\times\mathbb{N} : (x,y)\,R\,(a,b)\}$$

O conjunto quociente de $\mathbb{N}\times\mathbb{N}$ por R, constituído pela família das classes de equivalência em $\mathbb{N}\times\mathbb{N}$, pela relação R, será denotado por $(\mathbb{N}\times\mathbb{N})\diagup R$, ou seja,

$$(\mathbb{N}\times\mathbb{N})\diagup R = \left\{\overline{(a,b)} : (a,b)\in\mathbb{N}\times\mathbb{N}\right\}$$

Definição 2.2.3 *O conjunto quociente $(\mathbb{N}\times\mathbb{N})\diagup R$ determinado acima é chamado de o* ***conjunto dos números inteiros*** *e será denotado por $\mathbb{Z}$.*

Observação 2.2.4 *Representaremos os números inteiros pelas letras gregas minúsculas:*

$$\alpha,\beta,\gamma,\delta,\cdots,\theta,\cdots$$

Exemplo 2.2.5 *O conjunto*

$$\theta = \{(n,n) \mid n\in\mathbb{N}\}$$

é um número inteiro. De fato,

$$\begin{aligned} \theta &= \{(x,y)\in\mathbb{N}\times\mathbb{N} : x=y\} \\ &\overset{(1.2.5)}{=} \{(x,y)\in\mathbb{N}\times\mathbb{N} : x+n=y+n\} \\ &\overset{(2.2.1)}{=} \{(x,y)\in\mathbb{N}\times\mathbb{N} : (x,y)\,R\,(n,n)\} \\ &= \overline{(n,n)}\in((\mathbb{N}\times\mathbb{N})\diagup R) = \mathbb{Z} \end{aligned}$$

Exemplo 2.2.6 *O conjunto*

$$\varepsilon = \{(n+1, n) \mid n \in \mathbb{N}\}$$

também é um número inteiro, pois

$$\begin{aligned}
\varepsilon &= \{(x,y) \in \mathbb{N}\times\mathbb{N} : x = y+1\} \\
&\overset{(1.2.5)}{=} \{(x,y) \in \mathbb{N}\times\mathbb{N} : x+n = y+1+n\} \\
&\overset{(1.2.4.(1))}{=} \{(x,y) \in \mathbb{N}\times\mathbb{N} : x+n = y+n+1\} \\
&\overset{(2.2.1)}{=} \{(x,y) \in \mathbb{N}\times\mathbb{N} : (x,y)\, R\, (n+1,n)\} \\
&= \overline{(n+1,n)} \in ((\mathbb{N}\times\mathbb{N})/R) = \mathbb{Z}
\end{aligned}$$

2.3 OPERAÇÕES COM NÚMEROS INTEIROS

Pretendemos agora definir duas operações no conjunto $\mathbb{Z}$: uma que chamaremos adição e outra multiplicação, indicadas, respectivamente, com os símbolos $+$ e $\cdot$ (quando não houver dúvida omitiremos o símbolo da multiplicação, como no caso dos números naturais).

Definição 2.3.1 *Dados os números inteiros α e β, se $(a,b) \in \alpha$ e $(c,d) \in \beta$ definimos* ***a soma***

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

e **o produto**

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

Observação 2.3.2 *A soma e o produto dos números inteiros α e β foram definidas utilizando-se representantes (a,b) e (c,d) das classes de equivalências α e β, respectivamente. Devemos então nos assegurar que se escolhermos outros representantes (a',b') e (c',d'), respectivamente, as definições* (2.3.1. (1)) *e* (2.3.1. (2)) *não mudam, ou seja, se*

$$(a,b)\, R\, (a',b') \;\; e \;\; (c,d)\, R\, (c',d')$$

então

(1) $(a+c, b+d)\, R\, (a'+c', b'+d')$

e

(2) $(ac+bd, ad+bc)\, R\, (a'c'+b'd', a'd'+b'c')$

Demonstração. Parte (1)**:** Obsersando as hipóteses, temos

$$\left.\begin{array}{r} (a,b)\, R\, (a',b') \overset{(2.2.1)}{\Rightarrow} a+b' = b+a' \\ (c,d)\, R\, (c',d') \overset{(2.2.1)}{\Rightarrow} c+d' = d+c' \end{array}\right\}$$

$$\begin{aligned} &\Rightarrow && (a+b')+(c+d') = (b+a')+(d+c') \\ &\overset{(1.2.2.(2))}{\Rightarrow} && a+(b'+c)+d' = b+(a'+d)+c' \\ &\overset{(1.2.4.(1))}{\Rightarrow} && a+(c+b')+d' = b+(d+a')+c' \\ &\overset{(1.2.2.(2))}{\Rightarrow} && (a+c)+(b'+d') = (b+d)+(a'+c') \\ &&& \overset{(2.2.1)}{\Rightarrow} (a+c, b+d)\, R\, (a'+c', b'+d') \end{aligned}$$

Parte (2)**:**Ainda, conforme as hipóteses, temos:

$$\left.\begin{array}{r} (a,b)\, R\, (a',b') \overset{(2.2.1)}{\Rightarrow} a+b' = b+a' \\ (c,d)\, R\, (c',d') \overset{(2.2.1)}{\Rightarrow} c+d' = d+c' \end{array}\right\}$$

$$\begin{aligned} &\Rightarrow && (a+b')\cdot(c+c')+(a'+b)\cdot(d+d')+(c+d')\cdot(a+a')+(d+c')\cdot(b+b') \\ &= && (a'+b)\cdot\left(c+c^{'}\right)+(a+b')\cdot(d+d')+(d+c')\cdot(a+a')+(c+d')\cdot(b+b') \\ &\Rightarrow && ac+ac'+b'c+b'c'+a'd+a'd'+bd+bd'+ca+ca'+d'a+d'a'+db+db'+c'b+c'b' \\ &= && a'c+a'c'+bc+bc'+ad+ad'+b'd+b'd'+da+da'+c'a+c'a'+cb+cb'+d'b+d'b' \\ &\Rightarrow && 2\,(ac+bd+a'd'+b'c')+ac'+b'c+a'd+bd'+ca'+d'a+db'+c'b \\ &= && 2\,(ad+bc+a'c'+b'd')+a'c+bc'+ad'+b'd+da'+c'a+cb'+d'b \end{aligned}$$

e, usando as leis do corte, temos:

$$ac+bd+a'd'+b'c' = ad+bc+a'c'+b'd'$$

assim, por (1.2.4. (1))

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

e portanto

$$(ac+bd, ad+bc)\, R\, (a'd'+b'c', a'c'+b'd')$$

■

Definição 2.3.3 *As aplicações* $A : \mathbb{Z}\times\mathbb{Z} \longmapsto \mathbb{Z}$ *e* $M : \mathbb{Z}\times\mathbb{Z} \longmapsto \mathbb{Z}$ *definidas por* $A(\alpha,\beta) = \alpha+\beta$ *e* $M(\alpha,\beta) = \alpha\cdot\beta$ *são chamadas de adição e multiplicação de números inteiros, respectivamente.*

2.4 PROPRIEDADES DAS OPERAÇÕES

As operações de adição e de multiplicação, definidas sobre o conjunto $\mathbb{Z}$ dos números inteiros, gozam das seguintes propriedades.

Teorema 2.4.1 *Sejam α, β e γ números inteiros quaisquer, então:*

(1) $\alpha+(\beta+\gamma)=(\alpha+\beta)+\gamma$ (*associatividade*)

(2) $\alpha+\beta=\beta+\alpha$ (*comutatividade*)

Demonstração. Parte (1)**:** Consideremos $\alpha = \overline{(a,b)}$, $\beta = \overline{(c,d)}$ e $\gamma = \overline{(e,f)}$, com a, b, c, d, e e $f \in \mathbb{N}$; temos:

$$\begin{aligned}
\alpha+(\beta+\gamma) &= \overline{(a,b)}+\overline{(c,d)}+\overline{(e,f)} \\
&\overset{(2.3.1.(1))}{=} \overline{(a,b)}+\overline{(c+e,d+f)} \\
&\overset{(2.3.1.(1))}{=} \overline{(a+(c+e),b+(d+f))} \\
&\overset{(1.2.2.(2))}{=} \overline{((a+c)+e,(b+d)+f)} \\
&\overset{(2.3.1.(1))}{=} \overline{(a+c,b+d)}+\overline{(e,f)} \\
&\overset{(2.3.1.(1))}{=} \left(\overline{(a,b)}+\overline{(c,d)}\right)+\overline{(e,f)} \\
&= (\alpha+\beta)+\gamma
\end{aligned}$$

Parte (2)**:** Consideremos $\alpha = \overline{(a,b)}$ e $\beta = \overline{(c,d)}$, com a, b, c e $d \in \mathbb{N}$; temos:

$$\begin{aligned}
\alpha+\beta &= \overline{(a,b)}+\overline{(c,d)} \overset{(2.3.1.(1))}{=} \overline{(a+c,b+d)} \\
&\overset{(1.2.4.(1))}{=} \overline{(c+a,d+b)} \overset{(2.3.1.(1))}{=} \overline{(c,d)}+\overline{(a,b)} \\
&= \beta+\alpha
\end{aligned}$$

■

O próximo teorema mostra que o número inteiro zero, que corresponde ao elemento neutro da adição, é dada pela classe de equivalência $\overline{(n,n)}$, com $n \in \mathbb{N}$

Teorema 2.4.2 *Existe um e apenas um elemento θ em $\mathbb{Z}$ tal que*

$$\alpha+\theta=\alpha$$

para qualquer que seja α em $\mathbb{Z}$.

Demonstração. Existência: Consideremos o elemento

$$\theta \overset{(2.2.5)}{=} \overline{(n,n)}$$

e seja $\alpha = \overline{(a,b)}$,com a e $b \in \mathbb{N}$. Como $(a+n, b+n)\, R\, (a,b)$, então

$$\alpha + \theta \overset{(hipótese)}{=} \overline{(a,b)} + \overline{(n,n)} \overset{(2.3.1.(2))}{=} \overline{(a+n, b+n)} = \overline{(a,b)}$$

Unicidade: Suponhamos que θ_1 e θ_2 são elementos de $\mathbb{Z}$ que satisfazem (2.4.2). Então

$$\theta_1 \overset{(2.4.2)}{=} \theta_1 + \theta_2 \overset{(2.4.1.(2))}{=} \theta_2 + \theta_1 \overset{(2.4.2)}{=} \theta_2$$

■

Teorema 2.4.3 *Para cada $\alpha \in \mathbb{Z}$ existe um e apenas um elemento $\alpha^{\#}$ tal que*

$$\alpha + \alpha^{\#} = \theta$$

Demonstração. Existência: Sejam $\alpha = \overline{(a,b)}$ e $\alpha^{\#} = \overline{(b,a)}$, temos

$$\begin{aligned} \alpha + \alpha^{\#} \overset{(hipótese)}{=} \overline{(a,b)} + \overline{(b,a)} &\overset{(2.3.1.(1))}{=} \overline{(a+b, b+a)} \\ &\overset{(1.2.4.(1))}{=} \overline{(a+b, a+b)} \\ &\overset{(2.2.5)}{=} \theta \end{aligned}$$

Unicidade: Sejam $\alpha^{\#}$ e $\alpha^{\#\#}$ elementos que verificam (2.4.3). Logo

$$\alpha + \alpha^{\#} = \theta \text{i}$$

$$\overset{(2.2)}{\alpha + \alpha^{\#\#}} = \theta \text{ii} \tag{2.4}$$

vamos ter:

$$\begin{aligned} \alpha^{\#\#} &\overset{(2.4.2)}{=} \alpha^{\#\#} + \theta \overset{(i)}{=} \alpha^{\#\#} + \left(\alpha + \alpha^{\#}\right) \overset{(2.4.1.(1))}{=} \left(\alpha^{\#\#} + \alpha\right) + \alpha^{\#} \\ &\overset{(2.4.1.(2))}{=} \left(a + \alpha^{\#\#}\right) + \alpha^{\#} \overset{(ii)}{=} \theta + \alpha^{\#} \overset{(2.4.1.(2))}{=} \alpha^{\#} + \theta \overset{(2.4.2)}{=} \alpha^{\#} \end{aligned}$$

■

Notação 2.4.4 *O elemento $\alpha^{\#}$ que aparece em* (2.4.3) *é chamado simétrico ou oposto de α, e será denotado por $-\alpha$. Assim, a soma $a + (-\beta)$ será indicada por $\alpha - \beta$.*

Teorema 2.4.5 *Para cada α e β em $\mathbb{Z}$, existe um único elemento ρ em $\mathbb{Z}$ tal que*

$$\alpha + \rho = \beta$$

Demonstração. Se (2.4.5) é verificada, seja $\alpha^{\#} \in \mathbb{Z}$ tal que $\alpha + \alpha^{\#} = \theta$. Então

$$\begin{aligned} \alpha + \rho &= \beta \Rightarrow \alpha^{\#} + (\alpha + \rho) = \alpha^{\#} + \beta \\ \overset{(2.4.1.(1))}{\Rightarrow} \left(\alpha^{\#} + \alpha\right) + \rho &= \alpha^{\#} + \beta \overset{(2.4.1.(2))}{\Rightarrow} \left(\alpha + \alpha^{\#}\right) + \rho = \alpha^{\#} + \beta \\ \overset{(2.4.3)}{\Rightarrow} \theta + \rho &= \alpha^{\#} + \beta \overset{(2.4.1.(2))}{\Rightarrow} \rho + \theta = \alpha^{\#} + \beta \\ \overset{(2.4.2)}{\Rightarrow} \rho &= \alpha^{\#} + \beta \end{aligned}$$

Inserindo $\rho = \alpha^{\#} + \beta$ em (2.4.5), verificamos que a identidade é mantida. ■

Teorema 2.4.6 *(Lei do Corte). Sejam α, β e γ números inteiros quaisquer. Então*

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

Demonstração. Consideremos α, β e γ números inteiros quaisquer. Então

$$\begin{aligned} \alpha + \gamma &= \beta + \gamma \Rightarrow (\alpha + \gamma) + \gamma^{\#} = (\beta + \gamma) + \gamma^{\#} \\ \overset{(2.4.1.(1))}{\Rightarrow} \alpha + \left(\gamma + \gamma^{\#}\right) &= \beta + \left(\gamma + \gamma^{\#}\right) \\ \overset{(2.4.3)}{\Rightarrow} \alpha + \theta &= \beta + \theta \overset{(2.4.2)}{\Rightarrow} \alpha = \beta \end{aligned}$$

■

Teorema 2.4.7 *Sejam α, β, γ e θ números inteiros. Então*

(1) $(\alpha \cdot \beta) \cdot \gamma = \alpha \cdot (\beta \cdot \gamma)$ (*associatividade*)

(2) $\alpha \cdot \beta = \beta \cdot \alpha$ (*comutatividade*)

(3) $(\alpha + \beta) \cdot \gamma = \alpha \cdot \gamma + \beta \cdot \gamma$ (*distributividade a direita*)

(4) $\gamma \cdot (\alpha + \beta) = \gamma \cdot \alpha + \gamma \cdot \beta$ (*distributividade a esquerda*)

(5) $\alpha \cdot \theta = \theta$

Demonstração. Parte (1)**:** Consideremos $\alpha = \overline{(a,b)}, \beta = \overline{(c,d)}$ e $\gamma = \overline{(e,f)}$ com a, b, c, d, e e $f \in \mathbb{N}$;

$$
\begin{aligned}
\Rightarrow \quad (\alpha \cdot \beta) \cdot \gamma &= \left(\overline{(a,b)} \cdot \overline{(c,d)}\right) \cdot \overline{(e,f)} \\
&\overset{(2.3.1.(2))}{=} \overline{(ac+bd, ad+bc)} \cdot \overline{(e,f)} \\
&\overset{(2.3.1.(2))}{=} \overline{((ac+bd)\,e + (ad+bc)\,f, (ac+bd)\,f + (ad+bc)\,e)} \\
&\overset{(1.4.3.(4))}{=} \overline{((ac)\,e + (bd)\,e + (ad)\,f + (bc)\,f, (ac)\,f + (bd)\,f + (ad)\,e + (bc)\,e)} \\
&\overset{(1.4.3.(3))}{=} \overline{(a\,(ce) + b\,(de) + a\,(df) + b\,(cf)\,, a\,(cf) + b\,(df) + a\,(de) + b\,(ce))} \\
&\overset{(1.2.4.(1))}{=} \overline{(a\,(ce) + a\,(df) + b\,(de) + b\,(cf)\,, a\,(cf) + a\,(de) + b\,(df) + b\,(ce))} \\
&\overset{(1.4.3.(2))}{=} \overline{(a\,(ce+df) + b\,(de+cf)\,, a\,(cf+de) + b\,(df+ce))} \\
&\overset{(1.2.4.(1))}{=} \overline{(a\,(ce+df) + b\,(de+cf)\,, a\,(de+cf) + b\,(ce+df))} \\
&\overset{(2.3.1.(2))}{=} \overline{(a,b)} \cdot \overline{(ce+df, de+cf)} \\
&\overset{(1.2.4.(1))}{=} \overline{(a,b)} \cdot \overline{(ce+df, cf+de)} \\
&\overset{(2.3.1.(2))}{=} \overline{(a,b)} \cdot \left(\overline{(c,d)} \cdot \overline{(e,f)}\right) \\
= \quad \alpha \cdot (\beta \cdot \gamma)
\end{aligned}
$$

Parte (2)**:** Consideremos $\alpha = \overline{(a,b)}$ e $\beta = \overline{(c,d)}$, com a, b, c e $d \in \mathbb{N}$;

$$
\begin{aligned}
\Rightarrow \quad \alpha \cdot \beta = \overline{(a,b)} \cdot \overline{(c,d)} &\overset{(2.3.1.(2))}{=} \overline{(ac+bd, ad+bc)} \\
&\overset{(1.4.3.(6))}{=} \overline{(ca+db, da+cb)} \\
&\overset{(1.2.4.(1))}{=} \overline{(ca+db, cb+da)} \overset{(2.3.1.(2))}{=} \overline{(c,d)} \cdot \overline{(a,b)} = \beta \cdot \alpha
\end{aligned}
$$

Parte (3)**:** Consideremos $\alpha = \overline{(a,b)}, \beta = \overline{(c,d)}$ e $\gamma = \overline{(e,f)}$ com a, b, c, d, e e $f \in \mathbb{N}$;

$$\begin{aligned}
\Rightarrow \quad (\alpha+\beta)\cdot\gamma &= \left(\overline{(a,b)} + \overline{(c,d)}\right)\cdot\overline{(e,f)} \\
&\overset{(2.3.1.(1))}{=} \overline{(a+c,b+d)}\cdot\overline{(e,f)} \\
&\overset{(2.3.1.(2))}{=} \overline{((a+c)\,e+(b+d)\,f,(a+c)\,f+(b+d)\,e)} \\
&\overset{(1.4.3.(4))}{=} \overline{(ae+ce+bf+df,af+cf+be+de)} \\
&\overset{(1.2.4.(1))}{=} \overline{(ae+bf+ce+df,af+be+cf+de)} \\
&\overset{(2.3.1.(1))}{=} \overline{(ae+bf,af+be)} + \overline{(ce+df,cf+de)} \\
&\overset{(2.3.1.(2))}{=} \overline{(a,b)}\cdot\overline{(e,f)} + \overline{(c,d)}\cdot\overline{(e,f)} = \alpha\cdot\gamma + \beta\cdot\gamma
\end{aligned}$$

Parte (4)**:** Temos

$$\begin{aligned}
&\gamma\cdot(\alpha+\beta) \overset{(2.4.7.(2))}{=} (\alpha+\beta)\cdot\gamma \overset{(2.4.7.(3))}{=} \alpha\cdot\gamma+\beta\cdot\gamma \overset{(2.4.7.(2))}{=} \gamma\cdot\alpha+\gamma\cdot\beta \\
\Rightarrow \quad &\gamma\cdot(\alpha+\beta) = \gamma\cdot\alpha+\gamma\cdot\beta
\end{aligned}$$

Parte (5)**:** Sejam $\alpha = \overline{(a,b)}$ e $\theta = \overline{(n,n)}$. Devemos mostrar que

$$\overline{(a,b)}\cdot\overline{(n,n)} = \overline{(n,n)}$$

e isto é equivalente a verificar que

$$(an+bn,an+bn)\,R\,(n,n)$$

o que é verdade, pois

$$(an+bn,an+bn)\,R\,(n,n) \overset{(2.2.1)}{\Leftrightarrow} an+bn+n = an+bn+n$$

Portanto, $\alpha\cdot\theta = \theta$ ■

Teorema 2.4.8 *Sejam α, β e γ números inteiros e suponhamos que $\gamma \neq \theta$. Então*

(1) $\alpha\cdot\beta = \theta \Rightarrow \alpha = \theta$ ou $\beta = \theta$

(2) $\alpha\cdot\gamma = \beta\cdot\gamma \Rightarrow \alpha = \beta$ (*lei do corte*)

(3) $\alpha\cdot(-\beta) = (-\alpha)\cdot\beta = -(\alpha\cdot\beta)$ (*r*egra de sinais)

(4) $-(-\alpha) = \alpha$ (regra de sinais)

(5) $(-\alpha)\cdot(-\beta)=\alpha\cdot\beta$ (regra de sinais)

Demonstração. Parte (1)**:** Se $\alpha\neq\theta$ e $\beta\neq\theta$ então $\alpha\cdot\beta\neq\theta$. Para verificar isso, consideremos $\alpha=\overline{(a,b)}$ e $\beta=\overline{(c,d)}$, com a,b,c e $d\in\mathbb{N}$ e $a\neq b$ e $c\neq d$. Vamos examinar os casos $c>d$ e $d>c$.

No primeiro caso, existe $p\in\mathbb{N}$, tal que

$$c=d+p \tag{i}$$

Como

$$a\neq b\Rightarrow a\cdot p\neq b\cdot p \tag{ii}$$

Portanto

$$\begin{aligned}
&(a\cdot c)+(b\cdot d)\overset{(i)}{=}a\cdot(d+p)+b\cdot d\\
&\overset{(1.4.3.(2))}{=}a\cdot d+a\cdot p+b\cdot d\overset{(ii)}{\neq}a\cdot d+b\cdot p+b\cdot d\\
&\overset{(1.4.3.(2))}{=}a\cdot d+b\,(p+d)\overset{(1.2.4.(1))}{\neq}a\cdot d+b\,(d+p)\overset{(i)}{=}a\cdot d+b\cdot c\\
\Rightarrow\ &(a\cdot c)+(b\cdot d)\neq(a\cdot d)+(b\cdot c)
\end{aligned}$$

Agora, como

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

segue por (2.2.5. (1)) que $\alpha\cdot\beta\neq\theta$.

No segundo caso, existe $q\in\mathbb{N}$, tal que

$$d=c+q \tag{iii}$$

Como

$$a\neq b\Rightarrow a\cdot q\neq b\cdot q \tag{iv}$$

Portanto

$$\begin{aligned}
&(a\cdot c)+(b\cdot d)\overset{(iii)}{=}a\cdot c+b\cdot(c+q)\overset{(1.4.3.(2))}{=}a\cdot c+b\cdot c+b\cdot q\\
&\overset{(iv)}{\neq}a\cdot c+b\cdot c+a\cdot q\overset{(1.2.4.(1))}{=}a\cdot c+a\cdot q+b\cdot c\\
&\overset{(1.4.3.(2))}{=}a\cdot(c+q)+b\cdot c\overset{(iii)}{=}(a\cdot d)+(b\cdot c)\overset{(1.2.4.(1))}{=}(b\cdot c)+(a\cdot d)\\
\Rightarrow\ &(a\cdot c)+(b\cdot d)\neq(b\cdot c)+(a\cdot d)
\end{aligned}$$

Agora, como

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

segue por (2.2.5. (1)) que $\alpha \cdot \beta \neq \theta$.

Parte (2)**:** Consideremos $\alpha = \overline{(a,b)}, \beta = \overline{(c,d)}$ e $\gamma = \overline{(e,f)}$ com a, b, c, d, e e $f \in \mathbb{N}$;

Suponhamos por absurdo que $\alpha \neq \beta$, ou seja, $\overline{(a,b)} \neq \overline{(c,d)}$, portanto,

$$a + d \neq b + c$$

Logo

$$\begin{array}{rcl}
 & \left\{ \begin{array}{l} (a+d)\cdot e \neq (b+c)\cdot e \overset{(1.4.3.(4))}{\Rightarrow} ae + de \neq be + ce \\ (a+d)\cdot f \neq (b+c)\cdot f \overset{(1.4.3.(4))}{\Rightarrow} af + df \neq bf + cf \end{array} \right. \\
\Rightarrow & ae + de + (bf + cf) \neq (be + ce) + af + df \\
\overset{(1.2.4.(1))}{\Rightarrow} (ae + bf) + (cf + de) & \neq & (af + be) + (ce + df) \\
\overset{(2.2.1)}{\Rightarrow} \left(\overline{ae + bf, af + be}\right) & \neq & \left(\overline{ce + df, cf + de}\right) \\
\overset{(2.3.1.(2))}{\Rightarrow} \left(\overline{a,b}\right) \cdot \left(\overline{e,f}\right) & \neq & \left(\overline{c,d}\right) \cdot \left(\overline{e,f}\right) \\
\overset{(\text{hipótese})}{\Rightarrow} \alpha \cdot \gamma & \neq & \beta \cdot \gamma
\end{array}$$

absurdo. Logo se $\alpha \cdot \gamma = \beta \cdot \gamma \Rightarrow \alpha = \beta$

Parte (3)**:**Primeiro caso: Vamos mostrar que

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

Temos

$$\alpha \cdot \beta + \alpha \cdot (-\beta) \overset{(2.4.7.(4))}{=} \alpha \cdot (\beta + (-\beta)) \overset{(2.4.3)}{=} \alpha \cdot \theta \overset{(2.4.7.(5))}{=} \theta$$

Mas, pelo teorema (2.4.3) existe um único $\gamma \in \mathbb{Z}$ tal que $\gamma + \alpha \cdot \beta = \theta$, que é o elemento denotado por $-(\alpha \cdot \beta)$. Como $\alpha \cdot (-\beta)$ também tem essa propriedade, segue que $\alpha \cdot (-\beta) = -(\alpha \cdot \beta)$.

Segundo caso: Vamos mostrar que

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

Temos

$$\alpha \cdot \beta + (-\alpha) \cdot \beta \overset{(2.4.7.(3))}{=} (\alpha + (-\alpha)) \cdot \beta \overset{(2.4.3)}{=} \theta \cdot \beta \overset{(2.4.7.(2))}{=} \beta \cdot \theta \overset{(2.4.7.(5))}{=} \theta$$

Mas, pelo teorema (2.4.3) existe um único $\gamma \in \mathbb{Z}$ tal que $\gamma + \alpha \cdot \beta = \theta$, que é o elemento denotado por $-(\alpha \cdot \beta)$. Como $(-\alpha) \cdot \beta$ também tem essa propriedade, segue que $(-\alpha) \cdot \beta = -(\alpha \cdot \beta)$.

Parte (4)**:** Por (2.4.3), temos

$$\alpha + \alpha^{\#} = \theta$$

e aplicando (2.4.1. (2)), resulta

$$\alpha^{\#} + \alpha = \theta$$

o que implica

$$\alpha = -\left(\alpha^{\#}\right)$$

e portanto

$$\alpha = -(-\alpha)$$

Parte (5)**:** Sabemos que,

$$(-\alpha) \cdot (-\beta) \overset{(2.4.8.(3))}{=} -(\alpha \cdot (-\beta)) \overset{(2.4.8.(3))}{=} -(-(\alpha \cdot \beta)) \overset{(2.4.8.(4))}{=} \alpha \cdot \beta$$

■

2.5 RELAÇÃO DE ORDEM EM $\mathbb{Z}$

Definição 2.5.1 *Sejam $\alpha = \overline{(a,b)}$ e $\beta = \overline{(c,d)}$ números inteiros. Diremos que α* ***é menor que*** *β se $a + d < b + c$; isto é*

$$\alpha < \beta \Leftrightarrow a + d < b + c$$

Diremos que α **é maior que** β, e escrevemos $\alpha > \beta$, se $\beta < \alpha$.

