Universidade Estadual Paulista "Júlio de Mesquita Filho"
Instituto de Geociências e Ciências Exatas
Campus de Rio Claro

Sobre as Construções dos Sistemas Numéricos: $\mathbb{N}, \mathbb{Z}, \mathbb{Q}$ e $\mathbb{R}$.

Tassia Roberta Zangiacomo

Dissertação apresentada ao Programa de Pós-Graduação – Mestrado Profissional em Matemática em Rede Nacional-PROFMAT como requisito parcial para a obtenção do grau de Mestre

Orientadora
Profa. Dra. Elíris Cristina Rizziolli

2017

TERMO DE APROVAÇÃO

Tassia Roberta Zangiacomo

Sobre as Construções dos Sistemas Numéricos: $\mathbb{N}, \mathbb{Z}, \mathbb{Q}$ e $\mathbb{R}$.

Dissertação APROVADA como requisito parcial para a obtenção do grau de Mestre no Curso de Pós-Graduação Mestrado Profissional em Matemática Universitária do Instituto de Geociências e Ciências Exatas da Universidade Estadual Paulista "Júlio de Mesquita Filho", pela seguinte banca examinadora:

Profa. Dra. Elíris Cristina Rizziolli
Orientadora

Prof. Dr. Helton Hideraldo Bíscaro
Universidade de São Paulo

Profa. Dra. Suzinei Aparecida Siqueira Marconato
Universidade Estadual Paulista "Júlio de Mesquita Filho"

Rio Claro, 20 de fevereiro de 2017

Aos meus pais.

Agradecimentos

A Deus, que tornou tudo possível.

Ao meu pai, meu laço mais lindo, que me impulsiona a buscar sempre mais, que me incentiva a realizar meus desejos pessoais, e que sempre me ensinou a traçar limites para, então, expandi-los.

À minha mãe, por acreditar em meus sonhos e por me admirar mais que qualquer outra pessoa já fez.

À minha irmã, pela afinidade incomparável e pela amizade inquestionável.

Aos meus avós, pela alegria sem fim e pelo amor sem limites.

Ao meu amor, pela paciência dedicada e pelo apoio oferecido durante cada minuto desse projeto.

Aos amigos de turma Gabriela, Juliana, Luiz, e Rogério, que não me deixaram desanimar sequer um dia. Pessoas incríveis que conheci ao acaso, mas que, devido à cumplicidade vivenciada, jamais serão esquecidos.

Aos amigos de longa data, distrações e suportes nos momentos de completa tensão.

Aos professores desta caminhada, por acreditarem neste programa e em mim.

À minha orientadora, pela infinita boa vontade e por ter se tornado um exemplo de pessoa e profissional a ser seguida.

O único lugar onde o sucesso vem antes do trabalho é no dicionário.

Albert Einstein.

Resumo

Este trabalho tem como objetivo construir os sistemas numéricos usuais, a saber, o conjunto dos números naturais ($\mathbb{N}$), o conjunto dos números inteiros ($\mathbb{Z}$), o conjunto dos números racionais ($\mathbb{Q}$) e o conjunto dos números reais ($\mathbb{R}$). Iniciamos o trabalho tratando de noções sobre conjuntos e relações binárias. Em seguida, apresentamos o conjunto dos números naturais, definido através dos axiomas de Peano; o conjunto dos números inteiros via uma relação de equivalência com o conjunto dos números naturais; o conjunto dos números racionais, que são obtidos também via relação de equivalência, mas dessa vez com o conjunto dos números inteiros; a construção do conjunto dos números reais, feita via cortes no conjunto dos números racionais; e, para todos esses casos, mostramos a imersão do conjunto anterior no conjunto que surge na sequência. Por fim, observamos alguns materiais do ensino fundamental e médio com o intuito de investigar de que forma esses temas estão sendo apresentados para os alunos.

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

Abstract

This work aims to construct the usual numerical systems, namely the set of natural numbers ($\mathbb{N}$), the set of integers ($\mathbb{Z}$), the set of rational numbers ($\mathbb{Q}$) and the set of real numbers ($\mathbb{R}$). We begin the work dealing with notions about sets and binary relations. Next, we present the set of natural numbers, defined by Peano's axioms; the set of integers via an equivalence relation with the set of natural numbers; the set of rational numbers, which are also obtained via equivalence relation, but this time with the set of integers; the construction of the set of real numbers, made through cuts in the set of rational numbers; end for all these cases we show the immersion of the previous set in the ensemble that appears in the sequence. Finally, we observed some materials in elementary school and high school in order to investigate how these themes are being presented to the students.

Keywords: Natural Numbers, Integer Numbers , Rational Numbers, Real Numbers.

Sumário

1 Introdução

Nesse trabalho, tratamos das construções formais do conjunto dos números naturais, conjunto dos números inteiros, conjunto dos números racionais e conjunto dos números reais.

A fim de entendermos o surgimento dos conjuntos numéricos, vamos recorrer a uma breve motivação histórica da origem de cada um deles. Não procuramos aqui contar a história da invenção do número em si, pois isso seria tema para outra dissertação. Buscamos apenas compreender de que maneira ou em qual momento os conjuntos numéricos apareceram. Para esta pequena pesquisa foram utilizadas as referências [1] e [2].

A necessidade de contar surgiu com o desenvolvimento das atividades humanas, por volta de 4000 antes de Cristo. Em algumas comunidades primitivas aldeias iam se transformando em cidades. A vida ia ficando mais complexa.

O exemplo mais clássico da necessidade de contar é o do pastoreio. O pastor dispunha de algumas formas para controlar o seu rebanho. Pela manhã, ele soltava as suas ovelhas e analisava a situação ao final da tarde, ele buscava meios de saber se alguma tinha sido roubada, fugido, se perdido do rebanho ou se havia sido acrescentado uma nova ovelha ao rebanho. Assim eles tinham a correspondência um a um, onde cada ovelha correspondia a uma pedrinha que era armazenada em um saco, ou um nó em uma corda, ou em marcas nas paredes ou ossos, entre outros diversos tipos de marcação.

O primeiro número que surgiu foi o número natural. Historicamente é difícil atribuir uma data para o seu aparecimento, apenas sabe-se que o conceito de número natural, nos seus primeiros tempos de aparecimento e formação, está implicitamente ligado ao ato de contar.

A ideia de contar parece ter sempre estado presente. Hoje, apesar de o conceito de número nos parecer muito natural, foi um desenvolvimento lento e complexo que envolveu diversas civilizações. São milhares de anos desde as primeiras manifestações até a teoria que hoje conhecemos.

Há quem acredite que o processo histórico do conceito dos números é muito semelhante à nossa própria formação no conhecimento desse tema. A princípio admite-se os números naturais e eles são suficientes, assim como foram suficientes por muito tempo.

Por volta de 3000 antes de Cristo, Sesóstris, o antigo faraó, repartiu as terras ao longo das margens do rio Nilo entre alguns agricultores privilegiados. Na época das cheias, as águas do rio Nilo subiam acima do seu leito normal, inundando muitas regiões dessas terras. Quando as águas baixavam, uma faixa de terras férteis ficava descoberta e estavam prontas para o cultivo. Então o faraó decretou: "... reparte-se o solo do Egito às margens do rio Nilo entre seus habitantes. Se o rio levar qualquer parte do lote de um homem, o faraó mandará funcionários examinarem e determinarem por medida, a extensão da perda."

No momento em que os funcionários (que eram chamados de agrimensores ou estiradores de corda) eram chamados, levavam consigo cordas de um determinado tamanho (unidade de medida). Essa corda era esticada para que se verificasse quantas vezes aquela unidade de medida estava contida nos lados do terreno. Porém, nem sempre as medidas tiradas pela corda eram inteiras.

Para solucionar o problema da medição das terras, os egípcios criaram um novo número, o número fracionário, que era representado com o uso de frações. Assim deu-se o surgimento dos números racionais.

As frações, no princípio, eram admitidas pelos gregos como razão entre números e não como números propriamente ditos.

Na Grécia, por volta de 530 antes de Cristo, existia uma espécie de sociedade secreta intitulada os pitagóricos, uma vez que o mestre da sociedade era o filósofo e matemático Pitágoras. Os pitagóricos eram grandes estudiosos da Matemática e defendiam que qualquer fato da natureza podia ser explicado por meio dos números naturais, mas acabaram descobrindo propriedades interessantes que abalaram profundamente a ideia de que os números naturais eram suficientes. Segundo Pitágoras, dependendo da soma de seus fatores, um número poderia ser perfeito, deficiente ou excessivo, o que deu início ao teorema de Pitágoras e, consequentemente, aos números irracionais. A origem histórica da necessidade de criação dos números não racionais está intimamente ligada com fatos de natureza geométrica e aritmética, como por exemplo, o problema da medida da diagonal do quadrado definida a partir do seu lado.

