Universidade Federal do Piauí - UFPI

Departamento de Matemática

Programa de Pós-Graduação em Matemática Profissional

A construção dos Números Inteiros e Racionais pelo Método da Simetrização e Aplicações

Vivian Maria Barbosa Saraiva Cipriano

Teresina
2016

Vivian Maria Barbosa Saraiva Cipriano

Dissertação de Mestrado:

A construção dos Números Inteiros e Racionais pelo Método da Simetrização e Aplicações

Trabalho de Dissertação para a defesa de título de Mestre em Matemática pela Universidade Federal do Piauí (UFPI).

Orientador: Prof. Dr. Roger Peres de Moura

Teresina
2016

FICHA CATALOGRÁFICA
Serviço de Processamento Técnico da Universidade Federal do Piauí
Biblioteca Setorial do CCN

C577c Cipriano, Vivian Maria Barbosa Saraiva.
A construção dos números inteiros e racionais pelo método da simetrização e aplicações / Vivian Maria Barbosa Sariava Cipriano. – Teresina: 2016.
101f. il.

Dissertação (Mestrado Profissional) – Universidade Federal do Piauí, Centro de Ciências da Natureza, Pós-Graduação em Matemática, 2016.
Orientador: Prof. Dr. Roger Peres de Moura.

1. Matemática – Estudo e Ensino. 2. Matemática – Didática. I. Título

CDD 510.7

Vivian Maria Barbosa Saraiva Cipriano

A construção dos Números Inteiros e Racionais pelo Método da Simetrização e Aplicações

Trabalho de Dissertação para a defesa de título de Mestre em Matemática pela Universidade Federal do Piauí (UFPI).

Trabalho aprovado. Teresina, 26 de agosto de 2016:

Roger Peres de Moura

Prof. Dr. Roger Peres de Moura
Orientador

Liane Mendes Feitosa Soares

Profª. Dra. Liane Mendes Feitosa Soares (UFPI)
Examinador Interno

Walter Araújo Rocha Júnior

Prof. Ms. Walter Araújo Rocha Júnior (IFMA)
Examinador Externo

Teresina
2016

Agradecimentos

Agradeço primeiramente à Deus, pois sem ele nada é possível.

Agradeço a meus pais, Raimundo e Beronisa, pelo amor incondicional, por terem me educado tão bem e por sempre me incentivarem a perseguir meus sonhos.

Aos meus irmãos, Vanessa e Gustavo, por estarem sempre do meu lado e à Alzenir pelas palavras de incentivo.

À minha tia/amiga Nádya, pela acolhida e os momentos de descontração.

Ao meu noivo Diego, meu companheiro, por ter me dado todo suporte necessário para essa conquista, por sua imensurável paciência e seu carinho.

Aos meus colegas de mestrado, pela parceria nos estudos e pela força nos momentos difíceis do curso.

Aos meus professores do PROFMAT pelos ensinamentos em especial ao Professor Roger Moura que tão bem me orientou na realização deste trabalho.

À CAPES pelo apoio financeiro que viabilizou o meu deslocamento à Teresina afim de participar do PROFMAT.

Existe um paralelismo fiel entre o progresso social e a atividade matemática, os países socialmente atrasados são aqueles em que a atividade matemática é nula ou quase nula.
(Jacques Chapellon)

Resumo

Este trabalho apresenta a construção do conjunto dos números Inteiros e dos números Racionais pelo método da simetrização, popularizado pelo filósofo matemático Bertrand Russell, tomando como base o conjunto dos números Naturais. Apresenta também algumas aplicações desses conjuntos numéricos. Sobre números naturais consideramos o método de demonstração por indução finita e a notação de somatório e produtório. Como aplicação dos Inteiros exibimos os seguintes tópicos básicos da teoria elementar dos números: divisibilidade, congruência, números primos e um estudo sobre a mudança de base de um sistema de numeração. Como complemento do estudo dos Racionais são apresentados os conceitos de valor absoluto e de mudança de base de um sistema de numeração para esse conjunto. O objetivo principal é disponibilizar a alunos e professores de Matemática um material simples de entender, sem abrir mão do rigor matemático, que possa levar a uma real compreensão do conceito de número.

Palavras-chave: Números Naturais. Números Inteiros. Números Racionais.

Abstract

This work presents the construction of the set of integer numbers and Rational Numbers by the method of symmetrization, popularized by the mathematician philosopher Bertrand Russelll, based on the set of natural numbers. It also presents some applications of these numerical sets. About natural numbers we consider the demonstration method of finite induction and notation sum and productory operator. As application of the integers we show the following basic topics from the elementary number theory: divisibility, congruence, primes and a study on the basis change for a numbering system. As rational study are presented concepts complement absolute value and a base change numbering system for that set. The main purpose is to provide for mathematics students and teachers a simple material to understand, without giving up mathematical rigor, which can lead to a real understanding of the number concept.

Keywords: Natural Numbers. Integers Numbers. Rational numbers.

Lista de ilustrações

Sumário

1 Introdução

Na história da civilização humana, o surgimento da noção de contagem está atrelada ao momento em que o homem deixou de puramente primitivo e passou a desenvolver atividades racionalizadas como domesticar animais, cultivar alimento ou construir moradias. Para ter controle sobre o seu rebanho, por exemplo, o homem fazia correspondências biunívocas entre os animais e outros objetos. Guardar pedrinhas em sacos de couro, entalhar marcas em ossos, fazer nós em cordas eram algumas das formas com que eles administravam quantidades.

> Tudo começou com este artifício conhecido como *correspondência um a um*, que confere, mesmos aos espíritos mais desprovidos, a possibilidade de comparar com facilidade duas coleções de seres ou de objetos, da mesma natureza ou não, sem ter de recorrer à contagem abstrata. Mas este artifício do espírito não oferece apenas um meio de estabelecer uma comparação entre dois grupos: *ele permite também abarcar vários números sem contar nem mesmo nomear ou conhecer as quantidades envolvidas.* (IFRAH, 2005)

Mais tarde, com o progresso de tais atividades aliadas a relações sociais cada vez mais fortes, foi preciso que estas medidas fossem representadas de maneira a serem compreendidas por todos os indivíduos de uma mesma comunidade. Assim, começaram a surgir representações abstratas de número elaboradas por diferentes povos ao redor do mundo, de acordo com suas vivências e suas escritas. Os mais conhecidos são os sistemas de numeração egípcio, romano, babilônico, chinês e indo-arábico.

Os egípicios desenvolveram uma representação numérica com base em sua escrita hieroglífica. A numeração egípcia foi criada há cerca de 5.000 anos e usava símbolos diferentes para expoentes de 10 como representados na Figura 1. Esse sistema, tinha uma base decimal, não posicional e sua escrita baseava-se na adição dos valores dos símbolos. Assim, o número 1435 era representado por uma 'flor de lótus', quatro 'cordas enroladas', três 'cunhas' e cinco 'bastões', um excesso de símbolos que dificultava a comunicação.

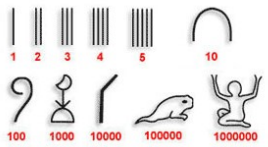

Figura 1 – Sistema de Numeração Egípcio

Já o sistema de numeração desenvolvido pelos babilônios, de escrita cuneiforme, era sexagesimal, ou seja, de base 60 e de representação bem simples, uma vez que utilizava apenas dois símbolos, como podemos ver na Figura 2. Ainda é utilizado, em no nosso dia

a dia, a notação sexagesimal na medição do tempo ou de ângulos de uma circunferência por exemplo.

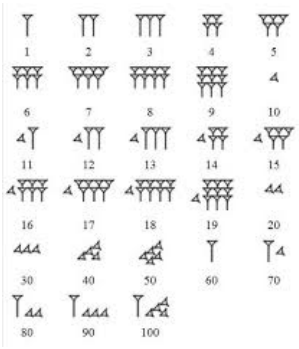

Figura 2 – Sistema de Numeração Babilônico

O sistema mais utilizado atualmente é o Sistema de Numeração Indo-Arábico, assim chamado por ter sido desenvolvidos pelos hindus e divulgado por povos árabes. Esse sistema é decimal e posicional e os símbolos evoluíram com o tempo e em diferentes regiões do mundo conforme podemos ver na Figura 3. Segundo Garbi (2006) foi Leonardo Fibonacci (1175 − 1250) quem difundiu para a Europa o sistema indo-arábico quando publicou a sua mais importante obra o Liber Abaci em 1202. Apesar de haver indícios de que o zero já era conhecido pelos gregos e mesopotâmios, foi somente neste sistema que ele ganhou status de número e fora lhe dado um símbolo (0). Antes disso, os demais sistemas apenas utilizavam espaços vazios para simbolizar a 'falta'.

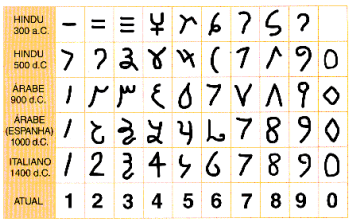

Figura 3 – Sistema de Numeração Indo-Arábico

Os primeiros conjuntos númericos criados fazem parte do que hoje chamamos de Conjunto dos Números Naturais, representados por $\mathbb{N}$. A formalização desse conjunto foi proposta em 1888 pelo matemático alemão Richard Dedekind (1831-1916). Em 1889, o matemática italiano Giuseppe Peano publicou um livro intitulado Arithmetices Principia: Nova Methodo Exposita, em que sistematizava um conjunto de axiomas que são usados até hoje na construção formal dos naturais, os Axiomas de Peano. Apesar desses axiomas já serem conhecidos por Dedekind, Lima (2013b) nos diz que, ao que tudo indica, Peano trabalhou independentemente.

Os naturais foram criados com o propósito de representar o resultado de contagens, e assim, com o passar do tempo, e principalmente com o avanço das relações comerciais,

tornou-se um conjunto muito limitado. De acordo com Domingues (1991) "Coube aos hindus a introdução na matemática dos números negativos. O objetivo era indicar débitos". Daí surge a necessidade de construir uma ampliação mínima de $\mathbb{N}$ que incluíssem os negativos. Este conjunto foi chamado de Números Inteiros e representados pela letra $\mathbb{Z}$ inicial de 'Zahl' número em alemão.

Depois de contruído $\mathbb{Z}$, surge a necessidade de amplicação desse conjunto, visto que equações do tipo $a \cdot x = b$ têm soluções em $\mathbb{Z}$ se, e somente se, a é um divisor de b. Nasce então o conjunto dos números Racionais, representados pela letra $\mathbb{Q}$, da palavra 'quotiens' que em latim significa 'quantas vezes' como números que representam partes de um inteiro. É preciso esclarecer que a ordem cronológica de surgimento desses conjuntos não é exatamente Naturais, Inteiros e Racionais, isso porque os números negativos levaram mais tempo para serem aceitos pelos matemáticos. Já as frações são conhecidas desde o Egito antigo quando eram utilizadas na demarcação de terras das margens do Rio Nilo. Segundo Boyer (2003) os egípcios utilizavam cordas com uma unidade de medida feita nela para fazerem essas medições verificando quantas vezes aquela unidade de medida estava contida nos lados do terreno. Porém, às vezes, os 'esticadores de corda' como eram chamados, não encontravam um número inteiro de vezes em que as cordas eram estiradas. A saída encontrada foi trabalhar com subdivisões dessas unidades de medida. Nascia assim os números fracionários.

Temos como propósito neste trabalho, dissertar sobre a construção formal dos números inteiros e racionais pelo método da simetrização e apresentar algumas aplicações. Esse método consiste na construção feita a partir dos números naturais que por sua vez é construído por base axiomática. Foi Bertrand Russell $(1872 - 1970)$ quem introduziu essa construção dos números em sua célebre obra de três volumes Principia Mathematica publicadas nos anos de 1910, 1912 e 1913 cuja página de rosto podemos ver na Figura 4. O 'Principia' foi escrito juntamente com o filósofo e matemático britânico Alfred North Whitehead $(1861 - 1947)$. Em 1919 foi publicado o livro 'Introdução à Filosofia Matemática', de Russell, com o objetivo de divulgar as ideias do Principia Mathematica uma vez que foi escrito numa abordagem menos técnica e linguagem mais acessível.

O trabalho está organizado em 5 capítulos da seguinte forma. No capítulo 2, abordamos os tópicos que dão suporte aos capítulos subsequentes a saber: os conceito de relações binárias, relações de equivalência, relação de ordem e o conceito de função. Além disso, demonstramos teoremas acerca desses conceitos, postulamos propriedades e exemplificamos para melhor entendimento.

No capítulo 3, fazemos a construção axiomática do conjunto dos números naturais através da Teoria dos Números Cardinais. Essa construção foi idealizada por Russell e Whitehead com base nos Axiomas de Peano. Para embasar a construção, descreveremos os conceitos e propriedades referentes ao estudo dos Monóides. Além disso, faremos a aplicação deste na notação de Somatório e Produtório e na Demonstração por Indução

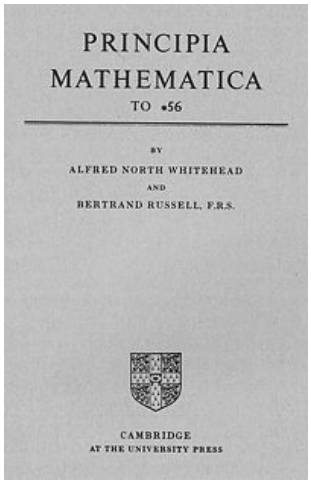

Figura 4 – Principia Mathematica

Finita. É importante ressaltar que neste trabalho, o Princípio da Indução Finita não foi descrito como axioma, tal qual fez Peano. Utilizamos como axioma o Princípio da Boa Ordenação por entender que ele é mais natural e aceitável que o axioma da indução. Nas palavras de Russell (2006):

> A noção de ordem tem uma importância enorme em matemática. Não apenas os inteiros, mas também os números racionais e os números reais possuem uma ordem de grandeza, e isto é essencial à maior parte das suas propriedades matemáticas.[...] Há partes da matemática que não dependem da noção de ordem, mas são pouquíssimas em comparação com as partes em que está envolvida esta noção.

No capítulo 4, procedemos com a construção dos números inteiros pelo método da simetrização da adição definida sobre $\mathbb{N}$. Esse processo foi descrito pela primeira vez por Richard Dedekind quando estabeleceu uma relação de equivalência entre pares ordenados de números naturais e descreveu os inteiros como o conjunto das classes de equivalência dessa relação. Feito isso, prosseguimos com a alicação ao estudo da divisibilidade e números primos, congruência e a mudança de base de um sistema de numeração.

E finalmente, no capítulo 5, faremos a construção do conjunto dos números racionais tomando como base o estudo da estrutura de anel e utilizando o mesmo raciocínio da construção dos inteiros. Ao fim do capítulo, aplicamos ao estudo da mudança de base para números racionais e no estudo do valor absoluto.

O objetivo deste trabalho é apresentar um material que apresente com clareza e simplicidade, sem desconsiderar o rigor matemático, a construção formal dos inteiros e racionais. Seu público alvo são alunos de graduação e professores de matemática, uma vez que a leitura do material pressupõe alguns conhecimentos prévios.

2 Relações Binárias e Funções

Neste capítulo apresentaremos os principais pré-requisitos dos assuntos a serem desenvolvidos no decorrer do trabalho. Começaremos com a definição de relações binárias e seus principais resultados para em seguida apresentarmos os importantes conceitos de relação de equivalência, relação de ordem e por último, o de função.

2.1 Definições Básicas.

Definição 1 *Sejam A e B conjuntos não-vazios arbitrários.*
(a) *Um* ***par ordenado*** *é um par de elementos (a, b), onde $a \in A$ e $b \in B$, que são escolhidos sempre nessa ordem. Dizemos que dois pares ordenados (a, b) e (c, d) são iguais se, e somente se, $a = c$ e $b = d$. Neste caso, escrevemos $(a, b) = (c, d)$. Graficamente, um par ordenado é representado por um ponto num plano.*
(b) *O* ***produto cartesiano*** *de A por B, indicado por $A \times B$, é o conjunto de todos os pares ordenados (a, b), com $a \in A$ e $b \in B$. Na notação de conjuntos,*

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

Observação 1 *Num conjunto de dois elementos, não importa a ordem desses elementos. Mas há vários conceitos Matemáticos, a de pares ordenados por exemplo, em que a ordem dos elementos é fundamental.*

Exemplo 2.1.1 *O produto cartesiano de $A = \{\, 1, 2, 3\,\}$ por $B = \{\, 2, 3\,\}$ é o conjunto $A \times B = \{(1, 2), (1, 3), (2, 2), (2, 3), (3, 2), (3, 3)\,\}$ representado graficamente abaixo.*

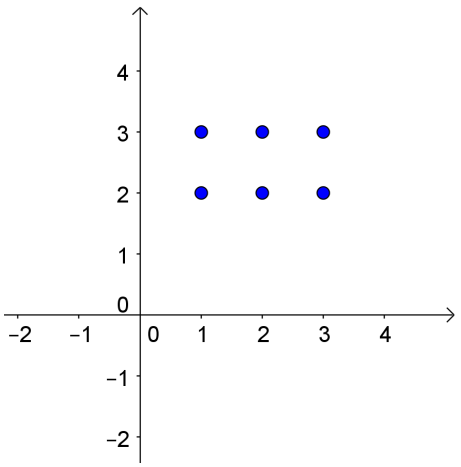

Figura 5 – Produto Cartesiano de $A = \{\, 1, 2, 3\}$ por $B = \{\, 2, 3\}$

Observação 2 *Se A e B são conjuntos finitos com m e n elementos respectivamente, então $A \times B$ é um conjunto finito com $m \cdot n$ elementos.*

Observação 3 *Geralmente $A \times B \neq B \times A$ (lembre-se, estamos considerando $A \neq \phi$ e $B \neq \phi$). Vale a igualdade se e somente se $A = B$.*

Exemplo 2.1.2 *O produto cartesiano de $A = [\,1, 3\,]$ por $B = [\,2, 3\,]$ é o conjunto*

$$A \times B = \{(x, y) \in \mathbb{R}^2 |\ 1 \leq x \leq 3 \text{ e } 2 \leq y \leq 3\}.$$

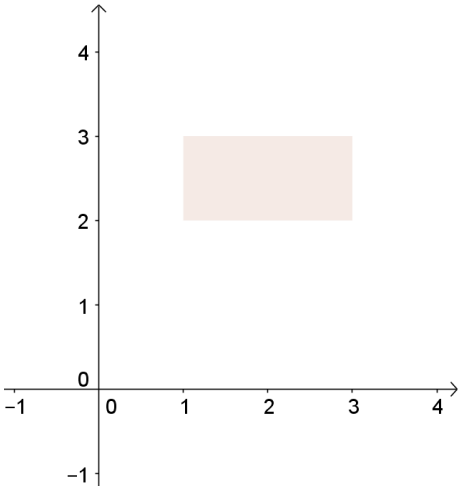

Figura 6 – Produto Cartesiano de $A = [\,1, 3\,]$ por $B = [\,2, 3\,]$

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

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

Podemos escrever uma relação binária por extenso ou quando conveniente, se possível, por uma lei de formação, como ilustrado nos exemplos a seguir.

Exemplo 2.1.3 *Considere em $A = \{1, 2, 3, 4, 5, 6\}$ as seguintes relações:*
$R_1 = \{\,(1, 1), (2, 2), (3, 3), (4, 4), (5, 5), (6, 6)\,\}$,
$R_2 = \{\,(1, 3), (1, 4), (1, 5), (1, 6), (2, 5), (2, 6)\,\}$,
$R_3 = \{\,(1, 1), (1, 2), (2, 1), (3, 1), (1, 3), (1, 4), (1, 5), (1, 6), (2, 5), (2, 6)\,\}$.
Podemos escrever essas relações como
$R_1 = \{(x, y) \in A^2 |\, x = y\}$,

$R_2 = \{(x, y) \in A^2 | \, 2x < y\}$,
$R_3 = \{(x, y) \in A^2 | \, 2x < y \text{ ou } x + 2y < 6\}$.

EXEMPLO 2.1.4 *Em* $\mathbb{Z}$ *considere* $R = \{ (x, y) \in \mathbb{Z}^2 \mid x^2 + y^2 = 25 \}$, *ou seja,*

$$\begin{aligned} R \;=\; & \{(0,5),\, (5,0),\, (0,-5),\, (-5,0),\, (3,4),\, (4,3),\, (-3,4),\, (4,-3),\, (3,-4), \\ & (-4,3),\, (-3,-4),\, (-4,-3)\,\}, \end{aligned}$$

cujo gráfico no plano cartesiano é representado na Figura 7. Temos, por exemplo, que $3R4$, *mas* $1 \not R 0$, *e mais geralmente,* $1 \not R y$, $\forall y \in \mathbb{Z}$.

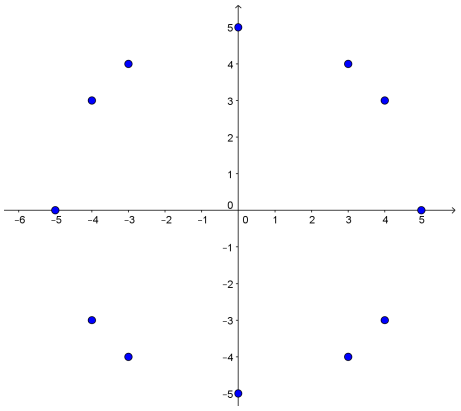

Figura 7 – $R = \{ (x, y) \in \mathbb{Z}^2 \mid x^2 + y^2 = 25 \}$

Note que a algumas relações binárias possuem um número infinito de elementos na relação como é o caso do exemplo abaixo.

EXEMPLO 2.1.5 *Em* $\mathbb{R}$, *a relação* $C = \{ (x, y) \in \mathbb{R}^2 \mid x^2 + y^2 = 25 \}$ *é a circunferência de raio* 5 *e centrado na origem.*

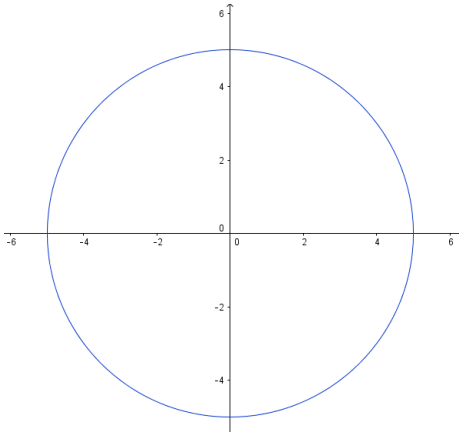

Figura 8 – $C = \{ (x, y) \in \mathbb{R}^2 \mid x^2 + y^2 = 25 \}$

Neste caso, existem dois valores para y tal que xRy, $\forall x \in \mathbb{R}$, a saber $y = \sqrt{25 - x^2}$ e $y = -\sqrt{25 - x^2}$.

EXEMPLO 2.1.6 *Sobre* $\mathbb{N}$, *definamos a relação* $R = \{\ (a,b) \in \mathbb{N}^2 \mid a \leq b\ \}$. *Temos esta relação representada no gráfico abaixo.*

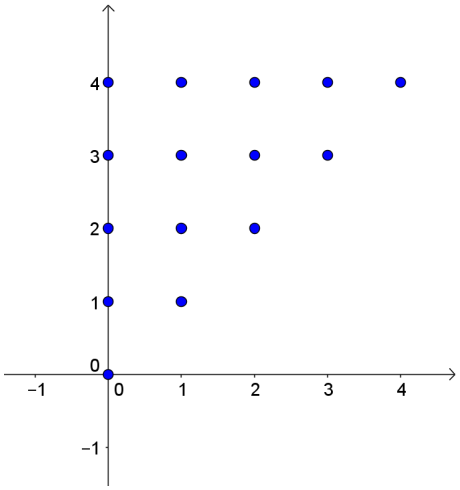

Figura 9 – $R = \{\ (a,b) \in \mathbb{N}^2 \mid a \leq b\ \}$

EXEMPLO 2.1.7 *Sobre* $\mathbb{R}$, *consideremos a relação* $R = \{\ (x,y) \in \mathbb{R}^2 \mid y \leq x + 2\ \}$ *representada graficamente abaixo.*

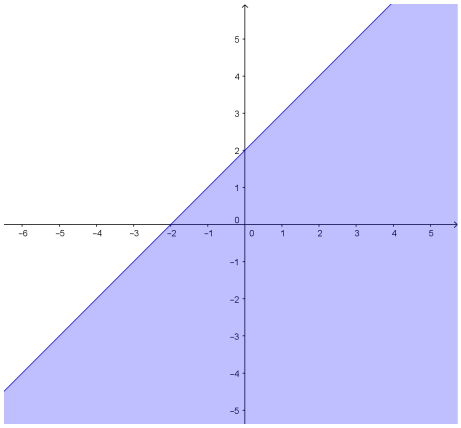

Figura 10 – $R = \{\ (x,y) \in \mathbb{R}^2 \mid y \leq x + 2\ \}$

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

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

$$\text{Dados } a, b \in B, \quad aR_Bb \iff aRb. \tag{2.1}$$

EXEMPLO 2.1.8 $R = \{\ (x,y) \in \mathbb{Z}^2 \mid x^2 + y^2 = 25\ \}$ *é uma relação induzida pela relação* $C = \{\ (x,y) \in \mathbb{R}^2 \mid x^2 + y^2 = 25\ \}$ *sobre o conjunto* $\mathbb{Z}$.

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

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

EXEMPLO 2.1.9 *A relação $R_1 = \{(1,1),(2,2),(3,3),(4,4),(5,5),(6,6)\}$ do Exemplo 2.1.3 é a relação diagonal de $A = \{1,2,3,4,5,6\}$.*

DEFINIÇÃO 5 *Seja R uma relação sobre A, isto é, $R \subset A \times A$. Definimos sobre A a relação R^{-1} como:*

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

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

EXEMPLO 2.1.10 *A relação inversa da relação*

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

do Exemplo 2.1.3 é a relação $R_2^{-1} = \{(3,1),(4,1),(5,1),(6,1),(5,2),(6,2)\}$.

EXEMPLO 2.1.11 *A relação inversa à relação $R = \{(0,5),\ (5,0),\ (0,-5),\ (-5,0),\ (3,4),\ (4,3),\ (-3,4),\ (4,-3),\ (3,-4),(-4,3),\ (-3,-4),\ (-4,-3)\}$ do Exemplo 2.1.4 é a própria R. Já a relação inversa à relação $R = \{(x,y) \in \mathbb{R}^2 \mid y \leq x+2\}$ do exemplo 2.1.7 é a relação $R^{-1} = \{(x,y) \in \mathbb{R}^2 \mid y \geq x+2\}$.*

A seguir apresentamos classificações de relações binárias que permitirão definir relações de equivalência e relação de ordem, fundamentais para a construção dos números naturias, inteiros e racionais, que faremos posteriormente.

DEFINIÇÃO 6 *Seja R uma relação sobre um conjunto $A \neq \phi$. Dizemos que R é:*

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

OBSERVAÇÃO 4 *Seja R uma relação sobre um conjunto $A \neq \phi$. Segue por contraposição que:*

1. *R não é reflexiva se, e somente se, existe $a \in A$ tal que $a \not R a$; ou seja, $\Delta_A \not\subseteq R$;*

2. *R não é simétrica se, e somente se, existem $a, b \in A$ tais que, aRb mas $b \not R a$; ou seja, $R \neq R^{-1}$;*

3. *R não é antissimétrica se, e somente se, existem $a, b \in A$, tais que aRb, bRa e $a \neq b$;*

4. *R não é transitiva se, e somente se, existem $a, b, c \in A$ tais que aRb e bRc, mas $a \not R c$.*

Exemplo 2.1.12 *Definem-se sobre $A = \{ a, b, c \}$ as seguintes relações:*

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

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

Exemplo 2.1.13 *Sobre $\mathbb{R}$ definamos as seguintes relações: $R = \{ (x,y) \in \mathbb{R} \times \mathbb{R} \mid x \leq y \}$ e $S = \{ (x,y) \in \mathbb{R} \times \mathbb{R} \mid x^2 = y \}$. R é reflexiva, mas S não é reflexiva, pois por exemplo, $(2,2) \notin S$.*

Exemplo 2.1.14 *Definem-se sobre $\mathbb{R}$ as seguintes relações: $R = \{ (x,y) \in \mathbb{R} \times \mathbb{R} \mid x^2 = y^2 \}$ e $S = \{ (x,y) \in \mathbb{R} \times \mathbb{R} \mid x \geq y \}$. R é simétrica, porém S não é simétrica, pois $(2,1) \in S$, mas $(1,2) \notin S$, ou seja, $2S1$ mas $1 \not S 2$. As relações dos exemplos 2.1.4 e 2.1.5 são também exemplos de relações simétricas, as dos exemplos 2.1.6 e 2.1.7 são não-simétricas.*

Exemplo 2.1.15 *Considere sobre $A = \{ 1, 2, 3 \}$ as seguintes relações: $R = \{ (1,1), (1,3) \}$ e $S = \{ (1,1), (1,3), (3,1) \}$. Temos que R é antissimétrica e S não é antissimétrica, pois $(1,3) \in S$ e $(3,1) \in S$, mas $1 \neq 3$. Observe que S é simétrica e R não o é.*

Observação 5 *Uma relação ser antissimétrica não significa que ela não seja simétrica e vice-versa, isto é, antissimetria não implica em não-simetria e vice-versa; em outras palavras, existem relações que são antissimétricas e simétricas simultaneamente. Por exemplo a relação $R = \{ (1,1), (2,2) \}$ sobre o conjunto $A = \{ 1, 2, 3 \}$ é simétrica e antissimétrica.*

2.2 Relações de Equivalência

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

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

EXEMPLO 2.2.1 *Seja* $A = \{\, a, b, c \,\}$ *e seja* $R = \{\, (a,a), (b,b), (c,c), (a,b), (b,a) \,\}$. *R é uma relação de equivalência sobre A.*

EXEMPLO 2.2.2 *A relação diagonal (ou seja, a relação de igualdade) é uma relação de equivalência sobre qualquer conjunto* $A \neq \phi$, *pois*
(a) $\forall\, x \in A$, $x = x$;
(b) $\forall\, x, y \in A$, $x = y \Longrightarrow y = x$;
(c) $\forall\, x, y, z \in A$, $x = y$ *e* $y = z \Longrightarrow x = z$.

EXEMPLO 2.2.3 *A relação* $R = \{(x,y) \in \mathbb{Q}^2 | x - y \in \mathbb{Z}\}$ *é uma relação de equivalência pois,*
(a) $x - x = 0$ *e* $0 \in \mathbb{Z}$, *logo R é reflexiva;*
(b) se $x - y = c$ *e* $c \in \mathbb{Z}$ *então* $y - x = -c$ *e* $-c \in \mathbb{Z}$ *o que faz de R uma relação simétrica e*
(c) se $x - y = c$ *e* $y - z = d$ *com* $c, d \in \mathbb{Z}$ *então* $x - z = (x - y) + (y - z) = c + d$ *e* $(c + d) \in \mathbb{Z}$ *portanto R é transitiva.*

Exibiremos a seguir um exemplo muito importante de relação de equivalência, a relação de congruência módulo m, a qual será alvo de uma abordagem mais detalhada no capítulo 4.

DEFINIÇÃO 8 *Seja* $m \in \mathbb{Z}^* = \mathbb{Z} - \{0\}$ *fixado. Definamos sobre* $\mathbb{Z}$ *a seguinte relação:* $a \equiv b \,mod.m$ *se, e somente se,* $\exists\ k \in \mathbb{Z}$ *tal que* $a - b = km$.
$\equiv$ *é uma relação de equivalência sobre* $\mathbb{Z}$.