Definição 2.5.2 *Dados α e β em $\mathbb{Z}$, diremos que α* ***é menor que ou igual à*** *β e escrevemos $\alpha \leq \beta$ se $\alpha < \beta$ ou $\alpha = \beta$. Analogamente, definimos a relação $\alpha \geq \beta$.*

Teorema 2.5.3 *A relação $<$ em $\mathbb{Z}$ não depende dos representantes usados na definição.*

Demonstração. Sejam $\alpha = \overline{(a,b)}$ e $\beta = \overline{(c,d)}$ números inteiros com $\alpha < \beta$ e sejam a', b', c' e d' números naturais tais que $(a',b')\,R\,(a,b)$ e $(c',d')\,R\,(c,d)$. Se $a+d<b+c$, como

$$a'+b=b'+a \qquad (i)$$

e

$$c'+d=d'+c \qquad (ii)$$

vamos ter,

$$\begin{aligned}
&(a'+d')+(b+c) \overset{(1.2.2.(2))}{=} a'+(d'+b)+c \overset{(1.2.4.(1))}{=} (a'+b)+(d'+c)\\
&\overset{(i \text{ e } ii)}{=} (b'+a)+(c'+d) \overset{(1.2.2.(2))}{=} b'+(a+c')+d\\
&\overset{(1.2.4.(1))}{=} (b'+c')+(a+d) \overset{\text{(hipótese)}}{<} (b'+c')+(b+c)\\
\Rightarrow\quad & a'+d' \overset{(1.3.2.(2))}{<} b'+c'
\end{aligned}$$

■

Teorema 2.5.4 *A relação $\leq$ em $\mathbb{Z}$ é uma relação de ordem total, isto é, se α, β e γ são números inteiros, temos*

(1) $\alpha \leq \alpha$ $(reflexiva)$

(2) $\alpha \leq \beta$ e $\beta \leq \gamma \Rightarrow \alpha \leq \gamma$ $(transitiva)$

(3) $\alpha \leq \beta$ e $\beta \leq \alpha \Rightarrow \alpha = \beta$ $(anti-simétrica)$

(4) $\alpha \leq \beta$ ou $\beta \leq \alpha$ $(ordem\ total)$

Demonstração. Parte (1)**:** Óbvia

Parte (2)**:** Sejam $\alpha = \overline{(a,b)}, \beta = \overline{(c,d)}$ e $\gamma = \overline{(e,f)}$ com a,b,c,d,e e $f \in \mathbb{N}$. Como, por hipótese,

$$\begin{aligned}
&\alpha \leq \beta \text{ e } \beta \leq \alpha \overset{\text{(definição)}}{\Rightarrow} a+d \leq b+c \text{ e } c+f \leq d+e\\
\Rightarrow\quad & a+d+c+f \leq b+c+d+e\\
&\overset{(2.4.1.(1) \text{ e } 2.4.1.(2))}{\Rightarrow} (a+f)+(d+c) \leq (b+e)+(c+d)\\
\Rightarrow\quad & a+f \leq b+e \Rightarrow \alpha \leq \gamma
\end{aligned}$$

Parte (3)**:** Sejam $\alpha = \overline{(a,b)}$ e $\beta = \overline{(c,d)}$ com a, b, c e $d \in \mathbb{N}$. Observando a hipótese, temos

$$\alpha \leq \beta \text{ e } \beta \leq \alpha \Rightarrow a + d \leq b + c \text{ e } c + b \leq d + a \overset{(1.4.4.(8))}{\Rightarrow} a + d = b + c$$

Parte (4)**:** Sejam $\alpha = \overline{(a,b)}$ e $\beta = \overline{(c,d)}$ com a, b, c e $d \in \mathbb{N}$. Pela lei da tricotomia, temos $a + d < b + c$ ou $c + b < d + a$ ou $a + d = b + c$, ou seja, $\alpha \leq \beta$ ou $\beta \leq \alpha$. ■

Teorema 2.5.5 *Sejam α, β, γ e θ números inteiros. Então*

(1) $\alpha > \theta$ e $\beta > \theta \Rightarrow \alpha \cdot \beta > \theta$

(2) $\alpha < \theta$ e $\beta < \theta \Rightarrow \theta < \alpha \cdot \beta$

(3) $\alpha < \theta$ e $\theta < \beta \Rightarrow \alpha \cdot \beta < \theta$

(4) $\alpha < \theta \Leftrightarrow -\alpha > \theta$

Demonstração. Parte (1)**:** Consideremos $\alpha = \overline{(a,b)}, \beta = \overline{(c,d)}$ e $\theta = \overline{(n,n)}$ com a, b, c, d e $n \in \mathbb{N}$. Como $\alpha > \theta$ e $\beta > \theta$ temos,

$$\begin{cases} \overline{(a,b)} > \overline{(n,n)} \overset{(2.5.1)}{\Rightarrow} a + n > b + n \overset{(1.3.2.(2))}{\Rightarrow} a > b \\ \overline{(c,d)} > \overline{(n,n)} \overset{(2.5.1)}{\Rightarrow} c + n > d + n \overset{(1.3.2.(2))}{\Rightarrow} c > d \end{cases}$$

Como,

$$\alpha \cdot \beta = \overline{(a,b)} \cdot \overline{(c,d)} \overset{(2.3.1.(2))}{=} \overline{(ac + bd, ad + bc)}$$

Para mostrarmos que

$$\alpha \cdot \beta > \theta$$

basta mostrarmos que

$$ac + bd > ad + bc$$

Como $\alpha > \theta$ e $\beta > \theta$ temos $a > b$ e $c > d$. Então, existe p tal que

$$c = d + p \tag{i}$$

e como

$$a > b \overset{(1.4.4.(4))}{\Rightarrow} ap > bp \tag{ii}$$

vamos ter

$$ac+bd \overset{(i)}{=} a\,(d+p)+bd \overset{(1.4.3.(2))}{=} ad+ap+bd \overset{(ii)}{>} ad+bp+bd$$
$$\overset{(1.4.3.(2))}{=} ad+b\,(p+d) \overset{(i)}{=} ad+bc$$

Parte (2) Consideremos $\alpha=\overline{(a,b)}, \beta=\overline{(c,d)}$ e $\theta=\overline{(n,n)}$ com a,b,c,d e $n\in\mathbb{N}$. Como $\alpha<\theta$ e $\beta<\theta$ temos,

$$\begin{cases} \overline{(a,b)}<\overline{(n,n)} \overset{(2.5.1)}{\Rightarrow} a+n<b+n \overset{(1.3.2.(2))}{\Rightarrow} a<b \\ \overline{(c,d)}<\overline{(n,n)} \overset{(2.5.1)}{\Rightarrow} c+n<d+n \overset{(1.3.2.(2))}{\Rightarrow} c<d \end{cases}$$

Como,

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

Para mostrarmos que

$$\theta<\alpha\cdot\beta$$

basta mostrarmos que

$$ad+bc<ac+bd$$

Como $\alpha<\theta$ e $\beta<\theta$ temos $a<b$ e $c<d$. Então, existe q tal que

$$d=c+q \qquad (i)$$

e como

$$a<b \overset{(1.4.4.(4))}{\Rightarrow} aq<bq \qquad (ii)$$

vamos ter

$$ad+bc \overset{(i)}{=} a\,(c+q)+bc \overset{(1.4.3.(2))}{=} ac+aq+bc \overset{(ii)}{<} ac+bq+bc$$
$$\overset{(1.4.3.(2))}{=} ac+b\,(q+c) \overset{(i)}{=} ac+bd$$

Parte (3)**:** Consideremos $\alpha=\overline{(a,b)}, \beta=\overline{(c,d)}$ e $\theta=\overline{(n,n)}$ com a,b,c,d e $n\in\mathbb{N}$. Como $\alpha<\theta$ e $\theta<\beta$ temos,

$$\begin{cases} \overline{(a,b)}<\overline{(n,n)} \overset{(2.5.1)}{\Rightarrow} a+n<b+n \overset{(1.3.2.(2))}{\Rightarrow} a<b \\ \overline{(n,n)}<\overline{(c,d)} \overset{(2.5.1)}{\Rightarrow} n+d<n+c \overset{(1.3.2.(2))}{\Rightarrow} d<c \end{cases}$$

Como,

$$\alpha \cdot \beta \overset{\text{(hipótese)}}{=} \overline{(a,b)} \cdot \overline{(c,d)} \overset{(2.3.1.(2))}{=} \overline{(ac+bd, ad+bc)}$$

Para mostrarmos que

$$\alpha \cdot \beta < \theta$$

basta mostrarmos que

$$ac + bd < ad + bc$$

Como $\alpha < \theta$ e $\theta < \beta$ temos $a < b$ e $d < c$. Então, existe r tal que

$$c = d + r \tag{i}$$

e como

$$a < b \overset{(1.4.4.(4))}{\Rightarrow} ar < br \tag{ii}$$

vamos ter

$$\begin{aligned} ac + bd &\overset{(i)}{=} a\,(d+r) + bd \overset{(1.4.3.(2))}{=} ad + ar + bd \overset{(ii)}{<} ad + br + bd \\ &\overset{(1.4.3.(2))}{=} ad + b\,(r+d) \overset{(i)}{=} ad + bc \end{aligned}$$

Parte (4)**:** Consideremos $\alpha = \overline{(a,b)}$ e $\theta = \overline{(n,n)}$ com a, b e $n \in \mathbb{N}$. Como $\alpha < \theta$ temos,

$$\begin{aligned} \overline{(a,b)} < \overline{(n,n)} &\overset{(2.5.1)}{\Leftrightarrow} a + n < b + n \\ &\overset{(1.3.2.(2))}{\Leftrightarrow} a < b \\ &\overset{(2.5.1)}{\Leftrightarrow} b > a \\ &\overset{(1.3.2.(2))}{\Leftrightarrow} b + n > a + n \\ &\overset{(2.5.1)}{\Leftrightarrow} \overline{(b,a)} > \overline{(n,n)} \\ &\overset{\text{(hipótese)}}{\Leftrightarrow} -\alpha > \theta \end{aligned}$$

■

Observação 2.5.6 *O teorema* (2.5.5) *também é válido se as desigualdades maior e menor forem substítuidas por maior que ou igual e menor que ou igual respectivamente.*

Teorema 2.5.7 *Sejam α, β, γ e θ números inteiros. Então*

(1) $\alpha < \beta \Leftrightarrow \alpha+\gamma < \beta+\gamma$ (*monotonicidade da adição*)

(2) $\alpha < \beta \Leftrightarrow \alpha - \beta < \theta$

(3) $\alpha < \beta \,\mathrm{e}\, \theta < \gamma \Rightarrow \alpha\cdot\gamma < \beta\cdot\gamma$ (*monotonicidade da multiplicação*)

(4) $-\alpha > -\beta \Rightarrow \alpha < \beta$

(5) $\alpha < \beta + \gamma \Rightarrow \alpha - \beta < \gamma$

Demonstração. Parte (1)**:** Consideremos $\alpha = \overline{(a,b)}, \beta = \overline{(c,d)}$ e $\gamma = \overline{(e,f)}$ com a, b, c, d, e e $f \in \mathbb{N}$;

($\Rightarrow$) Se

$$\begin{aligned}
\alpha &< \beta \overset{\text{(hipótese)}}{\Leftrightarrow} \overline{(a,b)} < \overline{(c,d)} \\
\overset{(2.5.1)}{\Leftrightarrow} a+d &< b+c \\
\overset{(1.3.2.(2))}{\Leftrightarrow} (a+d)+(e+f) &< (b+c)+(e+f) \\
\overset{(1.2.2.(2))}{\Leftrightarrow} a+(d+e)+f &< (b+c)+(e+f) \\
\overset{(1.2.4.(1))}{\Leftrightarrow} a+(e+d)+f &< b+c+(f+e) \\
\overset{(1.2.2.(2))}{\Leftrightarrow} (a+e)+(d+f) &< b+(c+f)+e \\
\overset{(1.2.4.(1))}{\Leftrightarrow} (a+e)+(d+f) &< b+(f+c)+e \\
\overset{(1.2.2.(2))}{\Leftrightarrow} (a+e)+(d+f) &< (b+f)+(c+e) \\
\overset{(2.5.1)}{\Leftrightarrow} \overline{(a+e,b+f)} &< \overline{(c+e,d+f)} \\
\overset{(2.3.1.(1))}{\Leftrightarrow} \overline{(a,b)}+\overline{(e,f)} &< \overline{(c,d)}+\overline{(e,f)} \\
\overset{\text{(hipótese)}}{\Leftrightarrow} \alpha+\gamma &< \beta+\gamma
\end{aligned}$$

Parte (2)**:** Consideremos $\alpha = \overline{(a,b)}$ e $\beta = \overline{(c,d)}$ com a, b, c e $d \in \mathbb{N}$;

Temos que

$$\begin{aligned}
\alpha &< \beta \overset{\text{(hipótese)}}{\Leftrightarrow} \overline{(a,b)} < \overline{(c,d)} \\
&\overset{(2.5.1)}{\Leftrightarrow} a+d < b+c \\
&\overset{(1.3.2.(2))}{\Leftrightarrow} (a+d)+n < (b+c)+n \\
&\overset{(2.5.1)}{\Leftrightarrow} \overline{(a+d,b+c)} < \overline{(n,n)} \\
&\overset{(2.3.1.(1))}{\Leftrightarrow} \overline{(a,b)}+\overline{(c,d)} < \overline{(n,n)} \\
&\overset{(2.2.5)}{\Leftrightarrow} \overline{(a,b)}+\overline{(c,d)} < \theta \\
&\overset{\text{(hipótese)}}{\Leftrightarrow} \alpha+(-\beta) < \theta \\
&\overset{(2.4.4)}{\Leftrightarrow} \alpha-\beta < \theta
\end{aligned}$$

Parte (3)**:**Por hipótese, temos que

$$\alpha < \beta \overset{(2.5.7.(2))}{\Rightarrow} \alpha-\beta < \theta$$

e $\theta < \gamma$, logo por $(2.5.5.\,(3))$

$$\begin{aligned}
(\alpha-\beta)\cdot\gamma &< \theta \\
&\overset{(2.4.7.(3))}{\Rightarrow} \alpha\gamma-\beta\gamma < \theta \\
&\overset{(2.5.7.(1))}{\Rightarrow} (\alpha\gamma-\beta\gamma)+\beta\gamma < \theta+\beta\gamma \\
&\overset{(2.4.1.(1))}{\Rightarrow} \alpha\gamma+(-\beta\gamma+\beta\gamma) < \theta+\beta\gamma \\
&\overset{(2.4.3)}{\Rightarrow} \alpha\gamma+\theta < \theta+\beta\gamma \\
&\overset{(2.4.2)}{\Rightarrow} \alpha\gamma < \beta\gamma
\end{aligned}$$

Parte (4)**:**Por hipótese, temos que

$$\begin{aligned}
-\alpha &> -\beta \overset{(2.5.1)}{\Rightarrow} -\beta < -\alpha \\
&\overset{(2.5.7.(2))}{\Rightarrow} -\beta-(-\alpha) < \theta \\
&\overset{(2.4.8.(4))}{\Rightarrow} -\beta+\alpha < \theta \\
&\overset{(2.5.7.(1))}{\Rightarrow} \beta+(-\beta+\alpha) < \beta+\theta \\
&\overset{(2.4.1.(1))}{\Rightarrow} (\beta+(-\beta))+\alpha < \beta+\theta \\
&\overset{(2.4.3)}{\Rightarrow} \theta+\alpha < \beta+\theta \\
&\overset{(2.4.2)}{\Rightarrow} \alpha < \beta
\end{aligned}$$

Parte (5)**:**Por hipótese, temos que

$$\begin{aligned}
\alpha &< \beta+\gamma \overset{(2.5.7.(1))}{\Rightarrow} \alpha+(-\beta) < (\beta+\gamma)+(-\beta)\\
\overset{(2.4.1.(2))}{\Rightarrow} \alpha-\beta &< (-\beta)+(\beta+\gamma)\\
\overset{(2.4.1.(1))}{\Rightarrow} \alpha-\beta &< (-\beta+\beta)+\gamma\\
\overset{(2.4.3)}{\Rightarrow} \alpha-\beta &< \theta+\gamma\\
\overset{(2.4.2)}{\Rightarrow} \alpha-\beta &< \gamma
\end{aligned}$$

■

Vamos introduzir a noção de módulo ou valor absoluto de números inteiros.

Definição 2.5.8 ***O módulo*** *ou* ***valor absoluto*** *de um número inteiro α é definido por*

$$|\alpha| = \begin{cases} \alpha & se \quad \alpha \geq \theta \\ -\alpha & se \quad \alpha < \theta \end{cases}$$

Teorema 2.5.9 *Sejam α, β, γ e θ números inteiros, onde $\gamma \geq \theta$. Vamos ter*

(1) $|\alpha| \geq \theta$

(2) $|-\alpha| = |\alpha|$

(3) $-|\alpha| \leq \alpha \leq |\alpha|$

(4) $|\alpha| \leq \gamma \Leftrightarrow -\gamma \leq \alpha \leq \gamma$

(5) $|\alpha+\beta| \leq |\alpha|+|\beta|$

(6) $|\alpha-\beta| \leq |\alpha|+|\beta|$

(7) $|\alpha|-|\beta| \leq |\alpha+\beta|$

(8) $|\alpha|-|\beta| \leq |\alpha-\beta|$

(9) $||\alpha|-|\beta|| \leq |\alpha-\beta|$

(10) $|\alpha \cdot \beta| = |\alpha| \cdot |\beta|$

Demonstração. Parte (1)**:** Vamos mostrar que

$$|\alpha| \geq \theta$$

Se

$$\alpha \geq \theta \overset{(2.5.8)}{\Rightarrow} |\alpha| = \alpha \geq \theta$$

Se

$$\alpha < \theta \overset{(2.5.8)}{\Rightarrow} |\alpha| = -\alpha$$

Mas

$$\alpha < \theta \overset{(2.5.5.(4))}{\Rightarrow} -\alpha > \theta$$

Logo

$$|\alpha| > \theta$$

Parte (2)**:** Vamos mostrar que

$$|-\alpha| = |\alpha|, \forall \alpha \in \mathbb{Z}$$

Se

$$\alpha \geq \theta \overset{(2.5.8)}{\Rightarrow} |\alpha| = \alpha$$

Como

$$\alpha \geq \theta \overset{(2.5.5.(4))}{\Rightarrow} -\alpha \leq \theta$$

então

$$|-\alpha| \overset{(2.5.8)}{=} -(-\alpha) \overset{(2.4.8.(4))}{=} \alpha \overset{(2.5.8)}{=} |\alpha|$$

Se

$$-\alpha < \theta \overset{(2.5.8)}{\Rightarrow} |-\alpha| = -(-\alpha) \overset{(2.4.8.(4))}{=} \alpha$$

Por outro lado

$$-\alpha < \theta \overset{(2.5.5.(4))}{\Rightarrow} \alpha > \theta$$

Logo

$$|\alpha| \overset{(2.5.8)}{=} \alpha = |-\alpha|$$

Parte (3)**:** Vamos mostrar que

$$-|\alpha| \leq \alpha \leq |\alpha|$$

Se

$$\alpha \geq \theta \overset{(2.5.5.(4))}{\Rightarrow} -\alpha \leq \theta$$

e pela transitividade, temos

$$-\alpha \leq \alpha$$

Por outro lado, temos

$$|\alpha| = \alpha$$

Portanto, as relações

$$-\alpha \leq \alpha \leq \alpha$$

podem ser escritas da seguinte forma,

$$-|\alpha| \leq \alpha \leq |\alpha|$$

Suponhamos agora que $\alpha < \theta$. Logo, por (2.5.5. (4))

$$-\alpha > \theta$$

e pela transitividade, temos

$$\alpha < -\alpha$$

Por outro lado, temos

$$|\alpha| \overset{(2.5.8)}{=} -\alpha$$

e como

$$\alpha = -(-\alpha)$$

as relações

$$\alpha \leq \alpha < -\alpha$$

podem ser escritas da seguinte forma,

$$-|\alpha| \leq \alpha \leq |\alpha|$$

Parte (4)**:** Vamos mostrar que

$$|\alpha| \leq \gamma \Leftrightarrow -\gamma \leq \alpha \leq \gamma$$

($\Rightarrow$) Se $\alpha \geq \theta$, temos pela definição (2.5.8)

$$|\alpha| = \alpha$$

Logo

$$\alpha \leq \gamma$$

desta última desigualdade resulta, em virtude de (2.5.7. (4))

$$-\gamma \leq -\alpha$$

e como

$$-\alpha \leq \theta \leq \alpha$$

teremos

$$-\gamma \leq \alpha \leq \gamma$$

Analogamente, se

$$\alpha < \theta \overset{(2.5.5.(4))}{\Rightarrow} -\alpha > \theta$$

e

$$|\alpha| = -\alpha$$

Logo

$$-\alpha \leq \gamma$$

de onde vem

$$-\gamma \leq \alpha$$

e como

$$\alpha \leq \gamma$$

teremos

$$-\gamma \leq \alpha \leq \gamma$$

($\Leftarrow$) Reciprocamente, suponhamos que

$$-\gamma \leq \alpha \leq \gamma$$

Se $\alpha \geq \theta$, temos pela definição (2.5.8)

$$|\alpha| = \alpha$$

Portanto

$$|\alpha| \leq \gamma$$

Se $\alpha < \theta$, temos

$$|\alpha| = -\alpha$$

de onde resulta

$$|\alpha| \leq \gamma$$

Parte (5)**:** Vamos mostrar que

$$|\alpha + \beta| \leq |\alpha| + |\beta|$$

Temos por (2.5.9. (3)) que, $-|\alpha| \leq \alpha \leq |\alpha|$ e $-|\beta| \leq \beta \leq |\beta|$, logo

$$\begin{aligned} & -|\alpha| + (-|\beta|) \leq \alpha + \beta \leq |\alpha| + |\beta| \\ \Rightarrow \quad & -|\alpha| - |\beta| \leq \alpha + \beta \leq |\alpha| + |\beta| \\ \overset{(2.4.8.(3))}{\Rightarrow} \quad & -(|\alpha| + |\beta|) \leq \alpha + \beta \leq (|\alpha| + |\beta|) \\ \overset{(2.5.9.(4))}{\Rightarrow} \quad & |\alpha + \beta| \leq |\alpha| + |\beta| \end{aligned}$$

Parte (6)**:** Vamos mostrar que

$$|\alpha - \beta| \leq |\alpha| + |\beta|$$

Temos que,

$$|\alpha-\beta| \overset{(2.4.4)}{=} |\alpha+(-\beta)| \overset{(2.5.9.(5))}{\leq} |\alpha|+|-\beta| \overset{(2.5.9.(2))}{=} |\alpha|+|\beta|$$

Parte (7)**:** Vamos mostrar que

$$|\alpha|-|\beta| \leq |\alpha+\beta|$$

Temos que,

$$\begin{aligned} & |\alpha| \overset{(2.4.2)}{=} |\alpha+\theta| \overset{(2.4.3)}{=} |\alpha+\beta+(-\beta)| \overset{(2.5.9.(5))}{\leq} |\alpha+\beta|+|-\beta| \\ \Rightarrow \quad & |\alpha| \overset{(2.5.9.(2))}{\leq} |\alpha+\beta|+|\beta| \overset{(2.5.7.(5))}{\Rightarrow} |\alpha|-|\beta| \leq |\alpha+\beta| \end{aligned}$$

Parte (8)**:** Vamos mostrar que

$$|\alpha|-|\beta| \leq |\alpha-\beta|$$

Temos que,

$$|\alpha| \overset{(2.4.2)}{=} |\alpha+\theta| \overset{(2.4.3)}{=} |\alpha+(-\beta)+\beta| \overset{(2.5.9.(5))}{\leq} |\alpha-\beta|+|\beta| \overset{(2.5.7.(5))}{\Rightarrow} |\alpha|-|\beta| \leq |\alpha-\beta|$$

Parte (9)**:** Por (2.5.9. (4)), demonstrar

$$||\alpha|-|\beta|| \leq |\alpha-\beta|$$

é equivalente a mostrar que

$$-|\alpha-\beta| \leq |\alpha|-|\beta| \leq |\alpha-\beta|$$

Temos por (2.5.9. (8)), que

$$|\alpha|-|\beta| \leq |\alpha-\beta|$$

Por outro lado,

$$\begin{aligned} & |\beta| \overset{(2.4.2)}{=} |\beta+\theta| \overset{(2.4.3)}{=} |\beta+(-\alpha)+\alpha| \overset{(2.5.9.(5))}{\leq} |\beta-\alpha|+|\alpha| \\ & \overset{(2.5.7.(5))}{\Rightarrow} |\beta|-|\alpha| \leq |\beta-\alpha| \overset{(2.4.1.(2))}{\Rightarrow} -|\alpha|+|\beta| \leq |-\alpha+\beta| \\ & \overset{(2.4.8.(3))}{\Rightarrow} -(|\alpha|-|\beta|) \leq |-(\alpha-\beta)| \\ \overset{(2.5.5.(4))}{\Rightarrow} |\alpha|-|\beta| \quad \geq \quad & -|-(\alpha-\beta)| \overset{(2.5.9.(2))}{\Rightarrow} -|\alpha-\beta| \leq |\alpha|-|\beta| \end{aligned}$$

o que completa a demonstração.

Parte (10)**:** Vamos mostrar que

$$|\alpha \cdot \beta| = |\alpha| \cdot |\beta|$$

Temos quatro casos a considerar:

Caso (i)**:**Se $\alpha \geq \theta$ e $\beta \geq \theta$ então por $(2.5.5.\,(1))$ $\alpha \cdot \beta \geq \theta$, logo

$$|\alpha \cdot \beta| \overset{(2.5.8)}{=} \alpha \cdot \beta \overset{(2.5.8)}{=} |\alpha| \cdot |\beta|$$

Caso (ii): Se $\alpha \geq \theta$ e $\beta \leq \theta$ então por $(2.5.5.\,(3))$ $\alpha \cdot \beta \leq \theta$, e portanto

$$|\alpha \cdot \beta| \overset{(2.5.8)}{=} -(\alpha \cdot \beta) \overset{(2.4.8.(3))}{=} \alpha \cdot (-\beta) \overset{(2.5.8)}{=} |\alpha| \cdot |\beta|$$

Caso (iii): Se $\alpha \leq \theta$ e $\beta \leq \theta$ então por $(2.5.5.\,(2))$ $\alpha \cdot \beta \geq \theta$, e assim

$$|\alpha \cdot \beta| \overset{(2.5.8)}{=} \alpha \cdot \beta \overset{(2.4.8.(3))}{=} (-\alpha) \cdot (-\beta) \overset{(2.5.8)}{=} |\alpha| \cdot |\beta|$$

Caso (iv): Se $\alpha \leq \theta$ e $\beta \geq \theta$ então por $(2.5.5.\,(3))$ $\alpha \cdot \beta \leq \theta$, logo

$$|\alpha \cdot \beta| \overset{(2.5.8)}{=} -(\alpha \cdot \beta) \overset{(2.4.8.(3))}{=} (-\alpha) \cdot \beta \overset{(2.5.8)}{=} |\alpha| \cdot |\beta|$$

■

Teorema 2.5.10 *Não existe* $\alpha \in \mathbb{Z}$ *tal que* $0 < \alpha < 1$.

Demonstração. Suponha-se o contrário e seja $\beta \in \mathbb{Z}$ o menor número inteiro com tal propriedade. Como,

$$0 < \beta < 1 \overset{(2.5.7.(3))}{\Rightarrow} 0 < \beta \cdot \beta < \beta < 1$$

agora $0 < \beta \cdot \beta < 1$ e $\beta \cdot \beta < \beta$, contradizendo a hipótese de que β é o menor inteiro com tal propriedade e o teorema fica demonstrado. ■

Teorema 2.5.11 *Se* α *e* β *são números inteiros tais que*

$$\alpha \cdot \beta = 1$$

então α *e* β *são ambos iguais a* 1 *ou a* -1.

Demonstração. Primeiro, observamos que nem α nem β podem ser igual a θ. Agora,

$$|\alpha \cdot \beta| \overset{(2.5.9.(10))}{=} |\alpha| \cdot |\beta| \overset{(\text{hipótese})}{=} 1$$

e, pelo teorema anterior, $|\alpha| \geq 1$ e $|\beta| \geq 1$. Se $|\alpha| > 1$ ou $|\beta| > 1$, então

$$|\alpha| \cdot |\beta| > 1$$

o que é uma contradição.

Logo, $|\alpha| = |\beta| = 1$, donde $\alpha = \pm 1$ e $\beta = \pm 1$. Portanto, de $(2.4.8.\,(5))$ o resultado segue ■

2.6 NÚMEROS INTEIROS POSITIVOS E NÚMEROS NATURAIS

Definição 2.6.1 *Um número inteiro α* ***é positivo se*** *$\alpha > \theta$. O conjunto dos números inteiros positivos será denotado por $\mathbb{Z}_+$.*

Observe que

$$\mathbb{Z}_+ = \left\{ \overline{(a,b)} \mid a, b \in \mathbb{N} \text{ e } a > b \right\}$$

Vamos agora identificar os conjuntos $\mathbb{N}$ e $\mathbb{Z}_+$.