Durante a transição da Idade Média para a Idade Moderna, os países da Europa Ocidental sofreram profundas transformações. Houve um significativo desenvolvimento do comércio e das cidades. A fim de superar as dificuldades que surgiam com o desenvolvimento científico, a necessidade de um novo número era cada vez maior. Os matemáticos precisavam de números específicos para representar soluções de determinados problemas, ou expressar, por exemplo, temperaturas acima e abaixo de 0°C entre tantas outras necessidades que surgiram com o avanço das ciências.

Muito se discutia sobre esse novo número, porém ele era tão difícil de enquadrar-se entre os números já conhecidos que os matemáticos o chamavam de número absurdo. Com os matemáticos chineses começou-se a entender que o número poderia ser compreendido por excessos ou faltas. Neste momento, os matemáticos começaram a escolher

uma melhor notação para expressar o novo número, que não indicaria apenas quantidade, mas também representasse o ganho ou a perda, surgindo assim o número com sinal, positivo ou negativo, um conjunto que ficou conhecido como números inteiros.

Os números inteiros, assim como os números racionais, não foram aceitos como números desde o princípio. Entre a aparição e aceitação do número negativo levou mais de mil anos. As mesmas dúvidas que surgem hoje no contato com os números inteiros, já instigava questionamentos de diversos matemáticos no passado.

Observe que ao contrário da sequência trabalhada durante a dissertação (números naturais, números inteiros, números racionais e números reais), a aparição dos números racionais deu-se antes dos números inteiros (mais especificamente os negativos).

Hoje, graças aos matemáticos do passado, já sabemos construir os conjuntos numéricos fazendo uso de uma ordem coerente e elegante, mas acabamos esquecendo do processo histórico sobre o qual os conceitos aqui tratados se desenvolveram.

Este trabalho está dividido da seguinte maneira: O segundo e o terceiro capítulos tratam de noções sobre conjuntos e relações binárias, respectivamente; aspectos que serão constantemente abordados nos capítulos seguintes. O quarto capítulo traz o conjunto dos números naturais, definido através dos axiomas de Peano e suas principais propriedades e aplicações. O quinto capítulo apresenta o conjunto dos números inteiros via uma relação de equivalência com o conjunto dos números naturais, citando e mostrando a validade de suas principais aplicações e propriedades e, no final deste, mostramos uma imersão do conjunto dos números naturais no conjunto dos números inteiros. O sexto capítulo, de uma maneira muito parecida com a do quinto capítulo, trata do conjunto dos números racionais, que são obtidos também via relação de equivalência, mas dessa vez com o conjunto dos números inteiros, mostrando suas aplicações e algumas de suas propriedades; e também, no final do capítulo, apresentamos uma imersão do conjunto dos números inteiros no conjunto dos números racionais. O sétimo capítulo traz a construção do conjunto dos números reais, feita via cortes no conjunto dos números racionais, mostrando que esse último visa suprir a incompletude dos outros conjuntos numéricos; analogamente mostramos a imersão do conjunto dos números racionais no conjunto dos números reais.

Quando finalizamos o estudo sobre as construções desses Sistemas Numéricos surgiu a curiosidade de saber como este tema tem sido abordado nos livros didáticos utilizados no Ensino Médio. Foi com esta motivação que consultamos uma amostra de livros didáticos. Apresentamos, no último capítulo, as impressões particulares acerca desta observação. A ideia não foi de realizar uma análise minuciosa de livros didáticos, por isso escolhemos não citar os livros folheados.

2 Noções sobre conjuntos

Ao longo desse trabalho, precisaremos de alguns conceitos elementares da teoria dos conjuntos. Para isso, segue uma breve abordagem acerca destes conceitos.

É importante ressaltar que será necessário que o leitor tenha como pré - requisito, e leve em consideração, as noções básicas de lógica.

Tais noções, bem como aprofundamentos sobre o tema deste capítulo, podem ser encotradas em [4].

2.1 Conjuntos

Consideremos que um conjunto é uma coleção de objetos que chamamos elementos e que cada um dos elementos é um dos componentes do conjunto.

Para dar nome aos conjuntos usaremos uma letra maiúscula do nosso alfabeto. Para os elementos, letras minúsculas.

Agora, para representar um conjunto, usamos uma das três formas seguintes:

(i) Listagem dos elementos: todos os elementos do conjunto são apresentados numa lista, delimitados por um par de chaves e separados por vírgulas.

Exemplo 2.1. $A = \{0, 1, 2, 3, 4, 5\}$.

(ii) Propriedade dos elementos: os elementos do conjunto são descritos por uma propriedade que todos eles possuem.

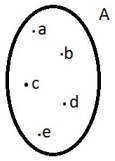
Exemplo 2.2. $A = \{x \ / \ x$ é um número par$\}$.

(iii) Diagrama de Venn: representamos o conjunto por um plano limitado por uma curva fechada.

Exemplo 2.3. Podemos representar o conjunto A,

$$A = \{a, b, c, d, e\},$$

da seguinte forma:



Definição 2.4. *Um conjunto que representa uma quantidade limitada de elementos é um conjunto finito. Caso contrário, é um conjunto infinito. Um conjunto que possui apenas um elemento é chamado de conjunto unitário.*

Definição 2.5. *Existe um conjunto que chamamos de conjunto universo e representamos por U ao qual pertencem todos os elementos envolvidos em uma determinada situação.*

Exemplo 2.6. Se a situação em questão envolve as letras do alfabeto, podemos considerar:

$$U = \{a, b, c, d, e, f, g, h, i, j, k, l, m, n, o, p, q, r, s, t, u, v, w, x, y, z\}.$$

Definição 2.7. *Existe um conjunto ao qual nenhum elemento está presente. Chamamos de conjunto vazio e o representamos por $\varnothing$.*

Observação 2.8. Uma das formas de definir o conjunto vazio é denotando um conjunto com qualquer propriedade contraditória. Temos como exemplo:

$$B = \{x \mid x \text{ é um número par e ímpar}\}.$$

Definição 2.9. *Se a é elemento de um conjunto A dizemos que a pertence a A e denotamos essa relação por $a \in A$. Caso contrário, dizemos que a não pertence a A e denotamos por $a \notin A$.*

Exemplo 2.10. Para o conjunto $A = \{a, b, c, d, e, f\}$, temos $b \in A$ e $t \notin A$.

Definição 2.11. *Se A e B são conjuntos e todo elemento de A também é elemento de B, dizemos que A é subconjunto de B e denotamos essa relação por $A \subset B$ (lemos "A está contido em B") ou por $B \supset A$ (lemos "B contém A"). Caso contrário, ou seja, se um dos elementos de A não é elemento de B, dizemos que A não está contido em B ou que B não contém A e denotamos por $A \not\subset B$ ou por $B \not\supset A$.*

Exemplo 2.12. Dados os conjuntos $A = \{a, b, c, d\}$, $B = \{a, b, c, d, e\}$ temos $A \subset B$, uma vez que todos os elementos de A também são elementos de B. Porém, $B \not\subset A$, já que $e \in B$ e $e \notin A$.

Definição 2.13. *Dois conjuntos A e B são iguais ($A = B$) quando $A \subset B$ e $B \subset A$.*

Das definições dadas acima, é possível mostrar dois resultados, que seguem.

Proposição 2.14. *O conjunto vazio sempre está contido em um conjunto A, para qualquer A.*

Demonstração: De fato, vamos supor, por contradição, que $\varnothing \not\subset A$. Isso significaria que existe um elemento no conjunto vazio que não pertence ao conjunto A. Como o conjunto vazio não possui nenhum elemento, isso seria absurdo. Portanto, $\varnothing \subset A$ para qualquer conjunto A. ■

Proposição 2.15. *Dado um conjunto A, se $A \subset \varnothing$, então $A = \varnothing$.*

Demonstração: Para mostrar que $A = \varnothing$, é necessário mostrar, segundo a definição 2.13, que $A \subset \varnothing$ e que $\varnothing \subset A$. Observe que o primeiro segue da hipótese, enquanto que o segundo segue da proposição acima (proposição 2.14). ■

2.2 Operações com conjuntos

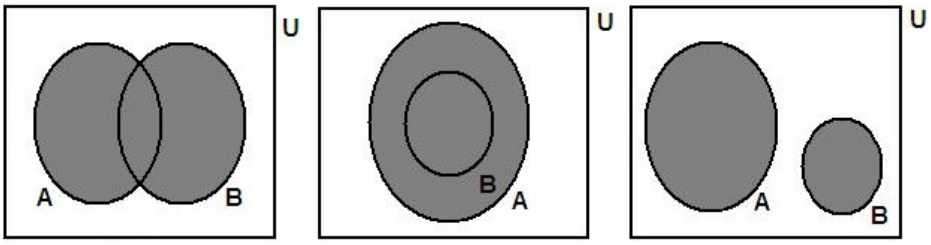
Definição 2.16. *A união de dois conjuntos A e B é o conjunto indicado por $A \cup B$ e definido por:*

$$A \cup B = \{x \ / \ x \in A \text{ ou } x \in B\}.$$

Exemplo 2.17. Sejam os conjuntos $A = \{a, b, c, d\}$ e $B = \{e, f, g\}$. Daí,

$$A \cup B = \{a, b, c, d, e, f, g\}.$$

Podemos visualizar a união dos conjuntos A e B ($A \cup B$) através das imagens:



Observação 2.18. Sendo a união de dois conjuntos A e B definida por $A \cup B = \{x \ / \ x \in A$ ou $x \in B\}$, um elemento y não pertencerá a $A \cup B$ se $y \notin A$ e $y \notin B$.