De fato, dado $a \in \mathbb{Z}$, temos que $a - a = 0m$. Logo, $a \equiv a$. Portanto, $\equiv$ é reflexiva. $\equiv$ é simétrica, pois dados $a, b \in Z$, se $a \equiv b \,\mathrm{mod}.m$, então existe $k \in \mathbb{Z}$ tal que $a - b = km$. Logo, $b - a = (-k)m$ e portanto $b \equiv a \,\mathrm{mod}.m$. Para provar a transitividade, sejam a, b e $c \in \mathbb{Z}$ tais que $a \equiv b \,\mathrm{mod}.m$ e $b \equiv c \,\mathrm{mod}.m$. Então, existem k_1, $k_2 \in \mathbb{Z}$ tais que, $a - b = k_1 m$ e $b - c = k_2 m$ e daí, $a - c = (a - b) + (b - c) = (k_1 + k_2)m$; portanto, $a \equiv c \,\mathrm{mod}.m$.

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

EXEMPLO 2.2.4 *Consideremos* $m = 2$. *Temos, por exemplo, que* $11 \equiv 5 \,mod.2$, *pois* $11 - 5 = 3 \cdot 2$ *e* $-7 \equiv 19 \,mod.2$, *pois* $-7 - 19 = (-13) \cdot 2$.

DEFINIÇÃO 9 *Seja R uma relação de equivalência sobre* $A \neq \phi$. *Dado* $a \in A$, *o conjunto*

$$\bar{a} = \{\, x \in A \mid a \equiv x \; mod.R \,\}$$

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

Observação 6 *$\bar{a}$ é subconjunto de A, e $\bar{a} \neq \phi$, pois pelo menos $a \in \bar{a}$. Por $\equiv mod.R$ ser simétrica, vale que $\bar{a} = \{\, x \in A \mid x \equiv a \, mod.R \,\}$.*

Lema 2.2.5 *$x \in \bar{a}$ se, e somente se, $\bar{x} = \bar{a}$. Ou seja, todo elemento de uma classe de equivalência pode ser considerado como representante dessa classe.*

Dem. ($\Rightarrow$) Se $x \in \bar{a}$, então dado $y \in \bar{x}$ temos que $y \equiv x$ e $x \equiv a$, daí pela transitividade, $y \in \bar{a}$. Logo $\bar{x} \subseteq \bar{a}$. Por outro lado, se $y \in \bar{a}$, então como $x \equiv a$ e $a \equiv y$, segue que $x \equiv y$ e portanto $y \in \bar{x}$; daí $\bar{a} \subseteq \bar{x}$. Concluimos assim que $\bar{a} = \bar{x}$.

($\Leftarrow$) segue imediatamente da Observação 6. ∎

O conjunto das classes de equivalência de A módulo R é chamado de **conjunto quociente** de A por R e será denotado por A/R. Em notação de conjunto,

$$A/R = \{\, \bar{a} \mid a \in A \,\}.$$

Exemplo 2.2.6*: Seja $A = \{\, a, b, c \,\}$ e seja $R = \{\, (a,a), (b,b), (c,c), (a,b), (b,a) \,\}$. Sabemos que R é uma relação de equivalência sobre A. As classes de equivalência de A são*

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

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

e $$\bar{c} = \{\, x \in A \mid x \equiv c \,\} = \{\, c \,\}.$$

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

Definição 10 *Seja $A \neq \phi$ e seja $\mathcal{P}$ um subconjunto do conjunto das partes de A. Dizemos que $\mathcal{P}$ é uma* ***partição*** *de A se, e somente se:*
(i) *dados $X, Y \in \mathcal{P}$, ou $X = Y$ ou $X \cap Y = \phi$, ou seja, os elementos de $\mathcal{P}$ ou são iguais ou são disjuntos;*
(ii) $\bigcup_{X \in \mathcal{P}} X = A$, *a união dos elementos de $\mathcal{P}$ é igual ao conjunto A.*

Exemplo 2.2.7 *Seja $A = \{\, 0, 1, 2, 3 \,\}$. O conjunto $\mathcal{P} = \{\, \{\, 0 \,\}, \{\, 1 \,\}, \{\, 2, 3 \,\} \,\}$ é uma partição de A. Considerando $R = \{\, (0,0), (1,1), (2,2), (3,3), (2,3), (3,2) \,\}$, temos que R é uma relação de equivalência sobre A. Perceba que $A/R = \mathcal{P}$.*

Observe que o conjunto A/R do Exemplo 2.2.6 é uma partição de A. Surge então uma pergunta: Será que todo conjunto quociente de um conjuto A por uma relação de equivalência R é uma partição de A? Outra pergunta, essa motivada pelo Exemplo 2.2.7

é: É possível associar a qualquer partição de um conjunto uma relação de equivalência de modo que o conjunto quociente módulo essa relação coincida com aquela partição? As respostas são dadas nos dois teoremas a seguir.

TEOREMA 2.2.8 *Se R é uma relação de equivalência sobre um conjunto $A \neq \phi$, então A/R é uma partição de A.*

Dem. Precisamos provar que A/R satisfaz (i) e (ii) da Definição 10.

(i) Dadas duas classes $\bar{a}, \bar{b} \in A/R$, ou $\bar{a} \cap \bar{b} = \phi$ ou $\bar{a} \cap \bar{b} \neq \phi$. Se $\bar{a} \cap \bar{b} \neq \phi$, então considerando um $c \in \bar{a} \cap \bar{b}$ temos que $a \equiv c$ e $c \equiv b$, e consequentemente, pela transitividade de R, $a \equiv b$. Logo, pelo Lema 2.2.5, $\bar{a} = \bar{b}$. Portanto, (i) está provada.

(ii) $\bigcup_{a \in A} \bar{a} \subseteq A$, pois $\bar{a} \subset A$, $\forall\, a \in A$. Por outro lado, dado $x \in A$, como $x \in \overline{x}$ (veja a Observação 6) segue que $x \in \bigcup_{a \in A} \bar{a}$, portanto $A \subseteq \bigcup_{a \in A} \bar{a}$. Logo, $\bigcup_{a \in A} \bar{a} = A$. ■

TEOREMA 2.2.9 *Se $\mathcal{P}$ é uma partição de A, então existe uma única relação de equivalência R sobre A tal que, $A/R = \mathcal{P}$.*

Dem. Existência: Seja $\mathcal{P}$ uma partição de A. Definamos sobre A a seguinte relação:

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

Na notação de conjunto,

$$R = \{\, (x, y) \in A \times A \mid \exists\ X \in \mathcal{P},\ \text{ onde } x, y \in X \,\}. \tag{2.2}$$

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

(b) Obviamente R é simétrica.

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

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

Unicidade: Suponhamos que existem $R_1 \neq R_2$ relações de equivalência sobre $A \neq \phi$ tal que, $A/R_1 = A/R_2 = \mathcal{P}$. Já que $R_1 \neq R_2$, então existem $a, b \in A$ tais que, $(a, b) \in R_1$ mas $(a, b) \notin R_2$. Daí segue que, em relação a R_1 $b \in \bar{a}$, ou seja $\bar{b} = \bar{a} \in \mathcal{P}$; mas $b \notin \bar{a}$ em relação a R_2, implica que $\bar{a} \neq \bar{b}$, o que é absurdo. Logo, $R_1 = R_2$. ■

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

EXEMPLO 2.2.10 *Seja $A = \{\, a, e, i, o, u \,\}$ e seja $\mathcal{P} = \{\, \{\, a, u \,\}, \{\, e, o \,\}, \{\, i \,\} \,\}$. É claro que $\mathcal{P}$ é uma partição de A. Determinemos R tal que, $A/R = \mathcal{P}$. Segue imediatamente de (2.2) e da definição de relação de equivalência, que*

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

EXEMPLO 2.2.11 *Consideremos sobre $\mathbb{Z}$ a seguinte partição:*

$$\mathcal{P} = \{\,\{\,0,\,\pm 3,\,\pm 6,\ldots\,\},\,\{\,...,-5,\,-2,\,1,\,4,\ldots\,\},\,\{\,\ldots,\,-1,\,2,\,5,\,8,\,\ldots\,\}\,\}.$$

A demonstração do Teorema 2.2.9 nos mostra como determinar uma relação de equivalência associada à partição $\mathcal{P}$. Devemos exibir uma relação de equivalência R tal que $A/R = \mathcal{P}$. Temos então três classes de equivalência:

$$\begin{aligned}
\bar{0} &= \{\,0,\,\pm 3,\,\pm 6,\,\ldots\,\} = \{\,x \in \mathbb{Z} \mid x = 3k,\,k \in \mathbb{Z}\,\},\\
\bar{1} &= \{\,\cdots,-5,\,-2,\,1,\,4,\ldots\,\} = \{\,x \in \mathbb{Z} \mid x = 3k+1,\,k \in \mathbb{Z}\,\}\ \ e\\
\bar{2} &= \{\,\ldots,\,-1,\,2,\,5,\,8,\ldots\,\} = \{\,x \in \mathbb{Z} \mid x = 3k+2,\,k \in \mathbb{Z}\,\}.
\end{aligned}$$

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

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

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

2.3 Relações de Ordem

DEFINIÇÃO 11 *Dizemos que uma relação binária R sobre um conjunto A é uma* ***relação de ordem*** *(sobre A) se, e somente se, R é:*
(a) *reflexiva,*
(b) *antissimétrica e*
(c) *transitiva.*

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

EXEMPLO 2.3.1 *Sobre $A = \{\,1,\,2,\,3,\,4\}$ é definida a seguinte relação:*

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

Então R é uma relação de ordem sobre A. Perceba que R não é relação de equivalência sobre A pois, por exemplo, $(1,3) \in R$ mas $(1,3) \notin R$.

DEFINIÇÃO 12 *Se uma ordem R sobre A verifica a condição*

$$\forall\, x,\, y \in A, \quad xRy \text{ ou } yRx, \tag{2.3}$$

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

Observe que a relação R do exemplo 2.3.1 não é uma ordem total sobre A pois dados $3, 4 \in A$ temos que $(3,4) \notin R$, e nem $(4,3) \notin R$,.

EXEMPLO 2.3.2 *Os conjuntos $(\mathbb{N}, \leq)$, $(\mathbb{Z}, \leq)$, $(\mathbb{Q}, \leq)$ e $(\mathbb{R}, \leq)$, onde $\leq$ é a conhecida relação menor que ou igual, são exemplos clássicos de conjuntos totalmente ordenados.*

DEFINIÇÃO 13 *Dados a, $b \in \mathbb{Z}$, dizemos que a é um* ***divisor*** *de b (ou que a divide b) se, e somente se, existe $c \in \mathbb{Z}$ tal que $b = a \cdot c$. Para indicar que a é divisor de b usaremos a notação $a|b$.*

EXEMPLO 2.3.3 *A relação de* ***divisibilidade*** *(ver a Definição 13) sobre conjunto dos números naturais $\mathbb{N}$ é uma relação de ordem.*

De fato, temos que:
(a) $\forall\, a \in \mathbb{N}$, $a|a$ (reflexivilidade);

(b) $\forall\, a,\, b \in \mathbb{N}$, se $a|b$ e $b|a$, então $a = b$ (antissimetria);

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

Mas $(\mathbb{N}, |\ )$ não é totalmente ordenado pois tomando-se 3 e 8 que são números naturais, temos que $3 \not| 8$ e $8 \not| 3$.

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

PROPOSIÇÃO 2.3.4 *Seja R uma relação sobre um conjunto $A \neq \phi$. Então:*
(a) *R é ordem se, e somente se, R^{-1} é ordem.*
(b) *R é ordem total se, e somente se, R^{-1} é ordem total.*

Dem. (a) Precisamos provar que se R é uma relação reflexiva, antissimétrica e transitiva, então R^{-1} também o é.

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

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

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

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

($\Leftarrow$) Como $(R^{-1})^{-1} = R$, o resultado segue da demonstração anterior.

(b): ($\Rightarrow$) Seja R uma ordem total sobre A. Então, segue da definição de ordem total que $\forall\, a, b \in A$, aRb ou bRa. Se aRb então $bR^{-1}a$ e se bRa então $aR^{-1}b$. Portanto $bR^{-1}a$ ou $aR^{-1}b$. Logo R^{-1} também é uma ordem total.

($\Leftarrow$) Segue pelo mesmo argumento de (a). ∎

Exemplo 2.3.5 *A ordem oposta à relação de divisibilidade em $\mathbb{N}$ é a relação de multiplicidade, ou seja, dados $a, b \in \mathbb{N}$, $a|b$ se, e somente se, b é múltiplo de a.*

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

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

$$\forall\ a, b \in A,\ a < b \iff a \leq b \ e\ a \neq b.$$

Exibimos na proposição abaixo uma outra caracterização de ordem estrita.

Proposição 2.3.6 *$<$ é ordem estrita sobre A associada a $\leq$ se, e somente se, $<$ satisfaz as seguintes afirmações:*
(a') *$\forall\, a \in A,\ a \not< a$;*
(b') *$\forall\, a, b \in A$, se $a < b$ então $b \not< a$;*
(c') *$<$ é transitiva.*

Dem. ($\Rightarrow$) (a') segue da Definição 14.

(b'): Dados a, $b \in A$, se $a < b$, então pela Definição 14, $a \leq b$ e $a \neq b$. Como $\leq$ é ordem, segue da anti-simetria que $b \not\leq a$ e portanto, $b \not< a$.

(c'): Dados a, b, $c \in A$, $a < b$ e $b < c \Leftrightarrow (a \leq b$ e $a \neq b)$ e $(b \leq c$ e $b \neq c) \Leftrightarrow (a \leq b$ e $b \leq c)$ e $(a \neq b$ e $b \neq c)$. Como $\leq$ é ordem, segue então da transitividade de $\leq$ que $a \leq c$. Falta somente provar que $a \neq c$. De $a \neq b$ e $b \neq c$ inferimos que $a \neq c$, pois se $a = c$, seguiria de $b \leq c$ e $a \leq b$, que $a = b$, o que é absurdo (pois contradiz a hiopótese $a \neq b$). Logo $a < c$. Portanto $<$ é transitiva.

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

$$aRb \ \text{ se, e somente se, } \ a = b \ \text{ ou } \ a < b. \tag{2.4}$$

Note que R é uma ordem sobre A, ou seja, satisfaz a reflexibilidade, antissimetria e transitividade.

Denotemos por $\prec$ a ordem estrita associada à ordem R. Afirmamos que $\prec$ coincide com $<$. De fato, dados $(a,b) \in \prec$ (ou seja, $a \prec b$), segue da definição de ordem estrita e de (2.4) que $a < b$, ou seja, $(a,b) \in <$; logo $\prec \subseteq <$. Agora, dado $(a,b) \in <$, temos que $a < b$, daí (por (2.4)) aRb e consequentemente, $(a,b) \in \prec$; logo $< \subseteq \prec$. Portanto, $<$ e $\prec$ coincidem, e a proposição está demonstrada. ∎

Vimos no Exemplo 2.3.3 a relação de divisibilidade é uma ordem sobre $\mathbb{N}$. Consideremos agora, por exemplo, a relação induzida por $|$ sobre $B = \{\, x \in \mathbb{N} \mid 2 \leq x \leq 10 \,\}$, $|_B$. Temos que

$$|_B = \{\, (2,2),\, (3,3),\, (4,4),\, (5,5),\, (6,6),\, (7,7),\, (8,8),\, (9,9),\, (10,10),\, (2,4),\, (2,6),\, (2,8),\, (2,10),\, (3,6),\, (3,9),\, (4,8),\, (5,10) \,\} \tag{2.5}$$

é uma ordem sobre B. Motivados por esse exemplo somos levados a perguntar se dada uma ordem R sobre um conjunto A, relações induzidas por R sobre subconjuntos de A são também ordens. A resposta encontra-se na proposição a seguir.

Proposição 2.3.7 *Seja $(A, \leq)$ um conjunto ordenado e seja $B \subset A$. Então, a relação $\leq_B$, induzida por $\leq$ sobre B, é uma ordem. Além disso, se $\leq$ é ordem total, então $\leq_B$ também o é.*

Dem. Se $a, b \in B$ então como $B \subset A$, $a, b \in A$. Assim, $a \leq b$, $\forall a, b \in B$. Isso mostra que $\leq_B$ também é uma relação de ordem. Pelo mesmo argumento, temos que se $\leq$ é ordem total, então B é um conjunto totalmente ordenado pela ordem $\leq_B$. ∎

Definição 15 *Seja $(A, \leq)$ um conjunto ordenado. Dizemos que um subconjunto B de A*

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

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

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

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

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

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

Proposição 2.3.8 *$\min B$ e $\max B$, caso existam, são únicos.*

Dem. Sejam m_1 e m_2 mínimos de B. Como $m_1, m_2 \in B$ então, $m_1 \leq m_2$ e $m_2 \leq m_1$. Como $(B; \leq)$ é um conjunto ordenado, pela antissimetria segue que $m_1 = m_2$. ■

EXEMPLO 2.3.9 *O conjunto dos números naturais com a ordem usual, $(\mathbb{N}, \leq)$, tem mínimo ($min\ \mathbb{N} = 0$) mas veremos que não possui máximo. Uma das propriedades fundamentais de $(\mathbb{N}, \leq)$, que exploraremos mais adiante, é que qualquer subconjunto seu possui mínimo.*

EXEMPLO 2.3.10 *Os **conjuntos numéricos** $\mathbb{Z}$ (números inteiros), $\mathbb{Q}$ (racionais) e $\mathbb{R}$ (reais), munidos da ordem usual $\leq$, não têm máximo nem mínimo.*

EXEMPLO 2.3.11 *Considere $2\mathbb{N} := \{\ a \in \mathbb{N} |\ a \text{ é par}\}$ e $B = \{\ x \in 2\mathbb{N} |\ 2 \leq x \leq 30\} \subset \mathbb{N}$, onde $\leq$ é a ordem usual de $\mathbb{N}$. Sabemos, pelo exemplo 2.3.3, que a **relação de divisibilidade** é uma ordem sobre B. Vejamos se B tem máximo e/ou mínimo em relação à divisibilidade:*

Conforme a Definição 15 (iv), $m = \min B \iff m|x\ \forall\ x \in B$ e $m \in B$. Portanto, $2 = \min B$. Do mesmos modo, $n = \max B \iff x|n,\ \forall\ x \in B$ e $n \in B$, daí é fácil ver que, apesar de ser limitado superiormente, B não possui máximo para a relação de divisibilidade.

Para finalizar enunciamos a noção de **boa ordenação**, que será de fundamental importância na construção do conjunto $\mathbb{N}$ dos números naturais.

DEFINIÇÃO 16 *Seja $(A, \leq)$ um conjunto totalmente ordenado. Dizemos que A é **bem ordenado** por $\leq$ se, e somente se, todo subconjunto não-vazio de A tem mínimo.*

EXEMPLO 2.3.12 *$\mathbb{N}$ munido da ordem usual é um conjunto bem ordenado.*

2.4 Funções ou Aplicações.

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

DEFINIÇÃO 17 *Sejam A e B conjuntos. Dizemos que uma relação f de A em B é uma **função** (ou **aplicação**) se, e somente se, para todo $x \in A$ existe um único $y \in B$ tal que $(x, y) \in f$. Ou equivalentemente,*
(i) para todo $x \in A$, existe um $y \in B$ tal que $(x, y) \in f$ (ou seja, $x\, f\, y$);
(ii) se $(x, y) \in f$ e $(x, y') \in f$ então $y = y'$.

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

$$f = \{\, (x, f(x)) \,|\, x \in A \,\}. \tag{2.6}$$

DEFINIÇÃO 18 *Sejam A e B conjuntos e sejam $X \subseteq A$ e $Y \subseteq B$.*
(i) Uma função f de A em B será designada por uma das seguintes notações: $f : A \to B$, ou $A \xrightarrow{f} B$, ou ainda $x \longmapsto f(x)$ onde x é um elemento arbitrário de A.
*(ii) A é o **domínio** e B é o **contradomínio** de f. O conjunto $f(A) = \{\, f(x) \,|\, x \in A \,\}$ é a **imagem** de f.*
*(iii) Os conjuntos $f(X) = \{\, f(x) \,|\, x \in A \,\}$ e $f^{-1}(Y) = \{\, x \,|\, f(x) \in B \,\}$ são, respectivamente, a **imagem (direta)** de X por f e a **imagem inversa** de Y por f.*
*(iv) Quando $f(A) = B$ dizemos que f é uma **função sobrejetora**. E dizemos que f é **injetora** (ou biunívoca) se, e somente se, dados $x_1, x_2 \in A$, $x_1 \neq x_2$ implicar que $f(x_1) \neq f(x_2)$; ou equivalentemente, $f(x_1) = f(x_2)$ implicar que $x_1 = x_2$.*
*(v) Uma função injetora e sobrejetora é chamada de **bijetora**.*

A representação (2.6) de uma função f é comumente chamada de **gráfico** de f.

EXEMPLO 2.4.1 *Sejam $f = \{(0,1),(1,1),(2,1),(2,2)\}$ um subconjunto de $A \times B$, onde $A = \{0,1,2\}$ em $B = \{1,2\}$. A relação f não é função, pois $(2,1),(2,2) \in f$, mas $1 \neq 2$. Já a relação $g = \{(0,1),(1,1),(2,2)\}$ de A em B é uma função. O domínio de g é A e sua imagem é B; assim, g é sobrejetora. $g(\{0,1\}) = \{1\}$. $g^{-1}(\{1\}) = \{0,1\}$.*

EXEMPLO 2.4.2 *A relação C do Exemplo 2.1.5 não é uma função, mas a relação $S = \{\, (x,y) \in [-5,5] \times \mathbb{R} \,|\, x^2 + y^2 = 25 \text{ e } y \geq 0 \,\}$ é uma função, a qual pode ser denotada como $f : [-5,5] \to \mathbb{R}$ onde $f(x) = \sqrt{25 - x^2}$. O gráfico de f é representado dessa forma:*

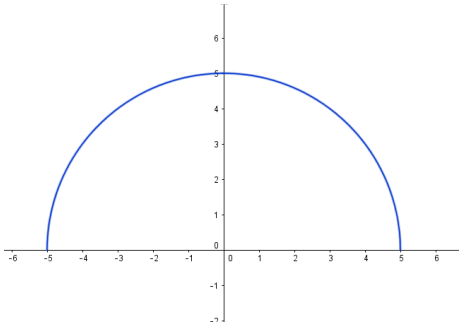

Figura 11 – Gráfico da função $f(x) = \sqrt{25 - x^2}$

EXEMPLO 2.4.3 *Determinemos todas as funções de $A = \{1,2\}$ em $B = \{a,b\}$, com $a \neq b$. Seja $f : A \to B$ uma função arbitrária. Então existem $y_1, y_2 \in B$ tais que $(1, y_1), (2, y_2) \in$*

f e portanto, $f = \{(1, y_1), (2, y_2) : y_1, y_2 \in B\}$. Como $y_1, y_2 \in B$ são arbitrários, as possívies funções de A em B são as seguintes:

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

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

Exemplo 2.4.4 *Sejam $A \neq \phi$ um conjunto e R uma relação de equivalência sobre A. Para cada $x \in A$, seja $f(x) = \overline{x}$. É bastante simples verificar que f é uma função e que é sobrejetora. Essa função é conhecida como* ***função (ou aplicação) quociente*** *de A em A/R.*

Definição 19 *Seja $f : X \to Y$ uma função injetora. Definimos a* ***função inversa*** *de f, denotada por f^{-1}, pela seguinte relação: $(y, x) \in f^{-1}$ se, e somente se, $(x, y) \in f$. Ou seja, $f^{-1} = \{(y, x) \,|\, (x, y) \in f\}$. O domínio de f^{-1} é o conjunto $f(X)$. Neste caso, f é bijetora se, e somente se, $f(X) = Y$.*

Definição 20 *Sejam $f : X \to Y$ e $g : Y \to Z$ funções. Definimos a* ***composta*** *de g e f, denotada por $g \circ f : X \to Z$, pela regra: $g \circ f(x) = g(f(x))$, é a função que leva os elementos de X aos elementos do conjunto Z.*

Exemplo 2.4.5 *Sejam $f, g : \mathbb{R} \to \mathbb{R}$ as funções definidas por $f(x) = 2x + 1$ e $g(x) = x^2 - 1$, $x \in \mathbb{R}$. Então as compostas $g \circ f$ e $f \circ g$ são dadas respectivamente por $(g \circ f)(x) = g(2x+1) = (2x+1)^2 - 1$ e $(f \circ g)(x) = 2(x^2 - 1) + 1$. Portanto, $g \circ f \neq f \circ g$. Geralmente isso acontece.*

3 Números Naturais

Vamos neste capítulo definir a mais elementar das estruturas algébricas, a estrutura de monóide. Falaremos também sobre monóides ordenados e isomorfismos para em seguida aplicarmos tais conceitos na construção e estudo do conjunto dos números naturais. Como aplicação desenvolvemos o método de demonstração por indução finita e descrevemos as notações de somatório e produtório.

3.1 Operações e Monóides

Antes de definirmos a estrutura de monóide é imprescindível estabelecermos o conceito de operação sobre um conjunto.

Definição 21 *Uma* ***operação*** *num conjunto A é uma aplicação de $A \times A$ em A, ou seja, é uma correspondência que, a cada par de elementos (a, b) de $A \times A$ associa um, e somente um, elemento de A.*

Vejamos alguns exemplos conhecidos de operações:

Exemplo 3.1.1 *A* ***adição usual*** $+$ *sobre o conjunto $\mathbb{N}$ dos números naturais, ou sobre o conjuto $\mathbb{Z}$ dos números inteiros, ou sobre $\mathbb{Q}$ ou ainda sobre $\mathbb{R}$, etc.*

Exemplo 3.1.2 *A* ***subtração*** $-$ *sobre o conjunto $\mathbb{Z}$ dos números inteiros ou sobre $\mathbb{Q}$ (números racionais), ou ainda sobre o conjunto $\mathbb{R}$ dos números reais, etc.*

Observemos que a subtração não é uma operação sobre $\mathbb{N}$, pois, por exemplo, $2, 3 \in \mathbb{N}$ mas $2 - 3 \notin \mathbb{N}$.

Exemplo 3.1.3 *A* ***multiplicação*** *é uma operação sobre os conjuntos $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$ e $\mathbb{R}$.*

Exemplo 3.1.4 *A* ***divisão*** $\div$ *é uma operação sobre os conjuntos $\mathbb{Q}^* := \mathbb{Q} - \{0\}$ e $\mathbb{R}^* = \mathbb{R} - \{0\}$, mas não define uma operação sobre $\mathbb{Z}^* := \mathbb{Z} - \{0\}$, muito menos sobre $\mathbb{N}^* := \mathbb{N} - \{0\}$, pois por exemplo, $2 \div 3 \notin \mathbb{N}$. Observe que $\div$ não é uma operação sobre $\mathbb{Q}$ nem sobre $\mathbb{R}$, pois não se pode dividir números por 0.*

Exemplo 3.1.5 *Duas operações muito importantes e amplamente utilizadas sobre o conjunto dos números reais são, $x * y = \dfrac{x+y}{2}$ e $x \bullet y = \sqrt{x \cdot y}$, usualmente chamadas de* ***média aritmética*** *e* ***média geométrica****, respectivamente.*

Indicaremos um conjunto A munido de uma operação $*$ pela notação $(A, *)$.

DEFINIÇÃO 22 *Seja $*$ uma operação sobre A e seja $B \subseteq A$ um subconjunto não vazio de A. Dizemos que B é* ***fechado*** *em relação à operação $*$ se, e somente se, $*$ é uma operação sobre B, ou seja,*

$$\textit{dados quaisquer } a,\, b \in B,\ a * b \in B.$$

EXEMPLO 3.1.6 *Dado $m \in \mathbb{Z}$, o conjunto dos múltiplos de m, $m\mathbb{Z} := \{\, x \in \mathbb{Z} \mid x = mn$, para algum $n \in \mathbb{Z}\,\}$, é fechado em relação às operações de adição e multiplicação usuais em $\mathbb{Z}$. Em particular, o conjunto dos inteiros pares é fechado em relação a essas duas operações.*

De fato, dados $a,\, b \in m\mathbb{Z}$, existem $k, l \in \mathbb{Z}$ tal que $a = mk$ e $b = ml$. Assim, temos que, $a + b = mk + ml = m(k + l) \in m\mathbb{Z}$ e $ab = (mk)(ml) = m(kml) \in m\mathbb{Z}$.

EXEMPLO 3.1.7 *O conjunto dos inteiros ímpares $2\mathbb{Z} + 1 := \{\, 2n + 1 \mid n \in \mathbb{Z}\}$ é fechado em relação à multiplicação, mas não o é em relação à soma.*

Considere $n_1, n_2 \in \mathbb{Z}$ temos que $2n_1+1$ e $2n_2+1$ são dois elementos desse conjunto. Assim, $(2n_1+1).(2n_2+1) = 2(2n_1n_2+n_1+n_2)+1 \in 2\mathbb{Z}+1$ mas $(2n_1+1)+(2n_2+1) = 2\,(n_1+n_2)+2$ que por sua vez não pertence ao conjunto $2\mathbb{Z}+1$.

EXEMPLO 3.1.8 *O conjunto dos inteiros não-negativos $\mathbb{N} := \{\, n \in \mathbb{Z} \mid n \geq 0\,\}$ é fechado em relação à adição, mas não o é em relação à subtração em $\mathbb{Z}$.*

De posse destes conceitos iniciais, podemos agora definir a estrutura de monóide.

DEFINIÇÃO 23 *Sejam, A um conjunto não-vazio e $*$ uma operação sobre A. Dizemos que $(A, *)$ é um* ***monóide*** *se, e somente se, verifica as seguintes propriedades:*
1. Para quaisquer $a, b, c \in A$, tem-se $(a * b) * c = a * (b * c)$,
designada por ***associatividade*** *ou propriedade associativa;*
2. existe $e \in A$ tal que, $a * e = a = e * a$, para todo $a \in A$,
o qual é chamado ***elemento neutro*** *de A para a operação $*$.*
Se além de ***(i)*** *e* ***(ii)*** *$(A, *)$ também satisfaz*
3. $a * b = b * a$, para quaisquer $a, b \in A$,
dizemos que $(A, *)$ é um ***monóide comutativo****.*

Um conjuto munido de uma operação que satisfaz (i) é chamado de **semigrupo**. Assim, um monóide nada mais é que um semigrupo que possui elemento neutro. Um conjunto com uma operação que satisfaz (iii) é chamado de **conjunto comutativo**.

Observemos que, se uma operação $*$ sobre um conjunto A tem elemento neutro, então ele é único. Com efeito, supondo que e e e' são elementos neutros de $(A, *)$, então $e = e * e' = e' * e = e'$. Daí segue que um monóide possui um único elemento neutro.