Teorema 2.6.2 *Os conjuntos $\mathbb{N}$ e $\mathbb{Z}_+$ são isomorfos, isto é, a aplicação*

$$\varphi : \mathbb{N} \longmapsto \mathbb{Z}_+$$

dada por tal que $\varphi(n) = \overline{(n+1,1)}$ é bijetora e tem as seguintes propriedades:

1. $\varphi(n_1 + n_2) = \varphi(n_1) + \varphi(n_2)$
2. $\varphi(n_1 \times n_2) = \varphi(n_1) \cdot \varphi(n_2)$
3. $n_1 < n_2 \Longleftrightarrow \varphi(n_1) < \varphi(n_2)$

Demonstração. Consideremos a aplicação

$$\varphi : n \in \mathbb{N} \longmapsto \varphi(n) = \overline{(n+1,1)} \in \mathbb{Z}_+$$

É claro que φ está bem definida. Agora, se $\varphi(n_1) = \varphi(n_2)$ vamos ter que

$$\overline{(n_1+1,1)} = \overline{(n_2+1,1)}$$

Portanto,

$$\begin{aligned} & & (n_1+1,1)\, R\, (n_2+1,1) \\ &\overset{(2.2.1)}{\Rightarrow} & n_1+1+1 &= n_2+1+1 \\ &\overset{(2.4.6)}{\Rightarrow} & n_1 &= n_2 \end{aligned}$$

Logo, φ é biunívoca.

A aplicação φ é sobrejetora. De fato, se $\alpha = \overline{(a,b)}$ é um elemento de $\mathbb{Z}_+$, com $a > b$, então, existe $n \in \mathbb{N}$ tal que $a = b + n$. Logo

$$\alpha = \overline{(a,b)} = \overline{(b+n,b)} = \overline{(b+n+1,b+1)} = \overline{(n+1,1)} = \varphi(n)$$

Parte (1): A aplicação φ preserva a soma. De fato, se n_1 e n_2 são números naturais, então

$$\begin{aligned}
\varphi(n_1) + \varphi(n_2) &= \overline{(n_1+1,1)} + \overline{(n_2+1,1)} \\
&= \overline{(n_1+1+n_2+1,1+1)} \\
&= \overline{(n_1+n_2+1+1,1+1)} \\
&= \overline{(n_1+n_2+1,1)} \\
&= \varphi(n_1+n_2)
\end{aligned}$$

Parte (2): A aplicação φ preserva o produto. De fato, se n_1 e n_2 são números naturais, então

$$\begin{aligned}
\varphi(n_1) \cdot \varphi(n_2) &= \overline{(n_1+1,1)} \cdot \overline{(n_2+1,1)} \\
&= \overline{((n_1+1)(n_2+1)+1, n_1+1+n_2+1)} \\
&= \overline{(n_1 \times n_2 + n_1 + n_2 + 1 + 1, n_1+n_2+1+1)} \\
&= \overline{(n_1 \times n_2 + 1, 1)} \\
&= \varphi(n_1 \times n_2)
\end{aligned}$$

Parte (3): A aplicação φ preserva a ordem. De fato, se $n_2 > n_1$, então existe $n \in \mathbb{N}$ tal que $n_2 = n_1 + r$ e

$$\varphi(n_2) = \varphi(n_1 + r) = \varphi(n_1) + \varphi(r) > \varphi(n_1)$$

pois $\varphi(m) > 0$, para todo $m \in \mathbb{N}$. ■

Observação 2.6.3 *Como $\mathbb{N}$ e $\mathbb{Z}_+$ são isomorfos segue que podemos identificar o conjunto dos números naturais como um subconjunto dos números inteiros. Ou seja, podemos identificar cada elemento $n \in \mathbb{N}$ com o elemento $\overline{(a,b)} \in \mathbb{Z}_+$ se $a = b + n$ com $n \in \mathbb{N}$, isto é, se*

$$(a,b)\, R\, (b+n,b)\, R\, (n+1,1)$$

Portanto, se $\mathbb{Z}_-$ é o conjunto dos números inteiros $\overline{(a,b)}$ com $a < b$, vamos ter

$$\mathbb{Z} = \mathbb{Z}_- \cup \{\theta\} \cup \mathbb{Z}_+$$

Como $\mathbb{Z}_+$ " = "$\mathbb{N}$, vamos escrever $\mathbb{Z}_- = -\mathbb{N}$ e $\theta = 0$. Desta forma

$$\mathbb{Z} \text{ " = " } \{\cdots, -n, \cdots, -1, 0, 1, \cdots, n, \cdots\}$$

Observe, então, que $-n$ é uma notação para o número inteiro $\overline{(1,n+1)}$.

A identificação dos números naturais como um subconjunto dos números inteiros permite estabelecer o **Princípio do Menor Elemento** para os números inteiros.

Definição 2.6.4 *Um subconjunto A de $\mathbb{Z}$ é* ***limitado inferiormente*** *se existe um elemento k em $\mathbb{Z}$, chamado de um limitante inferior para A, tal que*

$$k \leq \alpha$$

para todo α em A.

Um elemento α_0 em A é um menor elemento ou elemento mínimo de A, se for um limitante inferior para A.

Teorema 2.6.5 *Seja A um subconjunto não vazio e limitado inferiormente de $\mathbb{Z}$. Então, A tem um menor elemento.*

Demonstração. Seja φ a bijeção que identifica $\mathbb{N}$ com $\mathbb{Z}_+$ e seja K um limitante inferior para A. A função $\psi(n) = \varphi(n) + K - 1$ é biunívoca de $\mathbb{N}$ em $\mathbb{Z}$, preserva a ordem e $A \subset \psi(\mathbb{N})$. O conjunto $\psi^{-1}(A) \subset \mathbb{N}$ tem um menor elemento $n_0 \in \psi^{-1}(A)$. Então $\alpha_0 = \psi(n_0)$ é o menor elemento de A. ■

Observação 2.6.6 *A seção de Potência no capítulo 1 pode ser repetida aqui após a substituição de $\mathbb{N}$ por $\mathbb{Z}_+$.*

2.7 DIVISIBILIDADE

Definição 2.7.1 *Sejam α e β números inteiros. Diremos que β* ***divide*** *α, e escrevemos $\beta|\alpha$, se $\alpha = \beta \cdot \gamma$ para algum γ em $\mathbb{Z}$. Neste caso, diremos também que α* ***é divisível por*** *β,* ***que α é um múltiplo de*** *β e que β* ***é um divisor de*** *α. A negação de $\beta|\alpha$ será indicada por $\beta \nmid \alpha$ (leia-se: β não divide α). A relação "β é divisor de α" , que está sendo indicada com o símbolo $|$, é denominada relação de divisibilidade (sobre $\mathbb{Z}$). Notemos, $\alpha|0$ para todo inteiro α e que $0|\alpha$ se, e somentese, $\alpha = 0$; por causa desta última propriedade costuma-se excluir o caso em que o divisor é nulo, isto é, considera-se a restrição da relação de divisibilidade ao subconjunto $\mathbb{Z}' \times \mathbb{Z}$, onde $\mathbb{Z}' = \mathbb{Z} - \{0\}$.*

Teorema 2.7.2 *Se α e β são números inteiros positivos e $\beta|\alpha$ então $\beta \leq \alpha$.*

Demonstração. Como $\beta|\alpha$, existe γ em $\mathbb{Z}$ tal que $\alpha = \beta \cdot \gamma$. Como $\alpha > 0$ e $\beta > 0$ então também $\gamma > 0$. Portanto

$$\gamma \geq 1 \text{ e } \alpha = \beta \cdot \gamma \geq \beta \cdot 1 = \beta$$

■

Teorema 2.7.3 *Sejam α, β e γ números inteiros. Então*

(1) $\alpha|\alpha$

(2) $\alpha|\beta$ e $\beta|\gamma \Rightarrow \alpha|\gamma$

(3) $\alpha|\beta$ e $\alpha|\gamma \Rightarrow \alpha|\,(\beta \pm \gamma)$

(4) $\alpha|\beta \Rightarrow \alpha\gamma|\beta\gamma$

(5) $\alpha|\beta$ e $\alpha|\gamma \Rightarrow \alpha|\,(\beta \cdot \gamma)$

(6) $\alpha|\beta$ e $\beta|\alpha \Rightarrow \alpha = \pm\beta$

(7) $\alpha|\beta \Rightarrow \alpha|\beta\gamma$

Demonstração. Parte (1)**:** Basta notar que

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

Parte (2)**:** Por hipótese existem números inteiros ε e δ, tal que $\beta = \alpha \cdot \varepsilon$ e $\gamma = \beta \cdot \delta$, logo

$$\gamma = \beta \cdot \delta \overset{\text{(hipótese)}}{=} (\alpha \cdot \varepsilon) \cdot \delta \overset{(2.4.7.(1))}{=} \alpha \cdot (\varepsilon \cdot \delta)$$

portanto $\alpha|\gamma$.

Parte (3)**:** Por hipótese existem números inteiros ε e δ, tal que $\beta = \alpha \cdot \varepsilon$ e $\gamma = \alpha \cdot \delta$, logo

$$\beta \pm \gamma \overset{\text{(hipótese)}}{=} \alpha\varepsilon \pm \alpha\delta \overset{(2.4.7.(4))}{=} \alpha\,(\varepsilon \pm \delta)$$

portanto $\alpha|\,(\beta \pm \gamma)$.

Parte (4)**:** Por hipótese existe um número inteiro ε, tal que $\beta = \alpha \cdot \varepsilon$, logo por (2.4.8. (2))

$$\beta \cdot \gamma = (\alpha \cdot \varepsilon) \cdot \gamma \overset{(2.4.7.(2) \text{ e } 2.4.7.(1))}{=} (\alpha \cdot \gamma) \cdot \varepsilon$$

portanto $\alpha\gamma|\beta\gamma$.

Parte (5)**:**Por hipótese existem números inteiros ε e δ, tal que $\beta = \alpha \cdot \varepsilon$ e $\gamma = \alpha \cdot \delta$, logo

$$\beta \cdot \gamma \overset{\text{(hipótese)}}{=} \alpha\varepsilon \cdot \alpha\delta \overset{\text{(2.4.7.(2) e 2.4.7.(1))}}{=} \alpha\left(\alpha \cdot \varepsilon \cdot \delta\right)$$

portanto $\alpha|\beta\gamma$.

Parte (6)**:**Por hipótese existem números inteiros ε e δ, tal que $\beta = \alpha \cdot \varepsilon$ e $\alpha = \beta \cdot \delta$, logo

$$\begin{aligned} & \beta \cdot \alpha \overset{\text{(hipótese)}}{=} \alpha\varepsilon \cdot \beta\delta \\ \Rightarrow \quad & \beta\alpha \overset{\text{(2.4.1.(1) e 2.4.1.(2))}}{=} \varepsilon\delta \cdot \beta\alpha \\ \Rightarrow \quad & 1 \overset{\text{(2.4.8.(2))}}{=} \varepsilon\delta \end{aligned}$$

pelo teorema (2.5.11), temos $\delta = 1$ ou $\delta = -1$ e $\alpha = \beta \cdot \delta = \beta \cdot 1 = \beta$ ou $\alpha = -\beta$.

Parte (7)**:** Por hipótese existe um número inteiro ε, tal que $\beta = \alpha \cdot \varepsilon$, logo por (2.4.8. (2))

$$\beta \cdot \gamma = (\alpha \cdot \varepsilon) \cdot \gamma \overset{\text{(2.4.7.(1))}}{=} \alpha \cdot (\varepsilon \cdot \gamma)$$

portanto $\alpha|\beta\gamma$. ■

O teorema acima nos mostra que a relação de divisibilidade é reflexiva e transitiva (partes 2.7.3. (1) e 2.7.3. (2)) e é, compatível com a multiplicação (2.7.3. (4)); notemos que não vale a proposição simétrica, pois, por exemplo $2|\,(-2)$ e $(-2)\,|2$, com $2 \neq -2$. A parte (2.7.3. (4)) do teorema anterior pode se completada pelo seguinte

Corolário 2.7.4 *Se α, β e γ são números naturais e se $\gamma \neq 0$, então $\alpha|\beta$ se, e somente se, $\alpha\gamma|\beta\gamma$*

Demonstração. Com efeito, de

$$\alpha\gamma|\beta\gamma$$

vem

$$\beta\gamma = (\alpha\gamma)\,\varepsilon$$

com $\varepsilon \in \mathbb{Z}$, logo por (2.4.7. (2) e 2.4.7. (1))

$$\beta\gamma = (\alpha\varepsilon)\,\gamma$$

então

$$\beta = \alpha\varepsilon$$

portanto, $\alpha|\beta$. ■

É imediato que qualquer número inteiro α é divísivel por $\alpha, -\alpha, 1, -1$. Estes números são denominados divisores impróprios de α e qualquer outro divisor de α é denominado divisor próprio. Portanto, β é divisor próprio de α se $\beta|\alpha$ e se $\beta \neq \pm 1$ e $\beta \neq \pm\alpha$.

Afirmamos que o número 1 só admite divisores impróprios. Com efeito, se $\beta \backslash 1$, temos

$$1 = \alpha \cdot \beta$$

então, pelo teorema (2.5.11), $\beta = \pm 1$

O **algoritmo da divisão** ou **algoritmo de Euclides** é dado no seguinte teorema

Teorema 2.7.5 *Sejam α e β números inteiros com $\beta \neq 0$. Então, existe um único par (q, r) de números inteiros tal que*

$$\alpha = \beta \cdot q + r$$

com $0 \leq r < |\beta|$.

Demonstração. Existência: Suponhamos inicialmente que $\beta > 0$ e seja

$$A = \{\gamma \in \mathbb{Z} \mid \gamma \geq 0 \text{ e } \gamma = \alpha - \beta\chi; \chi \in \mathbb{Z}\}$$

O conjunto A é não vazio, pois, se $\chi = -|\alpha| \in \mathbb{Z}$, temos

$$\gamma = \alpha - \beta\chi = \alpha - \beta(-|\alpha|) = \alpha + \beta|\alpha| \geq \alpha + |\alpha| \geq 0$$

Então, como A é limitado inferiormente por zero e é não vazio, pelo princípio do menor elemento dos números inteiros, segue que A tem um menor elemento r. Logo, se $r \geq 0$

$$r = \alpha - \beta q \Rightarrow \alpha = r + \beta q, \text{ para } q \in \mathbb{Z}$$

Se por absurdo $\beta \leq r$, temos

$$r - \beta = \alpha - \beta q - \beta = \alpha - \beta(q + 1)$$

e portanto $r - \beta \in A$ com $r - \beta \leq r$, uma contradição.

No caso em que $\beta < 0$, existem inteiros q' e r', tais que

$$\alpha = (-\beta)\, q' + r' = \beta\,(-q') + r'$$

onde

$$0 \leq r' < -\beta = |\beta|$$

portanto basta escolher $q = -q'$ e $r = r'$para que (2.7.5) seja verificada.

Unicidade: Seja (q_1, r_1) um outro par de números inteiros tal que

$$\alpha = \beta q_1 + r_1$$

com

$$0 \leq r_1 < |\beta|$$

Como

$$\alpha = \beta q + r$$

com

$$0 \leq r < |\beta|$$

Temos

$$\begin{aligned}
\beta q + r &= \beta q_1 + r_1 \\
\Rightarrow \beta q - \beta q_1 &= r_1 - r \\
\overset{(2.4.7.(4))}{\Rightarrow} \beta\,(q - q_1) &= r_1 - r \\
\Rightarrow |\beta\,(q - q_1)| &= |r_1 - r| \\
\overset{(2.5.9.(10))}{\Rightarrow} |\beta|\,|q - q_1| &= |r - r_1|
\end{aligned}$$

Agora, se $r_1 \neq r$ segue do teorema (2.5.10) que $|q - q_1| \geq 1$, logo

$$|\beta|\,|q - q_1| \geq \beta \Rightarrow |r - r_1| \geq \beta$$

Mas por outro lado, temos

$$0 \leq r_1 < r \text{ ou } 0 \leq r < r_1$$

digamos que

$$r < r_1$$

portanto

$$0 < r_1 - r < r_1 < |\beta|$$

e temos uma contradição. Logo $r_1 = r$ e consequentemente $q = q_1$. ■

2.8 MÁXIMO DIVISOR COMUM

Vamos agora estudar o Máximo Divisor Comum de números inteiros.

Definição 2.8.1 *Um número inteiro d* ***é um máximo divisor comum de dois números inteiros*** α ***e*** β *se, e somente se, são válidas as seguintes condições:*

(1) $d|a$ e $d|\beta$;

(2) se $d'|\alpha$ e $d'|\beta$ então $d'|d$.

O máximo divisor comum dos números α e β é denotado por $mdc\,(\alpha, \beta)$.

Teorema 2.8.2 *Sejam α e β dois números inteiros, não nulos simultâneamente e seja $d = mdc\,(\alpha, \beta)$, nestas condições existem números inteiros r e s, tais que*

$$d = r \cdot \alpha + s \cdot \beta$$

Demonstração. Consideremos o conjunto

$$A = \{x \cdot \alpha + y \cdot \beta \in \mathbb{Z}_+ \mid x \in \mathbb{Z} \text{ e } y \in \mathbb{Z}\}$$

Observando-se que os números $-a, a, -b$ e b pertence a A e que pelo menos um deles é estritamente positivo, resulta que A é não vazio, portanto, existe $d_1 = \min A > 0$. Ora d_1é um elemento de A. Logo existem números inteiros r e s tais que

$$d_1 = r \cdot \alpha + s \cdot \beta \qquad (i)$$

e observando que $d|\alpha$ e $d|\beta$ resulta $d|d_1$ portanto $d \leq d_1$.

Afirmamos que $d_1|\alpha$. Com efeito, se $d_1 \nmid \alpha$ existiriam, conforme o teorema (2.7.5), números inteiros q e t tais que $\alpha = q \cdot d_1 + t$, onde $0 < t < d_1$; desta igualdade e de (i) viria

$$t = \alpha - qd_1 = \alpha - q\,(r\alpha + s\beta) = (1 - qr)\,\alpha + (-qs)\,\beta$$

e como $t > 0$, teríamos $t \in A$, contra o fato que $0 < t < d_1 = \min A$.

Demonstra-se, analogamente, que $d_1|\beta$ e portanto, d_1 é um divisor comum positivo de α e β, logo $d_1 \quad d$ e então $d_1 = d$. ■

Definição 2.8.3 *Dizemos que dois números inteiros α* ***e*** *β* ***são primos entre si*** *se $mdc\,(\alpha, \beta) = 1$.*

Teorema 2.8.4 *Sejam α e β números inteiros, com $\alpha \neq 0$ ou $\beta \neq 0$ e seja $d = mdc(\alpha, \beta)$. Se α' e β' são tais que $\alpha = \alpha' \cdot d$ e $\beta = \beta' \cdot d$, então*

$$mdc(\alpha', \beta') = 1$$

ou seja, α' e β' são primos entre si.

Demonstração. Sejam s e t tais que

$$\begin{aligned} & d \overset{\text{(hipótese)}}{=} mdc(\alpha, \beta) \overset{(2.8.2)}{=} s \cdot \alpha + t \cdot \beta \\ \Rightarrow \quad & d \overset{\text{(hipótese)}}{=} s \cdot (\alpha' \cdot d) + t \cdot (\beta' \cdot d) \\ \Rightarrow \quad & d \overset{(2.4.7.(1))}{=} (s \cdot \alpha') \cdot d + (t \cdot \beta') \cdot d \\ \Rightarrow \quad & d \overset{(2.4.7.(3))}{=} (s \cdot \alpha' + t \cdot \beta') \cdot d \\ \Rightarrow \quad & 1 \overset{(2.4.8.(2))}{=} s \cdot \alpha' + t \cdot \beta' \end{aligned}$$

Agora, se $d'|\alpha'$ e $d'|\beta'$, vamos ter $d'|1$. Portanto $mdc(\alpha', \beta') = 1$. ■

Teorema 2.8.5 *Se α, β e γ são números inteiros tais que $\alpha \backslash \gamma$, $\beta \backslash \gamma$ e se α e β são primos entre si, então $(\alpha\beta) \backslash \gamma$*

Demonstração. Em virtude do teorema(2.8.2) existem inteiros r e s tais que

$$r\alpha + s\beta = 1$$

donde segue

$$r(\alpha\gamma) + s(\beta\gamma) = \gamma$$

Assim,

$$\begin{cases} \alpha|\gamma \overset{(2.7.3.(4))}{\Rightarrow} \alpha\beta|\beta\gamma \overset{(2.7.3.(7))}{\Rightarrow} \alpha\beta|t\beta\gamma \\ \beta|\gamma \overset{(2.7.3.(4))}{\Rightarrow} \alpha\beta|\alpha\gamma \overset{(2.7.3.(7))}{\Rightarrow} \alpha\beta|s\alpha\gamma \end{cases} \overset{(2.7.3.(3))}{\Rightarrow} \alpha\beta|(s\alpha\beta + t\beta\gamma) \Rightarrow \alpha\beta|\gamma$$

■

Observação 2.8.6 *Terminaremos esta seção dando o processo das divisões sucessivas para a determinação do máximo divisor comum positivo de dois inteiros α e α_1.*

Suponhamos, sem perda de generalidade, que $\alpha_1 > 0$. De acordo, com o algorítmo da divisão, temos

$$\alpha = q_1\alpha_1 + \alpha_2, \text{ com } 0 \leq \alpha_2 < \alpha_1$$

Supondo-se que $\alpha_2 \neq 0$ e aplicando-se novamente o algorítmo da divisão teremos

$$\alpha_1 = q_2\alpha_2 + \alpha_3, \text{ com } 0 \leq \alpha_3 < \alpha_2$$

Supondo-se que $\alpha_3 \neq 0$ e repetindo-se o mesmo processo chegaremos, certamente, a uma divisão que é exata e teremos as relações

(1)
$$\begin{cases} \alpha = q_1\alpha_1 + \alpha_2, \text{ com } 0 \leq \alpha_2 < \alpha_1 \\ \alpha_1 = q_2\alpha_2 + \alpha_3, \text{ com } 0 \leq \alpha_3 < \alpha_2 \\ \alpha_2 = q_3\alpha_3 + \alpha_4, \text{ com } 0 \leq \alpha_4 < \alpha_3 \\ \cdots\cdots\cdots\cdots\cdots\cdots\cdots \\ \alpha_{n-1} = q_n\alpha_n + \alpha_{n+1}, \text{ com } 0 \leq \alpha_{n+1} < \alpha_n \\ \alpha_n = q_{n+1}\alpha_{n+1} \end{cases}$$

Nestas condições, afirmamos que $\alpha_{n+1} = mdc\,(\alpha, \alpha_1)$. Com efeito, temos $\alpha_{n+1}|\alpha_n$ e daí resulta, conforme a penúltima relação, $\alpha_{n+1}|\alpha_{n-1}$, levando-se em conta que $\alpha_{n-2} = q_{n-1}\alpha_n + \alpha_n$ tem-se $\alpha_{n+1}|\alpha_{n-2}$. Repetindo-se este raciocínio chegaremos as relações $\alpha_{n+1}|\alpha_1$ e $\alpha_{n+1}|\alpha$, o que verifica (2.8.1. (1)). Analogamente, se $d|\alpha$ e $d|\alpha_1$, temos, em virtude da primeira relação (2.8.2), $d|\alpha_2$ e, portanto, de acordo com a segunda relação de (2.8.2), $d|\alpha_3$; repetindo-se este raciocínio teremos $d|\alpha_{n+1}$, o que verifica (2.8.1. (2)) .

É usual dispor os cálculos, dados pelas relações (2.8.6. (1)), do seguinte modo

	q_1	q_2	q_3	$\cdots$		q_n	q_{n+1}
α	α_1	α_2	α_3	$\cdots$	α_{n-1}	α_n	α_{n+1}
α_2	α_3	α_4		$\cdots$	α_{n+1}	0	

Exemplo 2.8.7 *Determinar o máximo divisor comum dos números* 12740 *e* 7260.

	1	1	3	12	1	2	2
12740	7260	5480	1780	140	100	40	20
5480	1780	140	100	40	20	0	

Portanto, $mdc\,(12740, 7260) = 20$

O processo das divisões sucessivas para determinar o mdc de dois inteiros também nos dá um processo para determinar dois inteiros β e γ tais que $\beta\alpha + \gamma\alpha_1 = mdc\,(\alpha, \alpha_1)$. Com efeito, da primeira relação (2.8.6. (1)) tiramos $\alpha_2 = \alpha + (-q_1)\,\alpha_1$, isto é, α_2 é "uma combinação linear com coeficientes inteiros de α e α_1"; analogamente, temos $\alpha_3 = \alpha_1 + (-q_2)\,\alpha_2 = (-q_2)\,\alpha_1 + (1 + q_1q_2)\,\alpha_1$, isto é, α_3 também é uma combinação linear de α e α_1. Repetindo-se este processo chegaremos à relação $\alpha_{n+1} = \beta\alpha + \gamma\alpha_1$, com β e γ inteiros.

Exemplo 2.8.8 *Determinar dois inteiros β e γ tais que $\beta \cdot 12740 + \gamma \cdot 7260 = 20$.*

De acordo com os cálculos feitos acima, temos

$$\begin{aligned} 20 &= 100 - 2 \cdot 40 \\ 40 &= 140 - 100 \\ 100 &= 1780 - 12 \cdot 140 \\ 140 &= 5480 - 3 \cdot 1780 \\ 1780 &= 7260 - 5480 \\ 5480 &= 12740 - 7260 \end{aligned}$$

logo,

$$\begin{aligned} 20 &= 100 - 2 \cdot 40 = 100 - 2\,(140 - 100) = 3 \cdot 100 - 2 \cdot 140 \\ &= 3 \cdot (1780 - 12 \cdot 140) - 2 \cdot 140 = 3 \cdot 1780 - 38 \cdot 140 \\ &= 3 \cdot 1780 - 38 \cdot (5480 - 3 \cdot 1780) = 117 \cdot 1780 - 38 \cdot 5480 \\ &= 117 \cdot (7260 - 5480) - 38 \cdot 5480 = 117 \cdot 7260 - 155 \cdot 5480 \\ &= 117 \cdot 7260 - 155 \cdot (12740 - 7260) = 272 \cdot 7260 - 155 \cdot 12740 \\ &= (-155) \cdot 12740 + 272 \cdot 7260 \end{aligned}$$

Portanto, $\beta = -155$ e $\gamma = 272$.

2.9 MÍNIMO MÚLTIPLO COMUM

Para todo inteiro α indicaremos por $M\,(\alpha)$ (resp., $M_+\,(\alpha)$) o conjunto de todos os números inteiros (resp., inteiros positivos) que são múltiplos de α. Por exemplo, temos $M\,(0) = \{0\}$ e $M\,(-1) = M\,(1) = \mathbb{Z}$. Se α e β são dois números inteiros, então todo elemento γ de $M\,(\alpha) \cap M\,(\beta)$ satisfaz as condições $\alpha|\gamma$ e $\beta|\gamma$; diz-se, neste caso, que γ é um múltiplo comum de α e

β. O conjunto $M_+(\alpha) \cap M_+(\beta)$ é não vazio e minorado, portanto, existe o mínimo deste conjunto, que passa a ser denominado mínimo múltiplo comum de α e β e será indicado por $mmc(\alpha, \beta)$; é imediato que se γ é um múltiplo comum de α e β, então $mmc(\alpha, \beta) \leq |\gamma|$.

Teorema 2.9.1 *Quaisquer que sejam os números inteiros α e β, tem-se*

$$mdc(\alpha, \beta) \cdot mmc(\alpha, \beta) = |\alpha\beta|$$

Demonstração. É evidente que basta verificar a igualdade acima para $\alpha > 0$ e $\beta > 0$ e neste caso precisamos demonstrar que $dm = \alpha\beta$ onde $d = mdc(\alpha, \beta)$ e $m = mmc(\alpha, \beta)$. Notemos que o produto $\alpha\beta$ é múltiplo de d, logo, $\alpha\beta = dm_1$, onde m_1 é um inteiro positivo. Pondo-se $\alpha = \alpha_1 d$ e $\beta = \beta_1 d$ teremos $\alpha_1\beta_1 d = m_1$, ou seja, $\alpha\beta_1 = m_1 = \alpha_1\beta$, de onde resulta que m_1 é um múltiplo comum de α e β; portanto, $m \leq m_1$. Por outro lado, temos $m = m' d$ e como $\alpha | m$ e $\beta | m$ teremos $(\alpha_1 d) \,|\, (m' d)$ e $(\beta_1 d) \,|\, (m' d)$, logo, $\alpha_1 | m'$ e $\beta_1 | m'$, de onde vem pelo teorema (2.8.5), $(\alpha_1\beta_1) \,|\, m'$ e então $(\alpha_1\beta_1 d) \,|\, m' d$, ou seja, $m_1 | m$ e, portanto, $m_1 \leq m$. Fica assim demonstrado que $m_1 = m$ e, portanto, $\alpha\beta = dm$. ■

Definição 2.9.2 *Diz-se que um número natural m* ***é um mínimo múltiplo comum de dois números inteiros*** *α* ***e*** *β se, e somente se, são válidas as seguintes condições:*

(1) $\alpha | m$ e $\beta | m$;

(2) para todo número inteiro m', se $\alpha | m'$ e se $\beta | m'$, então $m | m'$.