A seguir, algumas propriedades acerca da união de conjuntos.

Proposição 2.19. *A operação que associa a cada dois conjuntos a sua união satisfaz as seguintes propriedades:*

(i) Associativa: Dados os conjuntos A, B, C quaisquer, $A \cup (B \cup C) = (A \cup B) \cup C$.

(ii) Comutativa: Dados os conjuntos A, B quaisquer, $A \cup B = B \cup A$.

(iii) Para quaisquer conjuntos A, B, temos que $A \subset A \cup B$ e $B \subset A \cup B$.

(iv) Sejam os conjuntos A, B quaisquer, se $A \subset B$, então $A \cup B = B$.

(v) Para qualquer conjunto A, temos que $A \cup \varnothing = A$.

Demonstração: Para a demonstração dos itens abaixo, usaremos a definição de união de conjuntos.

(i) *Associativa:* Para mostrar que $A \cup (B \cup C) = (A \cup B) \cup C$ para os conjuntos A, B, C quaisquer, precisamos mostrar, segundo a definição 2.13, a veracidade dos itens $A \cup (B \cup C) \subset (A \cup B) \cup C$ e $(A \cup B) \cup C \subset A \cup (B \cup C)$.

Veja que $A \cup (B \cup C) \subset (A \cup B) \cup C$: seja $x \in A \cup (B \cup C)$, então $x \in A$ ou $x \in B \cup C$. Ou seja, $x \in A$ ou $x \in B$ ou $x \in C$. Logo $x \in A \cup B$ ou $x \in C$. Segue que, $x \in (A \cup B) \cup C$. Portanto, $A \cup (B \cup C) \subset (A \cup B) \cup C$.

Note que $(A \cup B) \cup C \subset A \cup (B \cup C)$: seja $x \in (A \cup B) \cup C$, então $x \in A \cup B$ ou $x \in C$. Ou seja, $x \in A$ ou $x \in B$ ou $x \in C$. Logo $x \in A$ ou $x \in B \cup C$. Segue que, $x \in A \cup (B \cup C)$. Portanto, $(A \cup B) \cup C \subset A \cup (B \cup C)$.

Segue que dados os conjuntos A, B, C quaisquer, $(A \cup B) \cup C = A \cup (B \cup C)$.

(ii) *Comutativa:* Para mostrar que dados os conjuntos A, B quaisquer, $A \cup B = B \cup A$, precisamos mostrar que $A \cup B \subset B \cup A$ e $B \cup A \subset A \cup B$ (definição 2.13).

Observe que $A \cup B \subset B \cup A$: seja $x \in A \cup B$, então $x \in A$ ou $x \in B$, logo $x \in B$ ou $x \in A$. Segue que $x \in B \cup A$. Portanto, $A \cup B \subset B \cup A$.

Por outro lado, $B \cup A \subset A \cup B$: seja $x \in B \cup A$, então $x \in B$ ou $x \in A$, logo $x \in A$ ou $x \in B$. Segue que $x \in A \cup B$. Portanto, $B \cup A \subset A \cup B$.

Segue que dados os conjuntos A, B quaisquer, $A \cup B = B \cup A$.

(iii) Vamos mostrar que para quaisquer conjuntos A, B, temos que $A \subset A \cup B$. O caso $B \subset A \cup B$ é análogo.

Seja $x \in A$, logo $x \in A$ ou $x \in B$. Segue que $x \in A \cup B$. Portanto, $A \subset A \cup B$.

(iv) Para mostrar que dados os conjuntos A, B quaisquer, se $A \subset B$, então $A \cup B = B$, precisamos mostrar que $A \cup B \subset B$ e $B \subset A \cup B$ (definição 2.13).

Note que $A \cup B \subset B$: seja $x \in A \cup B$, então $x \in A$ ou $x \in B$. Se $x \in A$, como $A \subset B$, temos que $x \in B$. Segue que, em qualquer um dos casos, $x \in B$. Portanto, $A \cup B \subset B$.

Ainda, $B \subset A \cup B$ pelo item *(iii)*.

Segue que dados os conjuntos A, B quaisquer, se $A \subset B$, então $A \cup B = B$.

(v) Para mostrar que dado o conjunto A qualquer, $A \cup \varnothing = A$, precisamos mostrar que $A \cup \varnothing \subset A$ e que $A \subset A \cup \varnothing$ (definição 2.13).

Veja que $A \cup \varnothing \subset A$: seja $x \in A \cup \varnothing$, então $x \in A$ ou $x \in \varnothing$. Como $x \notin \varnothing$ (pois o conjunto vazio não possui elementos), segue que $x \in A$. Portanto, $A \cup \varnothing \subset A$.

Também, $A \subset A \cup \varnothing$pelo item *(iii)*.

Segue que dados o conjunto A qualquer, $A \cup \varnothing = A$.

■

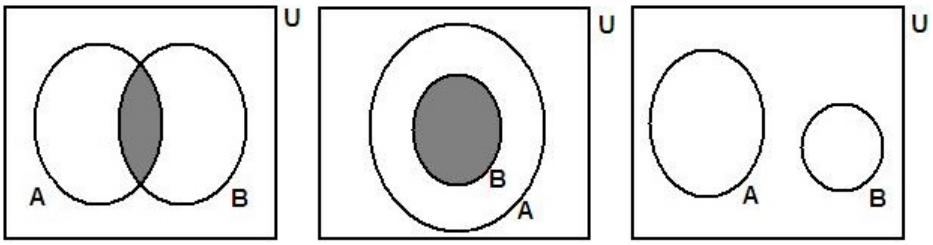
Definição 2.20. *A interseção de dois conjuntos A e B é o conjunto indicado por $A \cap B$ e definido por:*

$$A \cap B = \{x \ / \ x \in A \ e \ x \in B\}.$$

Exemplo 2.21. Sejam os conjuntos $A = \{a, b, c, d\}$ e $B = \{c, d, e, f, g\}$. Daí,

$$A \cap B = \{c, d\}.$$

Podemos visualizar a interseção dos conjuntos A e B $(A \cap B)$ através das imagens:



Observação 2.22. Sendo a interseção de dois conjuntos A e B definida por $A \cap B = \{x \ / \ x \in A \text{ e } x \in B\}$, um elemento y não pertencerá a $A \cap B$ se $y \notin A$ ou $y \notin B$.

A seguir, algumas propriedades acerca da interseção de conjuntos.

Proposição 2.23. *A operação que associa a cada dois conjuntos a sua interseção goza das seguintes propriedades:*

(i) Associativa: Dados os conjuntos A, B, C quaisquer, $A \cap (B \cap C) = (A \cap B) \cap C$.

(ii) Comutativa: Dados os conjuntos A, B quaisquer, $A \cap B = B \cap A$.

(iii) Para quaisquer conjuntos A, B, temos que $A \cap B \subset A$ e $A \cap B \subset B$.

(iv) Sejam os conjuntos A, B quaisquer, se $A \subset B$, então $A \cap B = A$.

(v) Para qualquer conjunto A, temos que $A \cap \varnothing = \varnothing$.

Demonstração: Para a demonstração dos itens abaixo, usaremos a definição de interseção de conjuntos.

(i) *Associativa:* Para mostrar que $A \cap (B \cap C) = (A \cap B) \cap C$ para os conjuntos A, B, C quaisquer, precisamos mostrar, conforme enunciado na definição 2.13, a veracidade dos itens $A \cap (B \cap C) \subset (A \cap B) \cup C$ e $(A \cap B) \cap C \subset A \cap (B \cap C)$.

Veja que $A \cap (B \cap C) \subset (A \cap B) \cap C$: seja $x \in A \cap (B \cup C)$, então $x \in A$ e $x \in B \cap C$. Ou seja, $x \in A$ e $x \in B$ e $x \in C$. Logo $x \in A \cap B$ e $x \in C$. Segue que, $x \in (A \cap B) \cap C$. Portanto, $A \cap (B \cap C) \subset (A \cap B) \cap C$.

Note que $(A \cap B) \cap C \subset A \cap (B \cap C)$: seja $x \in (A \cap B) \cap C$, então $x \in A \cap B$ e $x \in C$. Ou seja, $x \in A$ e $x \in B$ e $x \in C$. Logo $x \in A$ e $x \in B \cap C$. Segue que, $x \in A \cap (B \cap C)$. Portanto, $(A \cap B) \cap C \subset A \cap (B \cap C)$.

Segue que dados os conjuntos A, B, C quaisquer, $(A \cap B) \cap C = A \cap (B \cap C)$.

(ii) *Comutativa:* Para mostrar que dados os conjuntos A, B quaisquer, $A \cap B = B \cap A$, precisamos mostrar que $A \cap B \subset B \cap A$ e $B \cap A \subset A \cap B$ (definição 2.13).