EXEMPLO 3.1.9 *Os conjuntos* $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$ *e* $\mathbb{R}$ *são exemplos de monóides comutativos, tanto com a operação aditiva como com a operação multiplicativa usuais.*

EXEMPLO 3.1.10 *O conjunto dos inteiros ímpares* $2\mathbb{Z}+1 := \{x \in \mathbb{Z} \mid x = 2n+1,$ *para algum* $n \in \mathbb{Z}\}$ *munido da operação multiplicação usual, é um monóide comutativo. Com efeito, a associatividade e a comutatividade seguem imediatamente da associatividade e comutatividade de* $(\mathbb{Z}, \cdot)$*.Sabe-se que* 1 *é o elemento neutro de* $(\mathbb{Z}, \cdot)$ *e* 1 *é ímpar; daí* 1 *é o elemento neutro de* $(2\mathbb{Z}+1, \cdot)$*.*

EXEMPLO 3.1.11 *Se* $m \neq \pm 1$*,* $(m\mathbb{Z}, \cdot)$ *é um exemplo de semigrupo que não é monóide, pois o conjunto não apresenta o elemento neutro da multiplicação usual.*

EXEMPLO 3.1.12 *Seja* $M_{2\times 2} := \left\{ A = \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} ;\ a_{ij} \in \mathbb{R} \text{ e } \det A \neq 0 \right\}$ *o conjunto das matrizes* 2×2 *inversíveis.* $(M_{2\times 2}, \cdot)$*, onde* $\cdot$ *é o produto usual de matrizes, é um exemplo de monóide que não é comutativo.*

EXEMPLO 3.1.13 *Em* $\mathbb{N}^* = \mathbb{N} - \{0\}$ *definamos a seguinte operação* $*$*: Dados* a, $b \in \mathbb{N}^*$*,* $a * b = a^b$*. Temos que* $(\mathbb{N}^*, *)$ *não é monóide nem semigrupo. De fato, dados* a, b, $c \in \mathbb{N}^*$*,* $(a*b)*c = (a^b)*c = (a^b)^c = a^{bc}$ *e* $a*(b*c) = a*(b^c) = a^{b^c}$ *nem sempre são iguais. Além disso,* $a * e = a^e = a$ *se e só se* $e = 1$*; mas* $1 * a = 1^a = 1$ *para qualquer* $a \in \mathbb{N}^*$*; isso implica na não-existência de elemento neutro em* $\mathbb{N}^*$ *com esta operação.*

DEFINIÇÃO 24 *Seja* $(A, *)$ *um conjunto com elemento neutro para a operação* $*$ *sobre* A*. Dizemos que um elemento* $a \in A$ *é simetrizável (ou inversível), quando existe* $a' \in A$ *tal que,*

$$a * a' = e = a' * a. \tag{3.1}$$

O elemento a' *que satisfaz (3.1) é chamado* ***simétrico*** *de* a*.*

Denotaremos o conjunto dos elementos simetrizáveis de $(A, *)$ por $U_*(A)$, ou simplesmente, $U(A)$.

Observemos que por (3.1), se a' é o simétrico de um elemento simetrizável a, então a' é simetrizável e seu simétrico é o próprio a. Ou seja, $a \in U(A)$ se, e somente se $a' \in U(A)$ e $a'' = a$.

Em se tratando das operações de adição e de multiplicação, definidas por exemplo em conjuntos numéricos ou de matrizes, o simétrico de um elemento em relação à adição é chamado de elemento oposto. Os elementos simetrizáveis para a multiplicação são ditos inversíveis e neste caso o simétrico de um elemento é chamado de inverso daquele elemento.

EXEMPLO 3.1.14 *O conjunto dos elementos simetrizáveis de* $(\mathbb{Z}, +)$ *é* $U_+(\mathbb{Z}) = \mathbb{Z}$*. Enquanto que, para a operação multiplicação* $\cdot$ *em* $\mathbb{Z}$*,* $U_\cdot(\mathbb{Z}) = \{-1, 1\}$*. Em* $\mathbb{N}$*,* $U_+(\mathbb{N}) = 0$ *e* $U_\cdot(\mathbb{N}) = \{1\}$*.*

Exemplo 3.1.15 *O conjunto dos elementos simetrizáveis de* $(\mathbb{Q}, +)$ *é* $U_+(\mathbb{Q}) = \mathbb{Q}$*; enquanto que* $U_\cdot(\mathbb{Q}) = \mathbb{Q}^*$*. Em* $\mathbb{R}$*,* $U_+(\mathbb{R}) = \mathbb{R}$ *e* $U_\cdot(\mathbb{R}) = \mathbb{R}^*$*.*

A seguir listamos as principais propriedades do conjunto dos elementos simetrizáveis de um monóide $(A, *)$.

Teorema 3.1.16 *Seja* $(A, *)$ *um monóide. Então são válidas as seguintes propriedades:*
1. Se $a, b \in U_*(A)$*, então* $a * b \in U_*(A)$ *e* $(a * b)' = b' * a'$*. Em palavras,* $U_*(A)$ *é fechado para a operação* $*$*.*
2. $U_*(A)$ *é um monóide.*
3. Para cada $a \in U_*(A)$ *existe um único* $a' \in A$ *tal que,* $a * a' = e = a' * a$*, onde* e *é o elemento neutro de* $(A, *)$*. Em palavras: o simétrico de um elemento simetrizável é único.*
4. Se $a, b \in A$ *comutam entre si, então*

(i) $b \in U_*(A) \Longrightarrow a * b' = b' * a$*, onde* b' *é o simétrico de* b*;*

(ii) $a, b \in U_*(A) \Longrightarrow a' * b' = b' * a'$ *(se* a *e* b *comutam entre si, então* a' *e* b' *comutam entre si);*

Dem. 1. Sejam $a, b \in U_*(A)$ e sejam a' e b' seus respectivos simétricos. O candidato x a simétrico de $a * b$ é encontrado usando-se a propriedade associativa de A:

$$\begin{aligned}(a * b) * x = e &\Longrightarrow a' * [(a * b) * x] = (a' * a) * (b * x) = b * x = a' \\ &\Longrightarrow (b' * b) * x = b' * a' \\ &\Longrightarrow x = b' * a'.\end{aligned}$$

E realmente $b' * a'$ é o simétrico de $a * b$, pois $(b' * a') * (a * b) = b' * ((a' * a) * b) = b' * b = e$ e $(a * b) * (b' * a') = e$.

2. Dados $a, b, c \in U_*(A)$, segue de (P1) que $(a * b) * c$, $a * (b * c) \in U_*(A)$ e, pela associatividade de A segue que $(a * b) * c = a * (b * c)$. Agora, como $e * e = e$, segue que $e \in U_*(A)$ e é o elemento neutro de $*$ em $U_*(A)$. Portanto $U_*(A)$ é monóide.

3. A existência é pela própria definição de $U_*(A)$. Para provar a unicidade, seja $x \in A$ tal que, $a * x = e = x * a$; então pela propriedade associativa de A temos que

$$x = x * e = x * (a * a') = (x * a) * a' = e * a' = a'.$$

4. Para provar (i), além da hipótese $a * b = b * a$, usaremos o fato de que $(A, *)$ é monóide como segue:

$$\begin{aligned}a * b' &= e * (a * b') = (e * a) * b' = ((b' * b) * a) * b' = (b' * (b * a)) * b' \\ &= b' * ((a * b) * b') = b' * (a * (b * b')) = b' * (a * e) = b' * a,\end{aligned}$$

e portanto segue o resultado.

Agora provemos (ii) usando o fato de $(A, *)$ ser monóide e a propriedade (i), segue que

$$\begin{aligned} a' * b' &= (a' * b') * e = (a' * b') * (a * a') = (a' * (a * b')) * a' = ((a' * a) * b') * a' \\ &= (e * b') * a' = b' * a'. \end{aligned} \tag{3.2}$$

O teorema está então demonstrado. ■

TEOREMA 3.1.17 *Seja $(A, *)$ um monóide. Dados $a, b \in A$, se $b \in U_*(A)$, existe um único $x \in A$ tal que $b * x = a$ e um único $y \in A$ tal que $y * b = a$. Além disso, se $(A, *)$ é monóide comutativo, então $x = y$.*

Dem. Existência: Como por hipótese $b \in U_*(A)$, $b * x = a \iff b' * (b * x) = b' * a$. Tomando então $x = b' * a$, segue que

$$b * x = b * (b' * a) = (b * b') * a = e * a = a.$$

De modo análogo prova-se que existe $y \in A$ tal que $y * b = a$.

Unicidade: Dados $x_1, x_2 \in A$ tais que, $b * x_1 = a$ e $b * x_2 = a$, temos que

$$x_1 = e * x_1 = (b' * b) * x_1 = b' * (b * x_1) = b' * a = b' * (b * x_2) = (b' * b) * x_2 = x_2.$$ ■

Na notação aditiva, o $x \in A$ tal que $b + x = a$ é denominado diferença entre a e b, e é denotado por $a - b$ (lê-se a menos b). Logo, por definição $a - b = a + (-b)$, $b + (a - b) = a$, $b - b = 0$ e $0 - b = -b$, para todo $b \in U_+(A)$ e todo $a \in A$. A aplicação $(a, b) \longmapsto a - b$ de $A \times A$ em A é denominada subtração de a por b.

Na notação multiplicativa, o $x \in A$ tal que $b \cdot x = a$ é denominado quociente de a por b e é indicado por $\frac{a}{b}$ (lê-se a sobre b). Assim, por definição, $\frac{a}{b} = a \cdot b^{-1}$. Em particular, dados $a, b \in A$, com $b \in U.(A)$, vale: $b \cdot \frac{a}{b} = a$, $\frac{b}{b} = 1$ e $\frac{1}{b} = b^{-1}$. A aplicação $(a, b) \longmapsto \frac{a}{b}$ de $A \times A$ em A é denominada divisão de a por b.

DEFINIÇÃO 25 *Seja $(A, *)$ um semigrupo. Dizemos que $a \in A$ é um **elemento regular** à esquerda pela operação $*$, quando a satisfaz a lei do cancelamento à esquerda e à direita, ou seja, dados quaisquer $x, y \in A$, vale:*

$$a * x = a * y \implies x = y,$$

e,

$$x * a = y * a \implies x = y.$$

Todos os elementos de $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$ e $\mathbb{R}$ são regulares para a operação $+$ de adição usual. Para a operação multiplicação usual, o conjunto dos elementos regulares de $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$ e $\mathbb{R}$, é $\mathbb{N}^*$, $\mathbb{Z}^*$, $\mathbb{Q}^*$ e $\mathbb{R}^*$, respectivamente.

Observemos que, no exemplo acima, além de fornecer exemplo de que nem sempre todo elemento regular é simetrizável, nos dá indícios de que todo elemento simetrizável é regular. Isso é exatamente o que estabeleceremos com o próximo resultado.

Teorema 3.1.18 *Seja $(A, *)$ um monóide. Se $a \in U_*(A)$, então a é regular.*

Dem. Dados x, $y \in A$ e $a \in U_*(A)$, tais que, $a * x = a * y$, seque que $x = e * x = (a' * a) * x = a' * (a * x) = a' * (a * y) = (a' * a) * y = e * y = y$.
Analogamente prova-se que, $x * a = y * a \Longrightarrow x = y$.
Portanto a é regular. ∎

3.2 Monóides Ordenados.

Definição 26 *Seja $(A, *)$ um monóide comuntativo com a operação $*$ e seja $\preceq$ uma ordem sobre $(A, *)$. Dizemos que $*$ e $\preceq$ são compatívies se, e somente se, vale:*

$$\text{Dados } x, y, z \in A, \text{ se } x \preceq y \text{ então } x * z \preceq y * z. \tag{3.3}$$

Neste caso, dizemos que A é parcialmente ordenado por $\preceq$, ou, que $(A, *)$ é um monóide parcialmente ordenado. Se além de (3.3), $\preceq$ é uma ordem total, ou seja, satisfaz (2.3) (veja Definição 12), dizemos que A é ordenado por $\preceq$.

Usaremos a notação $(A, *, \preceq)$ para indicar que $\preceq$ é uma relação de ordem sobre A que satisfaz (3.3). O símbolo $\prec$ indicará a ordem estrita associada à ordem $\preceq$.

Daqui em diante, a menos que digamos o contrário, estaremos a considerar somente monóides totalmente ordenados, os quais serão chamados simplesmente de **monóides ordenados**.

Exemplo 3.2.1 *$(\mathbb{Z}, +, \leq)$ é um monóide ordenado.*
De fato, dados $x, y, z \in \mathbb{Z}$ se $x \leq y$ então $x + z \leq y + z$

A seguir listamos as principais propriedades dos monóides ordenados, das quais faremos uso na próxima seção.

Teorema 3.2.2 *Em um monóide ordenado $(A, *, \preceq)$ valem as seguintes propriedades:*
1. $a \preceq b$ e $c \preceq d \Longrightarrow a * c \preceq b * d$.
2. c é regular e $a \prec b \Longrightarrow a * c \prec b * c$.
3. $a * c \prec b * c \Longrightarrow a \prec b$.

Dem. 1. Da definição de monóide ordenado temos que,

$$a \preceq b \Longrightarrow a * c \preceq b * c$$

e

$$c \preceq d \Longrightarrow b * c \preceq b * d;$$

portanto, pela transitividade, $a * c \preceq b * d$.

2. De $a \prec b$ implica $a \neq b$; da regularidade de c segue que $a * c \neq b * c$. Mas $a \prec b$ implica $a \preceq b$ e daí, por (3.3), $a * c \preceq b * c$. Como $a * c \neq b * c$, segue o resultado.

3. A é totalmente ordenado. Então uma das duas seguintes possibilidades acontece: $a \preceq b$ ou $b \preceq a$.

Suponhamos $b \preceq a$. Então de (3.3) segue que $b*c \preceq a*c$, o que é absurdo! Portanto $a \preceq b$. Mas como $a * c \prec b * c$, segue que $a \prec b$. ■

TEOREMA 3.2.3 *Seja $(A, *, \leq)$ um monóide ordenado e seja e o elemento neutro de A para a operação $*$. Então valem as seguintes propriedades:*
1. Se $b \in U_*(A)$ então, $a \prec b \iff a * b' \prec e$;
2. Se a, $b \in U_*(A)$ então, $a \prec b \iff b^* < a^*$;
3. Se $a \in U_*(A)$ então, $e \prec a \iff a' \prec e$.

Dem. 1. ($\Rightarrow$) $b \in U_+(A) \Longrightarrow \exists\ -b \in A$ tal que $b + (-b) = 0$. Como por hipótese $a < b$, segue do Teorema 3.2.2 que $a - b < b + (-b) = 0$.

($\Leftarrow$) Se $a - b < 0$, então $(a - b) + b < b$, ou seja, $a < b$.

2. ($\Rightarrow$) $a < b$ implica por (a) que $a - b < 0$. Mas então, pelo Teorema 3.2.2(a), $-a + a - b < -a$, ou seja, $-b < -a$.

($\Leftarrow$) segue imediatamente do que acabamos de fazer em ($\Rightarrow$).

3. Feita de modo análogo a (a) e (b). ■

DEFINIÇÃO 27 *Sejam $(A, *, \preceq)$ e $(B, *, \preceq)$ monóides ordenados. Dizemos que uma aplicação $f : A \to B$ é um **isomorfismo** de $(A, *, \preceq)$ em $(B, *, \preceq)$ se, e somente se:*
***(a)** $f(a * b) = f(a) * f(b)$, $\forall\ a, b \in A$ (f é um homomorfismo);*
***(b)** f é bijetora.*
Se além disso, f preserva a ordem no sentido de que
***(c)** para quaisquer $a, b \in A$, $a \preceq b$ se, e somente se, $f(a) \preceq f(b)$,*
*dizemos que f é um **isomorfismo ordenado** de $(A, *, \preceq)$ em $(B, *, \preceq)$.*

TEOREMA 3.2.4 *Sejam $(A, *, \preceq)$ e $(B, \star, \preceq)$ monóides ordenados. Se 0_A e 0_B são os respectivos elementos neutros de A e B e se f é um isomorfismo de A em B, então $f(0_A) = 0_B$.*

Dem. Como f é bijetora, segue que para todo $b \in B$ existe um único $a \in A$ tal que $f(a) = b$. Daí segue que, dado qualquer $b \in B$, $f(0_A) \star b = f(0_A) \star f(a) = f(0_A * a) = f(a) = b$. Assim, $f(0_A)$ é elemento neutro de $(B, \star, \leq)$. Segue da unicidade de 0_B que $f(0_A) = 0_B$. ■

3.3 Construção do conjunto dos números naturais

Com posse das informações das seções anteriores, construiremos o conjunto dos números naturais por meio de uma base axiomática. Seja $(N, +, \leq)$ um semigrupo comutativo totalmente ordenado (que será representado pelo símbolo $\mathbb{N}$) satisfazendo os seguintes axiomas:

N1. Existem a, $b \in \mathbb{N}$ tal que $a \neq b$, ou seja, $\mathbb{N}$ não é unitário.

N2. Todo elemento de $\mathbb{N}$ é regular para a operação $+$ (vale a lei do cancelamento da adição em $\mathbb{N}$).

N3. Dados a, $b \in \mathbb{N}$, se $b \leq a$, então existe $c \in \mathbb{N}$ tal que, $a = b + c$.

N4. $\mathbb{N}$ é bem ordenado pela ordem $\leq$, ou seja, todo subconjunto não-vazio de $\mathbb{N}$ tem mínimo. Em outras palavras, $\forall\ A \subseteq \mathbb{N}$ não vazio $\exists!\ m \in A$ tal que $m \leq a$, $\forall\ a \in A$.

O axioma N4 é também conhecido como **princípio do menor número natural**. Em particular $\mathbb{N}$ tem mínimo, o qual é chamado de zero e é representado pelo símbolo 0.

Observação 7 *Vamos aceitar como verdade a existência de um cojunto satisfazendo os quatro axiomas acima. Sua construção é feita via teoria dos números cardinais. É importante registrar que a base axiomática acima é a mais simples e mais econômica possível.*

A estrutura algébrica $\mathbb{N}$, onde N satisfaz os quatro axiomas acima, $+$ sendo associativa e comutativa e $\leq$ sendo uma ordem total, é denominado o **conjunto dos números naturais**.

Veremos que se $(E, +, \leq)$ satisfaz os axiomas acima, então $(E, +, \leq)$ é isomorfo a $\mathbb{N}$.

Teorema 3.3.1 *O mínimo de $\mathbb{N}$ é o elemento neutro para a operação adição $+$.*

Dem. Temos que $0 \in \mathbb{N}$, e do fato de $\mathbb{N}$ ser ordenado, $0 \leq 0$; daí, de N3 segue que existe $a \in \mathbb{N}$ tal que $0 = 0 + a$. Como $0 = min\mathbb{N}$, temos que $0 \leq a$; logo por (3.3), $0 + 0 \leq a + 0$, e daí segue que $0 + 0 \leq 0$. Como $0 = min\mathbb{N}$, concluimos que $0 + 0 = 0$.

Agora, dado $x \in \mathbb{N}$, vale que $(x + 0) + 0 = x + (0 + 0) = x + 0$. Como 0 é regular para a operação $+$, segue que $x + 0 = x$. Logo, 0 é o elemento neutro para adição usual em $\mathbb{N}$. ∎

Teorema 3.3.2 *$\mathbb{N}$ satisfaz as seguintes propriedades:*
1. (Recíproca de N3) Se $a, b, c \in \mathbb{N}$ são tais que $b + c = a$, então $b \leq a$.
2. Dados $a, b \in \mathbb{N}$; $b < a$ se e somente se $\exists!\ c \neq 0$ tal que, $a = b + c$.
3. Dados $a, b, c \in \mathbb{N}$; $b < a$ se e somente se $b + c < a + c$.

4. Se $a, b \in \mathbb{N}$, e $b \leq a$, então $\exists!\ c \in \mathbb{N}$ tal que $b + c = a$. O número c é chamado de diferença entre a e b e é denotado por $a - b$.

Dem. 1. Sabemos que $0 \leq c$, pois $0 = \min \mathbb{N}$. Por (3.3), $b = b + 0 \leq b + c$; como $b + c = a$, P1. está demonstrada.

2. ($\Rightarrow$) $b < a$ implica que $b \leq a$; daí, por N3 existe um $c \in \mathbb{N}$ tal que $b + c = a$. Ora, $c \neq 0$, pois caso contrário teríamos $b = a$, o que é absurdo. Isso prova a existência.

Vejamos a unicidade: Dado um c' tal que $b + c' = a$, tem-se que $b + c' = b + c$; mas por N2 concluimos que $c = c'$.

($\Leftarrow$) Veja o ítem (c) do teorema 3.2.2.

3. ($\Rightarrow$) Se $b < a$ segue de N3 que existe um $c \in \mathbb{N}$ tal que $a = b + c$. Por N2, podemos escrever que $(a + c) = (b + c) + c$. Logo, $b + c < a + c$.

($\Leftarrow$) Se $b + c < a + c$ existe um $d \in \mathbb{N}$ tal que $(a + c) = (b + c) + d$. Pela lei do cancelamento vale que $a = b + d$. Portanto, $b < a$.

4. A existência é garantida pelo axioma N3 e a unicidade segue procedendo-se como da demonstração de P2. ∎

A propriedade 4. acima é a unicidade de 1. e N3.

Vamos denotar $\mathbb{N} - \{0\}$ pelo símbolo $\mathbb{N}^*$. O axioma N1 assegura que $\mathbb{N}^* \neq \phi$; logo, por N4 concluimos que $\mathbb{N}^*$ tem mínimo, o qual vamos chamar de 1, ou seja, $1 = \min \mathbb{N}^*$.

Teorema 3.3.3 *Dados $n, a, b \in \mathbb{N}$, valem:*
(i) $n < n + 1$;
(ii) se $n \neq 0$, então $n - 1 < n$;
(iii) $a < b$ se, e somente se, $a + 1 \leq b$.

Dem. (i) Como $0 \neq 1$ e como $0 = \min \mathbb{N}$, segue que $0 < 1$. Então por P3, $0 + n < 0 + n + 1$, e portanto, $n < n + 1$.

(ii) Como $n \neq 0$, segue que $1 \leq n$ e podemos escrever $(n - 1) + 1 = n$ (onde $n - 1$ é a diferença entre n e 1). De (i) concluimos então que $n - 1 < n$.

(iii) ($\Rightarrow$) $a < b$ implica que $b - a \neq 0$; como $b - a \in \mathbb{N}$, segue que $1 \leq b - a$. Logo, por (3.3) $a + 1 \leq b + (a - a)$ e isso implica que $a + 1 \leq b$.

($\Leftarrow$) Se $a + 1 \leq b$ então $b - a \in \mathbb{N}$ e assim $1 \leq b - a$. E novamente por (3.3) temos que $1 \leq b - a \Longrightarrow 1 + a \leq b - a + a \Longrightarrow 1 + a \leq b \Longrightarrow 1 + a + (-1) \leq b - 1$ o que por (ii)finalmente implica em $a \leq b - 1 \leq b$. ∎

Algumas notações importantes: Dados $m, n \in \mathbb{N}$, indicaremos por

$$I_n = \{\, x \in \mathbb{N} \,|\, n \leq x \,\}, \quad I_n^* = \{\, x \in \mathbb{N} \,|\, n < x \,\},$$
$$[m, n] = I_m \cap (I_n^*)^C = \{\, x \in \mathbb{N} \,|\, m \leq x \text{ e } x \leq n \,\},$$
$$[m, n) = I_m \cap I_n^C = \{\, x \in \mathbb{N} \,|\, m \leq x \text{ e } x < n \,\} \text{ e}$$
$$(m, n] = I_m^* \cap I_n^C = \{\, x \in \mathbb{N} \,|\, m < x \text{ e } x \leq n \,\}.$$

Por exemplo, $I_0 = \mathbb{N}$ e $I_0^* = \mathbb{N}^*$.

PROPOSIÇÃO 3.3.4 *Para todo $n \in \mathbb{N}$, tem-se que $[n, n+1] = \{n, n+1\}$, ou seja, não existe $x \in \mathbb{N}$ tal que $n < x < n+1$.*

Dem. Suponhamos que existe $x \in \mathbb{N}$ tal que $n < x < n+1$. De $n < x$ segue que existe $a \in \mathbb{N}^*$ tal que $x = n + a$ e portanto, $n + a < n + 1$; daí, pela Lei do Cancelamento $a < 1$. Logo $a = 0$, pois $1 = \min \mathbb{N}^*$ e $a \notin \mathbb{N}^*$. Mas isso implica que $x = n$, o que é uma contradição. ∎

O teorema a seguir, conhecido como **Princípio de Indução Finita** nos diz que o único subconjunto de $\mathbb{N}$ que possui o $\min \mathbb{N}$ e que os sucessores dos elementos desse subconjunto pertencem a ele, é o conjunto dos números naturais $\mathbb{N}$.

TEOREMA 3.3.5 (*Princípio de Indução Finita*) *Seja $S \subseteq \mathbb{N}$ tal que,*
(i) $0 \in S$;
(ii) para qualquer $n \in \mathbb{N}$, se $n \in S$ então $n + 1 \in S$.
Então $S = \mathbb{N}$.

Dem. Suponhamos $S \neq \mathbb{N}$; então consideremos o conjunto S' tal que $S' := \mathbb{N} - S \neq \phi$. Como $\mathbb{N}$ é bem ordenado (axioma N4), existe $a = \min S'$. Como $0 \in S$, segue que $1 \leq a$. Então pelo teorema 3.3.3 item (ii), $a - 1 < a$. Mas $a = \min S'$ e portanto, $a - 1 \notin S'$; logo $a - 1 \in S$. Mas então por (ii) $a \in S$, o que é um absurdo. ∎

COROLÁRIO 3.3.6 *Seja $m \in \mathbb{N}$ e seja $S \subseteq I_m$ tal que:*
(i) $m \in S$,
(ii) para todo $n \in \mathbb{N}$, se $n \in S$ então $n + 1 \in S$.
Nestas condições, $S = I_m$.

Dem. Seja $S_1 = [0, m) \cup S$; provemos que $S_1 = \mathbb{N}$. Observemos que $S \cap [0, m) = \phi$.

$0 \in S_1$, pois $0 \in [0, m)$.

Seja $n \in \mathbb{N} \cap S_1$. Se $n \in S$, então por (ii) $n + 1 \in S$ e portanto, $n + 1 \in S_1$. Agora, se $n \in [0, m)$, então $n + 1 < m$ ou $n + 1 = m$, ou seja, $n + 1 \in [0, m)$ ou $n + 1 \in S$; em ambos os casos, $n + 1 \in S_1$.

Dos dois argumentos acima, podemos concluir pelo teorema 3.3.5 que $S_1 = \mathbb{N}$ e assim, $S = I_m$. ∎

COROLÁRIO 3.3.7 *Seja* $S \subseteq [a, b]$ $(a \leq b)$ *tal que:*
(i) $a \in S$*;*
(ii) dado $n \in \mathbb{N}$*, se* $n < b$ *e se* $n \in S$ *então* $n + 1 \in S$*.*
Então $S = [a, b]$*.*

Dem. Seja $S_1 = S \cup I_b^*$ (essa união é disjunta). Vamos provar que $S_1 = I_a$.

Obviamente $a \in S_1$. Agora, dado $n \in \mathbb{N} \cap S_1$, se $n \in S$ então $n+1 < b$ ou $n+1 = b$; em ambos os casos $n + 1 \in S_1$. E se $n \notin S$, então $n \in I_b^*$ e daí, $n + 1 \in I_b^*$, pois $b < n + 1$. Logo, $n + 1 \in S_1$. Segue então do corolário 3.3.6 que $S_1 = I_a$. Logo, $S = [a, b]$. ∎

COROLÁRIO 3.3.8 *Seja* $m \in \mathbb{N}$ *e seja* $S \subseteq I_m$ *um conjunto tal que:*
(i) $m \in S$*;*
(ii) dado $n \in \mathbb{N}$*, se* $m \leq n$ *e se* $[m, n) \subseteq S$*, então* $n \in S$*.*
Sob estas hipóteses, $S = I_m$*.*

Dem. Basta notar que o conjunto $S' = [0, m) \cup S$ satisfaz as hipóteses do teorema 3.3.5. Portanto, $S = I_m$. ∎

3.4 Multiplicação, múltiplos e potências em $\mathbb{N}$.

DEFINIÇÃO 28 *A operação de multiplicação em* $\mathbb{N}$*,* $\cdot : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ *é aquela que satisfaz os dois seguintes axiomas:*
(M1) Para todo $a \in \mathbb{N}$*,* $a \cdot 0 = 0$*;*
(M2) para todo $a, b \in \mathbb{N}$*,* $a \cdot (b + 1) = a \cdot b + a$*.*

TEOREMA 3.4.1 *A operação de multiplicação sobre* $\mathbb{N}$ *satisfaz as seguintes propriedades:*
(P1) $0 \cdot n = 0 = n \cdot 0$*, para todo* $n \in \mathbb{N}$*.*
(P2) $1 = \min \mathbb{N}^*$ *é o elemento neutro para a operação de multiplicação em* $\mathbb{N}$*.*
(P3) Vale a distributividade da multiplicação em relação à soma, ou seja, para quaisquer $a, b, c \in \mathbb{N}$*,*
a) $(a + b) \cdot c = a \cdot c + b \cdot c$*, (à direita)*
b) $c \cdot (a + b) = c \cdot a + c \cdot b$ *(à esquerda).*
(P4) $(\mathbb{N}, \cdot)$ *é um monóide comutativo.*
(P5) Se $a, b \in \mathbb{N}$ *são tais que* $a \cdot b = 0$*, então* $a = 0$ *ou* $b = 0$*.*
(P6) Dados $a, b, c \in \mathbb{N}$ *quaisquer, se* $a < b$ *e* $0 < c$ *então* $a \cdot c < b \cdot c$*.*

Dem. Faremos a demonstração das propriedades 1 a 4 usando o princício de indução finita.

(P1). Seja $S = \{\, n \in \mathbb{N} \,|\, 0 \cdot n = 0 = n \cdot 0 \,\} \subseteq \mathbb{N}$.

(i) $0 \in S$, pois por (M1) da Definição 28, $0 \cdot 0 = 0$.

(ii) Dado $n \in \mathbb{N}$, se $n \in S$, então pela Definição 28 segue que

$$(n+1) \cdot 0 = 0 \text{ e } 0 \cdot (n+1) = 0 \cdot n + 0 = 0 + 0 = 0.$$

Logo, pelo Teorema 3.3.5, $S = \mathbb{N}$.

(P2). Seja $S = \{ n \in \mathbb{N} \,|\, 1 \cdot n = n \cdot 1 = n \} \subseteq \mathbb{N}$.

(i) Pelo item 1, $0 \in S$.

(ii) Dado $n \in \mathbb{N}$, se $n \in S$, então por $(M2)$ $1 \cdot (n+1) = 1 \cdot n + 1 = n + 1$. Portanto, $n + 1 \in S$.

Logo, pelo Teorema 3.3.5, $S = \mathbb{N}$.

(P3). Vamos provar a distributividade à direita. Sejam $a, b \in \mathbb{N}$ fixados e seja

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

(i) $0 \in S$, pois $(a+b) \cdot 0 = 0$ e $a \cdot 0 + b \cdot 0 = 0 + 0 = 0$.

(ii) Dado $c \in \mathbb{N}$, se $c \in S$, então por $(M2)$

$$(a+b) \cdot (c+1) = (a+b) \cdot c + (a+b) = a \cdot c + b \cdot c + a + b = a \cdot (c+1) + b \cdot (c+1).$$

Logo, $c+1 \in S$ e portanto, $S = \mathbb{N}$. A distributividade à esquerda segue de modo análogo.

(P4). Falta provar a associatividade e a comutatividade. Vejamos primeiro a associatividade, ou seja, dados quaisquer $a, b, c \in \mathbb{N}$, $(a \cdot b) \cdot c = a \cdot (b \cdot c)$.