Observação 2.9.3 *Se $\alpha = 0$ ou $\beta = 0$, então $m = 0$ é o único número que satisfaz as condições acima. Se $\alpha \neq 0$ e $\beta \neq 0$ e se m e m_1 são mínimos múltiplos comuns de α e β, segundo a definição acima, então $m | m_1$ e $m_1 | m$, logo, $m_1 = \pm m$ (2.7.3. (6)); isto nos mostra que se impuzermos, na definição acima, a condição $m \geq 0$, então o única número inteiro m que satisfaz as condições (2.9.2. (1)) e (2.9.2. (2)) é o mínimo múltiplo comum de α e β como foi definido no início da secção.*

Exemplo 2.9.4 *Determinar o mínimo múltiplo comum positivo dos números inteiros* 486 *e* 288.

Temos

	1	1	2	5
486	288	198	90	18
198	90	18	0	

logo, $mdc\,(486, 288) = 18$ e pela aplicação do teorema (2.9.1), temos

$$18m = 486 \cdot 288$$

logo,

$$m = 7488$$

2.10 NÚMEROS PRIMOS

Definição 2.10.1 *Um número inteiro positivo $\alpha \neq 1$* ***é primo*** *se $d|\alpha$ implicar que $d = \pm\alpha$ ou $d = \pm 1$.*

Teorema 2.10.2 *Se p é um número primo e $p|\,(\alpha \cdot \beta)$ então $p|\alpha$ ou $p|\beta$.*

Demonstração. Suponhamos que p não divide α, então $mdc\,(\alpha, p) = 1$. Logo, existem inteiros s e t tais que

$$1 = s \cdot p + t \cdot \alpha$$

e tem-se por (2.4.8. (2)) que

$$\beta = \beta \cdot s \cdot p + \beta \cdot t \cdot \alpha$$

Mas

$$p|\,(\alpha \cdot \beta) \Rightarrow \exists \gamma \in \mathbb{Z}\ |\alpha \cdot \beta = p \cdot \gamma$$

Assim,

$$\begin{aligned} \beta &= \beta \cdot s \cdot p + \beta \cdot \alpha \cdot t \Rightarrow \beta = \beta \cdot s \cdot p + p \cdot \gamma \cdot t \\ \overset{(2.4.7.(4))}{\Rightarrow}\ \beta &= p \cdot (\beta \cdot s + \gamma \cdot t) \Rightarrow p \backslash \beta \end{aligned}$$

■

A seguir demonstraremos o **Teorema Fundamental Da Aritmética**

Teorema 2.10.3 *Todo número inteiro positivo α, $\alpha \neq 0, 1$, pode ser decomposto num produto de fatores primos, e a decomposição é única.*

Demonstração. Existência: Como 2 é um número primo segue que $\alpha = 2$ é uma decomposição. Suponhamos então que a decomposição existe para todo $\beta \in \mathbb{Z}$, tal que $2 \leq \beta < \alpha$. Se α for primo não há o que demonstrar. Se α não é um número primo então existem inteiros positivos p e q tais que

$\alpha = p \cdot q$ e $1 < p, q < \alpha$. Pela hipótese de indução p e q são produtos de fatores primos. Consequentemente, $\alpha = p \cdot q$ também o é.

Unicidade: Sejam $\alpha = p_1 \cdot p_2 \cdot \cdots \cdot p_m$ e $\alpha = q_1 \cdot q_2 \cdot \cdots \cdot q_n$. Se $m = 1$ então $p_1 = q_1 \cdot \cdots \cdot q_n$ e necessariamente $n = 1$. Logo, $p_1 = q_1$ neste caso.

Suponhamos agora que se α admite uma decomposição num produto de $m - 1$ fatores primos então a decomposição é única. Vamos demonstrar que se α admite uma decomposição em m fatores primos, esta decomposição também é única. Seja $\alpha = p_1 \cdot p_2 \cdot \cdots \cdot p_m = q_1 \cdot q_2 \cdot \cdots \cdot q_n$. Então $p_1 | q_1 \cdot \cdots \cdot q_n$ e portanto $p_1 | q_j$, para algum j. Como q_j é primo segue que $p_1 = q_j$, Façamos $\alpha' = \alpha | p_1$. Então $\alpha' \neq 0$, $\alpha' \neq \pm 1$ e $\alpha' = p_2 \cdot \cdots \cdot p_m = q_1 \cdot \cdots \cdot \tilde{q_j} \cdot \cdots \cdot q_n$ (aqui $\tilde{q_j}$ denota a ausência do termo q_j). Pela hipótese de indução $m - 1 = n - 1$ (o que implica $m = n$) e cada p_i é igual a q_k , para algum k. Logo, a decomposição em m fatores também é única. Mais ainda, se α admite uma decomposição em m fatores não admite uma decomposição em n fatores, com $m \neq n$. ■

Teorema 2.10.4 *Sejam $p_1, \cdots, p_n$ números primos que dividem α. Então, o produto $p_1 \cdot \cdots \cdot p_n$ também divide α.*

Demonstração. Vamos provar por indução
De fato $n = 2$, $p_1 | \alpha$ e $p_2 | \alpha$, temos por (2.7.1) que

$$\alpha = p_1 d_1 \text{ e } \alpha = p_2 d_2, \text{ para } d_1, d_2 \in \mathbb{Z}$$

logo

$$p_1 d_1 = p_2 d_2$$

donde

$$p_1 | p_2 d_2$$

e como p_2 é primo, $p_1 | d_2$. Logo $d_2 = d_3 p_1$ e $\alpha = d_3 p_1 p_2$; ou seja

$$p_1 p_2 | \alpha$$

Suponhamos que $p_1, p_2, p_3, \cdots, p_k$ são números primos onde

$$p_1 \cdot p_2 \cdot p_3 \cdot \cdots \cdot p_k | \alpha$$

com

$$p_1 | \alpha,\ p_2 | \alpha, p_3 | \alpha, \cdots, p_k | \alpha$$

Vamos mostrar que

$$p_1 \cdot p_2 \cdot p_3 \cdot \cdots \cdot p_k \cdot p_{k+1} | \alpha$$

sendo $p_1, p_2, p_3, \cdots, p_k, p_{k+1}$ números primos, com

$$p_1|\alpha,\ p_2|\alpha, p_3|\alpha, \cdots, p_k|\alpha, p_{k+1}|\alpha$$

Temos por hipótese que

$$p_1 \cdot p_2 \cdot p_3 \cdot \cdots \cdot p_k | \alpha \text{ e } p_{k+1}|\alpha$$

logo por (2.7.1), temos que

$$\alpha = p_1 \cdot p_2 \cdot p_3 \cdot \cdots \cdot p_k \cdot d_k \text{ e } \alpha = p_{k+1} \cdot d_{k+1}$$

para d_k e $d_{k+1} \in \mathbb{Z}$. Mas

$$p_{k+1} \cdot d_{k+1} = p_1 \cdot p_2 \cdot p_3 \cdot \cdots \cdot p_k \cdot d_k$$

donde

$$p_{k+1} | p_1 \cdot p_2 \cdot p_3 \cdot \cdots \cdot p_k \cdot d_k$$

e como $p_1, p_2, p_3, \cdots, p_k$ são primos,

$$p_{k+1}|d_k$$

Logo

$$d_k = d_{k+2} p_{k+1}, \text{ para } d_{k+2} \in \mathbb{Z}$$

e

$$\alpha = p_1 \cdot p_2 \cdot p_3 \cdot \cdots \cdot p_k \cdot p_{k+1} \cdot d_{k+2}$$

Portanto

$$p_1 \cdot p_2 \cdot p_3 \cdot \cdots \cdot p_k \cdot p_{k+1} | \alpha$$

■

Observação 2.10.5 *Como consequência do teorema acima, para verificarmos se um inteiro α é divisível por um número d basta decompor o inteiro d em fatores primos e verificar se α é divisível por esses fatores.*

2.11 CONGRUÊNCIA MÓDULO m

Seja m um número inteiro maior do que 1.

Definição 2.11.1 *Sejam $\alpha, \beta, m \in \mathbb{Z}$. Dizemos que α* ***é congruente a β, módulo*** *m, se $\alpha - \beta$ é divisível por m. Neste caso, escrevemos*

$$\alpha \equiv \beta \,(\mathrm{mod}\, m) \Leftrightarrow m|\alpha - \beta$$

A notação $\alpha \not\equiv \beta \,(\mathrm{mod}\, m)$ significa que α não é congruente a β módulo m.

Notemos que se $m = 0$, então, $\alpha \equiv \beta \,(\mathrm{mod}\, 0)$ se, e somente se, $\alpha \equiv \beta$; por causa disso costuma-se excluir o caso em que o módulo m é nulo. Observemos que $\beta|\alpha$ se, e somente se, $\alpha \equiv 0 \,(\mathrm{mod}\, \beta)$

A relação "α congruente a β módulo m", entre elementos de $\mathbb{Z}$, é denominada congruência módulo m, ou, simplesmente, congruência.Um outro mode de dar a definição acima é o seguinte: $\alpha \equiv \beta \,(\mathrm{mod}\, m)$ se, e somente se, existe $q \in \mathbb{Z}$ tal que $\alpha - \beta = qm$.

Exemplo 2.11.2 *Temos* $16 \equiv -4 \,(\mathrm{mod}\, 10)$*, pois,* $16 - (-4) = 20$ *é um múliplo de 10; por outro lado,* $16 \not\equiv 1 \,(\mathrm{mod}\, 10)$*, pois,* $16 - 1 = 15$ *não é um múltiplo de* 10.

O teorema seguinte, garante que a congruência módulo m é uma relação de equivalência.

Teorema 2.11.3 *A congruência módulo m é uma relação de equivalência em $\mathbb{Z}$, ou seja*

(1) $\alpha \equiv \alpha \,(\mathrm{mod}\, m)$ $(reflexiva)$

(2) $\alpha \equiv \beta \,(\mathrm{mod}\, m) \Rightarrow \beta \equiv \alpha \,(\mathrm{mod}\, m)$ $(simétrica)$

(3) $\alpha \equiv \beta \,(\mathrm{mod}\, m)$ e $\beta \equiv \gamma \,(\mathrm{mod}\, m) \Rightarrow \alpha \equiv \gamma \,(\mathrm{mod}\, m)$ $(transitiva)$

e compatível com as operações de adição e multiplicação.

(4) $\alpha \equiv \beta \,(\mathrm{mod}\, m) \Rightarrow \alpha + \gamma \equiv \beta + y \,(\mathrm{mod}\, m)$

(5) $\alpha \equiv \beta \,(\mathrm{mod}\, m) \Rightarrow \alpha\gamma \equiv \beta y \,(\mathrm{mod}\, m)$

Demonstração. Parte (1)**:** $\alpha - \alpha = 0 = 0 \cdot m$, logo $\alpha \equiv \alpha \,(\mathrm{mod}\, m)$
Parte (2)**:**De fato,

$$\begin{aligned} \alpha &\equiv \beta \,(\mathrm{mod}\, m) \overset{(2.11.1)}{\Rightarrow} \alpha - \beta = qm, \text{ com } q \in \mathbb{Z} \\ &\Rightarrow \beta - \alpha = (-q)\, m, \text{ com } -q \in \mathbb{Z} \\ \overset{(2.11.1)}{\Rightarrow} \beta &\equiv \alpha \,(\mathrm{mod}\, m) \end{aligned}$$

Parte (3)**:**Com efeito,

$$\left.\begin{array}{l} \alpha \equiv \beta \,(\mathrm{mod}\, m) \\ \beta \equiv \gamma \,(\mathrm{mod}\, m) \end{array}\right\} \overset{(2.5.7.(3))}{\Rightarrow} \left.\begin{array}{l} \alpha - \beta = qm, \text{ com } q \in \mathbb{Z} \\ \beta - \gamma = q'm, \text{ com } q' \in \mathbb{Z} \end{array}\right\}$$

$$\left.\begin{array}{l} \alpha = \beta + qm \\ \gamma = \beta + q'm \end{array}\right\} \overset{(2.5.7.(3))}{\Rightarrow}$$

$$\begin{aligned} &\Rightarrow \alpha - \gamma = (\beta + qm) - (\beta + q'm) \\ \overset{(2.4.7.(4))}{\Rightarrow} \alpha - \gamma &= qm - q'm + \beta - \beta \\ \overset{(2.4.1.(1))}{\Rightarrow} \alpha - \gamma &= qm - q'm + \beta - \beta \\ \overset{(2.4.7.(3))}{\Rightarrow} \alpha - \gamma &= (q - q')\, m \\ \overset{(2.11.1)}{\Rightarrow} \alpha &\equiv \gamma \,(\mathrm{mod}\, m) \end{aligned}$$

Como a relação é reflexiva, simétrica e transitiva concluímos que é uma relação de equivalência.

Parte ((4) e (5))**:**Temos que $\alpha - \beta = qm$, com $q \in \mathbb{Z}$, logo $(\alpha + \gamma) - (\beta + \gamma) = qm$ e $\alpha\gamma - \beta\gamma = qm$, donde vem $\alpha + \gamma \equiv \beta + y \,(\mathrm{mod}\, m)$ e $\alpha\gamma \equiv \beta y \,(\mathrm{mod}\, m)$ ■

É imediato que $\alpha \equiv \beta \,(\mathrm{mod}\, m)$ se, e somente se, $\alpha \equiv \beta \,\mathrm{mod}\,(-m)$; portanto, basta considerar as congruências de módulo positivo.

Teorema 2.11.4 *Se* $\alpha \equiv \beta \,(\mathrm{mod}\, m)$ *e se* $\gamma \equiv \delta \,(\mathrm{mod}\, m)$*, então,*

(1) $\alpha + \gamma \equiv \beta + \delta \,(\mathrm{mod}\, m)$

(2) $\alpha\gamma \equiv \beta\delta \,(\mathrm{mod}\, m)$

Demonstração. Parte (1)**:** Por hipótese, temos

$$\left.\begin{array}{l} \alpha \equiv \beta \,(\mathrm{mod}\, m) \overset{(2.11.3.(4))}{\Rightarrow} \alpha + \gamma \equiv \beta + \gamma \,(\mathrm{mod}\, m) \\ \gamma \equiv \delta \,(\mathrm{mod}\, m) \overset{(2.11.3.(4))}{\Rightarrow} \beta + \gamma \equiv \beta + \delta \,(\mathrm{mod}\, m) \end{array}\right\} \overset{(2.11.3.(3))}{\Rightarrow} \alpha + \gamma \equiv \beta + \delta \,(\mathrm{mod}\, m)$$

Parte (2)**:** Por hipótese, temos

$$\left.\begin{array}{l}\alpha \equiv \beta \,(\mathrm{mod}\, m) \overset{(2.11.3.(5))}{\Rightarrow} \alpha\gamma \equiv \beta\gamma \,(\mathrm{mod}\, m) \\ \gamma \equiv \delta \,(\mathrm{mod}\, m) \overset{(2.11.3.(5))}{\Rightarrow} \beta\gamma \equiv \beta\delta \,(\mathrm{mod}\, m)\end{array}\right\} \overset{(2.11.3.(3))}{\Rightarrow} \alpha\gamma \equiv \beta\delta \,(\mathrm{mod}\, m)$$

■

Corolário 2.11.5 *Se* $(\alpha_i)_{1\leq\, i\leq\, n}$ *e* $(\beta_i)_{1\leq\, i\leq n}$ *são duas famílias quaisquer de números inteiros e se* $\alpha_i \equiv \beta_i \,(\mathrm{mod}\, m)$ *para* $i = 1, 2, \cdots, n$*, então*

$$\sum_{i=1}^{n}\alpha_i \equiv \sum_{i=1}^{n}\beta_i \,(\mathrm{mod}\, m) \;\; e \prod_{i=1}^{n}\alpha_i \equiv \prod_{i=1}^{n}\beta_i \,(\mathrm{mod}\, m)$$

Em particular, tem-se o

Corolário 2.11.6 *Se* $\alpha \equiv \beta \,(\mathrm{mod}\, m)$*, então* $\alpha^n \equiv \beta^n \,(\mathrm{mod}\, m)$*, para todo número natural* n*.*

Demonstração. Basta tomar no colorário anterior $\alpha_i = \alpha$ e $\beta_i = \beta$ com $1 \leq i \leq n$. ■

Teorema 2.11.7 *Sejam* $\alpha, \beta, m \in \mathbb{Z}$*. Então* $\alpha \equiv \beta \,(\mathrm{mod}\, m)$ *se, e somente se,* α *e* β *tem o mesmo resto na divisão por* m*.*

Demonstração. ($\Rightarrow$) Se $\alpha \equiv \beta \,(\mathrm{mod}\, m)$, existem $p \in \mathbb{Z}$, tal que $\alpha - \beta = pm$. Pelo algoritmo de Euclides, existem $p_1, r_1, p_2, r_2 \in \mathbb{Z}$, tais que

$$\alpha = p_1 m + r_1 \;\; \text{e} \;\; \beta = p_2 m + r_2$$

donde,

$$\begin{array}{rcl} pm & = & \alpha - \beta \overset{\text{(hipótese)}}{=} (p_1 m + r_1) - (p_2 m + r_2) \\ & & \overset{(2.4.7.(4))}{=} p_1 m + r_1 - p_2 m - r_2 \overset{(2.4.1.(2))}{=} p_1 m - p_2 m + r_1 - r_2 \\ & & \overset{(2.4.7.(3))}{=} (p_1 - p_2)\, m + r_1 - r_2 \\ \Rightarrow & & pm = (p_1 - p_2)\, m + r_1 - r_2 \end{array}$$

A unicidade do Algorítmo de Euclides implica que $r_1 - r_2 = 0$, donde segue que

$$r_1 = r_2$$

($\Leftarrow$) Se $\alpha = p_1 m + r$ e $\beta = p_2 m + r$, vamos ter

$$\begin{aligned} \alpha - \beta &= (p_1 m + r) - (p_2 m + r) \overset{(2.4.7.(4))}{=} p_1 m + r - p_2 m - r \\ &\overset{(2.4.1.(2))}{=} p_1 m - p_2 m + r - r \overset{(2.4.7.(3))}{=} (p_1 - p_2)\, m \\ \Rightarrow\ & m | (\alpha - \beta) \overset{(2.11.1)}{\Rightarrow} \alpha \equiv \beta \,(\mathrm{mod}\, m) \end{aligned}$$

■

Corolário 2.11.8 *Todo inteiro α é congruente módulo m a um e somente um dos inteiros $0, 1, 2, \cdots, m-1$.*

Exemplo 2.11.9 *Determinar o resto da divisão de 37^{13} por 17.*

Temos $37 \equiv 3 \,(\mathrm{mod}\, 17)$, $37^2 \equiv 3^2 \,(\mathrm{mod}\, 17)$, $37^4 \equiv 3^4 \equiv 13 \,(\mathrm{mod}\, 17)$ e $37^8 \equiv 13^2 \equiv 16 \,(\mathrm{mod}\, 17)$, logo,

$$37^{13} \equiv 37^1 37^4 37^8 \equiv 3 \cdot 13 \cdot 16 \equiv 5 \cdot 16 \equiv 80 \equiv 12 \,(\mathrm{mod}\, 17)$$

portanto, o resto da divisão 37^{13} por 17 é igual a 12.

Exemplo 2.11.10 *Mostrar que o número Fermat $F_5 = 2^{\left(2^5\right)} + 1$ é divisível por 641. (Euler)*

Com efeito, temos $2^2 = 4$, $2^4 = 16$, $2^8 = 256$, $2^{16} = 65536 \equiv 154 \,(\mathrm{mod}\, 641)$, logo,

$$2^{\left(2^5\right)} \equiv 2^{32} \equiv \left(2^{16}\right)^2 \equiv 154^2 \equiv 23716 \equiv 640 \,(\mathrm{mod}\, 641)$$

logo,

$$2^{32} + 1 \equiv 641 \equiv 0 \,(\mathrm{mod}\, 641)$$

isto é, $641 | F_5$.

Para todo número inteiro α, colocaremos

$$\overline{\alpha} = \{x \in \mathbb{Z} \,|x \equiv \alpha \,(\mathrm{mod}\, m)\}$$

logo, $\overline{\alpha}$ é a classe de equivalência determinada por α segundo a relação de congruência módulo m; diremos, neste caso, que $\overline{\alpha}$ é a classe equivalência módulo m determinada pelo inteiro α, ou, que $\overline{\alpha}$ é a classe de restos módulo m determinada pelo inteiro α. O conjunto quociente de $\mathbb{Z}$ pela relação de congruência módulo m será indicado por $\mathbb{Z}_m$; portanto,$\mathbb{Z}_m$ é o conjunto de

todas as classes de equivalência módulo m. O corolário acima nos mostra que as classes de restos $\overline{0}, \overline{1}, \overline{2}, \cdots, \overline{(m-1)}$ são distintas duas a duas e, além disso, se $\overline{\alpha}$ é uma classe de restos módulo m, então existe um inteiro r, com $0 \leq r \leq m-1$, tal que $\overline{\alpha} = \overline{r}$; portanto temos

$$\mathbb{Z}_m = \left\{\overline{0}, \overline{1}, \cdots, \overline{(m-1)}\right\}$$

Exemplo 2.11.11 *Para $m = 2$ só temos duas classes de restos módulo 2, $\overline{0}$ e $\overline{1}$; a primeira é formada por todos os inteiros pares e a segunda por todos os inteiros ímpares:*

$$\begin{aligned} \overline{0} &= \{\cdots, -6, -4, -2, 0, 2, 4, 6, \cdots\} \\ \overline{1} &= \{\cdots, -5, -3, -1, 0, 1, 3, 5, \cdots\} \end{aligned}$$

Temos $\overline{0} \cap \overline{1} = \varnothing$, $\overline{0} \cup \overline{1} = \mathbb{Z}$ e $\mathbb{Z}_2 = \{\overline{0}, \overline{1}\}$

Exemplo 2.11.12 *Para $m = 5$ só temos cinco classes de restos módulo 5, $\overline{0}, \overline{1}, \overline{2}, \overline{3}$ e $\overline{4}$, onde*

$$\begin{aligned} \overline{0} &= \{\cdots, -10, -5, 0, 5, 10, \cdots\} \\ \overline{1} &= \{\cdots, -9, -4, 1, 6, 11, \cdots\} \\ \overline{2} &= \{\cdots, -8, -3, 2, 7, 12, \cdots\} \\ \overline{3} &= \{\cdots, -7, -2, 3, 8, 13, \cdots\} \\ \overline{4} &= \{\cdots, -6, -1, 4, 9, 14, \cdots\} \end{aligned}$$

estas classes não tem nenhum elemento em comum e, além disso, sua reunião é o conjunto $\mathbb{Z}$ dos números inteiros.

Capítulo 3

NÚMEROS RACIONAIS

Vamos tratar agora do conjunto dos números racionais. Se α e β são números inteiros, a equação $\alpha \cdot \varkappa = \beta$, com α e β em $\mathbb{Z}$, somente tem solução (em $\mathbb{Z}$) quando $\alpha|\beta$. Para que esta equação tenha sempre solução precisaremos ampliar o conjunto dos números inteiros definindo um novo conjunto - o conjunto dos números racionais. Este novo conjunto numérico deverá conter um subconjunto que possa ser identificado de maneira natural com o conjunto dos números inteiros.

3.1 OS NÚMEROS RACIONAIS

Teorema 3.1.1 *A relação R no conjunto $\mathbb{Z} \times \mathbb{Z}'$ definida por*

$$(\alpha, \beta) R (\gamma, \delta) \Leftrightarrow \alpha \cdot \delta = \beta \cdot \gamma$$

é uma relação de equivalência

Demonstração. Parte (1)**:** $\forall\ (\alpha, \beta) \in \mathbb{Z} \times \mathbb{Z}'$, tem-se $(\alpha, \beta) R (\alpha, \beta)$, pois $\alpha \cdot \beta = \beta \cdot \alpha$

Parte (2) Quaisquer que sejam (α, β) e (γ, δ) em $\mathbb{Z} \times \mathbb{Z}'$, se $(\alpha, \beta) R (\gamma, \delta)$, então, $(\gamma, \delta) R (\alpha, \beta)$, pois

$$\begin{aligned} (\alpha, \beta) R (\gamma, \delta) \overset{(3.1.1.(1))}{\Rightarrow} \alpha \cdot \delta &= \beta \cdot \gamma \Rightarrow \beta \cdot \gamma = \alpha \cdot \delta \\ \overset{(2.4.7.(2))}{\Rightarrow} \gamma \cdot \beta &= \delta \cdot \alpha \overset{(3.1.1.(1))}{\Rightarrow} (\gamma, \delta) R (\alpha, \beta) \end{aligned}$$

Parte (3) Quaisquer que sejam $(\alpha, \beta), (\gamma, \delta)$ e (ε, ζ) em $\mathbb{Z} \times \mathbb{Z}'$, se $(\alpha, \beta) R (\gamma, \delta)$ e se $(\gamma, \delta) R (\varepsilon, \zeta)$, então, $(\alpha, \beta) R (\varepsilon, \zeta)$

Se $(\alpha,\beta)\,R\,(\gamma,\delta)$ e $(\gamma,\delta)\,R\,(\varepsilon,\zeta)$, então $\alpha\cdot\delta=\beta\cdot\gamma$ e $\gamma\cdot\zeta=\delta\cdot\varepsilon$. Assim

$$\begin{aligned}
(\alpha\cdot\delta)\cdot(\gamma\cdot\zeta) &= (\beta\cdot\gamma)\cdot(\delta\cdot\varepsilon)\\
\overset{(2.4.7.(1))}{\Rightarrow}\ \alpha\cdot(\delta\cdot\gamma)\cdot\zeta &= \beta\cdot(\gamma\cdot\delta)\cdot\varepsilon\\
\overset{(2.4.7.(2))}{\Rightarrow}\ \alpha\cdot\zeta\cdot(\delta\cdot\gamma) &= \beta\cdot\varepsilon\cdot(\gamma\cdot\delta)\\
\overset{(2.4.7.(2))}{\Rightarrow}\ \alpha\cdot\zeta\cdot(\delta\cdot\gamma) &= \beta\cdot\varepsilon\cdot(\delta\cdot\gamma)\\
\overset{(2.4.8.(2))}{\Rightarrow}\ \alpha\cdot\zeta &= \beta\cdot\varepsilon\ \overset{(3.1.1.(1))}{\Rightarrow}\ (\alpha,\beta)\,R\,(\varepsilon,\zeta)
\end{aligned}$$

■

Definição 3.1.2 *O conjunto quociente $\mathbb{Q}=(\mathbb{Z}\times\mathbb{Z}')\diagup R$ é chamado de* ***o conjunto dos números racionais*** *e seus elementos de números racionais.*

Observação 3.1.3 *Representaremos os números racionais pelos símbolos* 0,1 *e pelas letras latinas minúsculas;*

$$r,s,t,\cdots$$

Exemplo 3.1.4 *O conjunto dos números racionais é formado por classes de equivalência de pares de números inteiros, isto é*

$$\mathbb{Q}=\left\{\overline{(\alpha,\beta)}\mid\alpha\in\mathbb{Z},\beta\in\mathbb{Z}'\right\}$$

Exemplo 3.1.5 *O conjunto*

$$0=\{(\theta,\beta)\mid\beta\in\mathbb{Z}'\}$$

é um elemento de $\mathbb{Q}$, pois,

$$\begin{aligned}
0 &= \{(\theta,\beta)\mid\beta\in\mathbb{Z}'\}\\
&= \{(\alpha,\beta)\in\mathbb{Z}\times\mathbb{Z}':\alpha=\theta\}\\
&= \{(\alpha,\beta)\in\mathbb{Z}\times\mathbb{Z}':\alpha\cdot\beta=\beta\cdot\theta,\ \beta\in\mathbb{Z}'\}\\
&= \{(\alpha,\beta)\in\mathbb{Z}\times\mathbb{Z}':(\alpha,\beta)\,R\,(\theta,\beta)\}\\
&= \overline{(\theta,\beta)}\in\mathbb{Z}\times\mathbb{Z}'\diagup R=\mathbb{Q}
\end{aligned}$$

Exemplo 3.1.6 *Também, o conjunto*

$$1=\{(\alpha,\alpha)\mid\alpha\in\mathbb{Z}'\}$$

é um elemento de $\mathbb{Q}$.