Observe que $A \cap B \subset B \cap A$: seja $x \in A \cap B$, então $x \in A$ e $x \in B$, logo $x \in B$ e $x \in A$. Segue que $x \in B \cap A$. Portanto, $A \cap B \subset B \cap A$.

Ainda, $B \cap A \subset A \cap B$: seja $x \in B \cap A$, então $x \in B$ e $x \in A$, logo $x \in A$ e $x \in B$. Segue que $x \in A \cap B$. Portanto, $B \cap A \subset A \cap B$.

Segue que dados os conjuntos A, B quaisquer, $A \cap B = B \cap A$.

(iii) Vamos mostrar que para quaisquer conjuntos A, B, temos que $A \cap B \subset A$ e $A \cap B \subset B$.

Seja $x \in A \cap B$, então $x \in A$ e $x \in B$. Segue que $A \cap B \subset A$ e $A \cap B \subset B$.

(iv) Para mostrar que dados os conjuntos A, B quaisquer, se $A \subset B$, então $A \cap B = A$, precisamos mostrar que $A \cap B \subset A$ e $A \subset A \cap B$ (definição 2.13).

Note que $A \cap B \subset A$ pelo item *(iii)*.

Por outro lado, $A \subset A \cap B$: seja $x \in A$, como $A \subset B$, segue que $x \in B$. Portanto, $x \in A$ e $x \in B$. Segue que $x \in A \cap B$. Portanto, $A \subset A \cap B$.

Segue que dados os conjuntos A, B quaisquer, se $A \subset B$, então $A \cap B = A$.

(v) Para mostrar que dado o conjunto A qualquer, $A \cap \varnothing = \varnothing$, precisamos mostrar que $A \cap \varnothing \subset \varnothing$ e que $\varnothing \subset A \cap \varnothing$ (definição 2.13).

Veja que $A \cap \varnothing \subset \varnothing$ pelo item *(iii)*.

Ainda, pela proposição 2.14, $\varnothing \subset A \cap \varnothing$.

Segue que dados o conjunto A qualquer, $A \cap \varnothing = A$.

■

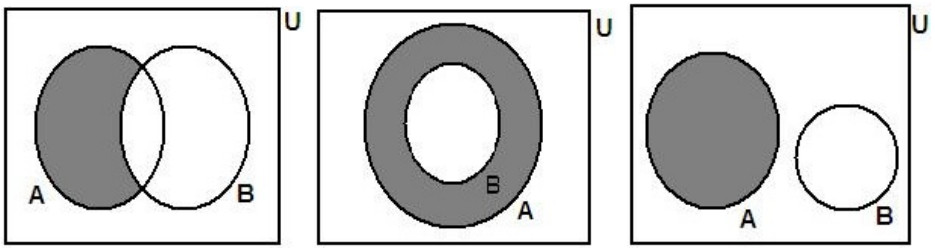
Definição 2.24. *Sejam A e B dois conjuntos quaisquer. Chamaremos a diferença entre A e B, e indicamos por $A-B$, o conjunto dos elementos de A que não pertencem a B. Ou seja,*

$$A - B = \{x \ / \ x \in A \ e \ x \notin B\}.$$

Exemplo 2.25. Sejam os conjuntos $A = \{a, b, c, d\}$, $B = \{c, d, e, f, g\}$, $C = \{c, d\}$. Daí,

$$A - B = \{a, b\};$$
$$B - A = \{e, f, g\};$$
$$A - C = \{a, b\}.$$

Visualizamos as diferenças dos conjuntos A e B $(A - B)$ em algumas situações através das imagens:

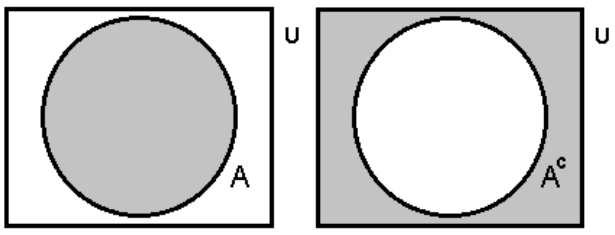


Definição 2.26. *Dados um conjunto U e um subconjunto A tal que $A \subset U$, chamamos de complementar de A em relação a U, e denotamos por A^C, o subconjunto de U formado pelos elementos de U que não pertencem a A. Conjunto complementar está relacionado à diferença dos conjuntos U e A, ou seja,*

$$A^C = U - A = \{x \ / \ x \in U \ e \ x \notin A\}.$$

Exemplo 2.27. Se U é o conjunto universo das letras do alfabeto e A é o conjunto das consoantes, temos que A^C será o conjunto formado pelas vogais.

Visualizamos o conjunto A e o conjunto complementar de A através das imagens:



A seguir, algumas propriedades acerca do complementar de conjuntos.

Proposição 2.28. *Sejam U um conjunto universo e A, B subconjuntos quaisquer de U. Da definição de complementar decorrem as seguintes propriedades:*

(i) $U^C = \varnothing$.

(ii) $\varnothing^C = U$.

(iii) $A \cup A^C = U$.

(iv) $(A^C)^C = A$.

(v) $A \cap A^C = \varnothing$.

(vi) $(A \cap B)^C = A^C \cup B^C$.

(vii) $(A \cup B)^C = A^C \cap B^C$.

Demonstração: Para a demonstração dos itens abaixo, usaremos a definição de complementar de conjuntos.

(i) Para mostrar que $U^C = \varnothing$, precisamos mostrar que $U^C \subset \varnothing$ e que $\varnothing \subset U^C$ (definição 2.13).

Veja que $U^C \subset \varnothing$, pois sendo $x \in U^C$, temos que $x \notin U$. Como U é o conjunto universo, consequentemente segue que $x \in \varnothing$.

Note que, pela proposição 2.14, $\varnothing \subset U^C$.

Segue que $U^C = \varnothing$.

(ii) Para mostrar que $\varnothing^C = U$, precisamos mostrar que $\varnothing^C \subset U$ e que $U \subset \varnothing^C$ (definição 2.13).

Observe que $\varnothing^C \subset U$: seja $x \in \varnothing^C$, temos que $x \notin \varnothing$. Consequentemente segue que $x \in U$.

Ainda, $U \subset \varnothing^C$: seja $x \in U$, então $x \notin \varnothing$, ou seja, $x \in \varnothing^C$.

Segue que $\varnothing^C = U$.

(iii) Para mostrar que dado o conjunto A qualquer, temos que $A \cup A^C = U$, precisamos mostrar que $A \cup A^C \subset U$ e que $U \subset A \cup A^C$ (definição 2.13).

Observe que $A \cup A^C \subset U$: seja $x \in A \cup A^C$, então $x \in A$ ou $x \in A^C$. Note que, da hipótese da proposição, $A \subset U$ e da definição 2.26, $A^C \subset U$. Portanto, em ambos os casos, $x \in U$. Portanto, $A \cup A^C \subset U$.

Também, $U \subset A \cup A^C$: seja $x \in U$, daí, temos que $x \in A$ ou $x \notin A$. Ou seja, $x \in A$ ou $x \in A^C$. Segue que $x \in A \cup A^C$. Portanto, $U \subset A \cup A^C$.

Segue que dado o conjunto A qualquer, temos que $A \cup A^C = U$.

(iv) Para mostrar que dado o conjunto A qualquer, temos que $(A^C)^C = A$, precisamos mostrar que $(A^C)^C \subset A$ e que $A \subset (A^C)^C$ (definição 2.13).

Veja que $(A^C)^C \subset A$: seja $x \in (A^C)^C$, logo $x \notin A^C$. Se $x \notin A^C$, então $x \in A$ (pois $A \cup A^C = U$). Portanto, $(A^C)^C \subset A$.

Por outro lado, $A \subset (A^C)^C$: seja $x \in A$, logo $x \notin A^C$. Se $x \notin A^C$, então $x \in (A^C)^C$. Portanto, $A \subset (A^C)^C$.

Segue que dado o conjunto A qualquer, temos que $(A^C)^C = A$.

(v) Para mostrar que dado o conjunto A qualquer, temos que $A \cap A^C = \varnothing$, precisamos mostrar que $A \cap A^C \subset \varnothing$ e que $\varnothing \subset A \cap A^C$ (definição 2.13).

Veja que $A \cap A^C \subset \varnothing$: seja $x \in A \cap A^C$, então $x \in A$ e $x \in A^C$. Ou seja, $x \in A$ e $x \notin A$. Note que tal fato é uma contradição. Segue que, segundo a observação 2.8, definimos um conjunto vazio. Portanto, $x \in \varnothing$. Logo, $A \cap A^C \subset \varnothing$

Note que, pela proposição 2.14, $\varnothing \subset A \cup A^C$.

Segue que dado o conjunto A qualquer, temos que $A \cap A^C = U$.

(vi) Para mostrar que dados os conjuntos A, B quaisquer, temos que

$(A \cap B)^C = A^C \cup B^C$, precisamos mostrar que $(A \cap B)^C \subset A^C \cup B^C$ e que

$A^C \cup B^C \subset (A \cap B)^C$ (definição 2.13).