Fixemos $a, b \in \mathbb{N}$ e seja $S = \{ c \in \mathbb{N} \,|\, (a \cdot b) \cdot c = a \cdot (b \cdot c) \} \subseteq \mathbb{N}$.

(i) $0 \in S$, pois $(a \cdot b) \cdot 0 = 0$ e $a \cdot (b \cdot 0) = a \cdot 0 = 0$.

(ii) Dado $c \in \mathbb{N}$, se $c \in S$, então por $(M2)$ e pela distributividade

$$(a \cdot b) \cdot (c+1) = (a \cdot b) \cdot c + a \cdot b = a \cdot (b \cdot c) + a \cdot b = a \cdot (b \cdot c + b) = a \cdot (b \cdot (c+1)).$$

Logo, $c + 1 \in S$ e portanto, $S = \mathbb{N}$.

Agora passemos à demonstração da comutatividade, ou seja, se $m, n \in \mathbb{N}$ então $m \cdot n = n \cdot m$. De fato, fixemos $m \in \mathbb{N}$ e seja $S = \{ n \in \mathbb{N} \,|\, m \cdot n = n \cdot m \} \subseteq \mathbb{N}$.

(i) Pelo item 1, $0 \in S$.

(ii) Se $n \in S$, então $m \cdot (n+1) = m \cdot n + m = n \cdot m + m = (n+1) \cdot m$. Logo, $n + 1 \in S$ e portanto, $S = \mathbb{N}$. Com isso provamos o item 4.

(P5). Suponhamos $a \neq 0$. Então $1 \leq a$ e além disso, $a - 1 \in \mathbb{N}$; daí $(a-1) \cdot b, (a-1) \cdot b + b \in \mathbb{N}$. Do fato de

$$0 \leq b \leq (a-1) \cdot b + b = [(a-1)+1] \cdot b = a \cdot b = 0,$$

segue que $b = 0$. Analogamente, supondo que $b \neq 0$ chegamos que $a = 0$. E isso mostra o resultado.

(P6). de $a < b$ segue que $0 < b - a$. Por hipótese $0 < c$, daí pelo item 5, $0 < (b-a) \cdot c$

e então

$$0 < b \cdot c - a \cdot c \implies a \cdot c < b \cdot c + (a - a) \cdot c \implies a \cdot c < b \cdot c. \quad \blacksquare$$

PROPOSIÇÃO 3.4.2 *A multiplicação em* $\mathbb{N}$ *satisfaz as seguintes propriedades:*
(i) Todo número natural não nulo é regular com a operação de multiplicação.
(ii) $U_{\cdot}(\mathbb{N}) = \{ 1 \}$.

Dem. (i) Sejam $a, b, c \in \mathbb{N}^*$ tais que $a \cdot b = a \cdot c$. Se tivéssemos $b \neq c$, então $b < c$ ou $c < b$. Mas daí, pelo ítem 6 do Teorema 3.4.1 teríamos que $a \cdot b < a \cdot c$ ou $a \cdot c < a \cdot b$, o que contradiz a hipótese $a \cdot b = a \cdot c$. Portanto, $b = c$.

(ii) Dado $a \in U_{\cdot}(\mathbb{N})$, existe um único $b \in \mathbb{N}$ tal que $a \cdot b = 1$. Então, pelo item 5 do Teorema 3.4.1 $1 \leq a$ e $1 \leq b$.

Suponhamos $1 < a$. Como $0 < b$, segue do item 6 do Teorema 3.4.1 que $b < a \cdot b = 1$, e portanto, $b = 0$, o que é um absurdo. Logo $a = b = 1$. $\blacksquare$

DEFINIÇÃO 29 *Dado* $a \in \mathbb{N}$, $a\mathbb{N} = \{ a \cdot n \mid n \in \mathbb{N} \}$ *é o conjunto dos múltiplos de* a *em* $\mathbb{N}$.

Observe que os múltiplos de a são os números naturais que satisfazem:
(i) $0 \cdot a = 0$ e
(ii) $(n + 1) \cdot a = n \cdot a + a$, para qualquer $n \in \mathbb{N}$.

TEOREMA 3.4.3 *Os múltiplos de um número natural* a *satisfazem as seguintes propriedades: dados quaisquer* $m, n \in \mathbb{N}$,

1. $(m + n) \cdot a = m \cdot a + n \cdot a$;
2. $(m \cdot n) \cdot a = m(n \cdot a) = n \cdot (m \cdot a)$;
3. $n \cdot (a + b) = n \cdot a + n \cdot b$.

Dem. Segue basicamente de (P3) e (P4) do Teorema 3.4.1. $\blacksquare$

DEFINIÇÃO 30 *Dado um* $a \in \mathbb{N}$, *a n-ésima potência de* a, *indicada por* a^n, *é a operação que satisfaz os dois seguintes axiomas:*
(i) $a^0 = 1$;
(ii) $a^{n+1} = a^n \cdot a$.
Denotaremos o conjunto das potências de a *por* $a^{\mathbb{N}}$; *ou seja,* $a^{\mathbb{N}} = \{ a^n \mid n \in \mathbb{N} \}$.

TEOREMA 3.4.4 *Dados quaisquer* $a, m, n \in \mathbb{N}$, *valem:*
1. $a^{m+n} = a^m \cdot a^n$;
2. $a^{m \cdot n} = (a^m)^n$;
3. $(a \cdot b)^n = a^n \cdot b^n$.

Dem. Faremos a demonstração dos itens pelo mesmo argumento: o Princípio de Indução Finita.

1. Fixemos $m \in \mathbb{N}$ e definamos $S_1 = \{\, n \in \mathbb{N} \,|\, a^{m+n} = a^m \cdot a^n \,\} \subseteq \mathbb{N}$.

(i) $0 \in S_1$, pois pela Definição 30, $a^{m+0} = a^m = a^m \cdot 1 = a^m \cdot a^0$.

(ii) Se $n \in S_1$, então por (ii) da Definição 30

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

Logo, pelo princípio de indução finita $S_1 = \mathbb{N}$. ∎

2. Fixemos $m \in \mathbb{N}$ e definamos $S_2 = \{\, n \in \mathbb{N} \,|\, a^{m \cdot n} = (a^m)^n \,\} \subseteq \mathbb{N}$.

(i) $0 \in S_2$, pois pelo intem (i) da Definição 30 temos que $a^{m \cdot 0} = a^0 = 1 = (a^m)^0$.

(ii) Se $n \in S_2$, então pelo item 1. demonstrado anteriormente

$$a^{m \cdot (n+1)} = a^{m \cdot n + m} = a^{mn} \cdot a^m = a^{\underbrace{m + m + \cdots + m}_{n \text{ vezes}}} \cdot (a^m) = \underbrace{a^m \cdot a^m \cdot \cdots \cdot a^m}_{n \text{ vezes}} \cdot a^m =$$

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

Logo, pelo princípio de indução finita $S_2 = \mathbb{N}$. ∎

3. Definamos $S_3 = \{\, n \in \mathbb{N} \,|\, (a \cdot b)^n = b^n \cdot a^n \,\} \subseteq \mathbb{N}$.

(i) $0 \in S_3$, pois, pelo intem (i) da Definição 30 temos que $(a \cdot b)^0 = 1 = 1 \cdot 1 = a^0 \cdot b^0$.

(ii) Se $n \in S_3$, então pela Definição 30

$$(a \cdot b)^{n+1} = (a \cdot b)^n \cdot (a \cdot b) = \underbrace{(a \cdot b) \cdots (a \cdot b)}_{n} \cdot (a \cdot b) = \underbrace{(a \cdot b) \cdots (a \cdot b)}_{n+1} = \underbrace{a \cdots a}_{n+1} \cdot \underbrace{b \cdots b}_{n+1} =$$

$a^{n+1} \cdot b^{n+1}$

Logo, pelo princípio de indução finita $S_3 = \mathbb{N}$. ∎

Para finalizar esta seção vamos demonstrar que qualquer semigrupo ordenado $(E, +, \leq)$ que satisfaz os axiomas N1, N2, N3 e N4, é determinado de modo único, a menos de um isomorfismo ordenado, ou seja, $(E, +, \leq)$ é isomorfo a $\mathbb{N}$ (veja a Definição 27). É importante observar que se $(E, +, \leq)$ satisfaz os axiomas N1, N2, N3 e N4, então também satisfaz as mesmas propriedades de $\mathbb{N}$ estabelecidas até aqui.

Lema 3.4.5 *Seja $(E, +, \leq)$ um semigrupo ordenado que satisfaz os axiomas N1, N2, N3 e N4, e sejam $0' = \min E$ e $1' = \min(E - \{0'\})$ os elementos neutros da adição e da multiplicação, respectivamente. Se fizermos a identificação $0' = 0 \cdot 1'$, então:*
(a) todo elemento $n' \in E$ pode ser representado como $n \cdot 1'$, ou seja $n' = n \cdot 1'$;
(b) $(m + n)' = m' + n'$, $\forall\ m, n \in \mathbb{N}$.

Dem. Usaremos o princípio de indução finita.

(a) Seja $S = \{n' \in E \,|\, n' = n \cdot 1'\}$.

(i) Por hipótese $0' \in S$. Observemos que, chamando $1' + 1'$ de $2'$, temos que $2' = 2 \cdot 1'$.

(ii) Dados $n' \in E$, se $n' \in S$, então $n' + 1' = n \cdot 1' + 1 \cdot 1' = (n + 1) \cdot 1'$. Logo, $n' + 1' \in S$.

Portanto, pelo princípio de indução finita $S = E$.

(b) Fixado $n \in \mathbb{N}$, seja $S' = \{m' \in E \,|\, (m + n)' = m' + n' \}$.

(i) Como $0'$ é o elemento neutro de E, $0' + n' = n' = (n + 0)'$, e portanto $0' \in S'$.

(ii) Se $m' \in S'$, então $(m + 1 + n)' = (m + 1 + n) \cdot 1' = m \cdot 1' + 1 \cdot 1' + n \cdot 1' = (m + 1) \cdot 1' + n' = (m + 1)' + n'$. Portanto, $(m + 1)' \in S'$.

Logo, pelo princípio de indução finita $S' = E$. ∎

Teorema 3.4.6 *Se $(E, +, \leq)$ é um semigrupo ordenado que satisfaz os axiomas N1, N2, N3 e N4, então $(E, +, \leq)$ é ordenadamente isomorfo a $\mathbb{N}$ (no sentido da Definição 27).*

Dem. Lembremos que $\mathbb{E} = (E, +, \leq)$ satisfaz as mesmas propriedades de $\mathbb{N}$ estabelecidas até aqui. Seja $f : \mathbb{N} \to \mathbb{E}$ a função definida por $f(n) = n \cdot 1'$.

(a) Dados $m, n \in \mathbb{N}$, pelo Lema 3.4.5 $f(m + n) = (m + n) \cdot 1' = m \cdot 1' + n \cdot 1' = f(m) + f(n)$. Logo f é homomorismo.

(b) provemos que f é bijetora. Do Lema 3.4.5 segue que f é sobrejetora. Agora, f é injetora, pois dados $m, n \in \mathbb{N}$,

$$f(m) = f(n) \iff m \cdot 1' = n \cdot 1' \iff (m - n) \cdot 1' = 0' = 0 \cdot 1' \iff m = n.$$

(c) Dados $m, n \in \mathbb{N}$, se $m \leq n$ então $f(m) \leq f(n)$. De fato, se $m \leq n$ então $n - m \in \mathbb{N}$ e $n = m + (n - m)$; daí, por (a) $f(n) = f(m) + f(n - m)$. Logo, pela propriedade P1 do Teorema 3.3.2 segue que $f(m) \leq f(n)$. E com isso o teorema está demonstrado. ∎

3.5 Aplicação: Demonstração por indução finita.

De acordo com Hefez (2003), o método de indução foi enunciada explicitamente pela primeira vez pelo matemático italiano Francesco Maurolycus (1494-1575) para demonstrar que, dado um $n \in \mathbb{N}$, $1 + 3 + \cdots + (2n - 1) = n^2$. Porém, segundo Garbi (2006), esse método somente foi popularizado muitos anos mais tarde pelo matemático francês Blaise Pascal (1623-1662) em suas pesquisas sobre o Triângulo Aritmético.

O princípio da indução finita foi enunciada como o 4º dos famosos 'Axiomas de Peano' do matemático italiano Giuseppe Peano no ano de 1889 em sua obra "Arithmetic Principia Novo Methodo Exposita", em tradução livre, Novo Método de Exposição dos Princípios da Aritmética. Mas, apesar de ter sido anunciada como um axioma, é um fato matemático passível de demonstração, como foi feito no Teorema 3.3.5.

Veremos agora que o princípio de indução finita é uma ferramenta muito útil para se demonstrar propriedades associadas aos números naturais da seguinte forma: Dada uma proprosição $P(n)$ (associada a cada número natural n) que não se sabe se é verdadeira ou falsa, deseja-se verificar se ela é verdadeira para todo $n \in \mathbb{N}$, ou para todo número natural $n \geq m$ ou então para todo número natural $n \in [m, r]$.

Podemos nos deparar com uma das seguintes situações: Com uma proposição $P(n)$ já formulada para ser verificada; ou então, a partir de observações (ou casos) particulares, teremos que formular uma proposição a ser verificada. Vejamos alguns exemplos dessas situações:

Exemplo 3.5.1 *Considere a seguinte proposição $P(n)$, $n \in \mathbb{N}^*$: "A soma dos n primeiros números naturais pares não nulos é $n \cdot (n+1)$." Podemos verificá-la usando o princípio de indução finita (Corolário 3.3.6) do seguinte modo:*

Seja $S = \{\, n \in \mathbb{N}^* \,|\, 2 + 4 + \cdots + 2n = n \cdot (n+1) \,\}$. Como $2 = 1 \cdot (1+1)$, segue que $1 \in S$. Agora, supondo que um $n \in S$ então $2 + 4 + \cdots + 2n + 2 \cdot (n+1) = n \cdot (n+1) + 2 \cdot (n+1) = (n+1) \cdot (n+2) = (n+1) \cdot [(n+1)+1]$; portanto, pelo corolário supracitado, $S = \mathbb{N}^*$, ou seja, $2 + 4 + \cdots + 2n = n \cdot (n+1)$, para todo número natural $n \geq 1$.

Exemplo 3.5.2 *Considere a seguinte proposição $P(n)$, $n \in \mathbb{N}^*$: Para todo $n \in \mathbb{N}$, $n \leq n^2$. Assim como no caso anterior, podemos verificá-la aplicando o princípio de indução finita procedendo do seguinte modo: chamemos de $S = \{\, n \in \mathbb{N} \,|\, n \leq n^2 \,\}$. Então obviamente $0 \in S$, e, dado $n \in \mathbb{N}$, se $n \in S$, então $n + 1 \leq n^2 + 1 \leq n^2 + 2n + 1 = (n+1)^2$ e isso implica que $n + 1 \in S$. Portanto, pelo princípio de indução finita (Teorema 3.3.5) $S = \mathbb{N}$, ou seja, $n \leq n^2 \ \forall\, n \in \mathbb{N}$.*

Os exemplos acima sugerem que o processo de demonstração geralmente é sempre o mesmo: Dada uma proposição $P(n)$, fazemos sua verificação para um índice inicial m; se $P(m)$ é verdadeira, passamos para a segunda etapa, que consiste em supor que $P(n)$ com $n \geq m$ é verdadeira e então provar que $P(n+1)$ também é verdadeira. A primeira etapa, que consiste em provar que $P(m)$ é verdadeira, chama-se **base da indução finita**; a segunda etapa chama-se **etapa de indução finita**. Supor que $P(n)$ é verdadeira chama-se **hipótese de indução**. Isso nos leva à formulação dos seguintes métodos de demonstração por indução finita:

Teorema 3.5.3 *Seja $m \in \mathbb{N}$. Para cada $n \in I_m$, seja $P(n)$ uma propriedade (a ser verificada), tal que:*
1. $P(m)$ é verdadeira;
2. para todo $n \in I_m$, se $P(n)$ é verdadeira, então $P(n+1)$ é verdadeira.
Nestas condições, $P(n)$ é verdadeira para todo $n \in I_m$.

Dem. Seja $S = \{\, n \in \mathbb{N} \,|\, n \geq m \text{ e } P(n) \text{ é verdadeira} \,\}$. Por *1.* temos que $m \in S$. Pelo ítem *2.* temos que, se $n \in S$ então $n+1 \in S$. Logo, pelo Corolário 3.3.6 $S = I_m$ e portanto, $P(n)$ é verdadeira para todo $n \geq m$. ∎

É essencial a verificação dos dois itens (1. e 2.) do Teorema 3.5.3 para se concluir a partir dele que uma propriedade $P(n)$ é verdadeira. Vejamos dois exemplos para ilustrar que ambas são imprescindíveis:

EXEMPLO 3.5.4 *Consideremos a seguinte propriedade: "Para todo $n \in \mathbb{N}$, n^2+n+1 é par". Supondo $P(n)$ verdadeira temos que $P(n+1)$ também o é. De fato, $(n+1)^2+(n+1)+1 = n^2+2n+1+n+1+1 = (n^2+n+1)+2(n+1)$; já que $2(n+1)$ é par e por hipótese n^2+n+1 é par, o resultado segue do Teorema 3.5.3. Mas a propriedade é falsa, pois 0^2+0+1 é ímpar! O problema foi que faltou a verificação do item 1. do referido teorema. Por ser de fácil verificação, pode acontecer de querermos ir imediatamente para o item 2., mas jamais devemos fazer isso, pois caso façamos podemos chegar a resultados completamente errados, como nesse exemplo.*

EXEMPLO 3.5.5 *Investiguemos a primalidade do número n^2-n+41. Tomando, por exemplo, os valores $0, 1, 2, 3, 4, 5, 6, 7$ para n obtemos respectivamente, $41, 41, 43, 47, 53, 61, 71, 83$, para n^2-n+41 e todos eles são primos (na verdade, para n até 40, n^2-n+41 é primo). Isso pode nos levar a conjecturar (ou concluir precipitadamente) que "para todo $n \in \mathbb{N}$, n^2-n+41 é primo", sem perceber que para $n = 41$, $n^2-n+41 = 41^2$ que obviamente não é primo. Se tentarmos verificar o item 2. do Teorema 3.5.3 jamais chegaremos à conclusão de que $(n+1)^2-(n+1)+41$ é primo.*

Para finalizar enunciamos as seguintes versões do princípio de indução finita que são geralmente usadas para demonstração de proposições mais sofisticadas relacionadas aos números naturais.

TEOREMA 3.5.6 *Seja $m \in \mathbb{N}$. Para cada $n \geq m$ seja $P(n)$ uma propriedade (a ser verificada), tal que:*
1. $P(m)$ é verdadeira;
2. para todo $n \in I_m$, se $P(k)$ é verdadeira para todo $k \in [m, n)$, então $P(n)$ é verdadeira. Nestas condições, $P(n)$ é verdadeira para todo $n \in I_m$.

Dem. Segue imediatamente do Corolário 3.3.6. ∎

EXEMPLO 3.5.7 *Dado $n \in \mathbb{N}$ temos que $2^n < n!$ para todo $n \geq 4$.*

De fato, para $n = 4$, $2^4 = 16 < 4! = 24$. Suponha que $2^n < n!$ é verdadeira para algum $n \in \mathbb{N}$ tal que $n \geq 4$. Assim, temos que $2^{n+1} = 2^n \cdot 2 < n! \cdot 2$ por hipótese de indução. Como $n \geq 4$, $n+1$ é sempre maior que 2, então
$2^{n+1} = 2^n \cdot 2 < n! \cdot 2 < n! \cdot (n+1) = (n+1)!$
Logo, a propriedade está demonstrado por indução.

Teorema 3.5.8 *Sejam $a, b \in \mathbb{N}$ tais que $a \leq b$. Para cada número natural $n \in [a, b]$ (i.e., $a \leq n \leq b$) seja $P(n)$ uma propriedade (a ser verificada) tal que:*
1. $P(a)$ é verdadeira;
2. para todo $n \in \mathbb{N}$, se $a \leq n < b$ e se $P(n)$ é verdadeira, então $P(n+1)$ também é verdadeira.
Nestas condições, $P(n)$ é verdadeira para todo $n \in [a, b]$.

Dem. A demonstração deste fato segue imediatamente do Corolário 3.3.7. ∎

3.6 Aplicação: Notação de Somatório e de Produtório.

A notação de somatório e produtório são imprescindíveis na resolução de problemas de matemática discreta. Elas nos permitem simplificar a exibição de somas e produtos de sequências numéricas.

Antes de definirmos a notação somatório e produtório, precisaremos definir sequências numéricas.

Definição 31 *Chamamos de sequência de números reais a função $x : \mathbb{N} \longrightarrow \mathbb{R}$ que associa a cada número natural n um elemento x_n.*

Representamos a sequência $(x_1, x_2, \cdots, x_n)$ na forma $(x_n)_{n\geq 1}$ e chamaremos x_n de n-ésimo termo da sequência.

Exemplo 3.6.1 *A sequência definida por $x_n = 2^n$, $n \in \mathbb{N}$ é a sequência $x_n = (2, 4, 8, \cdots)$ já a sequência cujo termo geral é $y_n = \dfrac{n}{n+1}$ é a sequência $y_n = \left(\dfrac{1}{2}, \dfrac{2}{3}, \dfrac{3}{4}, \cdots\right)$.*

Definição 32 *Chamamos de **Somatório** a representação matemática da soma dos termos de uma sequência. .*

Utiliza-se a letra grega sigma maiúscula Σ para simbolizar o somatório. Na notação $\sum_{i=m}^{n} x_i$ a letra i denota o indexador do somatório, m é o limite inferior e n é o limite superior do somatório. Assim,

$$\sum_{i=m}^{n} x_i = x_m + x_{m+1} + \cdots + x_n.$$

Observação 8 *Podemos descrever também uma soma com um número infinito de parcelas. Dada a sequência infinita $(x_1, x_2, \cdots, x_n, \cdots)$ representamos o seu somatório por $\sum_{i=1}^{\infty} x_i$.*

Proposição 3.6.2 *Seja a uma constante real e $(x_i)_{i\in\mathbb{N}}$ e $(y_i)_{i\in\mathbb{N}}$ sequências de números reais. O somatório satisfaz as seguintes propriedades:*

1. $\sum_{i=m}^{n} a = [n-(m-1)] \cdot a$;
2. $\sum_{i=m}^{n} a \cdot x_i = a \cdot \sum_{i=m}^{n} x_i$;
3. $\sum_{i=m}^{n} (x_i \pm y_i) = \sum_{i=m}^{n} x_i \pm \sum_{i=m}^{n} y_i$;
4. $\sum_{i=m}^{n} (x_i - x_{i-1}) = x_n - x_{m-1}$.

Dem. 1. É imediato uma vez que $\sum_{i=m}^{n} a = \underbrace{a + a + \cdots + a}_{[n-(m-1)] \ vezes} = [n-(m-1)] \cdot a$.

2. Pelo item 3 do Teorema 3.4.1, temos que:

$$\sum_{i=m}^{n} a \cdot x_i = a \cdot x_m + a \cdot x_{m+1} + \cdots + a \cdot x_n = a \cdot (x_m + x_{m+1} + \cdots + x_n) = a \cdot \sum_{i=m}^{n} x_i.$$

3. Da associatividade segue que:

$$\sum_{i=m}^{n} (x_i \pm y_i) = (x_m \pm y_m) + (x_{m+1} \pm y_{m+1}) + \cdots + (x_n \pm y_n) = (x_m + x_{m+1} \cdots x_n) \pm (y_m + y_{m+1} + \cdots + n_n) = \sum_{i=m}^{n} x_i \pm \sum_{i=m}^{n} y_i.$$

4. É fácil perceber que:

$$\sum_{i=m}^{n} (x_i - x_{i-1}) = (x_m - x_{m-1}) + (x_{m+1} - x_m) + \cdots + (x_n - x_{n-1}) = x_n - x_{m-1}. \quad \blacksquare$$

EXEMPLO 3.6.3 *A soma dos n primeiros números ímpares naturais é representada na notação de somatório por*

$$\sum_{i=1}^{n} (2i-1) = 1 + 3 + \cdots (2n-1).$$

EXEMPLO 3.6.4 *A média aritmética* $(\overline{x})$ *de n termos de uma sequência* $(x_i)_{i \in \mathbb{N}}$ *é representada por somatório da seguinte forma:*

$$\overline{x} = \frac{1}{n} \cdot \sum_{i=1}^{n} x_i = \frac{x_1 + x_2 + \cdots x_n}{n}.$$

Garbi (2006) conta a história de um feito do matemático alemão Carl Friedrich Gauss. Com apenas 9 anos seu professor de aritmética pediu-lhe que somasse os naturais de 1 a 100. Gauss então utilizou-se de um método simples, ilustrado abaixo, e chegou ao resultado 5050.

$$\begin{array}{r} S = 1 + 2 + \cdots + 99 + 100 \\ \underline{S = 100 + 99 + \cdots + 2 + 1} \\ 2S = 101.100 \\ S = 5050 \end{array} \quad +$$

Com este método chegamos facilmente a conclusão de que a soma (S_n) dos n primeiros naturais é $S_n = \dfrac{n(n+1)}{2}$. Podemos reescrever o método de Gauss usando a notação de somatório e atentando-se para a Proposição 3.6.2.
Primeiramente obervemos que:
$\sum_{i=1}^{n} i = 1 + 2 + \cdots + (n-1) + n$ e que
$\sum_{i=1}^{n} (n - i + 1) = n + (n-1) + \cdots + 2 + 1$
Assim,

$$\begin{aligned} S_n = \sum_{i=1}^{n} i &= \sum_{i=1}^{n} (n - i + 1) \\ \Longrightarrow 2S_n &= \sum_{i=1}^{n} i + \sum_{i=1}^{n} (n - i + 1) \\ \Longrightarrow 2S_n &= \sum_{i=1}^{n} i + \sum_{i=1}^{n} n - \sum_{i=1}^{n} i + \sum_{i=1}^{n} 1 = n \cdot n + n \cdot 1 \\ \Longrightarrow S_n &= \frac{n(n+1)}{2}. \end{aligned} \tag{3.4}$$

Definição 33 *Chamamos de* ***Produtório*** *a representação do produto dos termos de uma sequência numérica.*

Notação: Utilizamos a letra grega pi maiúscula Π para representar o produtório. O produtório simples seria representado na forma $\prod_{i=m}^{n} i = m \cdot (m+1) \cdot \ \cdots \ \cdot n$.

Observação 9 *Assim como no somatório, também podemos ter um produto de uma sequência numérica infinita. Dada a sequência infinita $(x_1, x_2, \cdots, x_n, \cdots)$ representamos o seu produtório por $\prod_{i=1}^{\infty} x_i$.*

Proposição 3.6.5 *Seja a uma constante real e $(x_i)_{i\in\mathbb{N}}$ e $(y_i)_{i\in\mathbb{N}}$ sequências de números reais. O Produtório satisfaz as seguintes propriedades:*

1. $\prod_{i=m}^{n} a = a^{n-(m-1)}$.
2. $\prod_{i=1}^{n} i = n!$.
3. $\prod_{i=m}^{n} x_i \cdot y_i = \prod_{i=m}^{n} x_i \cdot \prod_{i=m}^{n} y_i$.
4. $\prod_{i=m}^{n} a \cdot x_i = a^{n-(m-1)} \cdot \prod_{i=m}^{n} x_i$.

5. $\prod_{i=m}^{n} {x_i}^k = \left(\prod_{i=m}^{n} x_i\right)^k$.

6. $\prod_{i=m}^{n} \frac{x_i}{x_{i+1}} = \frac{x_m}{x_{n+1}}$

Dem. 1. $\prod_{i=m}^{n} a = \underbrace{a \cdot a \cdot \cdots \cdot a}_{[n-(m-1)] \ vezes} = a^{n-(m-1)}$.

2. $\prod_{i=1}^{n} i = 1 \cdot 2 \cdot \cdots \cdot n = n!$

3. $\prod_{i=m}^{n} x_i \cdot y_i = (x_1 \cdot y_1) \cdot (x_2 \cdot y_2) \cdot \cdots \cdot (x_n \cdot y_n) = (x_1 \cdot x_2 \cdot \cdots \cdot x_n) \cdot (y_1 \cdot y_2 \cdot \cdots \cdot y_n) = \prod_{i=m}^{n} x_i \cdot \prod_{i=m}^{n} y_i$

4. $\prod_{i=m}^{n} a \cdot x_i = (a \cdot x_1) \cdot (a \cdot x_2) \cdot \cdots \cdot (a \cdot x_n) = a^{n-(m-1)} \cdot \prod_{i=m}^{n} x_i$.

5. $\prod_{i=m}^{n} {x_i}^k = (x_1)^k \cdot (x_2)^k \cdot \cdots \cdot (x_n)^k = (x_1 \cdot x_2 \cdot \cdots \cdot x_n)^k = \left(\prod_{i=m}^{n} x_i\right)^k$.

6. $\prod_{i=m}^{n} \frac{x_i}{x_{i+1}} = \frac{x_m}{x_{m+1}} \cdot \frac{x_{m+1}}{x_{m+2}} \cdot \cdots \cdot \frac{x_n}{x_{n+1}} = \frac{x_m}{x_{n+1}}$

EXEMPLO 3.6.6 *Chama-se Fatorial de um número natural n, representado por n! o produtório:*

$$n! = \prod_{i=1}^{n} i = 1 \cdot 2 \cdot \cdots \cdot n$$

EXEMPLO 3.6.7 *A média geométrica de n termos de uma sequência* $(x_1, x_2, \cdots, x_n)$ *é representada utilizando o produtório na forma:*

$$\left(\prod_{i=1}^{n} x_i\right)^{\frac{1}{n}} = \sqrt[n]{x_1 \cdot x_2 \cdot \cdots \cdot x_n}$$

EXEMPLO 3.6.8 *A combinação simples de um número n de elementos tomados k a k é calculado como* $C_{n,k} = \frac{n!}{k!(n-k)!}$. *Na representação de produtório a fórmula da combinação simples é escrita como,*

$$C_{n,k} = \frac{\prod_{i=1}^{n} i}{(\prod_{i=1}^{k} i) \cdot (\prod_{i=1}^{n-k} i)}$$

4 Números Inteiros

Neste capítulo vamos construir o conjunto dos números inteiros $\mathbb{Z}$ a partir do conjunto dos números naturais $\mathbb{N}$ pelo processo de simetrização da adição definida sobre $\mathbb{N}$. Veremos que $\mathbb{N}$ pode ser considerado uma parte de $\mathbb{Z}$ e estenderemos suas propriedades para $\mathbb{Z}$. Vamos também explorar alguns resultados básicos de teoria dos números inteiros.

Sabemos que, dados a, $b \in \mathbb{N}$, existe $x \in \mathbb{N}$ tal que $b + x = a$ se, e somente se, $b \leq a$. Ou seja, em $\mathbb{N}$ a diferença $a - b$ faz sentido se, e somente se, $b \leq a$. Na ampliação mínima de $\mathbb{N}$ a ser feita, essa diferença sempre fará sentido.

Os elementos de $\mathbb{Z}$ serão pares ordenados (a, b) de números naturais que satisfazem equações da forma $a+d = b+c$, onde c e d são números naturais arbitrários. Mas observe que, a diferença $a-b$ satisfaz a equação $d+x = c$ se, e somente se, $a+d = b+c$. Isto mostra que não basta introduzir os novos elementos como pares ordenados de números naturais, deve-se também estabelecer um critério para que dois pares ordenados representem a mesma diferença.