De fato,

$$\begin{aligned} 1 &= \{(\alpha,\alpha) \mid \alpha \in \mathbb{Z}'\} \\ &= \{(\gamma,\delta) \in \mathbb{Z}\times\mathbb{Z}' : \gamma = \delta\} \\ &= \{(\gamma,\delta) \in \mathbb{Z}\times\mathbb{Z}' : \gamma\alpha = \delta\alpha,\ \alpha \in \mathbb{Z}'\} \\ &= \{(\gamma,\delta) \in \mathbb{Z}\times\mathbb{Z}' : (\gamma,\delta)\, R\, (\alpha,\alpha)\} \\ &= \overline{(\alpha,\alpha)} \in (\mathbb{Z}\times\mathbb{Z}')\diagup R = \mathbb{Q} \end{aligned}$$

3.2 ADIÇÃO DE NÚMEROS RACIONAIS

Definição 3.2.1 *Dados os números racionais r e s, se $(\alpha,\beta) \in r$ e $(\gamma,\delta) \in s$, definimos* ***a soma*** *de r e s por*

$$r + s = \overline{(\alpha,\beta)} + \overline{(\gamma,\delta)} = \overline{(\alpha\cdot\delta + \beta\cdot\gamma, \beta\cdot\delta)}$$

Observação 3.2.2 *A definição de soma de números racionais não depende dos representantes (α,β) e (γ,δ) utilizados.*

De fato, se $(\alpha',\beta')\, R\, (\alpha,\beta)$ e $(\gamma',\delta')\, R\, (\gamma,\delta)$ vamos ter $\alpha'\cdot\beta = \beta'\cdot\alpha$ e $\gamma'\cdot\delta = \delta'\cdot\gamma$ e consequentemente

$$\begin{aligned} (\alpha\cdot\delta + \beta\cdot\gamma)\cdot(\beta'\cdot\delta') &= \alpha\cdot\delta\cdot\beta'\cdot\delta' + \beta\cdot\gamma\cdot\beta'\cdot\delta' \\ &= \alpha'\cdot\delta\cdot\beta\cdot\delta' + \beta\cdot\gamma'\cdot\beta'\cdot\delta \\ &= (\alpha'\cdot\delta' + \gamma'\cdot\beta')\cdot(\beta\cdot\delta) \end{aligned}$$

ou seja

$$(\alpha\cdot\delta + \beta\cdot\gamma, \beta\cdot\delta)\, R\, (\alpha'\cdot\delta' + \beta'\cdot\gamma', \beta'\cdot\delta')$$

Teorema 3.2.3 *Para quaisquer que sejam os números racionais r, s e t, temos*

(1) $r + s = s + r$ (*comutatividade*)

(2) $r + (s + t) = (r + s) + t$ (*associatividade*)

Demonstração. Parte (1)**:** Consideremos $r = \overline{(\alpha,\beta)}$ e $s = \overline{(\gamma,\delta)}$, com α e $\gamma \in \mathbb{Z}$ e β e $\delta \in \mathbb{Z}'$; temos:

$$\begin{aligned} r + s &\overset{(hipótese)}{=} \overline{(\alpha,\beta)} + \overline{(\gamma,\delta)} \overset{(3.2.1)}{=} \overline{(\alpha\cdot\delta + \beta\cdot\gamma, \beta\cdot\delta)} \\ &\overset{(2.4.1.(2))}{=} \overline{(\beta\cdot\gamma + \alpha\cdot\delta, \beta\cdot\delta)} \overset{(2.4.7.(2))}{=} \overline{(\gamma\cdot\beta + \delta\cdot\alpha, \delta\cdot\beta)} \\ &\overset{(3.2.1)}{=} \overline{(\gamma,\delta)} + \overline{(\alpha,\beta)} \overset{(hipótese)}{=} s + r \end{aligned}$$

Parte (2)**:** Consideremos $r = \overline{(\alpha, \beta)}, s = \overline{(\gamma, \delta)}$ e $t = \overline{(\varepsilon, \zeta)}$, com α, γ e $\varepsilon \in \mathbb{Z}$ e β, δ e $\zeta \in \mathbb{Z}'$, temos:

$$
\begin{aligned}
r + (s + t) &\overset{(hipótese)}{=} \overline{(\alpha, \beta)} + \left[\overline{(\gamma, \delta)} + \overline{(\varepsilon, \zeta)}\right] \\
&\overset{(3.2.1)}{=} \overline{(\alpha, \beta)} + \overline{(\gamma \cdot \zeta + \delta \cdot \varepsilon, \delta \cdot \zeta)} \\
&\overset{(3.2.1)}{=} \overline{(\alpha \cdot \delta \cdot \zeta + \beta \cdot (\gamma \cdot \zeta + \delta \cdot \varepsilon), \beta \cdot \delta \cdot \zeta)} \\
&\overset{(2.4.7.(4))}{=} \overline{(\alpha \cdot \delta \cdot \zeta + \beta \cdot \gamma \cdot \zeta + \beta \cdot \delta \cdot \varepsilon, \beta \cdot \delta \cdot \zeta)} \\
&\overset{(2.4.7.(3))}{=} \overline{((\alpha \cdot \delta + \beta \cdot \gamma) \cdot \zeta + \beta \cdot \delta \cdot \varepsilon, \beta \cdot \delta \cdot \zeta)} \\
&\overset{(3.2.1)}{=} \overline{(\alpha \cdot \delta + \beta \cdot \gamma, \beta \cdot \delta)} + \overline{(\varepsilon, \zeta)} \\
&\overset{(3.2.1)}{=} \left[\overline{(\alpha, \beta)} + \overline{(\gamma, \delta)}\right] + \overline{(\varepsilon, \zeta)} \\
&\overset{(hipótese)}{=} (r + s) + t
\end{aligned}
$$

■

Teorema 3.2.4 *Para todo $r \in \mathbb{Q}$, existe um único elemento $0 \in \mathbb{Q}$ e um único elemento $r^\circ \in \mathbb{Q}$, tais que*

(1) $r + 0 = r$

e

(2) $r + r^\circ = 0$

Demonstração. Parte (1) . **Existência:** Considerando o elemento

$$0 = \{(\theta, \alpha) \mid \alpha \in \mathbb{Z}'\}$$

e $r = \overline{(\alpha, \beta)}$, temos

$$r + 0 = \overline{(\alpha, \beta)} + \overline{(\theta, \alpha)} \overset{(3.2.1)}{=} \overline{(\alpha \cdot \alpha + \beta \cdot \theta, \beta \cdot \alpha)} \overset{(2.4.7.(5))}{=} \overline{(\alpha \cdot \alpha, \beta \cdot \alpha)} = \overline{(\alpha, \beta)} = r$$

portanto $r + 0 = r$.

Unicidade: Suponhamos que 0_1 e 0_2 são elementos de $\mathbb{Q}$ que satisfazem (3.2.4. (1)). Então

$$0_1 \overset{(3.2.4.(1))}{=} 0_1 + 0_2 \overset{(3.2.3.(1))}{=} 0_2 + 0_1 \overset{(3.2.4.(1))}{=} 0_2$$

Parte (2) . **Existência:** Consideremos o elemento $0 = \overline{(\theta, \alpha)}$, $r = \overline{(\alpha, \beta)}$ e $r^\circ = \overline{(-\alpha, \beta)}$, temos:

$$\begin{aligned} r + r^\circ &\overset{(hipótese)}{=} \overline{(\alpha, \beta)} + \overline{(-\alpha, \beta)} \\ &\overset{(3.2.1)}{=} \overline{(\alpha \cdot \beta + \beta \cdot (-\alpha), \beta \cdot \beta)} \overset{(2.4.8.(3))}{=} \overline{(\alpha \cdot \beta - \beta \cdot \alpha, \beta \cdot \beta)} \\ &\overset{(2.4.7.(2))}{=} \overline{(\beta \cdot \alpha - \beta \cdot \alpha, \beta \cdot \beta)} \overset{(2.4.3)}{=} \overline{(\theta, \beta \cdot \beta)} \\ &\overset{(3.1.5.(1))}{=} 0 \end{aligned}$$

portanto $r + r^\circ = 0$.

Unicidade: Suponhamos que r_1° e r_2° são elementos de $\mathbb{Q}$ que satisfazem (3.2.4. (2)). Então

$$\begin{aligned} r_1^\circ &\overset{(3.2.4.(1))}{=} r_1^\circ + 0 \overset{(3.2.4.(2))}{=} r_1^\circ + [r + (r_2^\circ)] \overset{(3.2.3.(2))}{=} (r_1^\circ + r) + (r_2^\circ) \\ &\overset{(3.2.3.(1))}{=} [r + (r_1^\circ)] + (r_2^\circ) \overset{(3.2.4.(2))}{=} 0 + (r_2^\circ) \overset{(3.2.3.(1))}{=} (r_2^\circ) + 0 \\ &\overset{(3.2.4.(1))}{=} r_2^\circ \end{aligned}$$

portanto $r_1^\circ = r_2^\circ$. ■

Notação 3.2.5 *O elemento r° que aparece em* (3.2.4. (2)) *é chamado simétrico ou oposto de r, e será denotado por $-r$. Assim, a soma $r+(-s)$ será indicada por $r - s$.*

3.3 MULTIPLICAÇÃO DE NÚMEROS RACIONAIS

Definição 3.3.1 *Dados os números racionais r e s, se $(\alpha, \beta) \in r$ e $(\gamma, \delta) \in s$, definimos* ***o produto*** *de r e s por*

$$r \times s = \overline{(\alpha, \beta)} \times \overline{(\gamma, \delta)} = \overline{(\alpha \cdot \gamma, \beta \cdot \delta)}$$

Observação 3.3.2 *A definição de produto de números racionais não depende dos representantes (α, β) e (γ, δ), usados na definição.*

De fato, se $(\alpha', \beta') R (\alpha, \beta)$ e $(\gamma', \delta') R (\gamma, \delta)$ vamos ter $\alpha' \cdot \beta = \beta' \cdot \alpha$ e $\gamma' \cdot \delta = \delta' \cdot \gamma$ e consequentemente

$$\alpha \cdot \gamma \cdot \beta' \cdot \delta' = (\alpha \cdot \beta') \cdot (\delta' \cdot \gamma) = (\alpha' \cdot \beta) \cdot (\gamma' \cdot \delta) = \beta \cdot \delta \cdot \alpha' \cdot \gamma'$$

ou seja

$$(\alpha \cdot \gamma, \beta \cdot \delta) R (\alpha' \cdot \gamma', \beta' \cdot \delta')$$

Teorema 3.3.3 *Para quaisquer que sejam r, s e t em $\mathbb{Q}$, temos*

(1) $r \times s = s \times r$ (*comutatividade*)

(2) $r \times (s \times t) = (r \times s) \times t$ (*associatividade*)

(3) $r \times (s + t) = r \times s + r \times t$ (*distributividade*)

(4) $r \times 0 = 0$

Demonstração. Parte (1)**:**Consideremos $r = \overline{(\alpha, \beta)}$ e $s = \overline{(\gamma, \delta)}$, com α e $\gamma \in \mathbb{Z}$ e β e $\delta \in \mathbb{Z}'$; temos:

$$r \times s = \overline{(\alpha, \beta)} \times \overline{(\gamma, \delta)} \overset{(3.3.1)}{=} \overline{(\alpha \cdot \gamma, \beta \cdot \delta)} \overset{(2.4.7.(2))}{=} \overline{(\gamma \cdot \alpha, \delta \cdot \beta)} \overset{(3.3.1)}{=} \overline{(\gamma, \delta)} \times \overline{(\alpha, \beta)} = s \times r$$

Parte (2)**:** Consideremos $r = \overline{(\alpha, \beta)}, s = \overline{(\gamma, \delta)}$ e $t = \overline{(\varepsilon, \zeta)}$, com α, γ e ε $\in \mathbb{Z}$ e β, δ e $\zeta \in \mathbb{Z}'$, temos:

$$\begin{aligned}
r \times (s \times t) &\overset{(hipótese)}{=} \overline{(\alpha, \beta)} \times \left[\overline{(\gamma, \delta)} \times \overline{(\varepsilon, \zeta)}\right] \\
&\overset{(3.3.1)}{=} \overline{(\alpha, \beta)} \times \overline{(\gamma \cdot \varepsilon, \delta \cdot \zeta)} \\
&\overset{(3.3.1)}{=} \overline{(\alpha \cdot (\gamma \cdot \varepsilon), \beta \cdot (\delta \cdot \zeta))} \\
&\overset{(2.4.7.1)}{=} \overline{((\alpha \cdot \gamma) \cdot \varepsilon, (\beta \cdot \delta) \cdot \zeta)} \\
&\overset{(3.3.1)}{=} \overline{(\alpha \cdot \gamma, \beta \cdot \delta)} \times \overline{(\varepsilon, \zeta)} \\
&\overset{(3.3.1)}{=} \left[\overline{(\alpha, \beta)} \times \overline{(\gamma, \delta)}\right] \times \overline{(\varepsilon, \zeta)} \\
&\overset{(hipótese)}{=} (r \times s) \times t
\end{aligned}$$

Parte (3)**:** Consideremos $r = \overline{(\alpha, \beta)}, s = \overline{(\gamma, \delta)}$ e $t = \overline{(\varepsilon, \zeta)}$, com α, γ e ε $\in \mathbb{Z}$ e β, δ e $\zeta \in \mathbb{Z}'$, temos:

$$\begin{aligned}
r \times (s + t) &\overset{(hipótese)}{=} \overline{(\alpha, \beta)} \times \left[\overline{(\gamma, \delta)} + \overline{(\varepsilon, \zeta)}\right] \\
&\overset{(3.2.1)}{=} \overline{(\alpha, \beta)} \times \overline{(\gamma \cdot \zeta + \delta \cdot \varepsilon, \delta \cdot \zeta)} \\
&\overset{(3.2.1)}{=} \overline{(\alpha \cdot (\gamma \cdot \zeta + \delta \cdot \varepsilon), \beta \cdot \delta \cdot \zeta)} \\
&\overset{(2.4.7.(4))}{=} \overline{(\alpha \cdot \gamma \cdot \zeta + \alpha \cdot \delta \cdot \varepsilon, \beta \cdot \delta \cdot \zeta)} \\
&= \overline{(\alpha \cdot \gamma \cdot \beta \cdot \zeta + \beta \cdot \delta \cdot \alpha \cdot \varepsilon, \beta \cdot \delta \cdot \beta \cdot \zeta)} \\
&\overset{(3.2.1)}{=} \overline{(\alpha \cdot \gamma, \beta \cdot \delta)} + \overline{(\alpha \cdot \varepsilon, \beta \cdot \zeta)} \\
&\overset{(3.3.1)}{=} \overline{(\alpha, \beta)} \times \overline{(\gamma, \delta)} + \overline{(\alpha, \beta)} \times \overline{(\varepsilon, \zeta)} \\
&\overset{(hipótese)}{=} r \times s + r \times t
\end{aligned}$$

Parte (4)**:**Consideremos $r = \overline{(\alpha, \beta)}$ e $0 = \overline{(\theta, \alpha)}$, devemos mostrar que

$$\overline{(\alpha, \beta)} \times \overline{(\theta, \alpha)} = \overline{(\theta, \alpha)}$$

basta mostrarmos que,

$$(\alpha \cdot \theta, \beta \cdot \alpha) \, R \, (\theta, \alpha)$$

o que é verdade, pois se:

$$(\alpha \cdot \theta, \beta \cdot \alpha) \, R \, (\theta, \alpha) \overset{(3.1.1.(1))}{\Rightarrow} \alpha \cdot \theta \cdot \alpha = \beta \cdot \alpha \cdot \theta \overset{(2.4.7.(5))}{\Rightarrow} \theta = \theta$$

portanto, $\overline{(\alpha, \beta)} \times \overline{(\theta, \alpha)} = \overline{(\theta, \alpha)}$, ou seja, $r \times 0 = 0$ ■

Teorema 3.3.4 *Existe um único elemento* 1 *em* $\mathbb{Q}$*, tal que*

(1) $1 \times r = r$

para todo r em $\mathbb{Q}$, e se $r \neq 0$, existe um único elemento $r^{\Diamond}$em $\mathbb{Q}$ tal que

(2) $r \times r^{\Diamond} = 1$

Demonstração. Parte (1). **Existência:** Consideremos o elemento

$$1 = \{(\alpha, \alpha) \mid \alpha \in \mathbb{Z}'\}$$

Se $r = \overline{(\alpha, \beta)}$,temos

$$1 \times r \overset{(hipótese)}{=} \overline{(\alpha, \alpha)} \times \overline{(\alpha, \beta)} \overset{(3.3.1)}{=} \overline{(\alpha \cdot \alpha, \alpha \cdot \beta)} = \overline{(\alpha, \beta)} \overset{(hipótese)}{=} r$$

portanto $1 \times r = r$.

Unicidade: Suponhamos que $1^{>}$ e $1^{>>}$ são elementos de $\mathbb{Q}$ que satisfazem (3.3.4. (1)). Então

$$1^{>} \overset{(hipótese)}{=} 1^{>} \cdot 1^{>>} \overset{(3.3.3.(1))}{=} 1^{>>} \cdot 1^{>} \overset{(hipótese)}{=} 1^{>>}$$

Parte (2). **Existência:** Consideremos o elemento $r = \overline{(\alpha, \beta)} \neq 0$ e $r^{\Diamond} = \overline{(\beta, \alpha)}$, temos:

$$r \times r^{\Diamond} = \overline{(\alpha, \beta)} \times \overline{(\beta, \alpha)} \overset{(3.3.1)}{=} \overline{(\alpha \cdot \beta, \beta \cdot \alpha)} \overset{(2.4.7.(2))}{=} \overline{(\alpha \cdot \beta, \alpha \cdot \beta)} = \overline{(\alpha, \alpha)} \overset{(3.1.6)}{=} 1$$

portanto $r \times r^{\Diamond} = 1$.

Unicidade: Suponhamos que $r_1^{\lozenge}$ e $r_2^{\lozenge}$ são elementos de $\mathbb{Q}$ que satisfazem (3.3.4. (2)). Então

$$\begin{aligned} r_1^{\lozenge} &\overset{(3.3.4.(1))}{=} r_1^{\lozenge} \times 1 \\ &\overset{(hipótese)}{=} r_1^{\lozenge} \times \left(r \times r_2^{\lozenge}\right) \overset{(3.3.3.(2))}{=} \left(r_1^{\lozenge} \times r\right) \times r_2^{\lozenge} \\ &\overset{(3.3.3.(1))}{=} \left(r \times r_1^{\lozenge}\right) \times r_2^{\lozenge} \overset{(hipótese)}{=} 1 \times r_2^{\lozenge} \\ &= r_2^{\lozenge} \end{aligned}$$

■

Notação 3.3.5 *O elemento $r^{\lozenge}$ que aparece em* (3.3.4. (2)) *é chamado inverso de r, e será denotado por r^{-1}.*

Teorema 3.3.6 *(Regra de Sinais). Para todo r e s em $\mathbb{Q}$, temos*

(1) $(-r) \times s = r \times (-s) = -(r \times s)$

(2) $-(-r) = r$

(3) $(-r) \times (-s) = r \times s$

Demonstração. Parte (1)**:**Primeiro caso: Vamos mostrar que

$$(-r) \times s = -(r \times s).$$

Temos

$$(r \times s) + ((-r) \times s) \overset{(3.3.3.(1))}{=} s \times r + s \times (-r) \overset{(3.3.3.(3))}{=} s \times (r + (-r)) \overset{(3.2.4.(2))}{=} s \times 0 \overset{(3.3.3.(4))}{=} 0$$

Mas, por (3.2.4. (2)) existe um único $t \in \mathbb{Q}$ tal que $(r \times s) + t = 0$, que é o elemento denotado por $-(r \times s)$. Como $(-r) \times s$ também tem essa propriedade, segue que $(-r) \times s = -(r \times s)$.

Segundo caso: Vamos mostrar que

$$r \times (-s) = -(r \times s).$$

Temos

$$(r \times s) + (r \times (-s)) \overset{(3.3.3.(3))}{=} r \times (s + (-s)) \overset{(3.2.4.(2))}{=} r \times 0 \overset{(3.3.3.(4))}{=} 0$$

Mas, por (3.2.4. (2)) existe um único $t \in \mathbb{Q}$ tal que $r \times s + t = 0$, que é o elemento denotado por $-(r \times s)$. Como $r \times (-s)$ também tem essa propriedade, segue que $r \times (-s) = -(r \times s)$.

Parte (2)**:** Temos,

$$r = -(-r)$$

pois,

$$r + (-r) = 0 \overset{(3.2.3.(1))}{\Rightarrow} (-r) + r = 0 \overset{(3.2.4.(2))}{\Rightarrow} r = -(-r)$$

Parte (3)**:** Com efeito,

$$(-r) \times (-s) \overset{(3.3.6.(1))}{=} -(r \times (-s)) \overset{(3.3.6.(1))}{=} -(-(r \times s)) \overset{(3.3.6.(2))}{=} r \times s$$

■

Teorema 3.3.7 *Para todo r em $\mathbb{Q}$, com $r \neq 0$, temos*

$$\left(r^{-1}\right)^{-1} = r$$

Demonstração. Se $r \neq 0$ é um elemento qualquer de $\mathbb{Q}$, temos:

$$r \times r^{-1} = 1 \overset{(3.3.3.(1))}{\Rightarrow} r^{-1} \times r = 1 \overset{(3.3.4.(2))}{\Rightarrow} r = \left(r^{-1}\right)^{-1}$$

■

3.4 RELAÇÃO DE ORDEM EM $\mathbb{Q}$

Definição 3.4.1 *Seja $r \in \mathbb{Q}$. Diremos que r* ***é maior que*** *0, e escrevemos $r > 0$, se existir $(\alpha, \beta) \in r$ tal que*

$$\alpha \cdot \beta > \theta$$

Diremos que r **é menor que** 0, e escrevemos $r < 0$, se existir $(\alpha, \beta) \in r$ tal que $\alpha \cdot \beta < \theta$.

Observação 3.4.2 *A relação $<$ ou $>$ em $\mathbb{Q}$ não depende dos representantes usados na definição.*

Definição 3.4.3 *Dados r e s em $\mathbb{Q}$, diremos que r* ***é menor que ou igual à*** *s e escrevemos $r \leq s$ se $r < s$ ou $r = s$. Analogamente, definimos a relação $r \geq s$.*

Teorema 3.4.4 *(Lei da Tricotomia). Se $r \in \mathbb{Q}$, uma e apenas uma das seguintes afirmações é verdadeiras:*

(1) $r > 0$

ou

(2) $r = 0$

ou

(3) $r < 0$

Demonstração. Se $r = \overline{(\alpha, \beta)}$ então $\alpha \cdot \beta \in \mathbb{Z}$ e pela Lei da tricotomia para os números inteiros temos $\alpha \cdot \beta > \theta$ ou $\alpha \cdot \beta = \theta$ ou $\alpha \cdot \beta < \theta$. ■

Notação 3.4.5 *Denotaremos por $\mathbb{Q}_+$ o conjunto dos elementos $r \in \mathbb{Q}$ tais que $r > 0$.*

Estes elementos serão chamados de **positivos**. Se $r \notin \mathbb{Q}_+$ e $r \neq 0$, diremos que r é **negativo**.

Teorema 3.4.6 *Se r e s são elementos de $\mathbb{Q}_+$, então:*

(1) $r + s \in \mathbb{Q}_+$

(2) $r \times s \in \mathbb{Q}_+$

(3) $r^{-1} \in \mathbb{Q}_+$

Demonstração. Parte (1)**:** Consideremos $r = \overline{(\alpha, \beta)}$ e $s = \overline{(\gamma, \delta)}$, com α e $\gamma \in \mathbb{Z}$ e β e $\delta \in \mathbb{Z}'$.Como, r e s são elementos de $\mathbb{Q}_+$, temos:

$$\left.\begin{array}{c} r > 0 \overset{(3.4.1)}{\Rightarrow} \alpha \cdot \beta > \theta \\ s > 0 \overset{(3.4.1)}{\Rightarrow} \gamma \cdot \delta > \theta \\ \delta \cdot \delta > \theta \\ \beta \cdot \beta > \theta \end{array}\right\}$$

$$\begin{array}{rcl} \overset{(2.5.5.(1))}{\Rightarrow} \left.\begin{array}{c} (\alpha \cdot \beta) \cdot (\delta \cdot \delta) > \theta \\ (\gamma \cdot \delta) \cdot (\beta \cdot \beta) > \theta \end{array}\right\} & \Rightarrow & (\alpha \cdot \beta) \cdot (\delta \cdot \delta) + (\gamma \cdot \delta) \cdot (\beta \cdot \beta) > \theta \\ \overset{(2.4.7.(2))}{\Rightarrow} \alpha \cdot \delta \cdot \beta \cdot \delta + \beta \cdot \gamma \cdot \beta \cdot \delta & > & \theta \overset{(2.4.7.(3))}{\Rightarrow} (\alpha \cdot \delta + \beta \cdot \gamma) \cdot \beta \cdot \delta > \theta \\ \overset{(3.4.1)}{\Rightarrow} \overline{(\alpha \cdot \delta + \beta \cdot \gamma, \beta \cdot \delta)} & > & 0 \overset{(3.2.1)}{\Rightarrow} \overline{(\alpha, \beta)} + \overline{(\gamma, \delta)} > 0 \\ \overset{(\text{definição})}{\Rightarrow} r + s & > & 0 \end{array}$$

Parte (2)**:** Consideremos $r = \overline{(\alpha, \beta)}$ e $s = \overline{(\gamma, \delta)}$, com α e $\gamma \in \mathbb{Z}$ e β e $\delta \in \mathbb{Z}'$.Como, r e s são elementos de $\mathbb{Q}_+$, temos:

$$\left.\begin{array}{l} r > 0 \overset{(3.4.1)}{\Rightarrow} \alpha \cdot \beta > \theta \\ s > 0 \overset{(3.4.1)}{\Rightarrow} \gamma \cdot \delta > \theta \end{array}\right\} \overset{(2.5.5.(1))}{\Rightarrow} \alpha \cdot \beta \cdot \gamma \cdot \delta > \theta$$

$$\overset{(2.4.7.(2))}{\Rightarrow} \alpha \cdot \gamma \cdot \beta \cdot \delta > \theta$$

$$\overset{(3.4.1)}{\Rightarrow} \overline{(\alpha \cdot \gamma, \beta \cdot \delta)} > 0$$

$$\overset{(3.3.1)}{\Rightarrow} \overline{(\alpha, \beta)} \times \overline{(\gamma, \delta)} > 0$$

$$\overset{(\text{hip.})}{\Rightarrow} r \times s > 0$$

Parte (3)**:**Consideremos $r = \overline{(\alpha, \beta)}$ e $r^{-1} = \overline{(\beta, \alpha)}$, com $\alpha \in \mathbb{Z}$ e $\beta \in \mathbb{Z}'$.Como, r é elemento de $\mathbb{Q}_+$, temos:

$$r > 0 \overset{(3.4.1)}{\Rightarrow} \alpha \cdot \beta > \theta \overset{(2.4.7.(2))}{\Rightarrow} \beta \cdot \alpha > \theta \overset{(3.4.1)}{\Rightarrow} \overline{(\beta, \alpha)} > 0 \overset{(\text{def.})}{\Rightarrow} r^{-1} > 0$$

■

Definição 3.4.7 *Dados r e s em $\mathbb{Q}$, diremos que r* ***é maior que*** *s, e escrevemos $r > s$, ou que s* ***é menor que*** *r, e escrevemos $s < r$, se $r - s > 0$.*

Teorema 3.4.8 *Sejam r, s e t números racionais. Então:*

(1) $r < s$ ou $r = s$ ou $r > s$

(2) $r < 0 \Leftrightarrow -r > 0$

(3) $r < 0$ e $s < 0 \Rightarrow r \times s > 0$

(4) $r > 0$ e $s < 0 \Rightarrow r \times s < 0$

(5) $r < 0$ e $s < 0 \Rightarrow r + s < 0$

(6) $r < s$ e $s < t \Rightarrow r < t$

(7) $r < s \Leftrightarrow r + t < s + t$

(8) $r < s$ e $t < 0 \Rightarrow r \times t > s \times t$

Demonstração. Parte (1)**:** Se r e s são números racionais, temos

$$s + (-r) \in \mathbb{Q}$$

Logo, pela Lei da Tricotomia

$$\begin{array}{rcl} s+(-r) & > & 0 \Rightarrow s - r > 0 \Rightarrow s > r \\ s+(-r) & = & 0 \Rightarrow s - r = 0 \Rightarrow s = r \\ s+(-r) & < & 0 \Rightarrow s - r < 0 \Rightarrow s < r \end{array}$$