Note que $(A \cap B)^C \subset A^C \cup B^C$: seja $x \in U$ tal que $x \in (A \cap B)^C$, então $x \notin A \cap B$, ou seja, $x \notin A$ ou $x \notin B$. Logo, $x \in A^C$ ou $x \in B^C$. Segue que $x \in A^C \cup B^C$. Portanto, $(A \cap B)^C \subset A^C \cup B^C$.

Ainda, temos que $A^C \cup B^C \subset (A \cap B)^C$: seja $x \in U$ tal que $x \in A^C \cup B^C$, então $x \in A^C$ ou $x \in B^C$, ou seja, $x \notin A$ ou $x \notin B$. Daí, $x \notin A \cap B$. Segue que $x \in (A \cap B)^C$. Portanto $A^C \cup B^C \subset (A \cap B)^C$.

Segue que dados os conjuntos A, B quaisquer, temos que $(A \cap B)^C = A^C \cup B^C$.

(vii) Para mostrar que dados os conjuntos A, B quaisquer, temos que

$(A \cup B)^C = A^C \cap B^C$, precisamos mostrar que $(A \cup B)^C \subset A^C \cap B^C$ e que

$A^C \cap B^C \subset (A \cup B)^C$ (definição 2.13).

Veja que $(A \cup B)^C \subset A^C \cap B^C$: seja $x \in U$ tal que $x \in (A \cup B)^C$, então $x \notin A \cup B$, ou seja, $x \notin A$ e $x \notin B$. Logo, $x \in A^C$ e $x \in B^C$. Segue que $x \in A^C \cap B^C$. Portanto, $(A \cup B)^C \subset A^C \cap B^C$.

Por outro lado, $A^C \cap B^C \subset (A \cup B)^C$: seja $x \in U$ tal que $x \in A^C \cap B^C$, então $x \in A^C$ e $x \in B^C$, ou seja, $x \notin A$ e $x \notin B$. Daí, $x \notin A \cup B$. Segue que $x \in (A \cup B)^C$. Portanto $A^C \cap B^C \subset (A \cup B)^C$.

Segue que dados os conjuntos A, B quaisquer, temos que $(A \cup B)^C = A^C \cap B^C$.

■

Por fim, a última definição que utilizaremos.

Definição 2.29. *Uma partição de um conjunto X é qualquer coleção P de subconjuntos de X dotada das seguintes propriedades:*

(i) os subconjuntos são não vazios;

(ii) dois membros quaisquer de P ou são iguais ou são disjuntos;

(iii) a união dos membros de P é igual a X.

Podemos simplificar tal definição dizendo que uma partição de um conjunto X é qualquer coleção P de subconjuntos não vazios de X onde todo elemento de X pertence a um e apenas um dos elementos de P.

3 Relações binárias

Ao longo de todo esse trabalho usaremos constantemente alguns termos como, por exemplo, *relação de equivalência*, *relação de ordem* e *função*. Para isso, segue uma breve abordagem acerca destes conceitos.

No que segue, consideramos como pré-requisitos alguns conceitos elementares da teoria dos conjuntos. Mais detalhes sobre este assunto podem ser encontrados em [4].

Definição 3.1. *Dados dois conjuntos não vazios, A e B, chama-se produto cartesiano de A por B o conjunto formado por todos os pares ordenados (a,b) com a em A e b em B.*

Indicamos o produto cartesiano de A por B com a notação $A \times B$. Ou seja,

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

Exemplo 3.2. Dados os conjuntos $E = \{a,b,c\}$ e $F = \{c,d\}$, temos:

$$E \times F = \{(a,c),(a,d),(b,c),(b,d),(c,c),(c,d)\}.$$

Definição 3.3. *Dados dois pares ordenados, (a,b) e (c,d), dizemos que:*

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

Definição 3.4. *Chama-se relação binária de A em B todo subconjunto $\mathcal{R}$ de $A \times B$. Ou seja,*

$$\mathcal{R} \text{ é relação de } A \text{ em } B \text{ se, e somente se, } \mathcal{R} \subset A \times B.$$

Conforme essa definição, $\mathcal{R}$ é um conjunto de pares ordenados (a,b) pertencentes a $A \times B$ e para indicar que $(a,b) \in \mathcal{R}$, usaremos a notação $a\mathcal{R}b$ (lê-se "a relaciona-se com b segundo $\mathcal{R}$"). Se $(a,b) \notin \mathcal{R}$, escrevemos $a\not\mathcal{R}b$.

Ainda, os conjuntos A e B são denominados conjunto de partida e conjunto de chegada, respectivamente, da relação $\mathcal{R}$.

Exemplo 3.5. Dados os conjuntos $E = \{a, b, c\}$ e $F = \{c, d\}$, são exemplos de relações de A em B:

$$\mathcal{R}_1 = \{(a, c), (b, c), (c, d)\};$$

$$\mathcal{R}_2 = \{(a, d), (a, c), (c, c)\}.$$

Definição 3.6. *Quando $A = B$ e $\mathcal{R}$ é uma relação de A em B, dizemos que $\mathcal{R}$ é uma relação sobre A ou, ainda, $\mathcal{R}$ é uma relação em A.*

Exemplo 3.7. Dado o conjunto $E = \{a, b, c\}$ são exemplos de relações sobre E:

$$\mathcal{R}_1 = \{(a, a), (b, b), (c, c)\};$$

$$\mathcal{R}_2 = \{(a, b), (b, b), (c, b)\}.$$

Definição 3.8. *Dada uma relação $\mathcal{R}$ sobre A, dizemos que $\mathcal{R}$ é reflexiva quando todo elemento de A se relaciona consigo mesmo. Ou seja, para todo $a \in A$, $a\mathcal{R}a$.*

Exemplo 3.9. A relação sobre $G = \{a, b, c, d\}$ dada por

$$\mathcal{R} = \{(a, a), (b, b), (c, c), (d, d), (a, b), (a, d)\}$$

é reflexiva, pois $a\mathcal{R}a$, $b\mathcal{R}b$, $c\mathcal{R}c$ e $d\mathcal{R}d$.

Definição 3.10. *Dada uma relação $\mathcal{R}$ sobre A, dizemos que $\mathcal{R}$ é simétrica quando para todo $a, b \in A$, se $a\mathcal{R}b$ então $b\mathcal{R}a$.*

Exemplo 3.11. A relação sobre $G = \{a, b, c, d\}$ dada por

$$\mathcal{R} = \{(b, d), (c, c), (d, b), (a, b), (b, a)\}$$

é simétrica, pois, uma vez que $a\mathcal{R}b$, temos também que $b\mathcal{R}a$, e o mesmo acontece com $b\mathcal{R}d$ e $d\mathcal{R}b$.

Definição 3.12. *Dada uma relação $\mathcal{R}$ sobre A, dizemos que $\mathcal{R}$ é transitiva quando para todo $a, b, c \in A$, se $a\mathcal{R}b$ e $b\mathcal{R}c$ então $a\mathcal{R}c$.*

Exemplo 3.13. A relação sobre $G = \{a, b, c, d\}$ dada por

$$\mathcal{R} = \{(a, b), (b, c), (d, b), (a, c)\}$$

é transitiva, pois, uma vez que $a\mathcal{R}b$ e $b\mathcal{R}c$, temos também que $a\mathcal{R}c$.

Definição 3.14. *Dada uma relação $\mathcal{R}$ sobre A, dizemos que $\mathcal{R}$ é antissimétrica quando para todo $a, b \in A$, se $a\mathcal{R}b$ e $b\mathcal{R}a$, então $a = b$.*

Exemplo 3.15. A relação sobre $G = \{a, b, c, d \mid a = b\}$ dada por

$$\mathcal{R} = \{(a, a), (a, b), (b, a), (c, b), (a, d)\}$$

é antissimétrica, pois, uma vez que $a\mathcal{R}b$ e $b\mathcal{R}a$, temos que $a = b$.

3.1 Relação de equivalência

Definição 3.16. *Uma relação $\mathcal{R}$ sobre um conjunto A não vazio é chamada relação de equivalência sobre A se, e somente se, $\mathcal{R}$ é reflexiva, simétrica e transitiva. Ou seja, $\mathcal{R}$ deve satisfazer as seguintes propriedades:*

(i) Reflexiva: se $a \in A$, então $a\mathcal{R}a$;

(ii) Simétrica: se $a, b \in A$ e $a\mathcal{R}b$, então $b\mathcal{R}a$;

(iii) Transitiva: se $a, b, c \in A$, $a\mathcal{R}b$ e $b\mathcal{R}c$, então $a\mathcal{R}c$.

Exemplo 3.17. A relação sobre $G = \{a, b, c\}$ dada por

$$\mathcal{R} = \{(a, a), (b, b), (c, c), (a, b), (b, a)\}$$

é uma relação de equivalência, uma vez que satisfaz as propriedades reflexiva, simétrica e transitiva.