4.1 Construção do Conjunto dos Números Inteiros

Vamos primeiramente listar as propriedades satisfeitas por $\mathbb{N}$ a serem utilizadas nesta seção. Dados a, b, $c \in \mathbb{N}$, valem:

Propriedades da adição:	Propriedades da multiplicação:
$(A1)$ $(a + b) + c = a + (b + c)$;	$(M1)$ $(a \cdot b) \cdot c = a \cdot (b \cdot c)$;
$(A2)$ $a + b = b + a$;	$(M2)$ $a \cdot b = b \cdot a$;
$(A3)$ $a + 0 = a$;	$(M3)$ $a \cdot 1 = a$.
(LCA) $a + b = a + c \implies b = c$.	(D) Distributividade: $a \cdot (b + c) = a \cdot b + a \cdot c$.

Seja $E = \mathbb{N} \times \mathbb{N} = \{ (a, b) \mid a, b \in \mathbb{N}\}$. Com o propósito de eliminar as ambiguidades, definamos a seguinte relação sobre E:

Definição 34 *Dados (a, b), $(c, d) \in E$, definimos a relação R como*

$$(a, b)R(c, d) \text{ se, e somente se, } a + d = b + c.$$

Por exemplo, $(a, a)R(b, b)$, $\forall$ a, $b \in \mathbb{N}$. Em particular, $(a, a)R(0, 0)$ $\forall$ $a \in \mathbb{N}$.

Proposição 4.1.1 *R é uma relação de equivalência sobre E.*

Dem. Dado $(a, b) \in E$, como $a + b = b + a$ então $(a, b)R(a, b)$. Portanto R é reflexiva.

Dados (a,b), $(c,d) \in E$, pela Definição 34 $(a,b)R(c,d)$ equivale a dizer que $a+d = b+c$. Então $c+b = d+a$, ou seja, $(c,d)R(a,b)$. Logo R é simétrica.

Agora, sejam (a,b), (c,d), $(e,f) \in E$, tais que $(a,b)R(c,d)$ e $(c,d)R(e,f)$. Isto equivale a afirmar que $a+d = b+c$ e $c+f = d+e$. Então,

$$(a+d)+f = (b+c)+f \text{ e } b+(c+f) = b+(d+e).$$

Segue portanto da propriedade A1 e da Lei do Cancelamento que, $a+f = b+e$, ou seja, $(a,b)R(e,f)$. Logo R é transitiva. Com isso fica provado que R é uma relação de equivalência. ∎

Dado $(a,b) \in E$, $\overline{(a,b)}$ representará a classe de equivalência módulo R determinada por (a,b), isto é,

$$\overline{(a,b)} = \{\ (x,y) \mid (x,y)R(a,b)\ \}.$$

Por exemplo, $\overline{(a,a)} = \overline{(0,0)}$, $\forall a \in \mathbb{N}$.

Indicaremos por Z o conjunto quociente E/R, ou seja, $Z = \mathbb{N}\times\mathbb{N}/R$. Sabemos que:

1) dados (a,b), $(c,d) \in E$, $\overline{(a,b)} = \overline{(c,d)} \iff (a,b)R(c,d) \iff a+d = b+c$;

2) $Z := E/R$ é uma partição de E.

Apresentaremos nas próximas duas seções as operações definidas para o conjunto Z e suas propriedades.

4.1.1 Adição em Z.

Definição 35 *Dados $\overline{(a,b)}$, $\overline{(c,d)} \in Z$, definimos:*

$$\overline{(a,b)} + \overline{(c,d)} = \overline{(a+c, b+d)}. \tag{4.1}$$

Abaixo verificamos que a operação definida em (4.1) está bem definida, isto é, independentemente dos representantes das classes de equivalência que somarmos chegaremos ao mesmo valor.

Proposição 4.1.2 *Se $\overline{(a,b)} = \overline{(a',b')}$ e $\overline{(c,d)} = \overline{(c',d')}$, então $\overline{(a+c,b+d)} = \overline{(a'+c',b'+d')}$.*

Dem. $\overline{(a,b)} = \overline{(a',b')}$ e $\overline{(c,d)} = \overline{(c',d')} \iff (a,b)R(a',b')$ e $(c,d)R(c',d')$

$$\iff a+b' = b+a' \text{ e } c+d' = d+c'.$$

Somando-se as duas igualdades acima, obtemos:

$$(a+b')+(c+d') = (b+a')+(d+c'),$$

ou seja,

$$(a+c)+(b'+d') = (b+d)+(a'+c')$$

e portanto, $(a+c, b+d)R(a'+c', b'+d')$. Logo, $\overline{(a+c, b+d)} = \overline{(a'+c', b'+d')}$. ∎

TEOREMA 4.1.3 *O conjunto $(Z, +)$ é um monóide comutativo.*

Dem. Associatividade: Dados $\overline{(a,b)}$, $\overline{(c,d)}$, $\overline{(e,f)} \in Z$, como vale a associatividade para a adição em $\mathbb{N}$, segue que

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

Comutatividade: Dados $\overline{(a,b)}$, $\overline{(c,d)} \in Z$, como a adição em $\mathbb{N}$ é comutativa, segue que

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

Elemento neutro: Vamos primeiro encontrar o possível elemento neutro. Dado $\overline{(a,b)} \in Z$, segue da Lei do Cancelamento em $\mathbb{N}$ que

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

Daí fica evidente que o elemento neutro é $\overline{(0,0)}$. E com isso provamos o teorema. ∎

PROPOSIÇÃO 4.1.4 *O conjunto $(Z, +)$ satisfaz as seguintes propriedades:*
***1**. Dado $\overline{(a,b)} \in Z$, existe um único elemento de Z, denotado por $-\overline{(a,b)}$ (lê-se simétrico de $\overline{(a,b)}$), tal que, $\overline{(a,b)} + (-\overline{(a,b)}) = \overline{(0,0)}$.*
***2**. Todo elemento de Z é regular para a soma, isto é, em $(Z, +)$ vale a lei do cancelamento da adição (LCA): se $\overline{(a,b)} + \overline{(c,d)} = \overline{(a,b)} + \overline{(e,f)}$, então $\overline{(c,d)} = \overline{(e,f)}$.*

Dem. 1. Dado $\overline{(a,b)} \in Z$,

$$\overline{(a,b)} + \overline{(c,d)} = \overline{(0,0)} \iff \overline{(a+c, b+d)} = \overline{(0,0)} \iff a+c = b+d.$$

Para a igualdade $a+c = b+d$ se realizar, devemos tomar $c = b$ e $d = a$. Assim, o simétrico de $\overline{(a,b)} \in Z$ deve ser $\overline{(b,a)}$, ou seja, $-\overline{(a,b)} = \overline{(b,a)}$. De fato,

$$\overline{(a,b)} + \overline{(b,a)} = \overline{(a+b, a+b)} = \overline{(0,0)}.$$

2. Dado $\overline{(a,b)} \in Z$,

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

Portanto, vale a Lei do Cancelamento em Z. ■

Notação:

1. Dados $x = \overline{(a,b)}, y = \overline{(c,d)} \in Z$, temos pelo Teorema 4.1.3 que $-y = \overline{(d,c)} \in Z$ e $x + (-y) \in Z$. Vamos denotar $x + (-y)$ por $x - y$. Daí segue que a equação $z + y = x$, com z como incógnita, tem sempre solução em Z, a saber: $z = x - y$.

2. Vamos denotar o elemento neutro de $+$ em Z por $0'$, ou seja, $\overline{(0,0)} := 0'$.

4.1.2 Multiplicação em Z.

Definição 36 *Chamaremos de multiplicação em Z à operação definida por*

$$\overline{(a,b)} \cdot \overline{(c,d)} = \overline{(ac+bd, ad+bc)}, \tag{4.2}$$

para quaisquer $\overline{(a,b)}$, $\overline{(c,d)} \in Z$.

Assim como na adição, temos:

Proposição 4.1.5 *A multiplicação 4.2 em Z está bem definida, ou seja, se $\overline{(a,b)} = \overline{(a',b')}$ e $\overline{(c,d)} = \overline{(c',d')}$, então $\overline{(a,b)} \cdot \overline{(c,d)} = \overline{(a',b')} \cdot \overline{(c',d')}$, isto é, $\overline{(ac+bd, ad+bc)} = \overline{(a'c'+b'd', a'd'+b'c')}$.*

Dem. Como antes, $\overline{(a,b)} = \overline{(a',b')}$ e $\overline{(c,d)} = \overline{(c',d')} \iff a + b' = b + a'$ e $c + d' = d + c'$.
Logo,

$$c(a+b') + a'(c+d') + d(b+a') + b'(d+c') = c(b+a') + a'(d+c') + d(a+b') + b'(c+d')$$
$$\iff (ac+bd) + (a'd'+b'c') + cb' + a'c + da' + b'd = (ad+bc) + (a'c'+b'd') + ca' + a'd + db' + b'c$$
$$\iff (ac+bd) + (a'd'+b'c') = (ad+bc) + (a'c'+b'd')$$
$$\iff \overline{(ac+bd, ad+bc)} = \overline{(a'c'+b'd', a'd'+b'c')}. \quad ■$$

Proposição 4.1.6 *O conjunto $(Z, \cdot)$ é um monóide comutativo e satisfaz a distributividade em relação à soma, ou seja, em $(Z, \cdot)$ valem **(M1)** a associatividade, **(M2)** a comutatividade, **(M3)** existe um único $1' \in \mathbb{Z}$ tal que $\overline{(a,b)} \cdot 1' = \overline{(a,b)}$, $\forall\ \overline{(a,b)} \in \mathbb{Z}$, e **(D)** $x \cdot (y+z) = x \cdot y + x \cdot z$, $\forall\ x, y, z \in \mathbb{Z}$.*

Dem. (M3) Primeiramente devemos encotrar um candidato a elemento neutro, depois verificamos que ele é de fato o elemento neutro.

Dado $\overline{(a,b)} \in Z$,

$$\begin{aligned} \overline{(a,b)} \cdot \overline{(x,y)} = \overline{(a,b)} &\iff \overline{(ax+by, bx+ay)} = \overline{(a,b)} \\ &\iff ax + by + b = ay + bx + a \\ &\iff ax + by + b = ay + bx + a \\ &\iff a(y+1-x) = b(y+1-x), \end{aligned}$$

que pela arbitrariedade de a e b, implica que $x = y + 1$, e consequentemente,

$$\overline{(x,y)} = \overline{(y+1,y)} = \overline{(y,y)} + \overline{(1,0)} = 0' + \overline{(1,0)} = \overline{(1,0)}.$$

Seja $1' = \overline{(1,0)}$. De fato $1'$ é elemento neutro, pois é imediato que, dado $\overline{(a,b)} \in Z$, $\overline{(a,b)} \cdot \overline{(1,0)} = \overline{(a,b)}$.

A unicidade é bem simples: Se $e' \in Z$ é tal que, $\overline{(a,b)} \cdot e' = \overline{(a,b)}$, $\forall\ \overline{(a,b)} \in Z$, então $e' = 1' \cdot e' = 1'$. ∎

4.1.3 Relação de ordem em Z.

Sabemos que $(\mathbb{N}, \leq)$ é um monóide ordenado com a ordem $\leq$ compatível com a adição. Desejamos definir uma relação de ordem $\leq$ sobre Z, extensão de $\leq$ em $\mathbb{N}$, no sentido de que, $\leq$ sobre Z herde todas as propriedades de $(\mathbb{N}, \leq)$.

Definição 37 *Dados $x = \overline{(a,b)}$, $y = \overline{(c,d)} \in Z$, diremos que*

$$x \leq y \text{ se, e somente se, } a + d \leq b + c.$$

Por exemplo, um $x = \overline{(a,b)} \in Z, \quad x \leq 0'$ se, e somente se, $a \leq b$.

Proposição 4.1.7 *A relação $\leq$ da Definição 37 está bem definida, ou seja, se $\overline{(a,b)} = \overline{(a',b')}$ e $\overline{(c,d)} = \overline{(c',d')}$, então $\overline{(a,b)} \leq \overline{(c,d)} \iff \overline{(a',b')} \leq \overline{(c',d')}$.*

Dem. $\overline{(a,b)} \leq \overline{(c,d)} \iff a+d \leq b+c$. Por hipótese $a+b' = b+a'$ e $c+d' = d+c'$. Daí, pela hipótese e pela compatibilidade de $\leq$ em relação à adição em $\mathbb{N}$ segue que

$$(a'+d')+(a+d) \leq (a'+d')+(b+c) = (b+a')+(c+d') = (a+b')+(d+c')$$

e consequentemente, $(a'+d')+(a+d) \leq (b'+c')+(a+d)$. Daí, $(a'+d') \leq (b'+c')$. Portanto, $\overline{(a',b')} \leq \overline{(c',d')}$. A recíproca segue da mesma forma. ∎

Teorema 4.1.8 *A relação $\leq$ definida acima é uma ordem total em Z compatível com a adição. Em outras palavras, $(Z, +, \leq)$ é um monóide ordenado.*

Dem. Reflexividade: Dado $x = \overline{(a,b)} \in Z$, $x \leq x$, pois $a + b \leq b + a$.

Antissimetria: Dados $x = \overline{(a,b)}$ e $y = \overline{(c,d)}$ pertencentes a Z tais que $x \leq y$ e $y \leq x$, temos que $a + d \leq b + c$ e $c + b \leq d + a$. Daí, pela antissimetria de $\leq$ em $\mathbb{N}$ segue que $a + d = b + c$. Logo, $x = y$.

Transitividade: Dados $x = \overline{(a,b)}, y = \overline{(c,d)}, z = \overline{(e,f)} \in Z$, $x \leq y$ e $y \leq z$ então $a+d \leq b+c$ e $c+f \leq d+e$; adicionando f em ambos os lados da primeira desigualdade e b nos dois lados da segunda desigualdade, obtemos: $a+d+f \leq b+c+f$ e $b+c+f \leq b+d+e$. Pela transitividade de $\leq$ em $\mathbb{N}$ segue então que $a + d + f \leq b + d + e$. Agora usamos a LCA para obtermos: $a + f \leq b + e$. Consequentemente, $x \leq z$.

Está então provado que a relação $\leq$ dada na Definição 37 é uma ordem. Provemos que $\leq$ é total.

Sejam $x = \overline{(a,b)}$ e $y = \overline{(c,d)}$ elementos de Z. Do fato de $\leq$ ser ordem total em $\mathbb{N}$ e $a+d, b+c \in \mathbb{N}$ segue que $a+d \leq b+c$ ou $b+c \leq a+d$; mas isto implica que $x \leq y$ ou $y \leq x$. Logo $\leq$ é orde total em Z.

A relação $\leq$ é compatível com a adição em Z. De fato, dados $x = \overline{(a,b)}, y = \overline{(c,d)}, z = \overline{(e,f)}$ pertencentes a Z,

$$\begin{aligned} x \leq y &\iff a+d \leq b+c \\ &\iff a+e+d+f \leq b+f+c+e \\ &\iff \overline{(a+e,b+f)} \leq \overline{(c+e,d+f)} \\ &\iff x+z \leq y+z. \end{aligned}$$

Isso prova a compatibilidade com a adição e finaliza a demonstração do teorema. ■

Definição 38 *Dados $x, y \in Z$, dizemos que $x < y$ (lê-se "x é menor que y") se, e somente se, $x \leq y$ e $x \neq y$. Ou seja, chamando $x = \overline{(a,b)}$ e $y = \overline{(c,d)}$,*

$$x < y \iff a+d \leq b+c \text{ e } a+d \neq b+c.$$

Portanto, $x < y \iff a+d < b+c$.

Teorema 4.1.9 *Dados $x, y, z \in Z$, as seguintes propriedades são equivalentes:*
(a) $x < y$;
(b) $x+z < y+z$;
(c) $-y < -x$;
(d) $x - y < 0'$.

Dem. Sejam $x = \overline{(a,b)}$, $y = \overline{(c,d)}$ e $z = \overline{(e,f)}$. Para provar que $(a) \Leftrightarrow (b) \Leftrightarrow (c) \Leftrightarrow (d)$ é suficiente mostrarmos que $(a) \Longrightarrow (b) \Longrightarrow (c) \Longrightarrow (d) \Longrightarrow (a)$.

$(a) \Rightarrow (b)$: Temos que $x < y \iff a+d < b+c \Longrightarrow a+d \leq b+c$, ou seja, $x \leq y$. Daí, pela compatibilidade de $\leq$ com a adição segue que, $x+z \leq y+z$, o que equivale a dizer que, $x+z < y+z$ ou $x+z = y+z$, e

$$\begin{aligned} x+z \leq y+z &\iff a+e+d+f < b+f+c+e \text{ ou } a+e+d+f = b+f+c+e \\ &\iff a+e+d+f < b+f+c+e \text{ ou } a+d = b+c \\ &\iff x+z < y+z \text{ ou } x = y, \end{aligned}$$

onde usamos a LCA. Como $x \neq y$, segue que $x+z < y+z$.

$(b) \Rightarrow (c)$: $x+z < y+z \Longrightarrow x+z \leq y+z$; daí, pelo Teorema 4.1.8,

$x \leq y \Longrightarrow x+(-y) \leq y+(-y) = 0' \Longrightarrow x+(-x)+(-y) \leq -x \Longrightarrow -y \Longrightarrow -y \leq -x$. Como $x \neq y$, segue que $-y < -x$.

$(c) \Rightarrow (d)$: De $(a) \Rightarrow (b)$ temos que $-y < -x \Longrightarrow x+(-y) < x-x \Longrightarrow x-y < 0'$.

$(d) \Rightarrow (a)$: De $(a) \Rightarrow (b)$ temos que $x-y < 0' \Longrightarrow x+y+(-y) < 0'+y \Longrightarrow x < y$.

■

TEOREMA 4.1.10 *Sejam* $x = \overline{(a,b)}, y = \overline{(c,d)}, z = \overline{(e,f)} \in Z$. *Se* $x < y$ *e* $0' < z$, *então* $x \cdot z < y \cdot z$.

Dem. Temos que $xz = \overline{(ae+bf, be+af)}$ e $yz = \overline{(ce+df, cf+de)}$.

Como $x < y$ e $0' < z \iff a + d < b + c$ e $f < e$, segue que existem $g, h \in \mathbb{N}$ tais que $a + d + g = b + c$ e $f + h = e$. Então

$$be + ce = ae + de + ge, \quad bf + cf = af + df + g \text{ e } ge = gf + gh. \tag{4.3}$$

Assim, por (4.3) e a LCA

$$\begin{aligned}
&ae + de + ge + bf + cf + ge = be + ce + af + df + gf + gh \\
&\iff (ae + bf) + (cf + de) + gh + gf = (af + be) + (ce + df) + gf \\
&\iff (ae + bf) + (cf + de) + gh = (af + be) + (ce + df) \\
&\iff (ae + bf) + (cf + de) < (af + be) + (ce + df) \\
&\iff xz < yz. \quad \blacksquare
\end{aligned}$$

TEOREMA 4.1.11 *Em* Z *valem as seguintes propriedades:*
(i) $0' < x$ *e* $0' < y \implies 0' < xy$.
(ii) $x < 0'$ *e* $y < 0' \implies 0' < xy$.
(iii) $x < 0'$ *e* $0' < y \implies xy < 0'$.

Dem. (i): Pelo Teorema 4.1.10, $0' < x$ e $0' < y \implies 0'y < xy \iff 0' < xy$.

(ii): Pelos teoremas 4.1.9 e 4.1.10, $x < 0'$ e $y < 0' \implies x < 0'$ e $0' < -y \iff -(xy) < 0'$. Daí, pelo Teoremas 4.1.9, $0' < xy$.

(iii) Pelo Teorema 4.1.10, $x < 0'$ e $0' < y \implies xy < 0'y \iff xy < 0'$. $\blacksquare$

COROLÁRIO 4.1.12 *Se* $x, y \in Z$ *e* $xy = 0'$, *então* $x = 0'$ *ou* $y = 0'$.

Dem. Sejam $x = \overline{(a,b)}$ e $y = \overline{(c,d)}$.

$$\begin{aligned}
xy = 0' &\iff \overline{(ac+bd, ad+bc)} = \overline{(0,0)} \\
&\iff ac + bd = ad + bc \\
&\iff a(c-d) - b(c-d) = 0 \\
&\iff (a-b)(c-d) = 0 \\
&\iff a = b \text{ ou } c = d.
\end{aligned}$$

Se $a = b$, então $x = \overline{(a,a)} = \overline{(0,0)} = 0'$. Do mesmo modo, se $c = d$ então $y = 0'$. Logo, se $xy = 0' \implies x = 0'$ ou $y = 0'$. $\blacksquare$

O próximo resultado nos diz que todo número inteiro não nulo é regular para a operação de multiplicação em Z.

Corolário 4.1.13 *Sejam $x, y, z \in Z$, com $x \neq 0'$. Se $xy = xz$, então $y = z$.*

Dem. A demonstração deste corolário é imediata. ∎

Notação: Vamos denotar a estrutura algébrica $(Z, +, \cdot, \leq)$ pelo símbolo $\mathbb{Z}$.

Definição 39 *(i) Dizemos que um elemento $x \in \mathbb{Z}$ é positivo se, e somente se, $0' \leq x$. Quando $0' < x$ (ou seja, $0' \leq x$ e $x \neq 0'$) dizemos que x é estritamente positivo.*
(ii) Dizemos que um elemento $x \in \mathbb{Z}$ é negativo se, e somente se, $x \leq 0'$. Quando $x < 0'$ (ou seja, $x \leq 0'$ e $x \neq 0'$) dizemos que x é estritamente negativo.

Observação 10 *Do fato de $\mathbb{Z}$ ser (totalmente) ordenado, vale em $\mathbb{Z}$ a lei da tricotomia, que reza o seguinte: "Dado $x \in \mathbb{Z}$, ou $x < 0'$, ou $x = 0'$, ou $0' < x$."*

Notação: Sejam $N' = \{\, x \in \mathbb{Z} \,|\, 0' \leq x\}$ e $N'^* = N' - \{0'\}$.

Dado $x \in \mathbb{Z}$, sabemos que $-x \in \mathbb{Z}$; isto nos leva a definir o conjunto $-N'$ como segue:

Definição 40 *Chamamos de $-N'$ o conjunto $-N' = \{\, x \in \mathbb{Z} \,|\, -x \in N' \,\} = \{\, x \in \mathbb{Z} \,|\, x \leq 0' \,\}$.*

Da Definição 40 segue que $\mathbb{Z} = (-N'^*) \cup \{0'\} \cup N'^*$ (união disjunta) e isto é uma partição de $\mathbb{Z}$.

Nossos próximos passos são no sentido de mostrar que, com a soma, o produto e a ordem induzidas respectivamente pela soma, o produto e a ordem de $\mathbb{Z}$, N' é ordenadamente isomorfo a $\mathbb{N}$.

Proposição 4.1.14 *N' satisfaz as seguintes propriedades:*

1. *Se $x, y \in N'$, então $x + y \in N'$; ou seja, N' é fechado para a adição.*
2. *$(N', +, \leq)$ é um semigrupo comutativo (totalmente) ordenado.*
3. *Vale $N1$ e $N2$ em N', ou seja, existem pelo menos dois elementos em N' e todo elemento de N' é regular para a soma.*
4. *Vale $N3$ para N', ou seja, dados $x, y \in N'$ com $x \leq y$, existe um $z \in N'$ tal que $x + z = y$.*

Dem. 1. $x, y \in N' \iff 0' \leq x$ e $0' \leq y$. Pela compatibilidade de $\leq$ com a adição em $\mathbb{Z}$ segue que $0' \leq y \leq x + y$ e portanto, $x + y \in N'$. Assim, a operação de adição de $\mathbb{Z}$ induz uma adição em N'.

2. Deve ser provado que $(N', +)$ é um semigrupo comutativo e que a ordem total em $\mathbb{Z}$ induz uma ordem total em N' compatível com a adição. Deixamos isso a cargo do leitor.

3. Vejamos $N1$: Como $0' \leq 0'$ e $0' \leq 1'$, segue que $0', 1' \in N'$. A propiredade $(N2)$ é imediata, pois $N' \subset \mathbb{Z}$.

4. $x \leq y \Longrightarrow 0' \leq y - x$, e portanto, $y - x \in N'$. Tomando $z = y - x$ segue o resultado. ■

PROPOSIÇÃO 4.1.15 $N' = \{\, \overline{(n,0)} \,|\, n \in \mathbb{N} \,\}$.

Dem. Seja $x = \overline{(n,0)}$, onde $n \in \mathbb{N}$; então $0 \leq n$ e daí, $0 + 0 \leq 0 + n \Longrightarrow \overline{(0,0)} \leq \overline{(n,0)}$, e portanto, $x \in N'$. Logo, $\{\, \overline{(n,0)} \,|\, n \in \mathbb{N} \,\} \subseteq N'$.

Agora seja $x = \overline{(a,b)} \in N'$; então $b \leq a$ e daí, por $N3$ existe $n \in \mathbb{N}$ tal que $n + b = a$, ou seja, $a + 0 = b + n$. Assim, $\overline{(a,b)} = \overline{(n,0)}$ e portanto, $x \in \{\, \overline{(n,0)} \,|\, n \in \mathbb{N} \,\}$. Logo $N' \subseteq \{\, \overline{(n,0)} \,|\, n \in \mathbb{N} \,\}$ e está provada a proposição. ■

PROPOSIÇÃO 4.1.16 *N' satisfaz o axioma $N4$, isto é, todo subconjunto não vazio de N' tem mínimo.*

Dem. Sabemos da proposição anterior que $N' = \{\, \overline{(n,0)} \,|\, n \in \mathbb{N} \,\}$. Seja $S' \subseteq N'$, $S' \neq \phi$. Então existe $n \in \mathbb{N}$ tal que $\overline{(n,0)} \in S'$ e daí, o conjunto $S = \{\, n \in \mathbb{N} \,|\, \overline{(n,0)} \in S' \,\}$ é não vazio. Logo por $N4$ existe $a = \min S$.

Vamos provar que $\overline{(a,0)} \min S'$. De fato, seja $\overline{(b,0)} \in S'$ tal que $\overline{(b,0)} \leq \overline{(a,0)}$; então $b \leq a$. Como $a = \min S$ e $b \in S$, segue que $b = a$. Logo $\overline{(a,0)} \min S'$. ■

TEOREMA 4.1.17 *A aplicação $f : \mathbb{N} \to N'$ definida por $f(n) = \overline{(n,0)}$ é um isomorfismo ordenado, e portanto, $(N', +, \leq)$ e $\mathbb{N}$ são ordenadamente isomorfos. Além disso, $f(m \cdot n) = f(m) \cdot f(n)$, para quaisquer $m, n \in \mathbb{N}$.*

Dem. Esse resultado é uma consequência do Teorema 3.4.6, mas a título de ilustração iremos demonstrá-lo sem recorrer àquele teorema. Fica à cargo do leitor provar que $f(m \cdot n) = f(m) \cdot f(n)$, para quaisquer $m, n \in \mathbb{N}$.

f é um homomorfismo ordenado. De fato, dados $m, n \in \mathbb{N}$,

$$f(m+n) = \overline{(m+n,0)} = \overline{(m,0)} + \overline{(n,0)} = f(m) + f(n).$$

Além disso, $m \leq n \Longleftrightarrow m + 0 \leq n + 0 \Longleftrightarrow f(m) \leq f(n)$.

A função f é bijetora: Dados $m, n \in \mathbb{N}$, $f(m) = f(n) \iff \overline{(m,0)} = \overline{(n,0)} \Longleftrightarrow m + 0 = n + 0 \Longleftrightarrow m = n$. Logo, f é injetora. Agora, se $x \in N'$ então pela Proposição 4.1.15 existe $n \in \mathbb{N}$ tal que $f(n) = \overline{(m,0)} = x$; logo f é sobrejetora, completando a prova de que f é bijetora. ■

Assim, demonstramos que $\mathbb{N}$ e $(N', +, \leq)$ são monóides totalmente ordenados e isomorfos. Podemos então identificar cada elemento $x = \overline{(n,0)}$ de N' com o $n \in \mathbb{N}$. Em particular, a partir de agora vamos escrever 0 em vez de $0'$ e 1 no lugar de $1'$.
Já que podemos escrever todo elemento $\overline{(n,0)}$ de N' como n e já que $-N' = \{\, \overline{(0,n)} \,|\, n \in$

$\mathbb{N}\} = \{-\overline{(n,0)} \,|\, n \in \mathbb{N}\}$, faz sentido representarmos os elementos $\overline{(0,n)}$ de $-N'$ como $-n$ e consequentemente, representarmos $-N'$ da seguinte forma: $-N' = \{-n \,|\, n \in \mathbb{N}\}$, o qual passamos a chamar de $-\mathbb{N}$.

Sabemos que $\mathbb{Z} = (-N'^*) \cup \{0'\} \cup N'^*$. Logo, podemos enunciar que $\mathbb{Z}$ é isomorfo a $-\mathbb{N}^* \cup \{0\} \cup \mathbb{N}^* = \{\cdots, -2, -1, 0, 1, 2, \cdots\}$ e esse é o chamado **conjunto dos números inteiros**.

A seguir vamos ver mais algumas propriedades de $\mathbb{Z}$.

Definição 41 *Dizemos que um conjunto não vazio $S \subset \mathbb{Z}$ é limitado inferiormente se, e somente se, existe $a \in \mathbb{Z}$ tal que, $a \leq n$, para todo $n \in S$.*

Teorema 4.1.18 *[Princípio do Menor Inteiro] Todo subconjunto não vazio de $\mathbb{Z}$ limitado inferiormente tem mínimo.*

Dem. Seja $S \subset \mathbb{Z}$ não vazio e seja $b \in \mathbb{Z}$ tal que $b \leq n$, $\forall\, n \in S$. Consideremos o conjunto $M = \{n - b \,|\, n \in S\}$. Então $M \neq \phi$ e $M \subseteq \mathbb{N}$. Então, pelo princípio da boa ordem (axioma $N4$) existe $m' = \min M$ e além disso, existe $m \in S$ tal que $m' = m - b$.

Agora, $m - b = m' \leq n - b$, $\forall n \in S \Longleftrightarrow m \leq n$, $\forall n \in S$. Isso finda a demonstração.

■

Notação: Dado $a \in \mathbb{Z}$, vamos denotar por $I_a = \{x \in \mathbb{Z} \,|\, a \leq x\}$, $I_a^* = \{x \in \mathbb{Z} \,|\, a < x\}$ e $[a, b] = \{x \in \mathbb{Z} \,|\, a \leq x \leq b\}$.

Vejamos a versão do princípio de indução finita para o conjunto do números inteiros:

Teorema 4.1.19 *[Princípio de Indução Finita em $\mathbb{Z}$] Sejam $a \in \mathbb{Z}$ e $S \subseteq I_a$ tais que:*
(i) $a \in S$;
(ii) dado $n \in \mathbb{Z}$, se $a \leq n$ e $n \in S$, então $n + 1 \in S$.
Então $S = I_a$.

Dem. Suponhamos por absurdo que S satisfaz (i) e (ii) mas $S \neq I_a$. Neste caso o conjunto $S' = I_a - S$ é não vazio e a é cota inferior de S'; daí, pelo princípio do menor inteiro (Teorema 4.1.18) existe $m = \min S'$.