Parte (2)**:** Seja $r = \overline{(\alpha, \beta)}$ um número racional, com $\alpha \in \mathbb{Z}$ e $\beta \in \mathbb{Z}'$. Observemos que

$$\begin{array}{rcl} r & < & 0 \overset{\text{(hipótese)}}{\Leftrightarrow} \overline{(\alpha,\beta)} < 0 \overset{(3.4.1)}{\Leftrightarrow} \alpha \cdot \beta < \theta \\ \overset{(2.5.5.(4))}{\Leftrightarrow} -(\alpha \cdot \beta) & > & \theta \overset{(2.4.8.(3))}{\Leftrightarrow} (-\alpha) \cdot \beta > \theta \\ & \Leftrightarrow & \overline{(-\alpha,\beta)} > 0 \overset{(hipótese)}{\Leftrightarrow} -r > 0 \end{array}$$

Parte (3)**:** Sejam r e s números racionais, onde

$$\left.\begin{array}{l} r < 0 \overset{(3.4.8.(2))}{\Rightarrow} -r > 0 \\ s < 0 \overset{(3.4.8.(2))}{\Rightarrow} -s > 0 \end{array}\right\} \overset{(3.4.6.(2))}{\Rightarrow} (-r) \times (-s) > 0 \overset{(3.3.6.(3))}{\Rightarrow} r \times s > 0$$

Parte (4)**:** Sejam r e s números racionais.Temos

$$\begin{array}{rcl} \left.\begin{array}{c} r > 0 \\ s < 0 \overset{(3.4.8.(2))}{\Rightarrow} -s > 0 \end{array}\right\} \overset{(3.4.6.(2))}{\Rightarrow} r \times (-s) & > & 0 \\ \overset{(3.3.6.(1))}{\Rightarrow} -(r \times s) & > & 0 \\ \overset{(3.4.8.(2))}{\Leftrightarrow} r \times s & < & 0 \end{array}$$

Parte (5)**:** Consideremos $r = \overline{(\alpha, \beta)}$ e $s = \overline{(\gamma, \delta)}$, com α e $\gamma \in \mathbb{Z}$ e β e $\delta \in \mathbb{Z}'$.Por hipótese, temos:

$$\left.\begin{array}{c} r < 0 \overset{(3.4.1)}{\Rightarrow} \alpha \cdot \beta < \theta \\ s < 0 \overset{(3.4.1)}{\Rightarrow} \gamma \cdot \delta < \theta \\ \delta \cdot \delta > \theta \\ \beta \cdot \beta > \theta \end{array}\right\} \overset{(2.5.5.(3))}{\Rightarrow} \left.\begin{array}{l} (\alpha \cdot \beta) \cdot (\delta \cdot \delta) < \theta \\ (\gamma \cdot \delta) \cdot (\beta \cdot \beta) < \theta \end{array}\right\}$$

$$\begin{array}{rcl} \Rightarrow \alpha \cdot \delta \cdot \beta \cdot \delta + \beta \cdot \gamma \cdot \beta \cdot \delta & < & \theta \overset{(2.4.7.(3))}{\Rightarrow} (\alpha \cdot \delta + \beta \cdot \gamma) \cdot (\beta \cdot \delta) < \theta \\ \overset{(3.4.1)}{\Rightarrow} \overline{(\alpha \cdot \delta + \beta \cdot \gamma, \beta \cdot \delta)} & < & 0 \overset{(3.4.1)}{\Rightarrow} \overline{(\alpha,\beta)} + \overline{(\gamma,\delta)} < 0 \overset{(hipótese)}{\Rightarrow} r + s < 0 \end{array}$$

Parte (6)**:** Sejam r, s e t números racionais, onde

$$\left.\begin{array}{l} r<s \overset{(3.4.7)}{\Rightarrow} s-r>0 \\ s<t \overset{(3.4.7)}{\Rightarrow} t-s>0 \end{array}\right\} \overset{(3.4.6.(1))}{\Rightarrow} (t-s)+(s-r) > 0$$

$$\overset{(3.2.3.(1))}{\Rightarrow} t+(s+(-s))-r > 0 \overset{(3.2.4.(2))}{\Rightarrow} (t+0)-r>0$$

$$\overset{(3.2.4.(1))}{\Rightarrow} t-r > 0 \overset{(\text{definição})}{\Rightarrow} r<t$$

Parte (7)**:**($\Rightarrow$)Sejam r, s e t números racionais, onde

$$r<s \Rightarrow r+t<s+t$$

($\Leftarrow$)Sejam r, s e t números racionais, onde

$$r+t < s+t \overset{(3.4.1)}{\Rightarrow} (s+t)-(r+t)>0$$

$$\overset{(3.2.3.(1))}{\Rightarrow} (s+t)-(t+r) > 0 \overset{(3.2.3.(2))}{\Rightarrow} s+(t+(-t))+(-r)>0$$

$$\overset{(3.2.4.(2))}{\Rightarrow} s+0+(-r) > 0 \overset{(3.2.4.(1))}{\Rightarrow} s-r>0 \overset{(3.4.1)}{\Rightarrow} r<s$$

Parte (8)**:**Sejam r, s e t números racionais, onde

$$\left.\begin{array}{l} r<s \overset{(3.4.7)}{\Rightarrow} r-s<0 \\ t<0 \end{array}\right\} \overset{(3.4.8.(3))}{\Rightarrow} (r-s)\times t > 0$$

$$\overset{(3.3.3.(3))}{\Rightarrow} r\times t - s\times t > 0 \overset{(3.4.7)}{\Rightarrow} r\times t > s\times t$$

■

Teorema 3.4.9 *Se $r, s \in \mathbb{Q}$, onde $(\alpha, \beta) \in r$ e $(\gamma, \delta) \in s$ então*

$$r<s \Leftrightarrow \alpha\cdot\delta < \beta\cdot\gamma$$

Demonstração. Consideremos $r = \overline{(\alpha,\beta)}$ e $s = \overline{(\gamma,\delta)}$,com α e $\gamma \in \mathbb{Z}$ e β e $\delta \in \mathbb{Z}'$.Por hipótese, temos:

$$r < s \overset{(3.4.7)}{\Leftrightarrow} s-r>0 \overset{(3.2.5)}{\Leftrightarrow} s+(-r)>0$$

$$\overset{(hipótese)}{\Leftrightarrow} \overline{(\gamma,\delta)}+\overline{(-\alpha,\beta)} > 0 \overset{(3.2.1)}{\Leftrightarrow} \overline{(\gamma\cdot\beta+\delta\cdot(-\alpha),\delta\cdot\beta)}>0$$

$$\overset{(3.4.1)}{\Leftrightarrow} (\gamma\cdot\beta+\delta\cdot(-\alpha))\cdot(\delta\cdot\beta) > \theta \overset{(2.4.7.(3))}{\Leftrightarrow} (\gamma\cdot\beta)\cdot(\delta\cdot\beta)+(\delta\cdot(-\alpha))\cdot(\delta\cdot\beta)>\theta$$

$$\overset{(2.4.8.(3))}{\Leftrightarrow} (\gamma\cdot\beta)\cdot(\delta\cdot\beta)-(\delta\cdot\alpha)\cdot(\delta\cdot\beta) > \theta \overset{(2.5.7.(2))}{\Leftrightarrow} (\delta\cdot\alpha)\cdot(\delta\cdot\beta)<(\gamma\cdot\beta)\cdot(\delta\cdot\beta)$$

$$\overset{(2.5.7.(3))}{\Leftrightarrow} (\delta\cdot\alpha) < (\gamma\cdot\beta) \overset{(2.4.7.(2))}{\Leftrightarrow} (\alpha\cdot\delta)<(\beta\cdot\gamma)$$

■

Teorema 3.4.10 *Se r e s são racionais com $0 < r < s$ então $0 < s^{-1} < r^{-1}$.*

Demonstração. Consideremos $r = \overline{(\alpha, \beta)}$ e $s = \overline{(\gamma, \delta)}$,com α e $\gamma \in \mathbb{Z}$ e β e $\delta \in \mathbb{Z}'$.Por hipótese, temos:

$$s > 0 \overset{\text{(hipótese)}}{\Rightarrow} \overline{(\gamma, \delta)} > 0 \overset{(3.4.1)}{\Rightarrow} \gamma \cdot \delta > 0 \overset{(2.4.7.(2))}{\Rightarrow} \delta \cdot \gamma > 0 \overset{(3.4.1)}{\Rightarrow} \overline{(\delta, \gamma)} > 0 \overset{\text{(hipótese)}}{\Rightarrow} s^{-1} > 0$$

Além disso,

$$\begin{aligned} r &< s \overset{(hipótese)}{\Rightarrow} \overline{(\alpha, \beta)} < \overline{(\gamma, \delta)} \\ \overset{(3.4.9)}{\Rightarrow} \alpha \cdot \delta &< \beta \cdot \gamma \overset{(3.3.3(1))}{\Rightarrow} \delta \cdot \alpha < \gamma \cdot \beta \\ \overset{(3.4.9)}{\Rightarrow} \overline{(\delta, \gamma)} &< \overline{(\beta, \alpha)} \overset{(hipótese)}{\Rightarrow} s^{-1} < r^{-1} \end{aligned}$$

■

Teorema 3.4.11 *Se r, s são números racionais não-nulos, então*

$$(r \times s)^{-1} = s^{-1} \times r^{-1}$$

Demonstração. Consideremos $r = \overline{(\alpha, \beta)}$ e $s = \overline{(\gamma, \delta)}$,com α e $\gamma \in \mathbb{Z}$ e β e $\delta \in \mathbb{Z}'$. Temos:

$$\begin{aligned} r^{-1} &= \overline{(\beta, \alpha)} \\ s^{-1} &= \overline{(\delta, \gamma)} \end{aligned}$$

Assim,

$$r \times s \overset{\text{(hipótese)}}{=} \overline{(\alpha, \beta)} \times \overline{(\gamma, \delta)} \overset{(3.3.1)}{=} \overline{(\alpha \cdot \gamma, \beta \cdot \delta)}$$

e portanto,

$$(r \times s)^{-1} \overset{(hipótese)}{=} \overline{(\beta \cdot \delta, \alpha \cdot \gamma)} \overset{(2.4.7.(2))}{=} \overline{(\delta \cdot \beta, \gamma \cdot \alpha)} \overset{(3.3.1)}{=} \overline{(\delta, \gamma)} \times \overline{(\beta, \alpha)} \overset{(hipótese)}{=} s^{-1} \times r^{-1}$$

■

3.5 OS INTEIROS COMO SUBCONJUNTO DOS RACIONAIS

Teorema 3.5.1 *A aplicação*

$$\Phi : \mathbb{Z} \longmapsto \mathbb{Q}$$

dada por $\Phi(\alpha) = \overline{(\alpha, 1)}$ *é injetora e tem as seguintes propriedades*

1. $\Phi(\alpha + \beta) = \Phi(\alpha) + \Phi(\beta)$
2. $\Phi(\alpha \times \beta) = \Phi(\alpha) \times \Phi(\beta)$
3. $\alpha < \beta \Leftrightarrow \Phi(\alpha) < \Phi(\beta)$

Demonstração. A aplicação Φ está bem definida e

$$\Phi(\alpha_1) = \Phi(\alpha_2) \Rightarrow \overline{(\alpha_1, 1)} = \overline{(\alpha_2, 1)} \Rightarrow \alpha_1 \cdot 1 = 1 \cdot \alpha_2 \Rightarrow \alpha_1 = \alpha_2$$

ou seja, Φ é injetora.

Parte (1): Temos,

$$\Phi(\alpha) + \Phi(\beta) = \overline{(\alpha, 1)} + \overline{(\beta, 1)} = \overline{(\alpha \cdot 1 + \beta \cdot 1, 1 \cdot 1)} = \overline{(\alpha + \beta, 1)} = \Phi(\alpha + \beta)$$

Parte (2)**:**Temos,

$$\Phi(\alpha) \cdot \Phi(\beta) = \overline{(\alpha, 1)} \times \overline{(\beta, 1)} = \overline{(\alpha \cdot \beta, 1 \cdot 1)} = \overline{(\alpha \cdot \beta, 1)} = \Phi(\alpha \times \beta)$$

Parte (3)**:** Observemos que,

$$\alpha < \beta \Leftrightarrow \alpha \cdot 1 < \beta \cdot 1 \Leftrightarrow \overline{(\alpha, 1)} < \overline{(\beta, 1)} \Leftrightarrow \Phi(\alpha) < \Phi(\beta)$$

■

Observação 3.5.2 *A aplicação* Φ *permite identificar o conjunto dos números inteiros como uma parte dos números racionais: o subconjunto* $\Phi(\mathbb{Z})$*. Desta forma, podemos abusar da notação e escrever*

$$\mathbb{Z} = \left\{ \overline{(\alpha, 1)} \in \mathbb{Q} \mid \alpha \in \mathbb{Z} \right\}$$

ainda que α *e* $\left(\overline{\alpha, 1}\right)$ *sejam objetos distintos.*

Esta identificação fica mais clara utilizando-se a seguinte notação.

(1) $r \cdot s^{-1} = \frac{r}{s} = r/s$.

Com esta notação, se $r = \overline{(\alpha, \beta)}$, teremos $r = \frac{\overline{(\alpha,1)}}{\overline{(\beta,1)}}$

Agora, como os números racionais $\overline{(\alpha, 1)}$ e $\overline{(\beta, 1)}$ podem ser identificados com os números inteiros α e β, respectivamente, vamos escrever

(2) $r = \frac{\alpha}{\beta} = \alpha/\beta$

Isto é, o número racional r está sendo identificado com uma fração de números inteiros.

O seguinte teorema sumariza as propriedades essenciais das frações.

Teorema 3.5.3 *Sejam α, β, γ e δ números inteiros com $\beta \neq 0$ e $\delta \neq 0$. Então*

(1) $\frac{\alpha}{\beta} = \frac{\gamma}{\delta} \Leftrightarrow \alpha\delta = \gamma\beta$;

(2) $\frac{\beta}{\beta} = 1$;

(3) $\frac{\alpha}{\beta} + \frac{\gamma}{\delta} = \frac{\alpha\delta+\beta\gamma}{\beta\delta}$;

(4) $\frac{\alpha}{\beta} \cdot \frac{\gamma}{\delta} = \frac{\alpha\gamma}{\beta\delta}$;

(5) $\frac{\alpha}{\beta} = \frac{-\alpha}{-\beta}$;

(6) $\frac{-\alpha}{\beta} = \frac{\alpha}{-\beta} = -\frac{\alpha}{\beta}$;

e se α, β, γ e δ forem positivos, temos também

(7) $\frac{\alpha}{\beta} < \frac{\gamma}{\delta} \Leftrightarrow \alpha\delta < \beta\gamma$

Demonstração. Parte (1)**:** Sejam α, β, γ e δ números inteiros com $\beta \neq 0$ e $\delta \neq 0$. Temos que

$$\frac{\alpha}{\beta} = \frac{\gamma}{\delta} \overset{(3.5.2.(2))}{\Leftrightarrow} \overline{(\alpha, \beta)} = \overline{(\gamma, \delta)} \overset{(2.1.4.(2))}{\Leftrightarrow} (\alpha, \beta)\, R\, (\gamma, \delta) \overset{(3.1.1)}{\Rightarrow} \alpha \cdot \delta = \beta \cdot \gamma$$

Parte (2)**:** De fato,

$$\frac{\beta}{\beta} \overset{(3.5.2.(2))}{=} \overline{(\beta, \beta)} \overset{(3.1.6)}{=} 1$$

Parte (3)**:** Com efeito,

$$\frac{\alpha}{\beta}+\frac{\gamma}{\delta}\overset{(3.5.2.(2))}{=}\overline{(\alpha,\beta)}+\overline{(\gamma,\delta)}\overset{(3.2.1)}{=}\overline{(\alpha\delta+\beta\gamma,\beta\delta)}\overset{(3.5.2.(2))}{=}\frac{\alpha\delta+\beta\gamma}{\beta\delta}$$

Parte (4)**:** Temos que

$$\frac{\alpha}{\beta}\cdot\frac{\gamma}{\delta}\overset{(3.5.2.(2))}{=}\overline{(\alpha,\beta)}\cdot\overline{(\gamma,\delta)}\overset{(3.3.1)}{=}\overline{(\alpha\gamma,\beta\delta)}\overset{(3.5.2.(2))}{=}\frac{\alpha\gamma}{\beta\delta}$$

Parte (5)**:** Observe que

$$\frac{\alpha}{\beta}\overset{(3.5.2.(2))}{=}\overline{(\alpha,\beta)}=\overline{(-\alpha,-\beta)}\overset{(3.5.2.(2))}{=}\frac{-\alpha}{-\beta}$$

Parte (6)**:** Sabemos que

$$\frac{-\alpha}{\beta}\overset{(3.5.2.(2))}{=}\overline{(-\alpha,\beta)}=\overline{-(\alpha,\beta)}\overset{(3.5.2.(2))}{=}-\frac{\alpha}{\beta}$$

e

$$\frac{\alpha}{-\beta}\overset{(3.5.3.(2))}{=}\overline{(\alpha,-\beta)}=\left(-\left(\overline{(\alpha,\beta)}\right)^{-1}\right)^{-1}\overset{(3.3.7)}{=}-\overline{(\alpha,\beta)}\overset{(3.5.2.(2))}{=}-\frac{\alpha}{\beta}$$

logo,

$$\frac{-\alpha}{\beta}=\frac{\alpha}{-\beta}=-\frac{\alpha}{\beta}$$

Parte (7)**:** Temos por hipótese, que

$$\frac{\alpha}{\beta}<\frac{\gamma}{\delta}=\overline{(\alpha,\beta)}<\overline{(\gamma,\delta)}=\alpha\delta<\beta\gamma$$

■

É claro que trabalhar com os números racionais em forma de frações é muito mais cômodo. Mas deve-se ter sempre presente que um número racional não é uma fração, ainda que habitualmente se escreva "seja m/n um número racional".

Teorema 3.5.4 *(Densidade de $\mathbb{Q}$) Se r e s, com $r<s$, são dois números racionais, existe um número racional t tal que $r<t<s$*

Demonstração. Como $r < s$, temos

$$2r = r + r < r + s$$

e

$$r + s < s + s = 2s$$

Logo,

$$2r < r + s < 2s \Rightarrow r < \frac{1}{2}(r + s) < s$$

Portanto, $\frac{1}{2}(r + s)$ satisfaz a condição para ser t. ■

Exemplo 3.5.5 *Cada decimal periódico representa um número racional.*

Considere-se o decimal periódico

$$r, stdefdef \cdots = r, st + 0,00def + 0,00000def + \cdots$$

Agora,

$$r, st$$

é uma fração racional, pois é um decimal que termina, enquanto que

$$0,00def + 0,00000def + \cdots$$

é uma progressão geométrica infinita cujo primeiro termo é $a = 0,00def$, de razão $r = 0,001$, e cuja soma é

$$S = \frac{a}{1 - r} = \frac{0,00def}{0,999} = \frac{def}{99900}$$

uma fração decimal. Logo, o decimal periódico, sendo a soma de dois números racionais, é um número racional.

Vamos utilizar esta identificação para demonstrar a **Propriedade Arquimediana** dos números racionais.

Teorema 3.5.6 *Sejam p e q números racionais positivos. Então, existe um número natural m tal que*

$$q < mp$$

Demonstração. Se $p \geq q$ basta tomar $m = 2$. Agora, se $p < q$, vamos supor por absurdo que $mp \leq q$ para todo $m, m \in \mathbb{N}$. Sejam então $p = \frac{\alpha}{\beta}$ e $q = \frac{\gamma}{\delta}$. A hipótese de absurdo diz então que

$$m\alpha\delta \leq \gamma\beta \tag{i}$$

para todo $m, m \in \mathbb{N}$. Agora, se (i) vale para todo número natural m, vale me particular para $m = \gamma\beta + 1$; então, de (i) obtemos

$$\alpha\delta + \alpha\delta\gamma\beta \leq \gamma\beta$$

mas como $\alpha\delta \geq 1$, segue que

$$\alpha\delta\gamma\beta < \gamma\beta$$

e consequentemente $\alpha\delta < 1$, o que é absurdo. ■

Capítulo 4

NÚMEROS REAIS

Os capítulos 2 e 3 começam com a observação de que o conjunto X de números previamente estudado tinha uma imperfeição. Esta imperfeição foi sanada pela ampliação do conjunto X através da definição de uma conveniente relação de equivalência no conjunto dos pares ordenados de elementos de X. Deste modo, obtivemos, a partir de $\mathbb{N}$ os conjuntos $\mathbb{Z}$ e $\mathbb{Q}$ satisfazendo $\mathbb{N} \subset \mathbb{Z} \subset \mathbb{Q}$. Para o que se segue, é importante notar que cada um dos novos conjuntos $\mathbb{Z}$ e $\mathbb{Q}$ tem uma única caracterização simples, a saber,

$\mathbb{Z}$ é o menor conjunto no qual, para elementos arbitrários $m, s \in \mathbb{Z}$, a equação $m + x = s$ sempre possui uma solução.

$\mathbb{Q}$ é o menor conjunto no qual, para inteiros arbitrários $m \neq 0$ e s, a equação $mx = s$ sempre possui uma solução.

O conjunto dos números racionais contém subconjuntos tais que seus elementos são menores que qualquer elemento do seu complementar e todo número racional menor que um elemento qualquer do subconjunto em questão pertence também ao subconjunto; o subconjunto complementar goza também de propriedades análogas. Na verdade podemos construir subconjuntos de números racionais tais que, além dessa propriedade, o subconjunto não tenha supremo e nem o seu complementar tenha ínfimo. Conjuntos desse tipo e seus respectivos complementares, dividem o conjunto dos números racionais em duas partes disjuntas que não possuem elemento fronteira. Em outros termos: o conjunto dos números racionais não é completo (ou apresenta descontinuidades).

A situação, agora, não é a de que o conjunto $\mathbb{Q}$ tenha apenas uma imperfeição; ao contrário, existem muitas imperfeições, mencionamos apenas dois.

(1) A equação $x^2 = 2$ não possui solução em $\mathbb{Q}$. De fato, suponha o contrário, isto é que o racional $\frac{a}{b}$, reduzido a uma fração irredutível,

seja tal que $\left(\frac{a}{b}\right)^2 = 2$. Como $a^2 = 2b^2$, logo a^2 é um número inteiro par, o que implica que a é par, isto é, $a = 2a_1$ onde $a_1 \in \mathbb{Z}$. Portanto $(2a_1)^2 = 2b^2$, isto é, $b^2 = 2a_1^2$, de onde segue que b^2 é par, ou seja, b é par. Mas isso contradiz a hipótese de que $\frac{a}{b}$ era uma fração irredutível.

(2) Mostra-se que o comprimento C de uma circunferência de diâmetro $d \in \mathbb{Q}$ não é um número real, isto é, $C = \pi d \notin \mathbb{Q}$. Além disso, $\pi^2 \notin \mathbb{Q}$, de modo que π não é solução de nenhuma equação do tipo $x^2 = q$, com $q \in \mathbb{Q}$.

O objetivo da teoria dos números reais é justamente completar o conjunto dos números racionais criando um sistema contínuo de números.

A construção do conjunto dos números reais pode ser feita utilizando-se diversos métodos. Vamos fazer a construção utilizando a noção de corte no conjunto dos números racionais. A noção de corte foi introduzida por R. Dedekind, mas as idéias gerais remontam à Eudoxio (408-353 a.C.).

4.1 CORTES DE DEDEKIND

Definição 4.1.1 *Um par ordenado (A, B), de subconjuntos de números racionais,* ***é um corte*** *no conjunto dos números racionais se as seguintes condições são verificadas:*

(1) $A \neq \emptyset$ e $B \neq \emptyset$

(2) $A \cup B = \mathbb{Q}$

(3) $a \in A$ e $b \in B \Rightarrow a < b$;

(4) A não tem elemento máximo

O conjunto A é o conjunto minorante e o conjunto B é o conjunto majorante do corte, respectivamente.

Os elementos do conjunto minorante serão chamados de números minorantes e os elementos do conjunto majorante de números majorantes.

Definição 4.1.2 *Sejam (A, B) e (C, D) cortes no conjunto dos números racionais. Dizemos que (A, B)* ***é igual*** *(C, D) e escrevemos $(A, B) = (C, D)$ se, e somente se, o conjunto minorante de (A, B) for igual ao conjunto minorante de (C, D). Mas precisamente,*

$$(A, B) = (C, D) \Leftrightarrow A = C$$

Exemplo 4.1.3 *Seja r um número racional e consideremos os conjuntos*

$$A_r = \{x \in \mathbb{Q} \mid x < r\}$$

e

$$B_r = \{x \in \mathbb{Q} \mid x \geq r\}$$

Então, o par (A_r, B_r) é um corte, que denotaremos por $r^{\blacklozenge}$. De fato; tem-se:

Parte (1): A condição (4.1.1. (1)) é verificada pois é claro que A_r e B_r são conjuntos não vazios.

Parte (2): Dado um número racional arbitrário x, pela lei da tricotomia, teríamos $x \in A_r$ ou $x \in B_r$ logo $A_r \cup B_r = \mathbb{Q}$ e a condição (4.1.1. (2)) está satisfeita.

Parte (3): Seja $a \in A_r$ e $b \in B_r$, temos $a < r$ e $b \geq r$, portanto $a < b$.

Parte (4): O conjunto A_r não tem elemento máximo, pois se $a \in A_r$ então $a < r$, e por (3.5.4), existe $a_1 \in \mathbb{Q}$, tal que $a < a_1 < r$, logo $a_1 > a$.

Observação 4.1.4 *Um corte (A, B) no qual o conjunto majorante tem elemento mínimo denomina-se um* ***corte racional.*** *Assim, o corte do exemplo acima é um corte racional. Reciprocamente, todo corte racional é determinado por um número racional.*

De fato, se $r = \min B$ então $r^{\blacklozenge} = (A, B)$

Exemplo 4.1.5 *Sejam*

$$A = \left\{x \in \mathbb{Q} \mid x^2 < 2 \text{ } ou \text{ } x \leq 0\right\}$$

e

$$B = \left\{x \in \mathbb{Q} \mid x^2 > 2 \text{ } e \text{ } x > 0\right\}$$

O par (A, B) é um corte. O conjunto minorante não tem supremo nem o conjunto majorante tem ínfimo. Com efeito, tem-se:

Parte (1): A condição (4.1.1. (1)) é verificada pois é claro que A e B são conjuntos não vazios.

Parte (2): Como não existe um número racional r tal que $r^2 = 2$, segue que dado um número racional arbitrário r, pela Lei da Tricotomia, teremos $r \in A$ ou $r \in B$; logo $A \cup B = \mathbb{Q}$ e a condição (4.1.1. (2)) é verificada.

Parte (3): Seja $\begin{cases} a \in A \Rightarrow a^2 < 2 \text{ ou } a \leq 0 \\ b \in B \Rightarrow b^2 > 2 \text{ e } b > 0 \end{cases}$, temos:

$$a^2 < 2 < b^2 \Rightarrow a^2 < b^2 \Rightarrow |a| < b \Rightarrow -b < a < b$$

portanto $a < b$.

Parte (4): O conjunto A não tem elemento máximo, isto é, se $x \in A$ então existe $y, y \in A$, tal que $y > x$. De fato, seja $x = \frac{p}{q}$ e vamos procurar um número inteiro positivo n tal que $y = (np+1)/nq \in A$. Isto ocorre se

$$\begin{aligned} \frac{(np+1)^2}{n^2q^2} &< 2 \Leftrightarrow n^2p^2 + 2np + 1 < 2n^2q^2 \\ &\Leftrightarrow \left(p^2 - 2q^2\right) n^2 + 2np + 1 < 0 \end{aligned}$$

Como $x = \frac{p}{q} \in A$, temos que $p^2 - 2q^2 < 0$; logo, a desigualdade é verificada se tomarmos $n > máx\left\{\frac{-p+\sqrt{2}}{p^2-2q^2}, \frac{-p-\sqrt{2}}{p^2-2q^2}\right\}$.

Definição 4.1.6 *Um corte (A, B) no qual o conjunto majorante não tem elemento mínimo (em $\mathbb{Q}$) denomina-se um* ***corte irracional.***

Estamos agora em condições de introduzir o conceito de número real.