Definição 3.18. *Seja $\mathcal{R}$ uma relação de equivalência sobre A. Dado $a \in A$, a classe de equivalência determinada por a, módulo $\mathcal{R}$, é o subconjunto $\overline{a}$ de A constituído pelos elementos x tais que $x\mathcal{R}a$. Ou seja,*

$$\overline{a} = \{x \in A \ / \ x\mathcal{R}a\}.$$

Definição 3.19. *O conjunto das classes de equivalência módulo $\mathcal{R}$ será indicado por $\frac{A}{\mathcal{R}}$ e chamado conjunto-quociente de A por $\mathcal{R}$.*

Exemplo 3.20. Na relação de equivalência sobre $G = \{a, b, c\}$ dada por

$$\mathcal{R} = \{(a, a), (b, b), (c, c), (a, b), (b, a)\}$$

temos: $\overline{a} = \{a, b\}$; $\overline{b} = \{a, b\}$; $\overline{c} = \{c\}$ e $\frac{G}{\mathcal{R}} = \{\{a, b\}, \{c\}\}$.

Proposição 3.21. *Seja $\mathcal{R}$ uma relação de equivalência sobre um conjunto A. Dados $a, b \in A$, as seguintes proposições são equivalentes:*

(i) $a\mathcal{R}b$;

(ii) $a \in \overline{b}$;

(iii) $b \in \overline{a}$;

(iv) $\overline{a} = \overline{b}$.

Demonstração: Devemos provar que $a\mathcal{R}b \Rightarrow a \in \overline{b} \Rightarrow b \in \overline{a} \Rightarrow \overline{a} = \overline{b} \Rightarrow a\mathcal{R}b$.

$a\mathcal{R}b \Rightarrow a \in \overline{b}$: Decorre da definição de classe de equivalência.

$a \in \overline{b} \Rightarrow b \in \overline{a}$: Uma vez que $a \in \overline{b}$, temos que $a\mathcal{R}b$. Como $\mathcal{R}$ é simétrica, segue que $b\mathcal{R}a$ e, portanto, $b \in \overline{a}$.

$b \in \overline{a} \Rightarrow \overline{a} = \overline{b}$: Sabemos, por hipótese, que $b \in \overline{a}$, então $b\mathcal{R}a$. Como $\mathcal{R}$ é simétrica, segue que $a\mathcal{R}b$. Devemos mostrar que $\overline{a} \subset \overline{b}$ e que $\overline{b} \subset \overline{a}$.

Para mostrar que $\overline{a} \subset \overline{b}$, tomemos $x \in \overline{a}$, ou seja, $x\mathcal{R}a$. Considerando que $a\mathcal{R}b$ e que $\mathcal{R}$ é transitiva, $x\mathcal{R}b$, ou seja, $x \in \overline{b}$ e, daí, $\overline{a} \subset \overline{b}$.

De maneira análoga segue que $\overline{b} \subset \overline{a}$.

$\overline{a} = \overline{b} \Rightarrow a\mathcal{R}b$: Como $a \in \overline{a}$ e $b \in \overline{b}$, os conjuntos $\overline{a}$ e $\overline{b}$ não são vazios. Tomemos $x \in \overline{a}$ e, como $\overline{a} = \overline{b}$ por hipótese, segue que $x \in \overline{b}$. Então, $x\mathcal{R}a$ e $x\mathcal{R}b$. Segundo a simetria de $\mathcal{R}$, temos que $a\mathcal{R}x$ e $b\mathcal{R}x$. Sabemos então que $a\mathcal{R}x$ e $x\mathcal{R}b$. Segundo a transitividade de $\mathcal{R}$, temos que $a\mathcal{R}b$.

■

Proposição 3.22. *Se $\mathcal{R}$ é uma relação de equivalência sobre um conjunto A, então $\frac{A}{\mathcal{R}}$ é uma partição de A.*

Demonstração: Para mostrar que $\frac{A}{\mathcal{R}}$ é uma partição de A, é necessário mostrar que:

(i) os subconjuntos de $\frac{A}{\mathcal{R}}$ são não vazios;

(ii) dois membros quaisquer de $\frac{A}{\mathcal{R}}$ ou são iguais ou são disjuntos;

(iii) a união dos membros de $\frac{A}{\mathcal{R}}$ é igual a A.

De fato:

(i) Seja $\overline{a} \in \frac{A}{\mathcal{R}}$. Como $\mathcal{R}$ é uma relação de equivalência, é reflexiva, e $a\mathcal{R}a$ e, portanto, $a \in \overline{a}$. Assim, $\overline{a} \neq \varnothing$ para todo $\overline{a} \in \frac{A}{\mathcal{R}}$.

(ii) Sejam $\overline{a}$ e $\overline{b} \in \frac{A}{\mathcal{R}}$. Ou $\overline{a}$ e $\overline{b}$ são disjuntos ou $\overline{a} \cap \overline{b} \neq \varnothing$. Se $\overline{a}$ e $\overline{b}$ são disjuntos, o item está garantido, mas caso $\overline{a} \cap \overline{b} \neq \varnothing$, precisamos mostrar que $\overline{a} = \overline{b}$. Então seja $x \in \overline{a} \cap \overline{b}$, logo $x \in \overline{a}$ e $x \in \overline{b}$ e, portanto, $x\mathcal{R}a$ e $x\mathcal{R}b$. Daí, como $\mathcal{R}$ é uma relação de equivalência, é simétrica, então $a\mathcal{R}x$. Sabendo, por fim, que $a\mathcal{R}x$ e $x\mathcal{R}b$, como $\mathcal{R}$ é uma relação de equivalência, essa é transitiva, e temos que $a\mathcal{R}b$. Pela proposição 3.21, $\overline{a} = \overline{b}$.

(iii) Mostremos que $\bigcup \overline{a} = A$. Para cada $a \in A$, temos $\bar{a} \subset A$, portanto, $\bigcup \overline{a} \subset A$. Agora, seja x um elemento qualquer de A, então $x\mathcal{R}x$. Logo, $x \in \overline{x}$ e, consequentemente, $x \in \bigcup \overline{a}$. Portanto, $A \subset \bigcup \overline{a}$. Concluímos que, dado $a \in A$, $A = \bigcup \overline{a}$.

■

Proposição 3.23. *Se $\mathcal{P}$ é uma partição do conjunto A, então existe uma relação $\mathcal{R}$ de equivalência sobre A tal que $\frac{A}{\mathcal{R}} = \mathcal{P}$.*

Demonstração: Seja $\mathcal{R}$ a relação sobre A definida da seguinte forma: $x\mathcal{R}y$ se, e somente se, existe $S \in \mathcal{P}$ tal que $x, y \in S$, ou seja, x está relacionado com y quando existe um conjunto S da partição $\mathcal{P}$ ao qual x e y pertencem. Resta verificar que $\mathcal{R}$ é relação de equivalência, para tanto, mostremos que $\mathcal{R}$ satisfaz as propriedades reflexiva, simétrica e transitiva.

(i) *Reflexiva:* Para todo x em A existe um subconjunto $S \subset A$ tal que $S \in \mathcal{P}$ e $x \in S$; portanto, $x\mathcal{R}x$.

(ii) *Simétrica:* Se x e y são elementos quaisquer de A tais que $x\mathcal{R}y$, então $x, y \in S$, para algum $S \in \mathcal{P}$. Logo, $y, x \in S$, portanto, $y\mathcal{R}x$.

(iii) *Transitiva:* Sejam x, y e z elementos quaisquer de A tais que $x\mathcal{R}y$ e $y\mathcal{R}z$. Então, $x, y \in S$ para algum $S \in \mathcal{P}$ e $y, z \in T$ para algum $T \in \mathcal{P}$. Logo, $y \in S$ e $y \in T$. Como dois conjuntos quaisquer de $\mathcal{P}$ ou são disjuntos, ou são iguais, segue que $S = T$. Daí, x e y pertencem ao mesmo conjunto da partição $\mathcal{P}$ e, consequentemente, $x\mathcal{R}z$.

■

3.2 Relação de ordem

Definição 3.24. *Uma relação $\mathcal{R}$ sobre um conjunto A não vazio é chamada relação de ordem parcial sobre A se, e somente se, $\mathcal{R}$ é reflexiva, antissimétrica e transitiva. Ou seja, $\mathcal{R}$ deve satisfazer as seguintes propriedades:*

(i) Reflexiva: se $a \in A$, então $a\mathcal{R}a$;

(ii) Antissimétrica: se $a, b \in A$, $a\mathcal{R}b$ e $b\mathcal{R}a$, então $a = b$;

(iii) Transitiva: se $a, b, c \in A$ e $a\mathcal{R}b$ e $b\mathcal{R}c$, então $a\mathcal{R}c$.

Quando $\mathcal{R}$ é uma relação de ordem parcial sobre A, para dizer que $(a, b) \in \mathcal{R}$, usaremos a notação $a \leq b$ $(\mathcal{R})$, onde lemos "a precede b na relação $\mathcal{R}$". Já para $(a, b) \in \mathcal{R}$ e $a \neq b$, usamos a notação $a < b$ $(\mathcal{R})$, onde lemos "a precede estritamente b na relação $\mathcal{R}$".