Temos que $a < m$, pois $a \in S$. Daí $a \leq m - 1 < m$ e portanto $m - 1 \in S$. Segue então de (ii) que $m = (m - 1) + 1 \in S$, o que é uma contradição. E isso prova o teorema.

■

Corolário 4.1.20 *Seja $S \subseteq [a, b]$ um conjunto tal que:*
(a) $a \in S$;
(b) dado $n \in \mathbb{Z}$, se $n < b$ e $n \in S$, então $n + 1 \in S$.
Nestas condições, $S = [a, b]$.

Dem. Consideremos o conjunto $S_1 = S \cup I_b^*$. S_1 satisfaz (i) e (ii) do Teorema 4.1.19. Logo, $S_1 = I_a = [a, b] \cup I_b^*$ e portanto, $S = [a, b]$. ∎

COROLÁRIO 4.1.21 *Seja $a \in \mathbb{Z}$ e seja $S \subseteq I_a$ um conjunto tal que:*
(a) $a \in S$;
(b) dado $n \in \mathbb{Z}$, se $a \leq n$ e $[a, n] \subset S$, então $n + 1 \in S$.
Nestas condições, $S = I_a$.

Dem. Suponha, por absurdo, que S satisfaz (a) e (b) mas $S \neq I_a$. Neste caso o conjunto $S' = I_a - S$ não é vazio e n é cota inferior de S'. Daí temos que pelo princípio do menor inteiro existe m inteiro tal que $m = min\ S'$. Assim temos que $n < m$ e como $n \in S$ então $n \leq m - 1 < m$ e portanto $m - 1 \in S$. Por (ii) se $m - 1 \in S$ então $m = (m - 1) + 1 \in S$, o que é uma contradição. Logo, $S = I_a$.

4.2 Aplicação: Teoria elementar dos números

4.2.1 Divisibilidade e números primos.

DEFINIÇÃO 42 *Dados $a, b \in \mathbb{Z}$, dizemos que a é um divisor de b se, e somente se, existe um $c \in \mathbb{Z}$ tal que $b = ac$. Usamos a notação $a|b$ para indicar que a divide b. Quando a não divide b escrevemos $a \nmid b$. A relação $|$ é chamada de relação de divisibilidade sobre $\mathbb{Z}$. O elemento c tal que $b = ac$ é o quociente de b por a.*

EXEMPLO 4.2.1 *Por exemplo, $3|6$, $-4|20$, $5|15$, etc., enquanto que $2 \nmid 5$, $-5 \nmid 1$, $3 \nmid 10$. Observemos que $a|0$, para todo $a \in \mathbb{Z}$, 0 é divisor apenas dele próprio, ou seja, $0|0$ mas $0 \nmid b$ se $b \neq 0$.*

Vejamos algumas propriedades da relação de divisibilidade:

PROPOSIÇÃO 4.2.2 *Dados $a, b, c \in \mathbb{Z}$, valem as seguintes propriedades:*
1. *$a|a$ (reflexividade);*
2. *$a|b$ e $b|a \iff a = \pm b$;*
3. *$a|b$ e $b|c \implies a|c$ (transitividade);*
4. *$a|b$ e $a|c \implies a|(b \pm c)$;*
5. *Suponhamos que $a|(b \pm c)$. Então, $a|b \iff a|c$.*

Dem. 1. Como $a = 1.a$ e $1 \in \mathbb{N}$ então $a|a$.

2. $a|b$ e $b|a \iff$ existem $c, d \in \mathbb{Z}$ tais que $b = ac$ e $a = bd$. Substituindo o valor de a obtemos $b = (bd)c$ e daí, $b(dc-1) = 0$. Assim chegamos que $dc = 1$ e consequentemente, $c = d = 1$ ou $c = d = -1$. Logo, $a = b$ ou $a = -b$ e está provado o item 2.

3. $a|b$ e $b|c \iff$ existem $m, d \in \mathbb{Z}$ tais que $b = am$ e $c = bd$. Assim temos que $c = (am)d = a(md)$ e $(md) \in \mathbb{Z}$. Logo, $a|c$.

4. $a|b$ e $a|c \iff$ existem $d, e \in \mathbb{Z}$ tais que $b = ad$ e $c = ae$. Daí, $b \pm c = a(d \pm e)$ e como $d \pm e \in \mathbb{Z}$ segue que $a|(b \pm c)$.

5. Nossa hipótese geral é $a|(b \pm c)$, ou seja, existe $d \in \mathbb{Z}$ tal que $b \pm c = ad$. Ora, $a|b \iff$ existe $e \in \mathbb{Z}$ tal que $b = ae \iff c = ad \pm b = ad \pm ae = a(d \pm e) \iff a|c$. ∎

Proposição 4.2.3 *Sejam $a, b \in \mathbb{Z}$ e $n \in \mathbb{N}$. Então:*

1. $(a-b)|(a^n - b^n)$, *para todo* $n \in \mathbb{N}$;
2. $(a+b)|(a^{2n+1} + b^{2n+1})$, *para todo* $n \in \mathbb{N}$;
3. $(a+b)|(a^{2n} - b^{2n})$, *para todo* $n \in \mathbb{N}$.

Dem. Provaremos esta proposição usando o método de demonstração por indução finita sobre $n \in \mathbb{N}$.

1. (i) Temos que $(a-b)|(a^1 - b^1)$. Logo a propriedade é válida para $n = 1$.

(ii) Suponhamos que a propriedade seja válida para $n \in \mathbb{N}$, ou seja, $(a-b)|(a^n - b^n)$. Provemos que também é válida para $n+1$. Escrevamos

$$a^{n+1} - b^{n+1} = aa^n - ba^n + ba^n - bb^n = (a-b)a^n + b(a^n - b^n).$$

Como $(a-b)|(a-b)$ e, por hipótese, $(a-b)|(a^n - b^n)$, segue do ítem 4 da Propsição 4.2.2 que $(a-b)|(a^{n+1} - b^{n+1})$.

Assim, pelo princípio de indução finita, $(a-b)|(a^n - b^n)$, para todo $n \in \mathbb{N}$.

2. (i) A propriedade é válida para $n = 0$, pois $(a+b)|(a^1 + b^1)$.

(ii) Suponhamos que a propriedade é válida para n, isto é, $(a+b)|(a^{2n+1} + b^{2n+1})$. Escrevamos

$$\begin{aligned} a^{2(n+1)+1} + b^{2(n+1)+1} &= a^2a^{2n+1} - b^2a^{2n+1} + b^2a^{2n+1} + b^2b^{2n+1} \\ &= (a^2 - b^2)a^{2n+1} + b^2(a^{2n+1} + b^{2n+1}). \end{aligned}$$

Como $a^2 - b^2 = (a+b)(a-b)$, segue que $(a+b)|(a^2 - b^2)$. A hipótese de indução é que $(a+b)|(a^{2n+1} + b^{2n+1})$. Logo, pelo item 4 da Proposição 4.2.2 segue que $(a+b)|(a^{2(n+1)+1} + b^{2(n+1)+1})$.

Portanto, pelo método de demonstração por indução finita, $(a+b)|(a^{2n+1} + b^{2n+1})$, para todo $n \in \mathbb{N}$.

3. (i) Como $a^2 - b^2 = (a+b)(a-b)$, segue que $(a+b)|(a^2 - b^2)$. Logo a propriedade é válida quando $n = 1$.

(ii) Seja $n \in \mathbb{N}$ e suponhamos que $(a+b)|(a^{2n} - b^{2n})$. Então existe um $d \in \mathbb{Z}$ tal que $a^{2n} - b^{2n} = (a+b)d$. Temos daí chamando de $c = (a-b)a^{2n}$ que

$a^{2(n+1)} - b^{2(n+1)} = a^2a^{2n} - b^2b^{2n} + b^2b^{2n} - b^2b^{2n} = (a^2 - b^2)a^{2n} + b^2(a^{2n} - b^{2n}) = (a+b)(c+d)$. Portanto, $(a+b)|(a^{2(n+1)} - b^{2(n+1)})$.

Daí o resultado está provado por indução finita. ∎

DEFINIÇÃO 43 *Dado $a \in \mathbb{Z}$, o conjunto dos divisores de a será indicado por*

$$D(a) = \{\, x \in \mathbb{Z} \,:\, x|a \,\}.$$

Segue imediatamente da Definição 43 que: (i) $D(0) = \mathbb{Z}$; (ii) $D(a) = D(-a)$, para todo $a \in \mathbb{Z}$; (iii) dado qualquer $a \in \mathbb{Z}$, $\{\, -1, 1, -a, a \,\} \subseteq D(a)$.

TEOREMA 4.2.4 *Se $a \in \mathbb{N}^*$, então $D(a) \subseteq [-a, a]$.*

Dem. $b \in D(a) \iff b|a$, isto é, existe $c \in \mathbb{Z}^*$ tal que $a = bc$. Como $a > 0$, b e c têm o mesmo sinal, ou seja, $b > 0$ e $c > 0$, ou, $b < 0$ e $c < 0$.

Se $b > 0$, então $0 < b \leq a \iff b \in (0, a]$. Se $b < 0$, então do fato de $a = (-b)(-c)$ segue que $0 < -b \leq a$, e daí, $-a \leq b < 0$, ou seja, $b \in [-a, 0)$. Logo, $b \in [-a, a]$. ■

Do Teorema 4.2.4 podemos concluir facilmente que, se $a \neq 0$, então $D(a)$ é um conjunto finito.

COROLÁRIO 4.2.5 $D(1) = \{-1, 1\}$.

Dem. Pelo Teorema 4.2.4 concluímos que $D(1) \subseteq [-1, 1] = \{-1, 0, 1\}$. Como $0 \nmid 1$ e $1|1$ e $-1|1$, segue que $D(1) = \{-1, 1\}$. ■

DEFINIÇÃO 44 *Seja $a \in \mathbb{Z}$. Os números $\{-1, 1, -a, a\}$ são chamados de **divisores impróprios** de a. Os demais divisores de a, caso existam, são chamados de **divisores próprios** de a.*

EXEMPLO 4.2.6 *Os divisores próprios de 8 são os números $-4, -2, 2, 4$.*

Observemos que se $a \neq 0$ e b é um divisor próprio de a, então $-a < b < -1$ ou $1 < b < a$.

DEFINIÇÃO 45 *(i) Dizemos que um número $p \in \mathbb{Z} - \{0, \pm 1\}$ é **primo** se, e somente se, $D(p) = \{\, \pm 1, \pm p \,\}$.*
*(ii) Dizemos que um número $a \in \mathbb{Z} - \{0, \pm 1\}$ é **composto** se, e somente se, existe $b \in \mathbb{Z}$ divisor próprio de a, ou seja, $a = bc$ com $b, c \in \mathbb{Z} - \{0, \pm 1\}$.*

EXEMPLO 4.2.7 *Os números $\pm 2, \pm 3, \pm 5, \pm 7$ são primos e $\pm 6, \pm 9, \pm 15$ são compostos.*

TEOREMA 4.2.8 (FUNDAMENTAL DA ARITMÉTICA) *Todo número $a \in \mathbb{Z} - \{0, \pm 1\}$ ou é primo ou é um produto de números primos.*

Dem. Como $D(a) = D(-a)$, é suficiente provarmos o teorema para $a \in I_2$. Faremos isso usando o princípio de indução finita, mais precisamente, o Corolário 3.3.8.

Seja $S = \{\, a \in I_2 \,|\, a$ é primo ou é um produto de números primos $\}$. Então:

(i) $2 \in S$, pois 2 é primo.

(ii) Dado $a \in \mathbb{N}$, se $2 \leq a$ e se $[2, a) \subseteq S$, provemos que $a \in S$. Se a é primo então obviamente $a \in S$. Agora, se a é composto então existem $b, c \in \mathbb{Z}$ com $b, c \in [2, a)$ (isto é, $2 \leq b < a$ e $2 \leq c < a$) tal que $a = bc$. Segue então da hipótese que $b, c \in S$; logo $a \in S$.

Neste caso, concluimos do Corlário 3.3.8 que $S = I_2$. ∎

COROLÁRIO 4.2.9 *Todo número inteiro a, $a \neq 0$ e $a \neq \pm 1$, admite pelo menos um fator primo positivo.*

TEOREMA 4.2.10 *Existem infinitos números primos.*

Dem. É suficiente provarmos que existem infinitos números primos positivos.

Suponhamos que $\mathbb{N}$ tem finitos números primos, digamos $p_1, p_2, \cdots p_s$, e consideremos o seguinte número inteiro: $a = p_1 p_2 \cdots p_s + 1$.

Temos que $a > 1$; daí pelo Corolário 4.2.9, existe um primo $p > 0$ tal que $p|a$. Neste caso, $p|p_1 p_2 \cdots p_s$ (pois p tem que ser um deles) e $p|a$. Mas isto implica que $p|1$, o que é absurdo. Logo, $\mathbb{N}$ tem infinitos números primos e segue o resultado. ∎

TEOREMA 4.2.11 *[Algoritmo da Divisão] Se $a, b \in \mathbb{Z}$, com $b \neq 0$, então existe um único par $(q, r) \in \mathbb{Z} \times \mathbb{Z}$ tais que, $a = bq + r$, onde $0 \leq r < b$(se $b > 0$) ou $0 \leq r < -b$ (se $b < 0$).*

Dem. Existência: Vamos usar o princípio de indução finita. Consideremos primeiro o caso $b > 0$.

Seja $S = \{\, a - bx \,|\, a - bx \geq 0,\ x \in \mathbb{Z} \,\} \subseteq \mathbb{N}$. Então $S \neq \phi$. De fato, se $a \geq 0$, então tomando $x = -a$ temos que $a - bx = a(1 + b) \geq 0$ e neste caso $a - bx \in S$; agora, se $a < 0$, tomando $x = a$, segue que $a - bx = a(1 - b) \geq 0$ e assim, $a - bx \in S$.

Neste caso, existe $r = \min S$. $r \geq 0$ e $r = a - bq$, para algum $q \in \mathbb{Z}$, ou seja, $a = bq + r$.

Suponhamos por absurdo que $b \leq r$. Então $r = b + r'$ e $r' \geq 0$. Já que $b > 0$, segue que $r' < r$ e portanto, $r' \notin S$. Mas $r = a - bq$ e isto implica que $0 \leq r' = r - b = a - b(q+1)$ e consequentemente, $r' \in S$, o que é uma contradição. Logo $0 \leq r < b$.

Consideremos agora o caso $b < 0$. Então $-b > 0$ e daí, existem $q', r' \in \mathbb{Z}$ tais que

$$a = -bq' + r' = b(-q') + r', \text{ onde } 0 \leq r' < -b.$$

Portanto, escolhendo $q = -q'$ e $r = r'$ segue o resultado.

Unicidade: Sejam (q, r) e (q_1, r_1) pares de inteiros tais que

$$a = bq + r, \text{ onde } 0 \leq r < b \text{ ou } -b < r \leq 0$$

e

$$a = bq_1 + r_1, \text{ onde } 0 \leq r_1 < b \text{ ou } -b < r_1 \leq 0.$$

Suponhamos $r \neq r_1$. Vamos considerar sem perda de generalidade $r > r_1$.

$bq + r = a = bq_1 + r_1 \iff b(q_1 - q) = r - r_1$.

Daí, $b \geq 1$ e $q_1 - q \geq 1$. Logo, $r - r_1 = b(q_1 - q) \geq b$; mas isso é uma contradição, pois $r - r_1 < b$. ∎

Os inteiros q e r são chamados de quociente e resto da divisão euclideana de a por b, respectivamente. Observemos que $b|a$ se, e somente se, $r = 0$.

4.2.2 Congruências.

DEFINIÇÃO 46 *Sejam $a, b, m \in \mathbb{Z}$, com $m \neq 0$. Dizemos que a é congruente a b módulo m se, e somente se, $m|(a - b)$.*

Usaremos as notações $a \equiv b \, mod \, m$ para indicar que a é congruente a b módulo m e, $a \not\equiv b \, mod \, m$ para indicar que a não é congruente a b módulo m. Algumas vezes, quando não houver dúvida de quem é o m, poderemos usar $a \equiv b$ para indicar que $a \equiv b \, mod \, m$.

PROPOSIÇÃO 4.2.12 $a \equiv b \, mod \, m \iff a \equiv b \, mod \, -m$.

Dem. $a \equiv b \, mod \, m \iff m|(a - b) \iff$ existe $q \in \mathbb{Z}$ tal que, $a - b = mq$

$\iff a - b = (-m)(-q) \iff -m|(a - b) \iff a \equiv b \, mod(-m)$.

∎

OBSERVAÇÃO 11 *Devido a proposição acima, a congruência módulo m é estudada, sem perda de generalidade, para $m > 0$.*

TEOREMA 4.2.13 *Fixado $m \in \mathbb{Z}$, a congruência módulo m é uma relação de equivalência que é compatível com a adição e com a multiplicação em $\mathbb{Z}$.*

Dem. Provemos que $\equiv \, mod \, m$ é uma relação de equivalência:

Reflexividade: $\forall \, a \in \mathbb{Z}$, $a \equiv a$, pois $m|(a - a)$.

Simetria: Dados $a, b \in \mathbb{Z}$, $a \equiv b \, mod \, m \iff m|(a - b) \iff m|(b - a) \iff b \equiv a \, mod \, m$.

Transitividade: Dados $a, b, c \in \mathbb{Z}$, $a \equiv b \, mod \, m$ e $b \equiv c \, mod \, m \iff m|(a - b)$ e $m|(b - c) \iff$ existem $q_1, q_2 \in \mathbb{Z}$ tais que $a - b = mq_1$ e $b - c = mq_2 \iff a - c = (a - b) + (b - c) = m(q_1 + q_2) \implies m|(a - c) \iff a \equiv c \, mod \, m$.

Agoram vamos provar a compatibilidade com a adição. Sejam $a, b \in \mathbb{Z}$ tais que $a \equiv b \, mod \, m$ e seja $c \in \mathbb{Z}$. Então existe $q \in \mathbb{Z}$ tal que $a - b = mq$, daí, $(a + c) - (b + c) = mq$ e portanto, $a + c \equiv b + c \, mod \, m$. Logo, vale a compatibilidade com a adição.

Por fim, provemos a compatibilidade com a multiplicação. Sejam $a, b \in \mathbb{Z}$ tais que $a \equiv b \, mod \, m$ e seja $c \in \mathbb{Z}$. Então $m|(a-b)$ e portanto, $m|(a-b)c$, ou seja, $m|(ac-bc)$. Logo, $ac \equiv bc \, mod \, m$. ∎

Corolário 4.2.14 *Sejam $a, b, c, d \in \mathbb{Z}$, Se $a \equiv b \, mod \, m$ e $c \equiv d \, mod m$, então temos que $a + c \equiv (b + d) \, mod \, m$ e $ac \equiv bd \, mod \, m$.*

Dem. Se $a \equiv b \, mod \, m$ e $c \equiv d \, mod m$, então da compatibilidade com a adição temos que $a + c \equiv b + c \, mod \, m$ e e $b + c \equiv b + d \, mod m$. Daí, pela transitividade da congruência módulo m segue que $a + c \equiv (b + d) \, mod \, m$.

Agora, pela compatibilidade com a multiplicação

$a \equiv b \, mod \, m$ e $c \equiv d \, mod m \Longrightarrow ac \equiv bc \, mod \, m$ e $bc \equiv bd \, mod m$.

Logo, pela transitividade da congruência módulo m segue que $ac \equiv (bd) \, mod \, m$. ∎

Corolário 4.2.15 *Sejam $a, b \in \mathbb{Z}$. Se $a \equiv b \, mod \, m$, então $a^n \equiv b^n \, mod \, m$, para todo $n \in \mathbb{N}$.*

Dem. Da hipótese de que $a \equiv b \, mod \, m$, segue que $m|(a-b)$. Além disso, o item 1 da Proposição 4.2.3 nos diz que $(a-b)|(a^n-b^n)$, para todo $n \in \mathbb{N}$. Daí, pela transitividade da relação de divisibilidade em $\mathbb{Z}$ (veja o item 3 da Proposição 4.2.2) segue que $m|(a^n-b^n)$, para todo $n \in \mathbb{N}$ e consequentemente, $a^n \equiv b^n \, mod \, m$, para todo $n \in \mathbb{N}$. ∎

Teorema 4.2.16 *Dados $a, b \in \mathbb{Z}$, $a \equiv b \, mod \, m$ se, e somente se, a e b têm o mesmo resto quando divididos por m.*

Dem. ($\Rightarrow$) Pelo Teorema 4.2.11 (para b e m) existe um par $(q, r) \in \mathbb{Z} \times \mathbb{Z}$ tal que, $b = mq + r$, onde $0 \leq r < m$.

Como $a \equiv b \, mod \, m$, existe $s \in \mathbb{Z}$ tal que $a - b = ms$, ou seja, $a = b + ms$. Assim, $a = (mq + r) + ms = m(q + s) + r$. Da unicidade garantida pelo Teorema 4.2.11, segue que $q + s$ e s são respectivamente, o quociente e o resto da divisão de a por m. Portanto, a e b têm o mesmo resto quando divididos por m.

($\Leftarrow$) Por hipótese, existem (únicos!) $q_1, q_2 \in \mathbb{Z}$ tais que, $a = mq_1 + r$ e $b = mq_2 + r$. Logo, $a - b = m(q_1 - q_2)$, ou seja, $m|(a-b)$. Portanto, $a \equiv b \, mod \, m$. ∎

Corolário 4.2.17 *Todo inteiro a é congruente a um e somente um dos seguintes inteiros: $0, 1, 2, \cdots, m-1$.*

Dem. Do Teorema 4.2.11 aplicado a a e m temos que $a = mq + r$, onde $0 \leq r < m$ e o par $q, r \in \mathbb{Z}$ é único. Logo, $a \equiv r \, mod \, m$ e protanto, a só pode ser congruente a um dos e somente um dos inteiros $0, 1, 2, \cdots, m-1$. ∎

Já que a congruência módulo m é uma relação de equivalência em $\mathbb{Z}$, vejamos como fica o conjunto quociente. As classes de equivalência módulo m são chamadas de classes de restos módulo m.

Seja $m > 1$. Dado $a \in \mathbb{Z}$, denotaremos por $\bar{a} := \{ x \in \mathbb{Z} \,|\, x \equiv a \, mod \, m \}$, ou seja, $\bar{a}$ denotará a classe de equivalência determinada por a segundo a relação de equivalência $\equiv \; mod \, m$. Já o conjunto quociente de $\mathbb{Z}$ pela relação $\equiv \; mod \, m$, $\mathbb{Z}/ \equiv \; mod \, m$, será denotado por $\mathbb{Z}_m$.

Diz o Corolário 4.2.17 que dado $x \in \mathbb{Z}$, x e congruente módulo m a um e somente um dos elementos $0, 1, 2, \cdots, m-1$, segue que $x \in \bar{0}$, ou $x \in \bar{1}$, $\cdots$, ou $x \in \overline{m-1}$. Logo, $\mathbb{Z}_m = \{ \bar{0}, \bar{1}, \cdots, \overline{m-1} \}$.

EXEMPLO 4.2.18 *1. Para $m = 2$ temos:*

$$\bar{0} = \{ x \in \mathbb{Z} \,|\, x \equiv 0 \, mod \, 2 \} = \{ x \in \mathbb{Z} \,|\, x = 2n, \, n \in \mathbb{Z} \},$$

que é o conjunto dos inteiros pares;

$$\bar{1} = \{ x \in \mathbb{Z} \,|\, x \equiv 1 \, mod \, 2 \} = \{ x \in \mathbb{Z} \,|\, x = 2n + 1, \, n \in \mathbb{Z} \},$$

que é o conjunto dos inteiros ímpares, e essas são as duas únicas classes de equivalência de $\mathbb{Z}_2$, pois elas contêm todos os inteiros. Assim, $\mathbb{Z}_2 = \{\bar{0}, \bar{1}\}$

2. Para $m = 3$ temos:

$$\bar{0} = \{ x \in \mathbb{Z} \,|\, x \equiv 0 \, mod \, 3 \} = \{ x \in \mathbb{Z} \,|\, x = 3n, \, n \in \mathbb{Z} \},$$

que é o conjunto dos inteiros múltiplos de 3;

$$\bar{1} = \{ x \in \mathbb{Z} \,|\, x \equiv 1 \, mod \, 3 \} = \{ x \in \mathbb{Z} \,|\, x = 3n + 1, \, n \in \mathbb{Z} \},$$

$$\bar{2} = \{ x \in \mathbb{Z} \,|\, x \equiv 2 \, mod \, 3 \} = \{ x \in \mathbb{Z} \,|\, x = 3n + 2, \, n \in \mathbb{Z} \},$$

e essas são as três únicas classes de equivalência de $\mathbb{Z}_2$, pois elas contêm todos os inteiros. Assim, $\mathbb{Z}_3 = \{\bar{0}, \bar{1}, \bar{2}\}$.

OBSERVAÇÃO 12 (1) $a \equiv b \, mod \, m \iff \bar{a} = \bar{b}$.
(2) $\mathbb{Z}_m$ *é uma partição de* $\mathbb{Z}$, *ou seja,*

(*i*) $\forall \, \bar{a} \in \mathbb{Z}_m, \; \bar{a} \neq \phi$;

(*ii*) *dados* $\bar{a}, \, \bar{b} \in \mathbb{Z}_m$, *ou* $\bar{a} = \bar{b}$ *ou* $\bar{a} \cap \bar{b} = \phi$;

(*iii*) $\bigcup_{\bar{a} \in \mathbb{Z}_m} = \mathbb{Z}$.

Vimos que a congruência módulo m é compatível com a multiplicação, ou seja, $a \equiv b \, mod \, m \Longrightarrow ac \equiv bc \, mod \, m$, $\forall \, c \in \mathbb{Z}$. Mas a recíproca nem sempre é verdadeira; por exemplo, $5 \cdot 7 \equiv 5 \cdot 4 \, mod \, 5$, mas $7 \not\equiv 4 \, mod \, 5$. O teorema a seguir nos mostrará em que circunstâncias a recíproca desse fato é válida.

DEFINIÇÃO 47 *Sejam $a, b \in \mathbb{Z}$ não simultaneamente nulos.*
(i) Um número $d \in \mathbb{N}$ é um divisor comum de a e b se, e somente se, $d \in D(a) \cap D(b)$.
(ii) Se além disso, d é divisível por todo divisor comum de a e b (i.e., $c|a$ e $c|b \Rightarrow c|d$), dizemos que d é o máximo divisor comum de a e b.
(iii) Quando o máximo divisor comum de a e b é igual a 1, dizemos que a e b são primos entre si.

Usamos a notação $mdc(a, b)$ para indicar o máximo divisor cumum entre a e b. A definição acima faz sentido porque o conjunto dos divisores de um número é finito.

TEOREMA 4.2.19 *Seja $m \in \mathbb{N}^*$ e sejam $a, b, c \in \mathbb{Z}$ quaisquer tais que, $ac \equiv bc \, mod \, m$. Se $d = mdc(c, m)$, então $a \equiv b \, mod \, \widetilde{m}$, onde $m = d\widetilde{m}$, ou seja, $\widetilde{m}$ é o quociente da divisão euclideana de m por d.*

Dem. Da hipótese $ac \equiv bc \, mod \, m$ segue que $ac - bc = m \cdot q$, para algum $q \in \mathbb{Z}$. Por outro lado,

$d = mdc(c, m) \Longrightarrow m = d\widetilde{m}$ e $c = d\widetilde{c} \Longrightarrow ad\widetilde{c} - bd\widetilde{c} = d\widetilde{m}q \Longrightarrow a\widetilde{c} - b\widetilde{c} = \widetilde{m}q$,
onde usamos a lei do cancelamento da multiplicação. Como $\widetilde{m}$ e $\widetilde{c}$ são primos entre si, segue que $\widetilde{m}|(a - b)$ e daí, $a \equiv b \, mod \, \widetilde{m}$. ∎

COROLÁRIO 4.2.20 *Sejam $a, b, c \in \mathbb{Z}$ quaisquer tais que, $ac \equiv bc \, mod \, m$. Se c e m são primos entre si, então $a \equiv b \, mod \, m$.*

Dem. Se $ac \equiv bc \, mod \, m$ tem que existe $q \in \mathbb{Z}$ tal que $ac - bc = m \cdot q$. Assi, $ac - bc = m \cdot q \Longrightarrow c(a - b) = m \cdot q$. Como c e m são primos entre si então $c|q$ e $a - b|m$. Logo, $a \equiv b \, mod \, m$. ∎

COROLÁRIO 4.2.21 *Sejam $a, b, c \in \mathbb{Z}$ quaisquer tais que, $ac \equiv bc \, mod \, p$, onde p é primo e $p \nmid c$. Então $a \equiv b \, mod \, p$.*

Dem. De $ac \equiv bc \, mod \, p$ segue que $ac - bc = p \cdot q$, para algum $q \in \mathbb{Z}$. Pelo mesmo argumento do corolário anterior temos que $ac - bc = p \cdot q \Longrightarrow c(a - b) = p \cdot q$ e como $p \nmid c$ então $(a - b)|p$ e consequentemente $a \equiv b \, mod \, p$. ∎

4.3 Aplicação: Mudança de Base de um Sistema de Numeração

4.3.1 Sistemas de Numeração

Os números que usamos no nosso dia a dia fazem parte de um sistema chamado Sistema Decimal Posicional. Dizemos decimal porque utiliza dez algarismos na formação de seus números e posicional pois cada algarismo representa valores diferentes dependendo da posição ocupada. Eles são os Numerais Indo-Arábicos.

Além do sistema decimal existem outros sistemas de numeração que levam em conta a quantidade de algarismos utilizados para formar seus números. O sistema de numeração binário, por exemplo, leva apenas dois algarismos na composição de seus números e é base para toda a eletrônica digital e computação moderna. O sistema de numeração octal, de base 8, também foi muito utilizada em informática como uma alternativa mais compacta ao binário na programação em linguagem de máquina. Atualmente é mais utilizada para este fim o sistema hexadecimal, de base 16.

Veremos nesta seção como podemos converter números entre os sistemas de diferentes bases. Primeiramente precisamos do conceito de base de um sistema de numeração.

DEFINIÇÃO 48 *Base de um sistema de numeração é o conjunto* (*ou o número de elementos desse conjunto*) *de algarismos utilizados para escrever os números de determinado sistema.*

No sistema de numeração decimal a base é formada pelos algarismos { 0, 1, 2, 3, 4, 5, 6, 7, 8, 9 } e no sistema binário ela é formada apenas pelos algarismos 0 e 1. Nos sistema de numeração com base acima de dez usam-se os algarismos indo-arábicos acrescentando-se letras do nosso alfabeto. No sistema hexadecimal por exemplo são usados os mesmos dez símbolos do sistema decimal acrescidos das letras A, B, C, D, E e F.

Simbolicamente temos que $(a_n a_{n-1}...a_0)_\beta$ é o número $N = a_n a_{n-1}...a_0$ escrito em base β.

Para escrevermos a representação de um número em um determinado sistema de numeração utilizaremos o Algoritmos da Divisão de Euclides. Mostraremos a seguir como representar um número numa base $\beta \geq 2$ de acordo com Childs (1979).

DEFINIÇÃO 49 *Se $N = a_n a_{n-1}...a_0$ é um número inteiro escrito numa base $\beta \geq 2$ qualquer, então podemos escrever N como soma de potências de base β na forma:*

$$N = a_n.\beta^n + a_{n-1}.\beta^{n-1} + ... + a_0.\beta^0,$$

com $0 \leq a_i < \beta$ para todo $i \in \mathbb{N}$
chamada de Formal Polinomial da escrita de número.