Definição 4.1.7 *O conjunto $\mathbb{R}$ formado por todos os cortes, racionais ou irracionais, é chamado de o* ***conjunto dos números reais*** *e seus elementos de* ***números reais****.*

Observação 4.1.8 *Segundo a definição acima, um número real é um corte! Quando o corte for racional diremos que o número real é racional e quando o corte for irracional diremos que o número real é irracional. Por abuso de linguagem falaremos de números racionais e números irracionais. No segundo caso a terminologia é válida, mas no primeiro caso deveríamos justificar a linguagem identificando os números racionais com os números reais racionais.*

4.2 RELAÇÃO DE ORDEM EM $\mathbb{R}$

Definição 4.2.1 *Sejam α e β números reais. Diremos que α* ***é maior do que*** *β, e escrevemos $\alpha > \beta$, se existir um número minorante de α que é um número majorante de β. Mais precisamente: Se $\alpha = (A, B)$ e $\beta = (C, D)$, temos*

$$\alpha > \beta \Leftrightarrow \{\exists x \in \mathbb{Q} \mid x \in A \cap D\}$$

Diremos que α ***é menor do que*** β**,** *e escrevemos* $\alpha < \beta$*, se existir um número majorante de* α *que é um número minorante de* β*. Mais precisamente: Se* $\alpha = (A, B)$ *e* $\beta = (C, D)$*, temos*

$$\alpha < \beta \Leftrightarrow \{\exists x \in \mathbb{Q} \mid x \in B \cap C\}$$

Teorema 4.2.2 *Sejam* $\alpha = (A, B)$ *e* $\beta = (C, D)$ *números reais. Então, temos*

(1) $\alpha \leq \beta \Leftrightarrow A \subset C$

(2) $\alpha < \beta \Leftrightarrow A \subset C$ e $A \neq C$

Demonstração. Parte (1)**:** ($\Rightarrow$) Temos por hipótese que $\alpha \leq \beta$.
Suponhamos que $\alpha = \beta$, logo por (4.1.2)

$$A = C$$

portanto

$$A \subset C$$

Se $\alpha < \beta$, então existe $x \in B \cap C$, isto é, $x \in C$ com $x \notin A$. Isto mostra que $A \neq C$. Afirmamos agora que $A \subset C$. De fato, se $a \in A$ e como $x \in B$, então $a < x$, o que acarreta $a \in C$, pois se a não pertencesse a C, então a pertenceria a D, donde seguiria $x < a$, uma contradição.

($\Leftarrow$) Temos por hipótese que $A \subset C$, logo para todo $x \in C$, temos:
Se $x \in A$, então $A = C$, logo por (4.1.2) $\alpha = \beta$;
Se $x \notin A$, então $x \in B \cap C$, ou seja, $\alpha < \beta$.

Parte (2)**:** ($\Rightarrow$) Se $\alpha < \beta$, então existe $x \in B \cap C$, isto é, existe $x \in C$ com $x \notin A$. Isto mostra que $A \neq C$. Afirmamos agora que $A \subset C$. De fato, se $a \in A$ e como $x \in B$, então $a < x$, o que acarreta $a \in C$, pois se a não pertencesse a C, então a pertenceria a D, donde seguiria $x < a$, uma contradição.

($\Leftarrow$) Se $A \subset C$ e $A \neq C$, existe $x \in C$ tal que $x \notin A$, donde segue que existe $x \in B \cap C$, ou seja, $\alpha < \beta$. ■

Teorema 4.2.3 *Sejam* α *e* β *números reais. Então:*

(1) $\alpha > \beta \Rightarrow \beta < \alpha$

(2) $\alpha < \beta \Rightarrow \beta > \alpha$

Demonstração. Parte (1)**:** Suponhamos que $\alpha = (A, B)$ e $\beta = (C, D)$, com $A, B, C, D \subset \mathbb{Q}$. Temos por hipótese que $\alpha > \beta$, logo existe $x \in \mathbb{Q}$, tal que $x \in A \cap D$, isto é, $x \in D \cap A$. Portanto

$$\beta < \alpha$$

Parte (2)**:** Considerando que $\alpha = (A, B)$ e $\beta = (C, D)$, com $A, B, C, D \subset \mathbb{Q}$ e tendo por hipótese que $\alpha < \beta$, temos que existe $x \in \mathbb{Q}$, tal que $x \in B \cap C$, ou seja, $x \in C \cap B$. Portanto

$$\beta > \alpha$$

■

Teorema 4.2.4 *(Lei da Tricotomia). Se α e β são números reais então, uma e apenas uma das seguintes afirmações são verdadeiras:*

(1) $\alpha = \beta$

ou

(2) $\alpha < \beta$

ou

(3) $\alpha > \beta$

Demonstração. Suponhamos que $\alpha = (A, B)$ e $\beta = (C, D)$. Observemos inicialmente que $\alpha = \beta$ e $\alpha > \beta$ não ocorre, pois se ocorresse $\alpha > \beta$ implicaria a existência de um número $x \in A \cap D$, o que acarretaria $A \supsetneq C$, uma contradição com o fato que $\alpha = \beta$ $(A = C)$. Analogamente, as relações $\alpha = \beta$ e $\alpha < \beta$ também não ocorrem.

Agora, se $\alpha > \beta$ e $\alpha < \beta$ ocorresse, então existiriam números $x \in A \cap D$ e $y \in B \cap C$, donde seguiria $x < y$ e $y < x$, uma contradição. Portanto, uma e apenas uma das condições ocorre.

Mostremos agora, que se $\alpha \neq \beta$ então $\alpha < \beta$ ou $\alpha > \beta$. De fato, se $\alpha \neq \beta$, então $A \neq C$, isto é, o conjunto dos minorante de α e β não coincidem. Assim, ou existe $x \in A \cap D$, caso em que $\alpha > \beta$; ou existe $y \in B \cap C$, caso em que $\alpha < \beta$. ■

Definição 4.2.5 *Se α e β são números reais, diremos que α* ***é maior que ou igual à*** *β, e escrevemos $\alpha \geq \beta$, se $\alpha > \beta$ ou $\alpha = \beta$; diremos que α* ***é menor que ou igual à*** *β, e escrevemos $\alpha \leq \beta$ se $\alpha < \beta$ ou $\alpha = \beta$.*

Teorema 4.2.6 *Sejam α e β números reais. Então*

(1) $\alpha \leq \beta \Rightarrow \beta \geq \alpha$

(2) $\alpha \geq \beta \Rightarrow \beta \leq \alpha$

Demonstração. Parte (1)**:** Temos que

$$\alpha \leq \beta \overset{(4.2.5)}{\Rightarrow} \alpha < \beta \text{ ou } \alpha = \beta \overset{(4.2.3.(2))}{\Rightarrow} \beta > \alpha \text{ ou } \beta = \alpha \overset{(4.2.5)}{\Rightarrow} \beta \geq \alpha$$

Parte (2)**:** Temos que

$$\alpha \geq \beta \overset{(4.2.5)}{\Rightarrow} \alpha > \beta \text{ ou } \alpha = \beta \overset{(4.2.3.(1))}{\Rightarrow} \beta < \alpha \text{ ou } \beta = \alpha \overset{(4.2.5)}{\Rightarrow} \beta \leq \alpha$$

■

Teorema 4.2.7 *Sejam α, β e γ números reais. Então:*

(1) $\alpha \geq \alpha$ $(reflexiva)$

(2) $\alpha \geq \beta$ e $\beta \geq \alpha \Rightarrow \alpha = \beta$ $(anti - simétrica)$

(3) $\alpha \geq \beta$ e $\beta \geq \gamma \Rightarrow \alpha \geq \gamma$ $(transitiva)$

(4) $\alpha \geq \beta$ ou $\beta \geq \alpha$ $(ordem\ total)$

Demonstração. Parte (1)**:** É claro que $\alpha \geq \alpha$.
Parte (2)**:** Por hipótese, temos que

$$\begin{cases} \alpha \geq \beta \overset{(4.2.5)}{\Rightarrow} \alpha > \beta \text{ ou } \alpha = \beta \\ \beta \geq \alpha \overset{(4.2.5)}{\Rightarrow} \beta > \alpha \text{ ou } \beta = \alpha \end{cases}$$

Temos quatro casos para analizar;
1^oCaso: Se $\alpha > \beta$ e $\beta > \alpha$, absurdo.
2^oCaso: Se $\alpha > \beta$ e $\beta = \alpha$, temos $\alpha > \alpha$, absurdo.
3^oCaso: Se $\alpha = \beta$ e $\beta > \alpha$, então $\alpha > \alpha$, absurdo.
4^oCaso: Se $\alpha = \beta$ e $\beta = \alpha$, então, $\alpha = \beta$
Parte (3)**:** Sejam $\alpha = (A, B)$, $\beta = (C, D)$ e $\gamma = (E, F)$, por hipótese

$$\begin{cases} \alpha \geq \beta \overset{(4.2.5)}{\Rightarrow} \alpha > \beta \text{ ou } \alpha = \beta \\ \beta \geq \gamma \overset{(4.2.5)}{\Rightarrow} \beta > \gamma \text{ ou } \beta = \gamma \end{cases}$$

Temos quatro casos para analizar:

1^oCaso: Se $\alpha > \beta$ e $\beta > \gamma \Rightarrow \alpha > \gamma$
Temos

$$\begin{cases} \alpha > \beta \overset{(4.2.1)}{\Rightarrow} \exists\ x \in A \cap D \\ \beta > \gamma \overset{(4.2.1)}{\Rightarrow} \exists\ y \in C \cap F \end{cases}$$

Como $y \in C$ e $x \in D$ então, por $(4.1.1.\,(3))$, $y < x$ e portanto $x \in F$. Assim $x \in A \cap F$, ou seja $\alpha > \gamma$
2^oCaso: Se $\alpha > \beta$ e $\beta = \gamma \Rightarrow \alpha > \gamma$. (Óbvio)
3^oCaso: Se $\alpha = \beta$ e $\beta > \gamma \Rightarrow \alpha > \gamma$. (Óbvio)
4^oCaso: Se $\alpha = \beta$ e $\beta = \gamma \Rightarrow \alpha = \gamma$. (Óbvio)
Parte (4)**:** Seja α e β números reais quaisquer, pela Lei da Tricotomia

$$\begin{aligned} \alpha &> \beta \text{ ou } \alpha = \beta \Rightarrow \alpha \geq \beta \\ \beta &> \alpha \text{ ou } \alpha = \beta \Rightarrow \beta \geq \alpha \end{aligned}$$

■

A relação de ordem em $\mathbb{R}$ permite introduzir o conceito de número real positivo.

Definição 4.2.8 *Um número real α é* ***positivo*** *se $\alpha > 0^{\blacklozenge}$ e é* ***negativo*** *se $\alpha < 0^{\blacklozenge}$. Denotaremos por $\mathbb{R}_+$ o conjunto dos números reais positivos e por $\mathbb{R}_-$ o conjunto dos números reais negativos.*

Observação 4.2.9 *O elemento $0^{\blacklozenge}$ que aparece em* $(4.2.8)$ *é o corte que foi introduzido em* $(4.1.3)$*, com $r = 0$, isto é, $0^{\blacklozenge} = \left(\mathbb{Q}_-, \mathbb{Q}_-^c\right)$.*

Notação 4.2.10 *Se C é um conjunto de números racionais, denotamos*

$$-C = \{-c \mid c \in C\}$$

Se o mínimo de C existir escreveremos $C' = C - \{\min C\}$ e $C' = C$ se o mínimo não existir,. Também, escreveremos $C'' = C \cup \{\min C\}$, se o mínimo de C existir e escreveremos $C'' = C$ se o mínimo de C não existir.

Teorema 4.2.11 *Seja $\alpha = (A, B)$ um número real. Então, o par $\alpha^{\triangleright} = (-B', -A'')$ é também um número real e temos:*

(1) $\alpha \in \mathbb{R}_+ \Rightarrow \alpha^{\triangleright} \in \mathbb{R}_-$;

(2) $\alpha \in \mathbb{R}_- \Rightarrow \alpha^{\triangleright} \in \mathbb{R}_+$.

Demonstração. Vamos verificar inicialmente que $\alpha^{\triangleright} = (-B', -A'')$ é um corte.

Parte (1): Como $A \neq \emptyset$ e $B \neq \emptyset$, segue que $-A'' \neq \emptyset$ e $-B' \neq \emptyset$.

Parte (2): Seja $x \in \mathbb{Q}$ e suponhamos que $x \notin -A''$, então $-x \notin -B'$ e $x \in -B'$; analogamente se $x \notin -B'$ então $x \in -A''$; portanto $\mathbb{Q} \subset (-B') \cup (-A'')$.

Parte (3): Se $r \in -B'$ e $s \in -A''$ então $-r \in B'$ e $-s \in A''$, logo $-s < -r$ e $r < s$.

Parte (4): Suponhamos que $-B'$ tenha elemento máximo m_0; então $-b \leq m_0$, para todo b, $b \in B'$, o que não é possível, pois B' por definição não tem elemento mínimo.

A seguir demonstraremos (4.2.11. (1)) e (4.2.11. (2)), onde $0^{\blacklozenge} = \left(\mathbb{Q}_-, \mathbb{Q}_-^c\right)$

Parte (1): Temos por hipótese que $\alpha \in \mathbb{R}_+$, logo por (4.2.8)

$$\alpha > 0^{\blacklozenge}$$

ou seja, existe $x \in A \cap \mathbb{Q}_-^c$. Mas, $x \in A$ e $x \in \mathbb{Q}_-^c$, implica $-x \in -A''$ e $-x \in \mathbb{Q}_-$. Portanto, existe $-x \in -A'' \cap \mathbb{Q}_-$, donde concluímos $\alpha^{\triangleright} < 0^{\blacklozenge}$, ou seja,

$$\alpha^{\triangleright} \in \mathbb{R}_-$$

Parte (2): Temos por hipótese que $\alpha \in \mathbb{R}_-$, logo por (4.2.8)

$$\alpha < 0^{\blacklozenge}$$

ou seja, existe $x \in B \cap \mathbb{Q}_-$. Mas $x \in B$ e $x \in \mathbb{Q}_-$, acarreta $-x \in -B'$ e $-x \in \mathbb{Q}_-^c$. Logo, existe $-x \in -B' \cap \mathbb{Q}_-^c$, donde concluímos $\alpha^{\triangleright} > 0^{\blacklozenge}$, ou seja,

$$\alpha^{\triangleright} \in \mathbb{R}_+$$

■

4.3 ADIÇÃO DE NÚMEROS REAIS

Notação 4.3.1 *Sejam A e B conjuntos de números racionais. Denotamos*

$$A + B = \{a + b \mid a \in A \text{ e } b \in B\}$$

Teorema 4.3.2 *Sejam $\alpha = (A, B)$ e $\beta = (C, D)$ números reais. Então, o par $\gamma = (A + C, (A + C)^c)$ é um corte, e portanto um número real, que é chamado de* ***soma*** *dos números reais α e β e é denotado por*

$$\gamma = \alpha + \beta$$

Demonstração. Parte (1): É claro que $A+C \neq \emptyset$ e se $b \notin A$ e $d \notin C$ então $a+c < b+d$, para todo $a \in A$ e $c \in C$. Logo, $b+d \notin A+C$ e $(A+C)^c \neq \emptyset$.

Parte (2): É claro que $(A+C) \cup (A+C)^c = \mathbb{Q}$.

Parte (3)**:** Sejam $r \in A+C$, $s \in (A+C)^c$ e suponhamos que $s < r = a+c$. Vamos ter, então $s-c < a$ e $s-c \in A$. Logo, $s = (s-c)+c \in A+C$, o que é absurdo. O caso $s = r$ está óbviamente excluído.

Parte (4)**:** Suponhamos que $m_0 = a_0+c_0$ seja o máximo de $A+C$. Então $a_0 = m_0 - c_0$ é o máximo de A; de fato, se $a_0 = m_0 - c_0 < a'$, $a' \in A$, então

$$m' = a' + c_0 > a_0 + c_0 = m_0$$

o que contraria a hipótese de que m_0 é o máximo de $A+C$. ■

Teorema 4.3.3 *Sejam α, β e γ números reais. Então, valem as seguintes propriedades:*

(1) $\alpha + \beta = \beta + \alpha$ (*comutatividade*)

(2) $(\alpha+\beta)+\gamma = \alpha+(\beta+\gamma)$ (*associatividade*)

Demonstração. Parte (1)**:** Se $\alpha = (A,B)$ e $\beta = (C,D)$ são números reais, temos:

$$\alpha+\beta \overset{(4.3.2)}{=} (A+C,(A+C)^c) \overset{(3.2.3.(1))}{=} (C+A,(C+A)^c) \overset{(4.3.2)}{=} \beta+\alpha$$

Parte (2)**:** Sejam $\alpha = (A,B), \beta = (C,D)$ e $\gamma = (E,F)$ números reais. Então, temos:

$$\begin{aligned}(\alpha+\beta)+\gamma &\overset{(4.3.2)}{=} (A+C,(A+C)^c)+(E,F) \overset{(4.3.2)}{=} ((A+C)+E,((A+C)+E)^c)\\ &\overset{(3.2.3.(2))}{=} (A+(C+E),(A+(C+E))^c) \overset{(4.3.2)}{=} (A,B)+(C+E,(C+E)^c)\\ &\overset{(4.3.2)}{=} \alpha+(\beta+\gamma)\end{aligned}$$

■

Teorema 4.3.4 *Para todo número real α temos*

$$\alpha + 0^{\blacklozenge} = \alpha$$

Mais ainda, o elemento $0^{\blacklozenge}$ é o único número real que satisfaz a equação acima.

Demonstração. Se $\alpha = (A, A^c)$ então

$$\alpha + 0^\blacklozenge = (A + \mathbb{Q}_-, (A + \mathbb{Q}_-)^c)$$

Vamos mostrar que $A = A + \mathbb{Q}_-$. Dado $r \in A$, seja $s \in A$ tal que $r < s$, fazendo $q = r - s$, vemos que $q < 0$, logo, $r = s + q \in A + \mathbb{Q}_-$. Reciprocamente, se $r \in A + \mathbb{Q}_-$ existem $a \in A$ e $q \in \mathbb{Q}_-$ tal que $r = a + q$ e $a + q < a$; portanto $r \in A$.

A demonstração da unicidade é análoga à que foi feita em (3.2.4. (1)). ■

Lema 4.3.5 *Seja $\alpha = (A, B)$ um número real e r um número racional positivo. Então existe $p \in A$ e $q \in B$ tal que $r = q - p$, e q não é o menor elemento de B.*

Demonstração. Seja $a \in A$ e para cada $n \in \mathbb{N}$ façamos $s_n = a + nr$. Então, existe um único número natural m tal que $s_m \in A$ e $s_{m+1} \in B$. Se s_{m+1} não for o mínimo de B, tomamos $p = s_m + \frac{1}{2}$ e $q = s_{m+1} + \frac{1}{2}$. Em ambos os casos temos $p \in A$, $q \in B$ e $r = q - p$. ■

Teorema 4.3.6 *Sejam α, β e γ números reais. Então*

$$\alpha < \beta \Rightarrow \alpha + \gamma < \beta + \gamma$$

Demonstração. Sejam $\alpha = (A, A^c)\,, \beta = (B, B^c)$ e $\gamma = (C, C^c)$. Como $\alpha < \beta$, existe $b \in B$ tal que $b \notin A$. Sejam $a \in A$ e $c \in C$ arbitrários. Sejam $b \in B \cap A^c$ e $b^\bullet \in B$ tais que $b < b^\bullet$. Tomando $2r = b^\bullet - b$, pelo Lema (4.3.5), existem $c^\bullet \in C$ e $c^{\bullet\bullet} \in C^c$ tais que

$$c - c^\bullet < c^{\bullet\bullet} - c^\bullet = \frac{b^\bullet - b}{2} < b^\bullet - b < b^\bullet - a.$$

Então

$$a + c < b^\bullet + c^\bullet \qquad (i)$$

para todo $a \in A$ e $c \in C$. Por outro lado, $b^\bullet + c^\bullet \notin A + C$, pois caso contrário existiriam $\hat{a} \in A$ e $\hat{b} \in C$ tais que $b^\bullet + c^\bullet = \hat{a} + \hat{b}$, o que contraria (i). Logo $b^\bullet + c^\bullet \in (B + C) \cap (A + C)^c$ e o teorema segue. ■

Teorema 4.3.7 *Para cada $\alpha \in \mathbb{R}$ existe um e apenas um elemento β, tal que*

$$\alpha + \beta = 0^\blacklozenge$$

Demonstração. Sejam $\alpha = (A, B)$ e $\beta = \alpha^{\triangleright}$, onde $\alpha^{\triangleright} = (-B', -A'')$ é o número real introduzido em (4.2.11). Vamos ter $\alpha + \beta = 0^{\blacklozenge}$. De fato, $r \in A + (-B')$, existe $p \in A$ e $q \in (-B')$ tal que $r = p + q$. Mas, como $q \in -B'$ segue que $-q \in B'$ e $-q \notin A''$. Logo, $p < -q$ e $r = p + q < 0$, ou seja $A + (-B') \subset \mathbb{Q}_-$. Reciprocamente, se $r \in \mathbb{Q}_-$ então $r < 0$. Pelo Lema (4.3.5) , existem $s \in A$ e $t \in B'$ tal que $t - s = -r$; ou seja $r = s + (-t)$, com $s \in A$ e $-t \in -B'$. Portanto, $r \in A + (-B')$ e $\mathbb{Q}_- \cup A + (-B')$. Consequentemente, $\mathbb{Q}_- = A + (-B')$ e $\alpha + \beta = 0^{\blacklozenge}$

A demonstração da unicidade é análoga à que foi feita em (3.2.4. (2)). ■

Notação 4.3.8 *O elemento β que aparece em* (4.3.7) *é chamado simétrico ou oposto de α, e será denotado por $-\alpha$.*

Lema 4.3.9 *Se α é um número real, temos que*

$$\alpha = -(-\alpha)$$

Demonstração. Por (4.3.7), temos

$$\alpha + \beta = 0^{\blacklozenge}$$

e aplicando (4.3.3. (1)), resulta

$$\beta + \alpha = 0^{\blacklozenge}$$

o que implica

$$\alpha = -\beta$$

Portanto,

$$\alpha = -(-\alpha)$$

■

Teorema 4.3.10 *Se α e β são números reais, então*

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

Demonstração. Temos que

$$\begin{aligned}
&(\alpha + \beta) + (-\alpha) + (-\beta) \\
&\overset{(4.3.3.(1))}{=} \alpha + (-\alpha) + \beta + (-\beta) \\
&\overset{(4.3.3.(2))}{=} (\alpha - \alpha) + (\beta - \beta) \\
&\overset{(4.3.7)}{=} 0^{\blacklozenge} + 0^{\blacklozenge} \\
&\overset{(4.3.4)}{=} 0^{\blacklozenge}
\end{aligned}$$

logo, por (4.3.7)

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

■

Observação 4.3.11 *Se α e β são números reais, então a equação*

$$\alpha+\varkappa=\beta$$

admite uma e uma única solução, que é dada por $\varkappa=\beta+(-\alpha)$.

O número real $\beta+(-\alpha)$ será denotado por $\beta-\alpha$ e será chamado de **diferença** entre β e α.

Vamos concluir esta seção introduzindo a noção de **módulo** ou **valor absoluto** de um número real.

Definição 4.3.12 *Se α é um número real o **módulo** ou **valor absoluto** de α, é definido por*

$$|\alpha|=\begin{cases}\alpha \text{ se } \alpha\geq 0^{\blacklozenge}\\ -\alpha \text{ se } \alpha<0^{\blacklozenge}\end{cases}$$

Teorema 4.3.13 *Se α é um número real, então*

(1) $\alpha\leq|\alpha|$

(2) $|-\alpha|=|\alpha|$

Demonstração. Parte (1)**:** Se $\alpha\geq 0^{\blacklozenge}$, temos $|\alpha|=\alpha$, logo a igualdade está satisfeita.

Se $\alpha<0^{\blacklozenge}$, então $|\alpha|=-\alpha$. Assim,

$$\alpha<0^{\blacklozenge}\overset{(4.2.11.(2))}{\Rightarrow}-\alpha>0^{\blacklozenge}\overset{(4.3.12)}{\Rightarrow}|\alpha|=-\alpha>0^{\blacklozenge}>\alpha\Rightarrow|\alpha|>\alpha$$

e a desigualdade ocorre.

Parte (2)**:** Se $\alpha\geq 0^{\blacklozenge}$, temos $|\alpha|=\alpha$. Como $\alpha\geq 0^{\blacklozenge}$, então $-\alpha\leq 0^{\blacklozenge}$. Assim:

$$|-\alpha|\overset{(4.3.10)}{=}-(-\alpha)\overset{(4.3.9)}{=}\alpha$$

e portanto, $|-\alpha|=|\alpha|$.

Se $\alpha<0^{\blacklozenge}$, então $|\alpha|=-\alpha$. Por outro lado $\alpha<0^{\blacklozenge}$, então $-\alpha>0^{\blacklozenge}$. Assim

$$|-\alpha|\overset{(4.3.13)}{=}-\alpha$$

e a igualdade ocorre. ■

4.4 MULTIPLICAÇÃO DE NÚMEROS REAIS

Notação 4.4.1 *Sejam A e B conjuntos de números racionais. Denotamos por $A \cdot B$ o conjunto*

$$A \cdot B = \{a \cdot b \mid a \in A \text{ e } b \in B\}$$

Se $\delta = (D, D^c)$ é um número real positivo, escreveremos $D_+ = D \setminus \mathbb{Q}_-$.

Teorema 4.4.2 *Sejam $\alpha = (A, A^c)$ e $\beta = (B, B^c)$ números reais positivos. Então, o par*

$$\delta = ((A_+ \cdot B_+) \cup \mathbb{Q}_-, ((A_+ \cdot B_+) \cup \mathbb{Q}_-)^c),$$

é um corte, e portanto define um número real, que é chamado de produto dos números reais α e β e é denotado por

$$\delta = \alpha \cdot \beta$$

Demonstração. Parte (1)**:** É claro que $(A_+ \cdot B_+) \cup \mathbb{Q}_- \neq \emptyset$. Agora, se $c \notin A$ e $d \notin B$ então $a < c$ e $b < d$, para todo $a \in A_+$ e $b \in B_+$, respectivamente. Logo, $ab < cd$, para todo $a \in A_+$ e $b \in B_+$; ou seja $cd \notin (A_+ \cdot B_+) \cup \mathbb{Q}_-$. Donde $((A_+ \cdot B_+) \cup \mathbb{Q}_-)^c \neq \emptyset$

Parte (2)**:** É claro que a união do conjunto minorante e do conjunto majorante é $\mathbb{Q}$

Parte (3)**:** Sejam $r \in ((A_+ \cdot B_+) \cup \mathbb{Q}_-)$ e $s \in ((A_+ \cdot B_+) \cup \mathbb{Q}_-)^c$ (lembremos que $((A_+ \cdot B_+) \cup \mathbb{Q}_-)^c = (A_+ \cdot B_+)^c \cap \mathbb{Q}_-^c$) e suponhamos que $s < r = a \cdot b$, com $a \in A_+$ e $b \in B_+$. Então $sb^{-1} < a$ e portanto $sb^{-1} \in A$. Logo $s = (sb^{-1}) \cdot b \in A_+ \cdot B_+$ o que contradiz a hipótese. O caso, $s = r$ está obviamente excluído.