Definição 3.25. *Um conjunto parcialmente ordenado é um conjunto sobre o qual se define uma certa relação de ordem parcial.*

Exemplo 3.26. A relação sobre $E = \{a, b, c\}$ dada por

$$\mathcal{R} = \{(a, a), (b, b), (c, c), (a, b)\}$$

é uma relação de ordem parcial.

Definição 3.27. *Seja $\mathcal{R}$ uma relação de ordem parcial sobre A. Os elementos $a, b \in A$ se dizem comparáveis mediante $\mathcal{R}$ se $a \leq b$ ou $b \leq a$.*

Definição 3.28. *Se dois elementos quaisquer de A forem comparáveis mediante $\mathcal{R}$, então $\mathcal{R}$ será chamada relação de ordem total sobre A. Nesse caso, o conjunto A é dito conjunto totalmente ordenado por $\mathcal{R}$.*

Exemplo 3.29. A relação sobre $E = \{a, b, c\}$ dada por

$$\mathcal{R} = \{(a, a), (b, b), (c, c), (a, b), (b, c), (a, c)\}$$

é uma relação de ordem total. Dizemos que E é totalmente ordenado por $\mathcal{R}$.

3.3 Função

Definição 3.30. *Seja $\mathcal{R}$ uma relação de E em F. Chama-se domínio de $\mathcal{R}$ o subconjunto de E constituído pelos elementos x para os quais existe algum y em F tal que $x\mathcal{R}y$. Ou seja,*

$$D(\mathcal{R}) = \{x \in E \ / \ \exists \ y \in F : x\mathcal{R}y\}.$$

Definição 3.31. *Seja $\mathcal{R}$ uma relação de E em F. Chama-se imagem de $\mathcal{R}$ o subconjunto de F constituído pelos elementos y tal que existe algum x em E com $x\mathcal{R}y$. Ou seja,*

$$Im(\mathcal{R}) = \{y \in F \ / \ \exists \ x \in E : x\mathcal{R}y\}.$$

Exemplo 3.32. Nas relações

$$\mathcal{R}_1 = \{(0, 1), (0, 5), (3, 2), (3, 4)\}$$
e
$$\mathcal{R}_2 = \{(1, 1), (2, 9), (2, 7), (1, 5)\}$$

concluímos que:

$$D(\mathcal{R}_1) = \{0, 3\} \text{ e } Im(\mathcal{R}_1) = \{1, 2, 4, 5\};$$
$$D(\mathcal{R}_2) = \{1, 2\} \text{ e } Im(\mathcal{R}_2) = \{1, 5, 7, 9\}.$$

Definição 3.33. *Seja f uma relação de E em F. Dizemos que f é uma função de E em F se, e somente se:*

(i) *o domínio de f é E, isto é, $D(f) = E$;*

(ii) *dado um elemento $a \in D(f)$, é único o elemento $b \in F$ tal que $(a, b) \in f$.*

Se f é uma função de E em F, para indicar que $(a, b) \in f$, escrevemos:

$$b = f(a).$$

Para indicar que f é uma função de E em F, usaremos a notação

$$f : E \to F.$$

O conjunto F é chamado contradomínio de f.

Exemplo 3.34. Dados os conjuntos $E = \{a, b, c, d\}$ e $F = \{j, k, l, m, n\}$, considere as relações:

$$\mathcal{R}_1 = \{(a, j), (b, l), (c, m), (d, m)\};$$
$$\mathcal{R}_2 = \{(a, k), (b, k), (c, n)\};$$
$$\mathcal{R}_3 = \{(a, l), (b, m), (c, n), (d, k), (d, n)\};$$
$$\mathcal{R}_4 = \{(a, j), (b, j), (c, j), (d, j)\}.$$

Observe que $\mathcal{R}_1$ e $\mathcal{R}_4$ satisfazem as condições (i) e (ii) da definição acima e, portanto, são funções. Já $\mathcal{R}_2$ e $\mathcal{R}_3$ não são, uma vez que $D(\mathcal{R}_2) \neq E$ e, em $\mathcal{R}_3$, $d \in E$ não tem um único correspondente em F, já que $(d, k), (d, n) \in \mathcal{R}_3$.

Definição 3.35. *Seja f uma função de E em F. Dado $A \subset E$, chamamos de imagem de A segundo f e indicamos por $f(A)$, o seguinte subconjunto de F:*

$$f(A) = \{f(x) \ / \ x \in A\}.$$

Exemplo 3.36. Dados os conjuntos $E = \{a, b, c, d, e\}$ e $F = \{j, k, l, m, n, o\}$, considere as funções de E em F:

$$f_1 = \{(a, j), (b, k), (c, l), (d, m), (e, j)\};$$
$$f_2 = \{(a, k), (b, k), (c, n), (d, o), (e, k)\}.$$

Temos que
$f_1(E) = \{j, k, l, m\}$;
$f_2(E) = \{k, n, o\}$.

Definição 3.37. *Seja f uma função de E em F. Dado $B \subset F$, chamamos de imagem inversa de B segundo f e indicamos por $f^{-1}(B)$, o seguinte subconjunto de E:*

$$f^{-1}(B) = \{x \in E \ / \ f(x) \in B\}.$$

Exemplo 3.38. Dados os conjuntos $E = \{a, b, c, d, e\}$ e $F = \{j, k, l, m, n, o\}$, considere as funções de E em F:

$$f_1 = \{(a, j), (b, k), (c, l), (d, m), (e, n)\};$$
$$f_2 = \{(a, k), (b, o), (c, n), (d, m), (e, l)\}.$$

Temos que
$f_1^{-1}(F) = \{a, b, c, d, e\}$;
$f_2^{-1}(F) = \{a, b, c, d, e\}$.

Definição 3.39. *Seja f uma função de E em F. Dizemos que f é uma função injetora se dois elementos quaisquer e distintos de E têm imagens distintas, ou seja:*

$$x_1 \neq x_2 \Rightarrow f(x_1) \neq f(x_2);\ \forall x_1, x_2 \in E.$$

Observação 3.40. Notemos que a contrapositiva dessa definição nos diz que:

$$\forall x_1, x_2 \in E,\ f(x_1) = f(x_2) \Rightarrow x_1 = x_2.$$

Logo, f não é injetora se existem $x_1, x_2 \in E$, tais que $f(x_1) = f(x_2)$ e $x_1 \neq x_2$.

Exemplo 3.41. Dados os conjuntos $E = \{a, b, c, d\}$ e $F = \{j, k, l, m, n\}$, são exemplos de funções injetoras:

$$\mathcal{R}_1 = \{(a, j), (b, l), (c, m), (d, k)\};$$
$$\mathcal{R}_2 = \{(a, k), (b, j), (c, n), (d, l)\}.$$

Exemplo 3.42. Dados os conjuntos $E = \{a, b, c, d\}$ e $F = \{j, k, l, m, n\}$, não são exemplos de funções injetoras:

$$\mathcal{R}_1 = \{(a, j), (b, j), (c, m), (d, k)\};$$
$$\mathcal{R}_2 = \{(a, k), (b, j), (c, k), (d, j)\}.$$

Em $\mathcal{R}_1$: $f(a) = f(b) = j$ com $a \neq b$.
Em $\mathcal{R}_2$: $f(a) = f(c) = k$ com $a \neq c$ e $f(b) = f(d) = j$ com $b \neq d$.

Definição 3.43. *Seja f uma função de E em F. Dizemos que f é uma função sobrejetora quando o contradomínio e a imagem coincidem, ou seja:*

$$Im(f) = F.$$

Observação 3.44. Notemos que para toda função $f : E \to F$, temos $Im(f) \subset F$. Sendo assim, basta verificar que $F \subset Im(f)$ para que $Im(f) = F$, ou seja, para que f seja sobrejetora. Para tanto, basta mostrar que para todo $y \in F$ existe $x \in E$ tal que $f(x) = y$. Observe que f não é sobrejetora se existe $y \in F$ tal que, qualquer que seja $x \in E$, $f(x) \neq y$.

Exemplo 3.45. Dados os conjuntos $E = \{a, b, c, d\}$ e $F = \{j, k, l\}$, são exemplos de funções sobrejetoras:

$$\mathcal{R}_1 = \{(a, j), (b, l), (c, k), (d, k)\};$$
$$\mathcal{R}_2 = \{(a, k), (b, j), (c, k), (d, l)\}.$$

Exemplo 3.46. Dados os conjuntos $E = \{a, b, c, d\}$ e $F = \{j, k, l, m\}$, não são exemplos de funções sobrejetoras:

$$\mathcal{R}_1 = \{(a, j), (b, l), (c, k), (d, j)\};$$
$$\mathcal{R}_2 = \{(a, k), (b, j), (c, m), (d, m)\}.$$

Em $\mathcal{R}_1$: não existe $x \in E$ tal que $f(x) = m$.
Em $\mathcal{R}_2$: não existe $x \in E$ tal que $f(x) = l$.