Particularmente temos que, se $N = a_n a_{n-1}...a_0$ é um número do sistema de numeração decimal então N pode ser escrito como:

$$N = a_n.10^n + a_{n-1}.10^{n-1} + ... + a_0.10^0.$$

EXEMPLO 4.3.1 *Os números* 243 *e* 1508 *do sistema decimal podem ser escritos como*
$243 = 2 \cdot 10^2 + 4 \cdot 10^1 + 3 \cdot 10^0$ *e*
$1008 = 1 \cdot 10^3 + 5 \cdot 10^2 + 8 \cdot 10^0$.

4.3.2 Conversão de Base

Uma forma de converter um número $N = a_n.\beta^n + a_{n-1}.\beta^{n-1} + ... + a_0.\beta^0$ de uma base β para uma base α seria rescrever o número N em função de potências de base α. O método descrito abaixo, baseado em Monteiro (1969), utiliza diretamente o algoritmo da divisão Euclidiana.

TEOREMA 4.3.2 *Para converter um número inteiro N escrito em base decimal para uma base α qualquer basta realizar sucessivas divisões de N por α. O resultado seria o quociente da última divisão seguidos dos restos dessas divisões em ordem inversa.*

Dem. Seja $N = a_n.10^n + a_{n-1}.10^{n-1} + ... + a_0.10^0$ um número escrito em base decimal. Dividindo N por α pelo Algoritmo de Euclides, obtemos um quociente q_0 e resto r_0 com $0 \leq r_0 < \alpha$, ou seja

$$N = \alpha \cdot q_0 + r_0. \tag{4.4}$$

Fazendo a divisão de q_0 por α obtemos um quociente q_1 e resto r_1, com $0 \leq r_1 < \alpha$.
Assim, $q_0 = \alpha \cdot q_1 + r_1$ e substituindo q_0 na expressão 4.4 temos que:

$$N = \alpha(\alpha q_1 + r_1) + r_0 = \alpha^2 q_1 + \alpha r_1 + r_0.$$

Repetindo o processo até obter um quociente $q_n \leq \alpha$ precebemos que N poderá ser escrito como:

$$N = \alpha^n q^n + \alpha^{n-1} r^{n-1} + \cdots \alpha r_1 + r_0$$
$$\text{ou seja}$$
$$N = (q^n r^{n-1} \cdots r_1 r_0)_\alpha.$$

Agora, faremos alguns exemplos analisando o processo por meio de um dispositivo prático mostrado abaixo.

EXEMPLO 4.3.3 *O número* 13 *escrito em base decimal quando convertido para a base binária resulta no número* $(1101)_2$.

De fato, dividindo o número 13 sucessivas vezes por 2 teremos:

13	2		
1	6	2	
	0	3	2
		1	1

Assim, $(13)_{10} = (1101)_2$.
Note que a conversão é feita escrevendo os algarismos 'de baixo pra cima' como verificado

na sequência abaixo.

$$\begin{aligned}(13)_{10} &= 2.6 + 1\\ &= 2.(2.3) + 1\\ &= 2^2.3 + 1\\ &= 2^2(2+1) + 1\\ &= 2^3 + 2^2 + 1\\ &= 1.2^3 + 1.2^2 + 0.2^1 + 1.2^0\\ &= (1101)_2\end{aligned}$$

.

EXEMPLO 4.3.4 *A conversão do número* 243 *de base decimal resulta no número* $(F3)_{16}$ *do sistema hexadecimal.*

Novamente dividindo 243 por 16 temos:

$$\begin{array}{r|l} 243 & 16 \\ \hline 3 & 15 \end{array}$$

Como o número 15 é representado pela letra F no sistema hexadecimal temos que,

$$\begin{aligned}(243)_{10} &= 15 \cdot 16 + 3\\ &= 15 \cdot 16^1 + 3 \cdot 16^0\\ &= (F3)_{16}\end{aligned}$$

.

Particularmente, para converter o número de uma base qualquer para a base decimal, basta fazer a soma dos elementos de sua representação descrita na Definição 49.

EXEMPLO 4.3.5 *Convertendo os números (a)* $(100111)_2$*, (b)* $(1234)_5$ *e (c)* $(23A)_{16}$ *para a base decimal temos que:*
(a) $(100111)_2 = 1 \cdot 2^5 + 0 \cdot 2^4 + 0 \cdot 2^3 + 1 \cdot 2^2 + 1 \cdot 2^1 + 1 \cdot 2^0 = (39)_{10}$*;*
(b) $(1234)_5 = 1 \cdot 5^3 + 2 \cdot 5^2 + 3 \cdot 5^1 + 4 \cdot 5^0 = (194)_{10}$*;*
(c) $(23A)_{16} = 2 \cdot 16^2 + 3 \cdot 16^1 + 10 \cdot 16^0 = (314)_{10}$.

Se acaso deseja-se fazer a conversão entre dois sistemas que não são decimais, primeiro encontra-se a representação decimal desse número e depois, pelo processo descrito anteriormente, faz-se a conversão ao sistema desejado.

EXEMPLO 4.3.6 *Escrevendo o número* $(1011111)_2$ *na notação octal obtem-se* $(137)_8$.

O número binário $(1011111)_2$ fica assim convertido para decimal:
$(1011111)_2 = 1 \cdot 2^6 + 0 \cdot 2^5 + 1 \cdot 2^4 + 1 \cdot 2^3 + 1 \cdot 2^2 + 1 \cdot 2^1 + 1 \cdot 2^0 = (95)_{10}$.
Dividindo-se o decimal 95 por 8 sucessivas vezes obtemos:

$$\begin{array}{r|l} 95 & 8 \\ \cline{2-2} 7 & 11 \quad \begin{array}{|l} 8 \\ \cline{1-1} 3 \quad 1 \end{array} \end{array}$$

Logo, $(1011111)_2 = (137)_8$.

5 Construção dos Números Racionais

Temos como objetivo neste capítulo construir o conjunto dos números racionais a partir do conjunto dos números inteiros. Em seguida, aplicamos os conceitos no estudo do valor absoluto e na conversão de sistemas de numeração para números racionais.

5.1 Anéis e Corpos.

Definição 50 *Seja $A \neq \phi$ um conjunto munido de duas operações $+$ e $\cdot$, chamadas de adição e multiplicação, respectivamente. Dizemos que $(A, +, \cdot)$ é um* ***anel*** *se, e somente se, para quaisquer $a, b, c \in A$ valem:*
(A1) $(a + b) + c = a + (b + c)$ *(associatividade);*
(A2) $a + b = b + a$ *(comutatividade)*
(A3) *existe* $0 \in A$ *tal que* $a + 0 = a$ *(elemento neutro);*
(A4) *para todo* $a \in A$ *existe* $-a \in A$ *tal que* $a + (-a) = 0$ *(elemento oposto);*
(M1) $(a \cdot b) \cdot c = a \cdot (b \cdot c)$*;*
(D1) $a \cdot (b + c) = a \cdot b + a \cdot c$ *(distributividade à esquerda);*
(D2) $(b + c) \cdot a = b \cdot a + c \cdot a$ *(distributividade à direita).*

Definição 51 *Seja $(A, +, \cdot)$ um anel. Dizemos que:*
1. A é um ***anel com unidade*** *se, e somente se, existe $1 \in A$ tal que $a \cdot 1 = 1 \cdot a = a$ para todo $a \in A$, ou seja, além de satisfazer as propriedades da Definição 50, A é um monóide em relação a operação de multiplicação.*
2. A é um ***anel comutativo*** *se, e somente se, $a \cdot b = b \cdot a$ para quaisquer $a, b \in A$, ou seja, A é um semigrupo comutativo em relação a operação de multiplicação $\cdot$.*

Exemplo 5.1.1 *os conjuntos $(\mathbb{Z}, +, \cdot)$, $(Q, +, \cdot)$ e $(\mathbb{R}, +, \cdot)$ são exemplos de anéis comutativos com unidade. Já $(\mathbb{N}, +, \cdot)$ não é nem anel pois não satisfaz a propriedade (A4) existência de elemento oposto.*

Exemplo 5.1.2 *Seja* $M_{2\times 2} := \left\{ A = \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} ;\ a_{ij} \in \mathbb{R} \text{ e } \det A \neq 0 \right\}$*, que é o conjunto das matrizes 2×2 inversíveis. $M_{2\times 2}$ com a adição e multiplicação usuais de matrizes é um exemplo de anel com unidade que não é comutativo.*

Exemplo 5.1.3 *O conjunto dos inteiros pares $(2\mathbb{Z}, +, \cdot)$ é um anel comutativo que não tem unidade. Já o conjunto dos inteiros ímpares $(2\mathbb{Z} + 1, +, \cdot)$ não é nem anel pois não satisfaz a propriedade (A3) existência de elemento neutro da adição.*

Definição 52 *Dizemos que $(A,+,\cdot)$ é um* ***anel de integridade****, se e somente se:*
1. $(A,+,\cdot)$ é um anel comutativo com unidade;
2. dados $a,b\in A$, $a\cdot b=0\iff a=0$ ou $b=0$.

Observação 13 *Nem todo anel comutativo com unidade é anel de integridade. Por exemplo, consideremos $A=\{f:\mathbb{R}\to\mathbb{R}\,|\,f\text{ é função}\}$. Munido das operações usuais de adição e de multiplicação usuais*

$$(f+g)(x)=f(x)+g(x)\ \text{ e }\ (f\cdot g)(x)=f(x)\cdot g(x)\ \ (x\in\mathbb{R}),$$

$(A,+,\cdot)$ é um anel comutativo com unidade pois satisfaz as condições das Definições 51 e 52 (O elemento neutro de A é a função nula $f\equiv 0$ e o elemento unidade é a função constante $f\equiv 1$), mas não é um anel de integridade. De fato, consideremos as funções $f:\mathbb{R}\to\mathbb{R}$ e $g:\mathbb{R}\to\mathbb{R}$ definidas por:

$$f(x)=\begin{cases} x, & se\quad x\geq 0,\\ 0, & se\quad x<0,\end{cases}\qquad e\qquad g(x)=\begin{cases} 0, & se\quad x\geq 0,\\ -x, & se\quad x<0.\end{cases}$$

Temos que $f\neq 0$ e $g\neq 0$, mas $f\cdot g\equiv 0$.

Exemplo 5.1.4 *$(\mathbb{Z},+,\cdot)$ é o nosso principal exemplo de anel de integridade. Os conjuntos $(\mathbb{Q},+,\cdot)$ e $(\mathbb{R},+,\cdot)$ também são aneis de integridade, mas eles são muito mais que isso.*

Definição 53 *Dizemos que um anel $(\mathbb{K},+,\cdot)$ é um corpo se, e somente se:*
a) $(\mathbb{K},+,\cdot)$ é um anel comutativo com unidade;
b) para todo $a\in\mathbb{K}-\{0\}$ existe um $a^{-1}\in\mathbb{K}$ tal que $a\cdot a^{-1}=1$, ou seja, $U.(\mathbb{K})=\mathbb{K}^*$ (todo elemento não nulo tem inverso multiplicativo).

Listamos abaixo os axiomas que definem uma estrutura de corpo. Dados $a,b,c\in\mathbb{K}$, valem:

$(A1)$ $(a+b)+c=a+(b+c)$;
$(A2)$ $a+b=b+a$;
$(A3)$ $\exists\ 0\in A$ tal que $a+0=a$;
$(A4)$ $\forall\ a\in A\ \exists\ -a\in A$ tal que $a+(-a)=0$;
$(M1)$ $(a\cdot b)\cdot c=a\cdot(b\cdot c)$;
$(M2)$ $a\cdot b=b\cdot a$;
$(M3)$ $\exists\ 1\in\mathbb{K}$ tal que $a\cdot 1=a$;
$(M4)$ $a\cdot a^{-1}=1\ \ (a\neq 0)$;
(D) $a\cdot(b+c)=a\cdot b+a\cdot c$.

Exemplo 5.1.5 *Vamos ver mais adiante que os conjuntos $\mathbb{Q}$ e $\mathbb{R}$ são corpos. Outros exemplos de corpos são os conjuntos $\mathbb{Z}_2$, $\mathbb{Z}_3$, $\mathbb{Z}_5$ e mais geralmente, $\mathbb{Z}_p$ com p primo.*

Observemos que o anel de integridade $\mathbb{Z}$ não é corpo, pois $U.(\mathbb{Z})=\{-1,1\}\neq\mathbb{Z}$.

Definição 54 *Seja $\mathbb{K}$ um corpo. Dados $a,b\in\mathbb{K}$ com $b\neq 0$, definimos o quociente de a por b por $\dfrac{a}{b}=a\cdot b^{-1}$.*

Lema 5.1.6 *Dados $a,b\in\mathbb{K}^*$, $(ab)^{-1}=a^{-1}b^{-1}$.*

Dem. De fato, como $(ab)(ab)^{-1} = 1$ e $(ab)(a^{-1}b^{-1}) = 1$, segue o resultado. ∎

TEOREMA 5.1.7 *Sejam $a, b, c, d \in \mathbb{K}$ com $b \neq 0$ e $d \neq 0$. Então:*

1. $\frac{a}{b} = \frac{c}{d} \iff a \cdot d = b \cdot c$;
2. $\frac{a}{b} + \frac{c}{d} = \frac{a \cdot d + b \cdot c}{b \cdot d}$;
3. $-\frac{a}{b} = \frac{-a}{b} = \frac{a}{-b}$;
4. $\frac{a}{b} \cdot \frac{c}{d} = \frac{a \cdot c}{b \cdot d}$;
5. $\left(\frac{a}{b}\right)^{-1} = \frac{b}{a}$;
6. $\frac{a}{1} = a$;
7. $\frac{a}{b} = 0 \iff a = 0$.

Dem. 1. ($\Rightarrow$) $\frac{a}{b} = a \cdot b^{-1}$ e $\frac{c}{d} = c \cdot d^{-1}$. Como por hipótese $\frac{a}{b} = \frac{c}{d}$, segue que $ab^{-1} = cd^{-1}$ e assim, multiplicando bd em ambos os lados dessa igualdade obtemos:

$$ad = (ab^{-1})(bd) = (cd^{-1})(bd) = bc,$$

ou seja, $a \cdot d = b \cdot c$.

($\Leftarrow$) Se $a \cdot d = b \cdot c$ então,

$$\frac{a}{b} = ab^{-1} = a(dd^{-1})b^{-1} = (ad)(d^{-1}b^{-1}) = (bc)(d^{-1}b^{-1}) = (cd^{-1})(bb^{-1}) = cd^{-1} = \frac{c}{d},$$

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

2. Da associatividade e comutatividade de $\mathbb{K}$ temos que,

$$\frac{a}{b} + \frac{c}{d} = ab^{-1} + cd^{-1} = a(dd^{-1})b^{-1} + (bb^{-1})cd^{-1} = (ad)(d^{-1}b^{-1}) + (bc)(d^{-1}b^{-1}).$$

Como pela distributividade e a definição de quociente

$$(ad)(d^{-1}b^{-1}) + (bc)(d^{-1}b^{-1}) = (ad + bc)(d^{-1}b^{-1}) = \frac{a \cdot d + b \cdot c}{b \cdot d},$$

segue o resultado.

3. Como $-\frac{a}{b} = -(ab^{-1}) = (-a)b^{-1} = \frac{-a}{b}$ e

$\frac{a}{-b} = a(-b)^{-1} = a(-b^{-1}) = (-a)b^{-1} = \frac{-a}{b}$,

segue que $-\frac{a}{b} = \frac{-a}{b} = \frac{a}{-b}$.

4. Para provar essa propriedade, fazemos uso da definição de quociente juntamente com a associatividade, a comutatividade e o Lema 5.1.6 do seguinte modo:

$$\frac{a}{b} \cdot \frac{c}{d} = (ab^{-1})(cd^{-1}) = (ac)(b^{-1}d^{-1}) = (ac)(bd)^{-1} = \frac{a \cdot c}{b \cdot d}.$$

Para construir o corpo de frações de um anel de integridade qualquer, além do que já foi falado, precisamos do conceito de subanel.

DEFINIÇÃO 55 *Seja $(A,+,\cdot)$ um anel e seja $B \subseteq A$. Dizemos que $(B,+,\cdot)$ é um* ***subanel*** *de $(A,+,\cdot)$ se, e somente se, B é fechado para as operações $+$ e $\cdot$ de A e $(B,+,\cdot)$ é um anel.*

TEOREMA 5.1.8 *Seja $(A,+,\cdot)$ um anel e seja $B \subseteq A$. Dizemos que $(B,+,\cdot)$ é um subanel de $(A,+,\cdot)$ se, e somente se, satisfaz as seguintes propriedades:*
(i) $0 \in B$;
(ii) dado $a \in A$, se $a \in B$ então $-a \in B$;
(iii) para quaisquer $a, b \in B$, $a+b \in B$ e $a \cdot b \in B$.

Dem. ($\Rightarrow$) (i) Seja 0 o elemento neutro de A para a soma. Do fato de $B \subseteq A$ ser anel, segue que B tem elemento neutro, digamos, 0_B. Além disso, $0_B + 0_B = 0_B = 0_B + 0$ e assim, pela lei do cancelamento, $0_B = 0$ e portanto, $0 \in B$.

(ii) Como B é anel, se $a \in B$, então por (A4) existe $a' \in B$ tal que, $a + a' = 0_B = 0$ e daí, vem que $a' = -a$, ou seja, a' coincide com o oposto de a em A.

(iii) segue imediatamente do fato de B ser anel. ∎

EXEMPLO 5.1.9 *$\mathbb{Z}$ é subanel de $\mathbb{Q}$ e de $\mathbb{R}$, $\mathbb{Q}$ é subanel de $\mathbb{R}$, $2\mathbb{Z}$ é subanel de $\mathbb{Z}$, $4\mathbb{Z}$ é subanel de $2\mathbb{Z}$ e $9\mathbb{Z}$ é subanel de $3\mathbb{Z}$.*

5.2 Os racionais como corpo de frações dos inteiros.

Dados $a, b \in \mathbb{Z}$, com $b \neq 0$, sabemos que existe $x \in \mathbb{Z}$ tal que $b \cdot x = a$ se, e somente se, $b|a$; ou seja, em $\mathbb{Z}$ a equação $b \cdot x = a$ tem solução se, e somente se, a é múltiplo de b e $b \neq 0$. Isto é porque $U.(\mathbb{Z}) = \{-1, 1\}$.

Temos como objetivo nesta seção construir um conjunto, que denotaremos por $\mathbb{Q}$, ampliação mínima de $\mathbb{Z}$, onde a equação $b \cdot x = a$ sempre tem solução, desde que $b \neq 0$. Em outras palavras, queremos que $U.(\mathbb{Q}) = \mathbb{Q}^*$. Esse conjunto será um corpo e é chamado de corpo dos números racionais. Faremos essa construção para um anel de integridade qualquer e a ampliação a ser obtida é chamada de corpo de frações do anel de integridade; assim, $\mathbb{Q}$ será o corpo de frações do anel de integridade $\mathbb{Z}$. Faremos o processo a partir de um anel de integridade qualquer.

Observemos que $\frac{a}{b}$ $(= a \cdot b^{-1})$ satisfaz a equação $d \cdot x = c$ $(d \neq 0,\ d|c)$ se, e somente se, $a \cdot d = b \cdot c$. Por exemplo, $5 \cdot x = 10 \Longrightarrow x = \{2, 4/2, 8/4, \dots\}$. Isso nos mostra que não basta introduzir os novos elementos (de $\mathbb{Q}$) como pares ordenados de números inteiros, também é necessários estabelecer um critério para que dois pares ordenados representem a mesma fração.

Seja A um anel de integridade e seja $E = A \times A^* := \{(a,b) \mid a \in A,\ b \in A^*\}$, onde $A^* = A - \{0\}$. Definiremos em E uma relação R do seguinte modo:

DEFINIÇÃO 56 *Se* $(a,b),(c,d) \in E$, *diremos que*

$$(a,b)R(c,d) \iff a \cdot d = b \cdot c. \tag{5.1}$$

EXEMPLO 5.2.1 *Para quaisquer* $a, b \in A^*$, $(a,a)R(b,b)$, *pois* $ab = ab$.

TEOREMA 5.2.2 *A relação* R *definida em* (5.1) *é uma relação de equivalência.*

Dem. Dado qualquer $(a,b) \in E$, $(a,b)R(a,b)$, pois $ab = ba$. Portanto, R é reflexiva.

Dados $(a,b),(c,d) \in E$,

$$(a,b)R(c,d) \iff ad = bc \iff cb = da \iff (c,d)R(a,b).$$

Portanto, R é simétrica.

Dados $(a,b),(c,d),(e,f) \in E$, se $(a,b)R(c,d)$ e $(c,d)R(e,f)$, então $ad = bc$ e $cf = de$; multiplicando f em ambos os lados da primeira igualdade e b na segunda e usando as propriedades do anel de integridade A (associatividade, comutatividade e LCM) obtemos:
$(ad)f = (bc)f$ e $b(cf) = (de)b \iff (af)d = (bc)f$ e $(bc)f = (be)d \implies af = be \iff (a,b)R(e,f)$.

Com isso fica provado que R é uma relação de equivalência. ∎

Dado $(a,b) \in E$, indicaremos por $\overline{(a,b)} = \{\,(x,y) \in E \mid (x,y)R(a,b)\,\}$ à classe de equivalência módulo R determinada por (a,b). E indicaremos por K o conjunto quociente de E por R, ou seja, $K = E/R = \dfrac{A \times A^*}{R} := \{\,\overline{(a,b)} \mid (a,b \in E\,)\}$. É óbvio que K é uma partição de E (veja o Teorema 2.2.8).

DEFINIÇÃO 57 *A adição e a multiplicação em* K *são definidas, respectivamente, do seguinte modo: Dados* $\overline{(a,b)},\overline{(c,d)} \in K$,

$$\overline{(a,b)} + \overline{(c,d)} = \overline{(ad+bc,bd)} \quad e \quad \overline{(a,b)} \cdot \overline{(c,d)} = \overline{(ac,bd)}. \tag{5.2}$$

PROPOSIÇÃO 5.2.3 *A soma e o produto em* K *definidos em* (5.2) *independem dos representantes* (a,b) *e* (c,d) *das classes de equivalência* $\overline{(a,b)}$ *e* $\overline{(c,d)}$, *ou seja, estas operações estão bem definidas em* K.

Dem. Devemos mostrar que, se $\overline{(a,b)} = \overline{(a',b')}$ e $\overline{(c,d)} = \overline{(c',d')}$, então

$$\overline{(ad+bc,bd)} = \overline{(a'd'+b'c',b'd')} \quad \text{e} \quad \overline{(ac,bd)} = \overline{(a'c',b'd')}. \tag{5.3}$$

De fato, por hipótese temos $ab' = ba'$ e $cd' = dc'$; assim,

$$(ad+bc)b'd' = (ab')(dd') + (bb')(cd') = (ba')(dd') + (bb')(dc') = (bd)(a'd') + (bd)(b'c'),$$

ou seja, $(ad+bc)b'd' = (bd)(a'd'+b'c')$. Daí, $\overline{(ad+bc,bd)} = \overline{(a'd'+b'c',b'd')}$.

Agora,

$$(ac)(b'd') = (ab')(cd') = (ba')(dc') = (bd)(a'c')$$

e isso equivale a afirmar que $\overline{(ac,bd)} = \overline{(a'c',b'd')}$. ∎

TEOREMA 5.2.4 *Munido das operações definidas em* (5.2)*, K é um corpo.*

Dem. Devemos provar que $(K, +, \cdot)$ verifica os axiomas (A1) – (A4), (M1) – (M4) e (D). Iremos demonstrar (A3), (A4), (M3) e (M4).

(A3): Queremos determinar $\overline{(x,y)} \in K$ tal que, $\overline{(a,b)} + \overline{(x,y)} = \overline{(a,b)}$, para todo $\overline{(a,b)} \in K$.

$$\begin{aligned}\overline{(a,b)} + \overline{(x,y)} = \overline{(a,b)} &\iff \overline{(ay+bx, by)} = \overline{(a,b)} \\ &\iff (ay+bx)b = bya \\ &\iff b^2x = 0, \quad \forall\, b \in A;\end{aligned}$$

consequentemente, $x = 0$ e portanto, $\overline{(x,y)} = \overline{(0,y)} = \overline{(0,1)}$. E de fato $\overline{(0,1)}$ é o elemento neutro, pois dado $\overline{(a,b)} \in K$,

$$\overline{(a,b)} + \overline{(0,1)} = \overline{(a\cdot 1 + b\cdot 0, b\cdot 1)} = \overline{(a,b)}.$$

(A4): Queremos provar que para todo $\overline{(a,b)} \in K$, existe um $\overline{(x,y)} \in K$ tal que,

$$\overline{(a,b)} + \overline{(x,y)} = \overline{(0,1)}.$$

Ora,

$$\overline{(a,b)} + \overline{(x,y)} = \overline{(0,1)} \iff \overline{(ay+bx, by)} = \overline{(0,1)} \iff ay + bx = 0.$$

Tomando então $x = -a$ e $y = b$ (ou seja, $\overline{(x,y)} = \overline{(-a,b)}$) temos que,

$$\overline{(a,b)} + \overline{(-a,b)} = \overline{(ab + b(-a), b^2)} = \overline{(0,b^2)} = \overline{(0,1)}.$$

Portanto, $\overline{(-a,b)}$ é o oposto de $\overline{(a,b)}$.

(M3): Queremos determinar $\overline{(x,y)} \in K$ tal que, $\overline{(a,b)} \cdot \overline{(x,y)} = \overline{(a,b)}$, para todo $\overline{(a,b)} \in K$.

$$\begin{aligned}\overline{(a,b)} \cdot \overline{(x,y)} = \overline{(a,b)} &\iff \overline{(ax, by)} = \overline{(a,b)}, \quad \forall\, a,\, b \in A, \\ &\iff (ab)x = (ab)y, \quad \forall\, a,\, b \in A, \\ &\iff \overline{(x,y)} = \overline{(x,x)} = \overline{(1,1)};\end{aligned}$$

de fato $\overline{(1,1)} \neq \overline{(0,1)}$ e $\overline{(1,1)} \cdot \overline{(a,b)} = \overline{(a,b)}$, para todo $\overline{(a,b)} \in K$. Portanto $\overline{(1,1)}$ é o elemento unidade de K.

M4: Queremos provar que para todo $\overline{(a,b)} \in K^*$, existe um $\overline{(x,y)} \in K$ tal que,

$$\overline{(a,b)} \cdot \overline{(x,y)} = \overline{(1,1)}.$$

Temos que,

$$\overline{(a,b)} \cdot \overline{(x,y)} = \overline{(1,1)} \iff \overline{(ax, by)} = \overline{(1,1)} \iff ax = 1 \text{ e } ay = 1.$$

Basta então tomar $x = b$ e $y = a$, ou seja, o elemento inverso de $\overline{(a,b)}$ é $\overline{(b,a)}$. Logo, todo elemento $\overline{(a,b)} \in K^*$ é inversível e $\overline{(a,b)}^{-1} = \overline{(b,a)}$. ∎

Vamos chamar o elemento neutro $\overline{(0,1)} = 0'$ e o elemento unidade $\overline{(1,1)} = 1'$.

Observemos que, dado qualquer $\overline{(a,b)} \in K$, podemos escrevê-lo na forma:

$$\overline{(a,b)} = \overline{(a,1)} \cdot \overline{(1,b)} = \overline{(a,1)} \cdot \overline{(b,1)}^{-1} = \frac{\overline{(a,1)}}{\overline{(b,1)}}. \tag{5.4}$$

Por esse motivo, o corpo $(K, +, \cdot)$ construido acima é chamado de corpo de frações do anel de integridade $(A, + \cdot)$.

TEOREMA 5.2.5 *Seja* $A' = \{\, \overline{(a,1)} \in K \mid a \in A \,\}$. *Então:*

1. $(A', +, \cdot)$ *é um subanel unitário de* K*;*
2. $(A', +, \cdot)$ *é um anel de integridade;*
3. *O corpo de frações de* A' *é* K*.*

Dem. Temos que $1' = \overline{(1,1)} \in A'$, logo $1_{A'} = 1'$.

1. Se $\overline{(a,1)}$, $\overline{(b,1)} \in A'$, então

$$\begin{aligned} \overline{(a,1)} + \overline{(b,1)} &= \overline{(a \cdot 1 + 1 \cdot b, 1 \cdot 1)} = \overline{(a+b,1)} \in A', \\ \overline{(a,1)} \cdot \overline{(b,1)} &= \overline{(ab,1)} \in A', \\ -\overline{(a,1)} &= \overline{(-a,1)} \in A'. \end{aligned}$$

Logo, pelo Teorema 5.1.8, A' subanel unitário de K. Agora, dado $\overline{(a,b)} \in K$, temos:

$$\overline{(a,b)} = \overline{(a,1)} \cdot \overline{(1,b)} = \overline{(a,1)} \cdot \overline{(b,1)}^{-1} = \frac{\overline{(a,1)}}{\overline{(b,1)}} \tag{5.5}$$

e assim, K é o corpo de frações de A' em K. ∎

TEOREMA 5.2.6 *A aplicação* $f : A \to A'$ *definida por* $f(a) = \overline{(a,1)}$ *é um isomorfismo de* A *em* A'*.*

Dem. Provemos que f é um homomorfismo com relação à soma e ao produto. Dados $a, b \in A$,

$$f(a+b) = \overline{(a+b,1)} = \overline{(a,1)} + \overline{(b,1)} = f(a) + f(b)$$

e

$$f(ab) = \overline{(ab,1)} = \overline{(a,1)}\,\overline{(b,1)} = f(a)f(b).$$

Que f é bijetora é muito simples de ver. Portanto f é isomorfismo. ∎

Podemos então identificar o anel A com A', pois são isomorfos. Assim, de agora em diante identificaremos os elementos $\overline{(a,1)} \in A'$ com $a \in A$, de modo que a partir de agora $\overline{(a,1)} = a$. Por exemplo, $0' := \overline{(0,1)} = 0$ e $1' := \overline{(1,1)} = 1$ e dessa forma, os elementos neutro e unidade de A ficam identificados como os elementos neutro e unidade de K, respectivamente. Além disso, A passa a ser um subanel unitário de K.

Temos que, se $\overline{(a,b)} \in K$, então por (5.4),

$$\overline{(a,b)} = \frac{\overline{(a,1)}}{\overline{(b,1)}} = \frac{a}{b},$$

pois $\overline{(a,1)} = a$ e $\overline{(b,1)} = b$. Com isso todo elemento $\overline{(a,b)} \in K$ pode ser (e será) indicado como $\frac{a}{b}$ e podemos escrever

$$K = \{ \frac{a}{b} \,|\, a, b \in A \text{ e } b \neq 0 \}.$$

Vejamos as propriedades básicas de K:

PROPOSIÇÃO 5.2.7 *Sejam $a, b, c, d \in A$ tais que $b, d \neq 0$. Então:*
(a) $\frac{a}{1} = a$ *e* $\frac{a}{b} = \frac{c}{d}$ *se, e somente se,* $ad = bc$;
(b) $\frac{a}{b} + \frac{c}{d} = \frac{ad+bc}{bd}$ *(adição em K) e* $\frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd}$ *(multiplicação em K);*
(c) $\left(\frac{a}{b}\right)^{-1} = \frac{b}{a}$, *quando $a \neq 0$ e $b \neq 0$. Em particular, se $a \neq 0$, então $a^{-1} = \frac{1}{a}$.*

Dem. Observemos que, quando $b \neq 0$, sempre podemos determinar o quociente de a por b, que é o elemento $\frac{a}{b}$. E valem todas as propriedades estabelecidas anteriormente para o quociente de dois elementos de um corpo K.