Parte (4)**:**Suponhamos que $m = a_0 b_0$ seja o máximo de $(A_+ \cdot B_+) \cup \mathbb{Q}_-$. Então, $a_0 = b_0 m^{-1}$ é o máximo de A_+; de fato, se $a_0 < a'$, $a' \in A_+$, então $m' = a' b_0 > m = a_0 b_0$, o que contraria a hipótese de que m é o máximo de $(A_+ \cdot B_+) \cup \mathbb{Q}_-$. ■

Definição 4.4.3 *Sejam α e β números reais quaisquer. O **produto** $\alpha \cdot \beta$ de α e β é definido por*

$$\alpha \cdot \beta = \begin{cases} -(|\alpha| \cdot |\beta|) & \text{se } \alpha > 0^\blacklozenge \text{ e } \beta < 0^\blacklozenge \text{ ou } \alpha < 0^\blacklozenge \text{ e } \beta > 0^\blacklozenge; \\ |\alpha| \cdot |\beta| & \text{se } \alpha < 0^\blacklozenge \text{ e } \beta < 0^\blacklozenge \text{ ou } \alpha > 0^\blacklozenge \text{ e } \beta > 0^\blacklozenge; \\ 0 & \text{se } \alpha = 0^\blacklozenge \text{ e } \beta = 0^\blacklozenge. \end{cases}$$

Teorema 4.4.4 ***(Regra de Sinais)*** *Sejam α e β números reais. Então, valem as seguintes propriedades:*

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

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

Demonstração. Parte (1)**:** Consideraremos quatro casos: Se α e β são positivos então $-\alpha$ e $-\beta$ são negativos, e temos

$$(-\alpha)\cdot\beta \overset{(4.4.3)}{=} -(|-\alpha|\cdot|\beta|) \overset{(4.3.13.(2))}{=} -(|\alpha|\cdot|\beta|) \overset{(4.3.12)}{=} -(\alpha\cdot\beta)$$

e

$$\alpha\cdot(-\beta) \overset{(4.4.3)}{=} -(|\alpha|\cdot|-\beta|) \overset{(4.3.13.(2))}{=} -(|\alpha|\cdot|\beta|) \overset{(4.3.12)}{=} -(\alpha\cdot\beta)$$

Se α é positivo e β é negativo então $-\alpha$ é negativo e $-\beta$ é positivo e $-\beta = |\beta|$. Portanto

$$(-\alpha)\cdot\beta \overset{(4.4.3)}{=} |-\alpha|\cdot|\beta| \overset{(4.3.13.(2))}{=} |\alpha|\cdot|\beta| \overset{(4.3.12)}{=} \alpha\cdot(-\beta)$$

e

$$-(\alpha\cdot\beta) \overset{(4.4.3)}{=} -[-(|\alpha|\cdot|\beta|)] \overset{(4.3.9)}{=} |\alpha|\cdot|\beta| \overset{(4.3.12)}{=} \alpha\cdot(-\beta)$$

Se α é negativo e β é positivo então $-\alpha$ é positivo e $-\beta$ é negativo. Assim, $-\alpha = |\alpha|$ e temos

$$\alpha\cdot(-\beta) \overset{(4.4.3)}{=} |\alpha|\cdot|-\beta| \overset{(4.3.13.(2))}{=} |\alpha|\cdot|\beta| \overset{(4.3.12)}{=} (-\alpha)\cdot\beta$$

e

$$-(\alpha\cdot\beta) \overset{(4.4.3)}{=} -[-(|\alpha|\cdot|\beta|)] \overset{(4.3.9)}{=} |\alpha|\cdot|\beta| \overset{(4.3.12)}{=} (-\alpha)\cdot\beta$$

Se α e β são negativos então $-\alpha$ e $-\beta$ são positivos e $-\alpha = |\alpha|$ e $-\beta = |\beta|$, assim

$$-(\alpha\cdot\beta) \overset{(4.4.3)}{=} -(|\alpha|\cdot|\beta|) \overset{(1^o\ \text{Caso})}{=} (-|\alpha|)\cdot|\beta| \overset{(4.3.9)}{=} \alpha\cdot(-\beta)$$

e

$$-(\alpha\cdot\beta) \overset{(4.4.3)}{=} -(|\alpha|\cdot|\beta|) \overset{(1^o\ \text{Caso})}{=} |\alpha|\cdot(-|\beta|) \overset{(4.3.9)}{=} (-\alpha)\cdot\beta$$

Parte (2)**:** Consideraremos quatro casos: Se α e β são positivos então $-\alpha$ e $-\beta$ são negativos, assim

$$(-\alpha)\cdot(-\beta) \overset{(4.4.3)}{=} |-\alpha|\cdot|-\beta| \overset{(4.3.13.(2))}{=} |\alpha|\cdot|\beta| \overset{(4.3.12)}{=} \alpha\cdot\beta$$

Se α é positivo e β é negativo, então $-\beta$ é positivo e $-\beta = |\beta|$, assim

$$(-\alpha)\cdot(-\beta) \overset{(\text{hipótese})}{=} (-\alpha)\cdot|\beta| \overset{(4.4.4.(1))}{=} \alpha\cdot(-|\beta|) \overset{(\text{hipótese})}{=} \alpha\cdot\beta$$

Se α é negativo e β é positivo então $-\alpha$ é positivo e $-\alpha = |\alpha|$ e $-\beta$ é negativo, assim

$$(-\alpha)\cdot(-\beta) = |\alpha|\cdot(-\beta) \overset{(4.4.4.(1))}{=} (-|\alpha|)\cdot\beta \overset{(4.3.9)}{=} \alpha\cdot\beta$$

Se α e β são negativos então $-\alpha$ e $-\beta$ são positivos e $-\alpha = |\alpha|$ e $-\beta = |\beta|$, assim

$$(-\alpha)\cdot(-\beta) \overset{(\text{hipótese})}{=} |\alpha|\cdot(-\beta) \overset{(4.4.4.(1))}{=} (-|\alpha|)\cdot\beta \overset{(\text{hipótese})}{=} \alpha\cdot\beta$$

■

Teorema 4.4.5 *Sejam α, β e γ números reais. Então, as seguintes propriedades são válidas:*

(1) $\alpha\cdot\beta = \beta\cdot\alpha$ (*comutatividade*)

(2) $\alpha\cdot(\beta\cdot\gamma) = (\alpha\cdot\beta)\cdot\gamma$ (*associatividade*)

(3) $\alpha\cdot(\beta+\gamma) = \alpha\cdot\beta + \alpha\cdot\gamma$ (*distributividade a esquerda*)

Demonstração. Parte (1)**:** Pela definição de produto e pela regra de sinais, basta demonstrar (1) no caso em que α e β são positivos. De fato, se $\alpha > 0^{\blacklozenge}$ e $\beta < 0^{\blacklozenge}$, então $\beta = -|\beta|$ e

$$\alpha\cdot\beta = \alpha\cdot(-|\beta|) \overset{(4.4.4.(1))}{=} -(\alpha\cdot|\beta|) \overset{(\text{hipótese})}{=} -(|\beta|\cdot\alpha) = (-|\beta|)\cdot\alpha = \beta\cdot\alpha$$

Os casos $\alpha < 0^{\blacklozenge}, \beta > 0^{\blacklozenge}$ e $\alpha < 0^{\blacklozenge}, \beta < 0^{\blacklozenge}$ são análogos. Então, se $\alpha = (A, A^c)$ e $\beta = (B, B^c)$ são positivos, temos:

$$\begin{aligned}
&\alpha\cdot\beta \overset{(4.4.2)}{=} ((A_+\cdot B_+)\cup\mathbb{Q}_-, ((A_+\cdot B_+)\cup\mathbb{Q}_-)^c)\\
&\overset{(3.3.3.(1))}{=} ((B_+\cdot A_+)\cup\mathbb{Q}_-, ((B_+\cdot A_+)\cup\mathbb{Q}_-)^c)\\
&\overset{(4.4.2)}{=} \beta\cdot\alpha
\end{aligned}$$

Parte (2)**:** Suponhamos α, β e γ positivos, onde $\alpha = (A, A^c)\,, \beta = (B, B^c)$ e $\gamma = (C, C^c)$, temos:

$$\begin{aligned}
&\alpha \cdot (\beta \cdot \gamma) \overset{(hipótese)}{=} (A, A^c) \cdot [(B, B^c) \cdot (C, C^c)] \\
&\overset{(4.4.2)}{=} (A, A^c) \cdot ((B_+ \cdot C_+) \cup \mathbb{Q}_-, ((B_+ \cdot C_+) \cup \mathbb{Q}_-)^c) \\
&\overset{(4.4.2)}{=} (A_+ \cdot (B_+ \cdot C_+) \cup \mathbb{Q}_-, (A_+ \cdot (B_+ \cdot C_+) \cup \mathbb{Q}_-)^c) \\
&\overset{(3.3.3.2)}{=} ((A_+ \cdot B_+) \cdot C_+ \cup \mathbb{Q}_-, ((A_+ \cdot B_+) \cdot C_+ \cup \mathbb{Q}_-)^c) \\
&\overset{(4.4.2)}{=} ((A_+ \cdot B_+) \cup \mathbb{Q}_-, ((A_+ \cdot B_+) \cup \mathbb{Q}_-)^c) \cdot (C, C^c) \\
&\overset{(4.4.2)}{=} [(A, A^c) \cdot (B, B^c)] \cdot (C, C^c) \\
&\overset{(hipótese)}{=} (\alpha \cdot \beta) \cdot \gamma
\end{aligned}$$

No caso em que um ou dois ou os três termos são negativos, basta escreve-lo na forma $-|\cdot|$, usar a Regra de Sinais e o caso positivo.

Parte (3)**:**Suponhamos α, β e γ positivos, onde $\alpha = (A, A^c)\,, \beta = (B, B^c)$ e $\gamma = (C, C^c)$, temos:

$$\begin{aligned}
&\alpha \cdot (\beta + \gamma) \overset{(4.3.2)}{=} (A, A^c) \cdot (B + C, (B + C)^c) \\
&\overset{(4.4.2)}{=} (A_+ (B_+ + C_+) \cup \mathbb{Q}_-, (A_+ (B_+ + C_+) \cup \mathbb{Q}_-)^c) \\
&\overset{(3.3.3.(3))}{=} ((A_+B_+ + A_+C_+) \cup \mathbb{Q}_-, ((A_+B_+ + A_+C_+) \cup \mathbb{Q}_-)^c) \\
&\overset{(4.3.2)}{=} (((A_+B_+) \cup \mathbb{Q}_-) + ((A_+C_+) \cup \mathbb{Q}_-)\,, (((A_+B_+) \cup \mathbb{Q}_-) + ((A_+C_+) \cup \mathbb{Q}_-))^c) \\
&\overset{(4.3.2)}{=} (A, A^c) \cdot (B, B^c) + (A, A^c) \cdot (C, C^c) \\
&\overset{(hipótese)}{=} \alpha \cdot \beta + \alpha \cdot \gamma
\end{aligned}$$

Se α é negativo e β e γ são positivos, segue do caso positivo e da Regra de Sinais. Se α é positivo ou negativo e β e γ são negativos temos $\beta + \gamma = -(|\beta| + |\gamma|)$ e a propriedade distributiva segue novamente da Regra de Sinais e do caso positivo. Os outros casos podem ser reduzidos ao caso em que $\alpha \cdot (\beta - \gamma) = \alpha \cdot \beta - \alpha \cdot \gamma$, onde α, β e γ são positivos e ainda $\beta > \gamma$. Neste caso, vamos ter

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

e somando $-(\alpha \cdot \gamma)$ em ambos os membros obtemos

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

A demonstração está completa. ■

Teorema 4.4.6 *Sejam α, β e γ números reais. Então, valem as seguintes propriedades:*

(1) $\alpha > 0^{\blacklozenge}$ e $\beta > 0^{\blacklozenge} \Rightarrow \alpha \cdot \beta > 0^{\blacklozenge}$;

(2) $\alpha \cdot \beta = 0^{\blacklozenge} \Rightarrow \alpha = 0^{\blacklozenge}$ ou $\beta = 0^{\blacklozenge}$;

(3) $\alpha < \beta$ e $\gamma > 0^{\blacklozenge} \Rightarrow \alpha \cdot \gamma < \beta \cdot \gamma$;

(4) $\alpha < \beta$ e $\gamma < 0^{\blacklozenge} \Rightarrow \alpha \cdot \gamma > \beta \cdot \gamma$;

Demonstração. Parte (1)**:** Sejam $\alpha = (A, A^c), \beta = (B, B^c)$ e $0^{\blacklozenge} = \left(\mathbb{Q}_-, \mathbb{Q}_-^c\right)$números reais tais que $\alpha > 0^{\blacklozenge}$ e $\beta > 0^{\blacklozenge}$. Então, por (4.2.2. (2)) $A \supsetneq \mathbb{Q}_-$ e $B \supsetneq \mathbb{Q}_-$, isto é, existem $a \in A_+$ e $b \in B_+$, tais que $a \cdot b \in A_+ \cdot B_+$. Assim, $A_+ \cdot B_+ \cup \mathbb{Q}_- \supsetneq \mathbb{Q}_-$ e portanto por (4.2.2. (2))

$$\alpha \cdot \beta = (A, A^c) \cdot (B, B^c) \overset{(4.4.2)}{=} (A_+ \cdot B_+ \cup \mathbb{Q}_-, (A_+ \cdot B_+ \cup \mathbb{Q}_-)^c) > 0^{\blacklozenge}$$

Parte (2)**:** Suponhamos $\alpha \neq 0^{\blacklozenge}$ e $\beta \neq 0^{\blacklozenge}$. Então temos que considerar quatro casos:

a) Se $\alpha > 0^{\blacklozenge}$ e $\beta > 0^{\blacklozenge}$, então

$$\alpha \cdot \beta > 0^{\blacklozenge}$$

o que contraria a hipótese.

b) Se $\alpha > 0^{\blacklozenge}$ e $\beta < 0^{\blacklozenge}$ então $\alpha > 0^{\blacklozenge}$ e $-\beta > 0^{\blacklozenge}$, logo

$$\alpha \cdot (-\beta) > 0^{\blacklozenge}$$

o que implica

$$\alpha \cdot \beta < 0^{\blacklozenge}$$

contrariando a hipótese.

c) Se $\alpha < 0^{\blacklozenge}$ e $\beta > 0^{\blacklozenge}$ então $-\alpha > 0^{\blacklozenge}$ e $\beta > 0^{\blacklozenge}$, logo

$$(-\alpha) \cdot \beta > 0^{\blacklozenge}$$

o que implica

$$\alpha \cdot \beta < 0^{\blacklozenge}$$

contrariando a hipótese.

d) Se $\alpha < 0^\blacklozenge$ e $\beta < 0^\blacklozenge$ então $-\alpha > 0^\blacklozenge$ e $-\beta > 0^\blacklozenge$, logo

$$(-\alpha)\cdot(-\beta) > 0^\blacklozenge$$

o que implica

$$\alpha\cdot\beta > 0^\blacklozenge$$

contrariando a hipótese.

Parte (3)**:** Temos por hipótese que $\begin{cases} \alpha < \beta \overset{(4.3.6)}{\Rightarrow} \beta - \alpha > 0^\blacklozenge \\ \gamma > 0^\blacklozenge \end{cases}$, logo:

$$\gamma\cdot(\beta-\alpha) > 0^\blacklozenge \overset{(4.4.5.(3))}{\Rightarrow} \gamma\cdot\beta - \gamma\cdot\alpha > 0^\blacklozenge \overset{(4.3.6)}{\Rightarrow} \gamma\cdot\beta > \gamma\cdot\alpha$$

ou seja, $\alpha\cdot\gamma < \beta\cdot\gamma$.

Parte (4)**:** Temos por hipótese que $\begin{cases} \alpha < \beta \overset{(4.3.6)}{\Rightarrow} \beta - \alpha > 0^\blacklozenge \\ \gamma < 0^\blacklozenge \overset{(4.2.11.(2))}{\Rightarrow} -\gamma > 0^\blacklozenge \end{cases}$, logo:

$$-\gamma\cdot(\beta-\alpha) > 0^\blacklozenge \overset{(4.4.5.(3))}{\Rightarrow} -\gamma\cdot\beta + \gamma\cdot\alpha > 0^\blacklozenge \overset{(4.3.6)}{\Rightarrow} \gamma\cdot\alpha > \gamma\cdot\beta$$

ou seja, $\alpha\cdot\gamma > \beta\cdot\gamma$. ■

4.5 OS RACIONAIS COMO SUBCONJUNTO DOS REAIS

Indicaremos por $\breve{\mathbb{Q}}$ o **conjunto dos números reais racionais**, isto é,

$$\breve{\mathbb{Q}} = \left\{ r^\blacklozenge \mid r \in \mathbb{Q} \right\},$$

onde $r^\blacklozenge = (A_r, B_r)$, com

$$A_r = \{x \in \mathbb{Q} \mid x < r\}$$

e

$$B_r = \{x \in \mathbb{Q} \mid x \geq r\}$$

Lema 4.5.1 *Se r e s são números racionais, então:*

(1) $r^\blacklozenge > 0^\blacklozenge \Leftrightarrow r > 0$

(2) $-r^\blacklozenge = (-r)^\blacklozenge$

(3) $r^{\blacklozenge} < 0^{\blacklozenge} \Leftrightarrow r < 0$

(4) $r^{\blacklozenge} + s^{\blacklozenge} = (r+s)^{\blacklozenge}$

(5) $r^{\blacklozenge} \cdot s^{\blacklozenge} = (r \cdot s)^{\blacklozenge}$

Demonstração. Parte (1)**:** Sejam $r^{\blacklozenge} = (A_r, A_r^c)$ e $0^{\blacklozenge} = \left(\mathbb{Q}_-, \mathbb{Q}_-^c\right)$. Então, temos: $r^{\blacklozenge} > 0^{\blacklozenge}$, ou seja

$$\begin{array}{rcl} r^{\blacklozenge} & > & 0^{\blacklozenge} \Leftrightarrow (A_r, A_r^c) > \left(\mathbb{Q}_-, \mathbb{Q}_-^c\right) \overset{(4.2.2.(2))}{\Leftrightarrow} A_r \supsetneq \mathbb{Q}_- \\ & \Leftrightarrow & \exists x \in A_r \mid x \geq 0 \Leftrightarrow 0 \leq x < r \Leftrightarrow r > 0 \end{array}$$

Parte (2)**:** Sejam $r^{\blacklozenge} = (A_r, A_r^c)$ e $(-r)^{\blacklozenge} = \left(A_{-r}, A_{-r}^c\right)$. Como $-r^{\blacklozenge} = \left(-\left(A_r^c\right)', -\left(A_r\right)''\right)$, para mostramos

$$-r^{\blacklozenge} = (-r)^{\blacklozenge}$$

basta verificarmos que

$$-\left(A_r^c\right)' = A_{-r}$$

Temos que

$$\left(A_r^c\right)' = A_r^c - \{\min A_r^c\} = A_r^c - \{r\} = \{x \in \mathbb{Q} \,|x > r\}$$

Logo

$$-\left(A_r^c\right)' = \left\{-x \mid x \in \left(A_r^c\right)'\right\} = \{-x \mid -x < -r\} = A_{-r}$$

Parte (3)**:** Isto resulta das equivalências:

$$r^{\blacklozenge} < 0^{\blacklozenge} \overset{(4.2.11.(2))}{\Leftrightarrow} -r^{\blacklozenge} > 0^{\blacklozenge} \overset{(4.5.1.(2))}{\Leftrightarrow} (-r)^{\blacklozenge} > 0^{\blacklozenge} \overset{(4.5.1.(1))}{\Leftrightarrow} -r > 0 \overset{(3.4.8.(2))}{\Leftrightarrow} r < 0$$

Parte (4)**:** Como $r^{\blacklozenge} = (A_r, A_r^c)$ e $s^{\blacklozenge} = (A_s, A_s^c)$, onde $A_r = \{x \in \mathbb{Q} \,|x < r\}$ e $A_s = \{x \in \mathbb{Q} \,|x < s\}$, para mostramos

$$r^{\blacklozenge} + s^{\blacklozenge} = (r+s)^{\blacklozenge}$$

basta verificarmos que

$$A_r + A_s = A_{r+s}$$

Para isso, precisamos provar que $A_r + A_s \subset A_{r+s}$ e $A_{r+s} \subset A_r + A_s$

Suponhamos inicialmente $x \in A_r + A_s$, então

$$x = a + b$$

para algum $a < r$ e algum $b < s$, com a e b racionais.

$$\left.\begin{array}{c} x = a + b \\ a < r \\ b < s \end{array}\right\} \Rightarrow x < r + s \Rightarrow x \in A_{r+s}$$

logo,

$$A_r + A_s \subset A_{r+s}$$

Suponhamos agora, $x \in A_{r+s}$, então

$$x < r + s$$

logo

$$x - r < s$$

Tomemos um rac ional u, com

$$x - r < u < s$$

Então

$$u < s \Rightarrow u \in A_s$$

e

$$x - r < u \Rightarrow x - u < r \Rightarrow x - u \in A_r$$

donde segue que

$$x = (x - u) + u, \text{ com } x - u \in A_r \text{ e } u \in A_s$$

Assim, $x \in A_r + A_s$ e portanto

$$A_{r+s} \subset A_r + A_s$$

Parte (5)**:**Considerando $r^{\blacklozenge} = (A_r, A_r^c)$, $s^{\blacklozenge} = (A_s, A_s^c)$ e $(r \cdot s)^{\blacklozenge} = (A_{r \cdot s}, A_{r \cdot s}^c)$, para mostrarmos que

$$r^{\blacklozenge} \cdot s^{\blacklozenge} = (r \cdot s)^{\blacklozenge}$$

vamos considerar quatro casos:

a) Se $r^{\blacklozenge} > 0^{\blacklozenge}$ e $s^{\blacklozenge} > 0^{\blacklozenge}$, temos

$$r^{\blacklozenge} \cdot s^{\blacklozenge} = (A_r, A_r^c) \cdot (A_s, A_s^c) = \Big(\big((A_r)_+ \cdot (A_s)_+\big) \cup \mathbb{Q}_-, \big(\big((A_r)_+ \cdot (A_s)_+\big) \cup \mathbb{Q}_-\big)^c\Big)$$

logo basta mostrarmos que

$$\big((A_r)_+ \cdot (A_s)_+\big) \cup \mathbb{Q}_- = A_{r\cdot s}$$

Para isso, precisamos provar que $\big((A_r)_+ \cdot (A_s)_+\big) \cup \mathbb{Q}_- \subset A_{r\cdot s}$ e $A_{r\cdot s} \subset \big((A_r)_+ \cdot (A_s)_+\big) \cup \mathbb{Q}_-$

($\subset$)Pela hipótese e por (4.5.1. (1)) temos que $r > 0$ e $s > 0$. Logo por (3.4.6. (2))

$$r \cdot s > 0$$

e isso implica

$$(r \cdot s)^{\blacklozenge} > 0$$

acarretando que

$$A_{r\cdot s} \supsetneq \mathbb{Q}_-$$

Suponhamos agora $x \in \big((A_r)_+ \cdot (A_s)_+\big)$, então

$$x = a \cdot b$$

para algum $0 \leq a < r$ e algum $0 \leq b < s$, com a e b racionais.

$$\left.\begin{array}{c} x = a \cdot b \\ a < r \\ b < s \end{array}\right\} \Rightarrow x < r \cdot s \Rightarrow x \in A_{r\cdot s}$$

logo,

$$(A_r)_+ \cdot (A_s)_+ \subset A_{r\cdot s}$$

Portanto

$$\big((A_r)_+ \cdot (A_s)_+\big) \cup \mathbb{Q}_- \subset A_{r\cdot s}$$

($\supset$) Temos

$$A_{r\cdot s} = (A_{r\cdot s})_+ \cup \mathbb{Q}_-$$

Se $x \in \mathbb{Q}_-$ é óbvio que $x \in \left((A_r)_+ \cdot (A_s)_+\right) \cup \mathbb{Q}_-$.
Suponhamos agora $x \in (A_{r\cdot s})_+$, logo

$$0 \leq x < r \cdot s$$

com $r > 0$ e $s > 0$. Assim

$$0 \leq \frac{x}{r} < s$$

Tomemos um racional $m > 0$, com

$$0 \leq \frac{x}{r} < m < s$$

Como,

$$0 < m < s \Rightarrow m \in (A_s)_+$$

e

$$\frac{x}{r} < m \Rightarrow 0 \leq \frac{x}{m} < r \Rightarrow \frac{x}{m} \in (A_r)_+$$

então

$$x = \frac{x}{m} \cdot m, \text{ com } \frac{x}{m} \in (A_r)_+ \text{ e } m \in (A_s)_+$$

isto é,

$$x \in (A_r)_+ \cdot (A_s)_+$$

o que mostra a inclusão

$$(A_{r\cdot s})_+ \subset (A_r)_+ \cdot (A_s)_+$$

Portanto

$$A_{r\cdot s} \subset \left((A_r)_+ \cdot (A_s)_+\right) \cup \mathbb{Q}_-$$

b) Se $r^\blacklozenge > 0^\blacklozenge$ e $s^\blacklozenge < 0^\blacklozenge$, temos $r > 0$ e $s < 0$, logo

$$\begin{aligned} r^\blacklozenge \cdot s^\blacklozenge &\overset{(4.4.3)}{=} -\left(\left|r^\blacklozenge\right| \cdot \left|s^\blacklozenge\right|\right) \overset{(4.3.12)}{=} -\left(r^\blacklozenge \cdot \left(-s^\blacklozenge\right)\right) \\ &\overset{(4.5.1.(2))}{=} -\left(r^\blacklozenge \cdot (-s)^\blacklozenge\right) \overset{\text{(Caso a)}}{=} -(r \cdot (-s))^\blacklozenge \\ &\overset{(3.3.6.(1))}{=} -(-(r \cdot s))^\blacklozenge \overset{(4.5.1.(2))}{=} (r \cdot s)^\blacklozenge \end{aligned}$$

c) Se $r^{\blacklozenge} < 0^{\blacklozenge}$ e $s^{\blacklozenge} > 0^{\blacklozenge}$, temos $r < 0$ e $s > 0$, assim

$$\begin{aligned} r^{\blacklozenge} \cdot s^{\blacklozenge} &\overset{(4.4.3)}{=} -\left(\left|r^{\blacklozenge}\right| \cdot \left|s^{\blacklozenge}\right|\right) \overset{(4.3.12)}{=} -\left(\left(-r^{\blacklozenge}\right) \cdot s^{\blacklozenge}\right) \\ &\overset{(4.5.1.(2))}{=} -\left((-r)^{\blacklozenge} \cdot s^{\blacklozenge}\right) \overset{\text{(Caso a)}}{=} -\left((-r) \cdot s\right)^{\blacklozenge} \\ &\overset{(3.3.6.(1))}{=} -\left(-\left(r \cdot s\right)\right)^{\blacklozenge} \overset{(4.5.1.(2))}{=} \left(r \cdot s\right)^{\blacklozenge} \end{aligned}$$

d) Se $r^{\blacklozenge} < 0^{\blacklozenge}$ e $s^{\blacklozenge} < 0^{\blacklozenge}$, temos $r < 0$ e $s < 0$, e portanto

$$\begin{aligned} r^{\blacklozenge} \cdot s^{\blacklozenge} &\overset{(4.4.3)}{=} \left|r^{\blacklozenge}\right| \cdot \left|s^{\blacklozenge}\right| \overset{(4.3.12)}{=} \left(-r^{\blacklozenge}\right) \cdot \left(-s^{\blacklozenge}\right) \\ &\overset{(4.5.1.(2))}{=} (-r)^{\blacklozenge} \cdot (-s)^{\blacklozenge} \overset{\text{(Caso a)}}{=} \left((-r) \cdot (-s)\right)^{\blacklozenge} \\ &\overset{(3.3.6.(3))}{=} \left(r \cdot s\right)^{\blacklozenge} \end{aligned}$$

■

Teorema 4.5.2 *A aplicação*

$$\varphi : \mathbb{Q} \to \breve{\mathbb{Q}}$$

dada por $\varphi(r) = r^{\blacklozenge}$ *é bijetora e tem as seguintes propriedades:*

(1) $\varphi(r+s) = \varphi(r) + \varphi(s)\,,\ \forall\ r, s \in \mathbb{Q}$

(2) $\varphi(r \cdot s) = \varphi(r) \cdot \varphi(r)\,,\ \ \forall r, s \in \mathbb{Q}$

(3) $r \leq s \Leftrightarrow \varphi(r) \leq \varphi(s)\,,\ \forall r, s \in \mathbb{Q}$

Tal aplicação φ nos perminte, então, identicar o racional r com o real $r^{\blacklozenge}$. Neste sentido, podemos olhar para $\mathbb{Q}$ como subconjunto de $\mathbb{R}$.

Demonstração. A demonstração de que a aplicação φ é bijetora não apresenta dificuldades.

Parte (1)**:**

$$\varphi(r+s) \overset{(4.5.2.(1))}{=} (r+s)^{\blacklozenge} \overset{(4.5.1.(1))}{=} r^{\blacklozenge} + s^{\blacklozenge} \overset{(4.5.2.(1))}{=} \varphi(r) + \varphi(s)$$

Parte (2)**:**

$$\varphi(r \cdot s) \overset{(4.5.2.(1))}{=} (r \cdot s)^{\blacklozenge} \overset{(4.5.1.(2))}{=} r^{\blacklozenge} \cdot s^{\blacklozenge} \overset{(4.5.2.(1))}{=} \varphi(r) \cdot \varphi(s)$$

Parte (3)**:**Considarando $r^{\blacklozenge} = (A_r, B_r)$ e $s^{\blacklozenge} = (A_s, B_s)$, para mostrarmos que:

$$r \leq s \Leftrightarrow r^{\blacklozenge} \leq s^{\blacklozenge}$$

basta mostrarmos a equivalência

$$r \leq s \Leftrightarrow A_r \subset A_s$$

($\Rightarrow$) Suponhamos $x \in A_r$, então $x < r$. Como por hipótese $r \leq s$, temos $x \in A_s$ e portanto $A_r \subset A_s$.

($\Leftarrow$) Suponhamos que $A_r \subset A_s$ com $s < r$. Então, $s \in A_r$, donde $s \in A_s$, isto é, $s < s$, uma contradição. Portanto $r \leq s$. ■