DEFINIÇÃO 58 *Chama-se **corpo dos números racionais** o corpo de frações do anel de integridade $\mathbb{Z}$ dos números inteiros.*

Notação: $\mathbb{Q} = \{ \frac{a}{b} \,|\, a, b \in \mathbb{Z} \text{ e } b \neq 0 \}$.

Observemos que, se $a, b \in \mathbb{Z}$, com $b \neq 0$, existe um único $x \in \mathbb{Q}$ tal que $bx = a$, a saber, $x = \frac{a}{b}$. Assim, está resolvido o problema proposto.

5.3 Relação de ordem no corpo dos números racionais.

DEFINIÇÃO 59 *Seja $(K, +, \cdot)$ um corpo e suponhamos que existe um conjunto $P \subset K$ satisfazendo as seguintes afirmações:*
a) Para quaisquer $x, y \in P$, $x + y \in P$ e $x \cdot y \in P$;
b) Dado $x \in K$, ou $x \in P$ ou $x = 0$ ou $-x \in P$.
*Então P é chamado conjunto dos **elementos positivos** de K.*

Do item b) da definição anterior temos que $K = -P \cup \{0\} \cup P$ (união disjunta) onde $-P = \{ x \in K | -x \in P \}$.

DEFINIÇÃO 60 *Dados $x, y \in K$, diremos que*

$x \leq y$ *se, e somente se,* $y - x \in P \cup \{0\}$, *ou seja,* $y - x \in P$ *ou* $y - x = 0$

Usaremos a notação $x < y$ para indicar que $y - x \in P$.

Vamos provar a seguir que $\leq$ é uma relação de ordem total sobre K compatível com a adição e a multiplicação em K.

TEOREMA 5.3.1 *Seja K um corpo contendo um conjunto P que satisfaz os itens a) e b) da definição 59. Então:*

(i) *$\leq$ define uma relação de ordem total sobre K.*

(ii) *dados $x, y, z \in K$, $x \leq y \Longrightarrow x + z \leq y + z$, ou seja, a ordem total $\leq$ é compatível com a adição em K;*

(iii) *dados $x, y, z \in K$, $x \leq y$ e $0 \leq z \Longrightarrow x \cdot z \leq y \cdot z$, isso quer dizer que $\leq$ é compatível com a multiplicação em K.*

Dem. (i) Precisamos provar que $\leq$ é (a) reflexiva, (b) antissimétrica e (c) transitiva e além disso (d) satisfaz a definição 12. Assim, sejam $x, y, z \in K$, temos que:

(a) $x \leq x$, pois $x - x = 0$.

(b) Sejam $x, y \in K$ tais que $x \leq y$ e $y \leq x$. Então, $y - x \in P \cup \{0\}$ e $x - y \in P \cup \{0\}$, ou seja, ou $y - x$ e $x - y \in P$ ou $x - y = 0$.
Se $y - x$ e $x - y \in P$ então teríamos pelo item a) da definição 59 que $(x-y)+(y-x) = 0 \in P$ o que é um absurdo. Portanto, $x - y = 0$, ou seja, $x = y$. Logo, $\leq$ é antissimétrica.
Sejam $x, y, z \in K$ tais que $x \leq y$ e $y \leq z$. Isso quer dizer que $x - y \in P \cup \{0\}$ e $z - y \in P \cup \{0\}$. Logo, segue do item a) da definição 59 que, $z - x = (z - y) + (y - x) \in P \cup \{0\}$, ou seja, $x \leq z$. Portanto, $\leq$ é transitiva.

(d) Sejam $x, y \in K$. Como $K = -P \cup \{0\} \cup P$, segue que $x - y \in P$ ou $x - y = 0$ ou $x - y = -P$, ou seja, $y - x \in P$ ou $x = y$ ou $x - y \in P$. Consequentemente, $x \leq y$ ou $y \leq x$, o que implica que $\leq$ é uma relação total de ordem sobre K. Assim, concluímos a demonstração do item **i)**.

(ii) Dados $x, y, z \in K$,

$$\begin{aligned} x \leq y &\Longleftrightarrow y - x \in P \\ &\Longleftrightarrow (y + z) - (x + z) \in P \\ &\Longleftrightarrow x + z \leq y + z \end{aligned}$$

(iii) Suponha que $y - x$ e $z \in z \in P \cup \{0\}$. Se $y - x = 0$ ou $z = 0$ então segue que $x \cdot z \leq y \cdot z$. Agora, se $y - x$ e $z \in P$ então o resultado segue de $P1$. E está demonstrado o teorema.

Segue imediatamente o teorema 5.3.1 o seguinte resultado:

COROLÁRIO 5.3.2 *A relação $<$ é uma ordem restrita sobre K, compatível com a adição e a multiplicação em K, ou seja,*
i') *satisfaz a definição 14;*
ii') *dados $x, y, z \in K$, $x < y \Longrightarrow x + y < y + z$ (monotoicidade da adição em K);*

iii') *dados $x, y, z \in K$, $x < y$ e $0 < z \Longrightarrow x \cdot z < y \cdot z$ (submonotonicidade da multiplicação em K).*

Exibimos agora a recíproca do Teorema 5.3.1.

Corolário 5.3.3 *Se $(K, +, \cdot)$ é um corpo totalmente ordenado e a ordem K satisfaz (ii) e (iii) do Teorema 5.3.1, então existe $P \subset K$ que satisfaz $(P1)$ e $(P2)$.*

Dem. Seja $\leq$ uma ordem total sobre K. Considere o conjunto:

$$= \{x \in K |\ 0 \leq x \ e \ x \neq 0\} = \{x \in K |\ 0 < x\}$$

Então $P \subset K$ e satisfaz $P1$ e $P2$. De fato, se $0 < x$ e $0 < y$ (isto é, $x, y \in P$), então pelo item (ii') do corolário 5.3.2, $0 < x + y$, ou seja, $x + y \in P$. Isto mostra que P satisfaz $P1$. Agora, dado $x \in K$, como K é totalmente ordenado, segue que $x \leq 0$ ou $0 \leq x$, e isso implica que, $x < 0$ ou $x = 0$, ou $0 < x$, ou seja, $-x \in P$, ou $x = 0$, ou $x \in P$. Logo, P satisfaz $P2$. ∎

O resultado abaixo segue imediatamente do que foi feito agora.

Corolário 5.3.4 *Num corpo totalmente ordenado K vale a lei da tricotomia: "Dados $x, y \in K$, ocorre só, e somente só, uma das seguintes alternativas: ou $x < y$ ou $x = y$ ou $y < x$."*

Observação 14 *Ter em mente a propriedade da tricotomia é importante pois é bastante corriqueiro se usar a afirmação recíproca da antissimetria para provar que duas expressões são iguais; ou seja, dadas duas expressões e_1 e e_2, $e_1 = e_2 \Longleftrightarrow e_1 \leq e_2$ e $e_2 \leq e_1$.*

Teorema 5.3.5 *O corpo dos números racionais $\mathbb{Q} = \left\{\frac{a}{b} | a, b \in \mathbb{N}, b \neq 0\right\}$ pode ser munido de uma relação de ordem total.*

Dem. Consideremos o conjunto $P = \left\{\frac{a}{b} |\ a \cdot b \in N^*\right\}$, que é o conjunto dos números $\frac{a}{b} \in \mathbb{Q}$ em que a e b têm o mesmo sinal. Provaremos que P é o conjunto dos números positivos de $\mathbb{Q}$, ou seja, que P satisfaz $P1$ e $P2$.
$P1$: Dados $x = \frac{a}{b}$ e $y = \frac{c}{d}$ elementos de P, temos que $x + y = \dfrac{ad + bc}{bd}$. Como $ab \in N^*$ (porque $\frac{a}{b} \in P$), $d^2 \in \mathbb{N}^*$ (porque $d \neq 0$), $cd \in \mathbb{N}^*$ (porque $\frac{c}{d} \in P$) e $b^2 \in \mathbb{N}^*$ (porque $b \neq 0$), temos que

$$(ad + bc) \cdot bd = (ad) \cdot (bd) + (bc) \cdot (bd) = (ab)\, d^2 + (cd)\, b^2 \in \mathbb{N}^*$$

e portanto, $x + y \in P$. Ademais, $x \cdot y = \frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd} \in P$, pois $(ac)(bd) = (ab)(cd) \in \mathbb{N}^*$, porque $ab, cd \in N^*$. Logo, P satisfaz $P1$.
$P2$: Dado qualquer $x = \frac{a}{b} \in \mathbb{Q}$, temos que, ou $ab = 0x$, ou $ab > 0$ ou $ab < 0$. Neste caso, ou $x = 0$ (pois $ab = 0 \Longrightarrow a = 0$), ou $x \in P$ (no caso de ser $ab > 0$), ou $-x \in P$ (no caso de $ab < 0$). Logo, P satisfaz $P2$.

Assim, pelo teorema 5.3.1, a relação

$$x \leq y \Longleftrightarrow y - x \in P \cap \{0\},$$

(onde $P = \left\{ \frac{p}{q} |\ p \cdot q \in \mathbb{N}^* \right\}$) define uma ordem total sobre $\mathbb{Q}$, compatível com a adição e a multiplicação, conforme os itens (i) e (ii) daquele teorema.

Notação: Vamos designar o conjunto dos números positivos de $\mathbb{Q}$ por $\mathbb{Q}_+$ e o conjunto dos números negativos de $\mathbb{Q}$ (ou seja, $-\mathbb{Q}_+$) por $\mathbb{Q}_-$.

5.4 Aplicação: Valor Absoluto

Apesar de defirnirmos valor absoluto para o conjunto dos racionais, o conceito de valor absoluto se aplica natualmente a qualquer corpo ordenado ou mesmo a qualquer anel de integridade ordenado. Por exemplo ao conjunto dos números inteiros, e ao conjunto dos números reais que não serão abordados nestre trabalho.

Definição 61 *Dado um número racional x, chama-se valor absoluto de x ou módulo de x e denotado por $|x|$, o número racional não negativo tal que*

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

Exemplo 5.4.1 *Temos, por exemplo, os seguintes valores absolutos, $|6| = 6$, $|-\sqrt{2}| = \sqrt{2}$, $|3 - \pi| = \pi - 3$.*

Proposição 5.4.2 *Seja x um número real e $|x|$ o seu valor absoluto. Então são válidas as seguintes propriedades:*
$(P1)$. Se $a \in R$ e $a \geq 0$ então $|x| < a \Longleftrightarrow -a < x < a$
$(P2)$. Se $a \in R$ então $|x| > a \Longleftrightarrow x < -a$ e $x > a$
$(P3)$. Se $x, y \in R$ então $|x \cdot y| = |x| \cdot |y|$
$(P4)$. Se $x, y \in R$ e $y \neq 0$ então $\left|\frac{x}{y}\right| = \frac{|x|}{|y|}$

Dem. $(P1)$. Pela definição de valor absoluto $|x| < a \Longleftrightarrow x < a$ ou $-x < a \Longleftrightarrow x < a$ ou $x > -a \Longleftrightarrow -a < x < a$.

$(P2)$. Também da definição segue que $|x| > a \Longleftrightarrow x > a$ ou $-x > a$ $|x| < a \Longleftrightarrow x < -a$ ou $x > a$.

$(P3)$. Note que $|x|^2 = x^2$, assim $|x \cdot y|^2 = (x \cdot y)^2 = x^2 \cdot y^2 = |x|^2 \cdot |y|^2 = (|x| \cdot |y|)^2$. Logo, $|x \cdot y| = \pm(|x| \cdot |y|)$ o que obviamente implica que $|x \cdot y| = |x| \cdot |y|$.

$(P4)$. Pelo mesmo argumento de $(P3)$ note que $|x|^2 = x^2$. Assim, $\left|\frac{x}{y}\right|^2 = \left(\frac{x}{y}\right)^2 = \frac{x^2}{y^2} = \frac{|x|^2}{|y|^2}$. Portanto, $\left|\frac{x}{y}\right| = \pm\left(\frac{x}{y}\right)$ que implica em $\left|\frac{x}{y}\right| = \frac{|x|}{|y|}$. ∎

Um importante resultado do estudo do Valor Absoluto é a Desigualdade Triangular. Esse fato tem origem na geometria Euclididana, nos 'Elementos' de Euclides onde ele afirma que em um triângulo o comprimento de um dos lados é sempre menor que a soma dos outros dois. É um resultado bastante utilizado na demonstração de outros fatos importante como a desigualdade entre as médias aritmética, geométrica e harmônica por exemplo.

Teorema 5.4.3 *(Desigualdade Triangular) Se $x, y \in \mathbb{Q}$ então $|x+y| \leq |x| + |y|$, ocorrendo a igualdade se, e somente se, x e y tiverem o mesmo sinal.*

Dem. Do item (1) da proposição 5.4.2 temos que $-|x| \leq x \leq |x|$ e também que $-|y| \leq y \leq |y|$. Somando essas duas expressões obtemos $-(|x| + |y|) \leq x + y \leq |x| + |y|$, daí segue que,

$$|x+y| \leq |x| + |y|. \quad \blacksquare$$

Podemos generalizar a Desigualdade Triangular para um número n qualquer de elementos.

Corolário 5.4.4 *Dados $a_1, a_2, \cdots a_n \in \mathbb{Q}$ temos que*

$$|a_1 + a_2 + \cdots + a_n| \leq |a_1| + |a_2| + \cdots + |a_n|, \tag{5.6}$$

ocorrendo a igualdade se, e somente se, $a_1, a_2, \cdots, a_n$ tiverem o mesmo sinal.

Dem. Podemos mostrar esse fato pelo método da indução finita sobre n. Para $n = 1$ é fácil perceber que $|a_1| \leq |a_1|$. Suponha que 5.6 seja verdadeira para um $n \in \mathbb{N}$ qualquer. Daí segue pelo teorema 5.4.3 que,

$$|(a_1 + a_2 + \cdots + a_n) + a_{n+1}| \leq |a_1 + a_2 + \cdots + a_n| + |a_{n+1}|$$

e então pela hipótese de indução temos que,

$$|a_1 + a_2 + \cdots a_n + a_{n+1}| \leq |a_1| + |a_2| + \cdots + |a_n| + |a_{n+1}|. \quad \blacksquare$$

Observação 15 *Geometricamente, o valor absoluto de um número $|x|$ ou $|x-0|$ constitui a distância do ponto x até o ponto 0, assim como $|x-a|$ nos dá a distância do ponto x até o ponto a.*

DEFINIÇÃO 62 *Uma equação é chamada de modular se a variável está dentro de um módulo. A equação $|x| = a$ significa os pontos da reta que estão a uma distância de a unidades do zero. Assim temos que, $x = -a$ ou $x = a$.*

EXEMPLO 5.4.5 *A equação $|x - 3| = 5$ significa os pontos da reta que estão a distância de 5 unidades do ponto 3. Então, pela definição anterior temos que $x - 3 = 5 \Longrightarrow x = 8$ ou $x - 3 = -5 \Longrightarrow x = -2$.*

EXEMPLO 5.4.6 *A solução da equação $|x + 1| + |2x - 1| = 3$ é o conjunto $\{1, 1\}$.*

De acordo com a Definição 61 temos que:

$$|x+1| = \begin{cases} x+1, se\ x \geq -1 \\ -x-1, se\ x < -1 \end{cases}$$

e

$$|2x-1| = \begin{cases} 2x-1, se\ x \geq \frac{1}{2} \\ -2x+1, se\ x < \frac{1}{2} \end{cases}$$

Assim, temos que para o intervalo $(-\infty, -1)$,

$$|x + 1| + |2x - 1| = 3 \Longrightarrow (-x - 1) + (-2x + 1) = 3 \Longrightarrow x = -1.$$

Com $x \in \left[-1, \frac{1}{2}\right)$ temos

$$|x + 1| + |2x - 1| = 3 \Longrightarrow (x + 1) + (-2x + 1) = 3 \Longrightarrow x = -1$$

e finalmente para o intervalo $\left[\frac{1}{2}, \infty\right)$,

$$|x + 1| + |2x - 1| = 3 \Longrightarrow (x + 1) + (2x + 1) = 3 \Longrightarrow x = 1. \quad \blacksquare$$

DEFINIÇÃO 63 *Uma inequação é chamada de modular se a variável está dentro de um módulo. De acordo com a proposição 5.4.2 temos que:*
$|x| < a \Longleftrightarrow -a < x < a$ ou $|x| \leq a \Longleftrightarrow -a \leq x \leq a$
$|x| > a \Longleftrightarrow x < -a$ e $x > a$ ou $|x| \geq a \Longleftrightarrow x \leq -a$ e $x \geq a$

EXEMPLO 5.4.7 *A inequação $|x-2| \leq 5$ denota os valores de x que estão a uma distância menor que 5 do ponto 2 da reta. Estes pontos estão no intervalo $-3 < x < 7$.*

De fato, por (P1) da Proposição 5.4.2 temos que:
$|x - 2| \leq 5 \Longrightarrow -5 < x - 2 < 5 \Longrightarrow -5 + 2 < x - 2 + 2 < 5 + 2 \Longrightarrow -3 < x < 7.$

EXEMPLO 5.4.8 *A inequação modular $1 \leq |x-1| \leq 3$ mostra os valores que estão a uma distância maior ou igual a 1 e menor ou igual a 3 do ponto $x = 1$.*

Da inequação segue que $|x-1| \leq 3$ e $|x-1| \geq 1$.
Do item 1 da Proposição 5.4.2 temos que:
$|x-1| \leq 3 \Longrightarrow -3 \leq x-1 \leq 3 \Longrightarrow -2 \leq x \leq 4$.
E do item 2 da Proposição 5.4.2 temos que:
$|x-1| \geq 1 \Longrightarrow x-1 \leq -1$ ou $x-1 \geq 1$ ou seja, $x \leq 0$ ou $x \geq 2$.
Fazendo a intersecção desses intervalos encontramos que a solução da inequação está no intervalo $[-2, 0]$ ou $[2, 4]$

5.5 Aplicação: Mudança de Base de um Sistema de Numeração para Números Racionais

Nesta seção veremos como fazer a conversão de números racionais do sistema de base decimal para outras bases. Primeiramente definiremos um racional decimal na notação de um polinômio de potências de base 10.

Definição 64 *Seja $N = a_n \cdot a_{n-1} \cdots a_0, a_{-1} \cdot a_{-2} \cdots a_{-m}$ um número racional finito (ou seja, tem um número finito de algarismos após a vírgula) de base decimal, então N pode ser escrito como:*

$$N = a_n \cdot 10^{n-1} + a_{n-1} \cdot 10^{n-2} + ... + a_0 \cdot 10^0 + a_{-1} \cdot 10^{-1} + a_{-2} \cdot 10^{-2} + ... + a_{-m} \cdot 10^{-m}$$

onde n é o número de algarismos da parte inteira e m é o número de algarismos da parte fracionária.

Exemplo 5.5.1 *Os números racionais decimais $132,74$ e $3,629$ podem ser ecritos como:*
$132,74 = 1 \cdot 10^2 + 3 \cdot 10^1 + 2 \cdot 10^0 + 7 \cdot 10^{-1} + 4 \cdot 10^{-2}$
$3,629 = 3 \cdot 10^0 + 6 \cdot 10^{-1} + 2 \cdot 10^{-2} + 9 \cdot 10^{-3}$

Converter um número de uma base decimal para uma base β qualquer seria rescrever esse número da notação da Definição 64 substituindo a base 10 das potências por β. Faremos isso inicialmente com o auxílio de operações matemáticas básicas até adaptar o polinômio para potências de base β.

Exemplo 5.5.2 *Convertendo o número $12,75$ da base decimal para base binária obtemos $(1100,011)_2$.*

Utilizando-se operações fundamentais o número é reescrito da notação decimal para a notação binária, separando por vígula a parte inteira da parte fracionária do

número.

$$\begin{aligned}
12,75_{10} &= 1.10^1 + 2.10^0 + 7.10^{-1} + 5.10^{-2} \\
&= (2^3 + 2) + 2 + 0,7 + 0,05 \\
&= 2^3 + 2^2 + \frac{75}{100} \\
&= 2^3 + 2^2 + \frac{3}{4} \\
&= 2^3 + 2^2 + (2+1).2^{-2} \\
&= 2^3 + 2^2 + 2^{-1} + 2^{-2} \\
&= 1.2^3 + 1.2^2 + 0.2^1 + 0.2^0 + 2^{-1} + 2^{-2} \\
&= (1100,11)_2
\end{aligned}$$

Logo, $12,75$ da base decimal resulta no número $(1100,011)_2$ de base binária.

EXEMPLO 5.5.3 *A conversão do número* $12,75$ *da base decimal para base octal resulta no número* $(14,6)_8$.

Utilizando as mesmas operações do exemplo anterior observe que:

$$\begin{aligned}
12,75_{10} &= 1.10^1 + 2.10^0 + 7.10^{-1} + 5.10^{-2} \\
&= (2+8) + 2 + 0,7 + 0,05 \\
&= 8 + 4 + \frac{3}{4} \\
&= 1 \cdot 8^1 + 4 \cdot 8^0 + \frac{6}{8} \\
&= 1 \cdot 8^1 + 4 \cdot 8^0 + 6 \cdot 8^{-1} \\
&= (14,6)_8
\end{aligned}$$

Logo, $12,75$ da base decimal resulta no número $(14,6)_8$ de base octal.

As operações realizadas nos exemplos acima, nos mostram como realizar na prática a conversão de racionais decimais. Essa conversão pode ser feita por partes. Primeiro, converteremos a parte inteira conforme descrito para números inteiros, para em seguida fazer a conversão da parte fracionária do número.

Veremos agora a descrição desse algoritmo fazendo a conversão do racional decimal $43,25$ para binário.
Primeiramente, converteremos a parte inteira do número por divisões sucessivas por 2. Assim,

43	2				
1	21	2			
	1	10	2		
		0	5	2	
			1	2	2
				0	1

Logo, $(43)_{10} = (101011)_2$.
Agora, converteremos a parte fracionária do número fazendo multiplicações sucessivas por 2 das partes fracionárias dos resultados até chegarmos em 1. Removemos então a parte inteira desses resultados para formar o binário. Dessa forma,
$0,375 \times \ 2 = 0,75 \rightarrow 0$
$0,75 \ \times \ 2 = 1,5 \rightarrow 1$
$0,5 \ \ \times \ 2 = 1 \rightarrow 1$
Portanto, $(43,375)_{10} = (101011,011)_2$.

Note que o processo descrito acima só foi usado com números racionais finitos. Como seria então tranformar por exemplo o número $4,2353535\cdots$ de representação infinita para binário ou para outras bases? Veremos isso a partir de agora, mas antes definiremos um racional infinito.

Definição 65 *Chamamos de dízimas periódicas a todo número escrito no sistema decimal que apresenta um número infinto de algarismos e que, a partir um certo algarismo, apresenta uma periodicidade de um ou mais algarismos.*

Exemplo 5.5.4 *São consideradas dízimas periódicas, por exemplo, os números* $2,43333...$ *e* $37,4545...$ *e são representados respectivamente como* $2,4\overline{3}$ *e* $37,\overline{45}$*, com um traço sobre o período.*

Definição 66 *Toda fração* $\frac{a}{b}$ *em que* $a, b \in Z$ *e* $b \neq 0$ *em que a divisão de a por b resultar numa dízima periódica é chamada de Fração Geratriz dessa dízima.*

Exemplo 5.5.5 *As frações geratriz das dízimas do exemplo 5.5.4 são:*
$\frac{73}{30} = 2,43333...$ *e*
$\frac{412}{11} = 37,4545...$

Faremos então a conversão destas duas dízimas periódicas, a primeira para base binária e a segunda para base octal pelo mesmo processo descrito para racionais finitos.

Exemplo 5.5.6 *Transformando a dízima* $(2,43333...)_{10}$ *de decimal para binário obtemos* $(10,011011101...)_{10}$.

De fato, primeiramente convertemos $(2)_{10}$ para o sistema binário e encontramos $(10)_2$ como podemos observar abaixo:

$$\begin{array}{r|l} 2 & 2 \\ \hline 0 & 1 \end{array}$$

Agora, fazendo a conversão da parte fracionária obtemos:
$0,4333... \times \ 2 = 0,8666...$
$0,8666... \times \ 2 = 1,7333...$
$0,7333... \times \ 2 = 1,4666...$
$0,4666... \times \ 2 = 0,9333...$
$0,9333... \times \ 2 = 1,8666...$
$0,8666... \times \ 2 = 1,7333...$
Perceba que a partir desse ponto teremos repetição dessas operações indefinidamente. Assim temos que a conversão nos traz que,
$(2,4333...)_{10} = (10,011011101...)_2$.

EXEMPLO 5.5.7 *Segue da conversão da dízima* $(37,4545...)_{10}$ *para o sistema octal o número* $(45,346314631...)$.

Fazendo a conversão da parte inteira por divisões sucessivas por 8 obtemos:

$$\begin{array}{r|l} 37 & 8 \\ \hline 5 & 4 \end{array}$$

Logo, $(37)_{10} = (45)_8$.
E, refazendo o processo acima agora com a base 8 temos:
$0,4545... \times \ 8 = 3,6363... \rightarrow 3$
$0,6363... \times \ 8 = 5,0909... \rightarrow 5$
$0,0909... \times \ 8 = 0,7272... \rightarrow 0$
$0,7272... \times \ 8 = 5,8181... \rightarrow 5$
$0,8181... \times \ 8 = 6,5454... \rightarrow 6$
$0,5454... \times \ 8 = 4,3636... \rightarrow 4$
$0,3636... \times \ 8 = 2,9090... \rightarrow 2$
$0,9090... \times \ 8 = 7,2727... \rightarrow 7$
$0,2727... \times \ 8 = 2,1818... \rightarrow 2$
$0,1818... \times \ 8 = 1,4545... \rightarrow 1$
Novamente, a partir desse ponto, teremos repetição dessas operações indefinidamente. Logo, $(37,4545...)_{10} = (45,35056427213505642721...)_8$.

É interessante notar que, apesar da conversão das dízimas para outras bases resultarem em números de representação infinita, um número infinito numa base binária por exemplo pode ser convertido num decimal racional finito. Vejamos o exemplo abaixo:

EXEMPLO 5.5.8 *O número* $(101,11001100...)_2$ *do sistema binário convertido para decimal resulta em* $(2,8)_{10}$.

Para converter o número binário $101,11001100...$ para base decimal faremos:
$10,11001100... = 1{\cdot}2^1{+}0{\cdot}2^0{+}1{\cdot}2^{-1}{+}1.2^{-2}{+}0{\cdot}2^{-3}{+}0{\cdot}2^{-4}{+}1{\cdot}2^{-5}{+}1{\cdot}2^{-6}{+}0{\cdot}2^{-7}{+}0{\cdot}2^{-8}{+}\cdots$

$10,11001100... = 2^1 + 2^{-1} + 2^{-2} + 2^{-5} + 2^{-6} + 2^{-1} + 2^{-9} + 2^{-10} + \cdots$
$10,11001100... = 2^1 + (2^{-1} + 2^{-2}) + 2^{-4}(2^{-1} + 2^{-2}) + 2^{-8}(2^{-1} + 2^{-2}) + \cdots$
$10,11001100... = 2^1 + \frac{3}{4} + 2^{-4}\frac{3}{4} + +2^{-8}\frac{3}{4} + \cdots$
$10,11001100... = 2^1 + 3 \cdot 2^{-2} + 3 \cdot 2^{-6} + 3 \cdot 2^{-10} + \cdots$
Sendo $(3 \cdot 2^{-2}, 3 \cdot 2^{-6}, 3 \cdot 2^{-10}, \cdots)$ uma Progressão Geométrica infinita de razão igual a 2^{-4} cuja soma (S) é:
$S = \frac{3 \cdot 2^{-2}}{1 - 2^{-4}} = 0,8.$
Logo, $(10,11001100...)_2 = 2^1 + 0,8 = (2,8)_{10}$.

6 Considerações Finais

O estudo da construção dos números é fundamental para o entendimento do conceito de número. Com o intuito de auxiliar nessa compreensão, buscou-se apresentar de forma clara, simples porém rigorosa, essa construção juntamente com as propriedades dos conjuntos numéricos dos Inteiros e Racionais.

Essa construção foi desenvolvida pelo método da simetrização, apresentada por Bertrand Russell na sua obra Introdução à Filosofia Matemática, e baseada nos trabalhos de Richard Dedekind.

Apresentou-se também aplicações desses conjuntos númericos a diferentes tópicos da matemática objetivando um melhor entendimento dos conceitos e propriedades estudadas.

Por perceber que a construção dos conjuntos numéricos são pouco abordados nos cursos de graduação, esse trabalho se faz válido como material de auxílio ao ensino deste tópico.

Referências

BOYER, C. B. *História da Matemática*. 2ª. ed. [S.l.]: Edgard Blucher, 2003. 19

CASTRUCCI, B. *Elementos de Teoria dos Conjuntos*. 1ª. ed. São Paulo: Livraria Nobel, 1972.

CHILDS, L. N. *A Concret Introduction to Higher Algebra*. 2ª. ed. New York: Springer, 1979. Undergraduate Texts in Mathematics. 77

DOMINGUES, H. H. *Fundamentos de Aritmética*. 1ª. ed. São Paulo: Atual Editora, 1991. 19

FERREIRA, J. *A Construção dos Números*. 1ª. ed. Rio de Janeiro: Coleção Textos Universitários - SBM, 2011.

GARBI, G. G. *A Rainha das Ciências: um passeio histórico pelo maravilhoso mundo da matemática*. 1ª. ed. São Paulo: Livraria da Física, 2006. 18, 51, 55

GODEMENT, R. *Cours d'alg'ebre*. first. Paris: Hermann, 1963.

HEFEZ, A. *Elementos de Aritmética*. 1ª. ed. Rio de Janeiro: Sociedade Brasileira de Matemática, 2003. (Textos Universitários). 51

IFRAH, G. *Os Números - A História de uma Grande Invenção*. 11ª. ed. Rio de Janeiro: Globo, 2005. Tradução: Stella M. de Freitas Senra. 17

LIMA, E. L. *Curso de Análise, Volume 1*. 14ª. ed. Rio de Janeiro: Projeto Euclides - IMPA, 2013.

LIMA, E. L. *Números e Funções Reais*. 1ª. ed. Rio de Janeiro: Coleção Profmat - SBM, 2013. 18

MONTEIRO, L. H. J. *Elementos de Álgebra*. 1ª. ed. Rio de Janeiro: IMPA, 1969. 78

RIPOLL, J. B.; RIPOLL, C. C.; SILVEIRA, J. F. P. da. *Números Racionais, Reais e Complexos*. 1ª. ed. Porto Alegre: UFRGS, 2006.

RUDIN, W. *Princípios de Análise Matemática*. 1ª. ed. [S.l.]: UnB, 1975.

RUSSELL, B. *Introdução à Filosofia Matemática*. 1ª. ed. Lisboa: Centro de Estudos de História e Filosofia da Ciência da Universidade de Évora, 2006. Traduzido do original de Bertrand Russell Introduction to Mathematical Philosophy, Londres: George Allen & Unwin, 1919,por Augusto J. Franco de Oliveira. 20