Definição 3.47. *Seja f uma função de E em F. Dizemos que f é uma função bijetora quando f é injetora e sobrejetora.*

Exemplo 3.48. Dados os conjuntos $E = \{a, b, c, d\}$ e $F = \{j, k, l, m\}$, são exemplos de funções bijetoras:

$$\mathcal{R}_1 = \{(a, j), (b, l), (c, k), (d, m)\};$$
$$\mathcal{R}_2 = \{(a, k), (b, j), (c, m), (d, l)\}.$$

Exemplo 3.49. A seguir vejamos alguns exemplos de funções que não são bijetoras.

Dados os conjuntos $E = \{a, b, c, d, e\}$ e $F = \{j, k, l, m, n\}$, a função

$$\mathcal{R}_1 = \{(a, j), (b, l), (c, k), (d, m), (e, j)\}$$

não é bijetora, uma vez que não é injetora e nem sobrejetora.

Dados os conjuntos $E = \{a, b, c, d\}$ e $F = \{j, k, l, m, n\}$, a função

$$\mathcal{R}_2 = \{(a, k), (b, j), (c, m), (d, l)\}$$

não é bijetora, uma vez que não é sobrejetora.

Dados os conjuntos $E = \{a, b, c, d, e\}$ e $F = \{j, k, l, m\}$, a função

$$\mathcal{R}_3 = \{(a, k), (b, j), (c, m), (d, l), (e, k)\}$$

não é bijetora, uma vez que não é injetora.

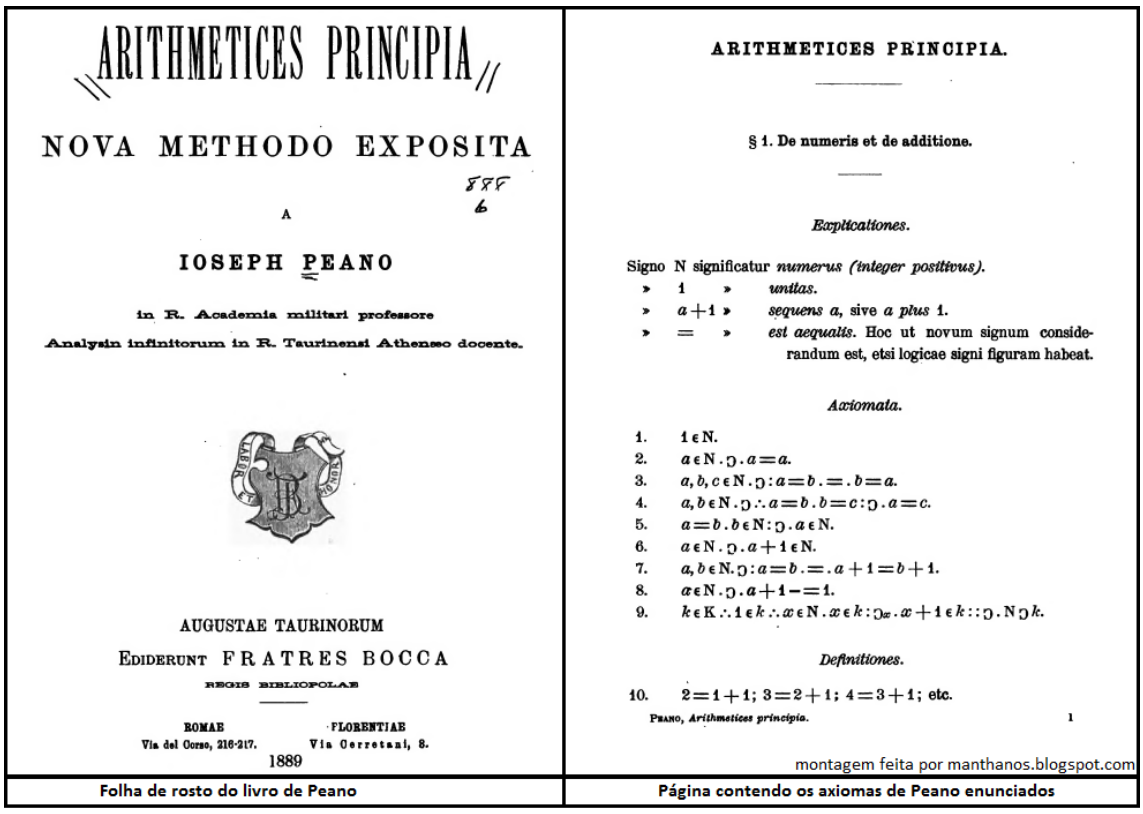
Para finalizar este capítulo, observamos que as relações e propriedades aqui tratadas serão utilizadas ao longo dos próximos capítulos.

4 Números Naturais

4.1 Axiomas de Peano

Para descrever o conjunto dos números naturais de forma sistemática, Giuseppe Peano[1] escolheu três conceitos primitivos. A saber: o *zero*, o *número natural* e a relação "*é sucessor de*". Neste contexto formulou alguns axiomas.

Podemos visualizar abaixo a folha de rosto do livro de Peano e também a página contendo os seus axiomas.



ARITHMETICES PRINCIPIA

NOVA METHODO EXPOSITA

A

IOSEPH PEANO

in R. Academia militari professore
Analysin infinitorum in R. Taurinensi Athenaeo docente.

AUGUSTAE TAURINORUM
EDIDERUNT FRATRES BOCCA
REGIS BIBLIOPOLAE

ROMAE Via del Corso, 216-217. FLORENTIAE Via Cerretani, 8.
1889

Folha de rosto do livro de Peano

ARITHMETICES PRINCIPIA.

§ 1. De numeris et de additione.

Explicationes.

Signo N significatur *numerus (integer positivus).*
» 1 » *unitas.*
» $a+1$ » *sequens a,* sive *a plus* 1.
» $=$ » *est aequalis.* Hoc ut novum signum considerandum est, etsi logicae signi figuram habeat.

Axiomata.

1. $1 \in N$.
2. $a \in N . \supset . a = a$.
3. $a, b, c \in N . \supset : a = b . = . b = a$.
4. $a, b \in N . \supset . \therefore a = b . b = c : \supset . a = c$.
5. $a = b . b \in N : \supset . a \in N$.
6. $a \in N . \supset . a + 1 \in N$.
7. $a, b \in N . \supset : a = b . = . a + 1 = b + 1$.
8. $a \in N . \supset . a + 1 - = 1$.
9. $k \in K . \therefore 1 \in k . \therefore x \in N . x \in k : \supset_x . x + 1 \in k :: \supset . N \supset k$.

Definitiones.

10. $2 = 1 + 1$; $3 = 2 + 1$; $4 = 3 + 1$; etc.

PEANO, *Arithmetices principia.* 1

montagem feita por manthanos.blogspot.com

Página contendo os axiomas de Peano enunciados

[1] Giuseppe Peano (27 de agosto de 1858 – 20 de abril de 1932) foi um matemático italiano. Autor de mais de 200 livros e artigos, ele foi um dos fundadores da lógica matemática e da teoria dos conjuntos. A axiomatização padrão dos números naturais é chamada de axiomas de Peano em sua homenagem. Ele fez contribuições fundamentais para o tratamento rigoroso e sistemático do método da indução matemática.

As formulações originais dos axiomas de Peano utilizavam o 1 como primeiro número natural, ao invés do 0. A escolha é arbitrária, uma vez que o primeiro axioma não concede à constante 0 nenhuma propriedade adicional. No entanto, como 0 é o elemento neutro da adição, a maioria das interpretações modernas dos axiomas de Peano se inicia no 0. Esse trabalho também considera o início dos números naturais a partir de 0, essa escolha foi feita pois usamos como referência básica a obra de Domingues, H. H. *Fundamentos de Aritmética*, [3], no qual faz esta consideração.

P_1. Zero é um número natural.

P_2. Se n é um número natural, então n tem um único sucessor que também é um número natural.

P_3. Zero não é sucessor de nenhum número natural.

P_4. Dois números naturais que têm sucessores iguais são, eles próprios, iguais.

P_5. Se uma coleção S de números naturais contém o zero e, também, o sucessor de todo elemento de S, então S é o conjunto de todos os números naturais.

Adotaremos 0 para indicar o zero, n^+ para indicar o sucessor de um número natural n e $\mathbb{N}$ para denotar o conjunto dos números naturais. Sendo assim, os Axiomas de Peano podem ser enunciados da seguinte forma:

P_1. $0 \in \mathbb{N}$.

P_2. $n \in \mathbb{N} \Rightarrow n^+ \in \mathbb{N}$.

P_3. $n \in \mathbb{N} \Rightarrow n^+ \neq 0$.

P_4. $n^+ = m^+ \Rightarrow n = m$.

P_5. Se $S \subset \mathbb{N}$ e

(i) $0 \in S$;

(ii) $n \in S \Rightarrow n^+ \in S$;

então $S = \mathbb{N}$.

Ao axioma P_5 denominamos *Princípio da Indução Finita.*

Proposição 4.1. *Se $n \in \mathbb{N}$, então $n^+ \neq n$.*

Demonstração: Definimos $S = \{n \in \mathbb{N} \ / \ n^+ \neq n\}$. Note que o axioma P_3 garante que zero não é sucessor de nenhum número natural, sendo assim, também é válido que $0 \neq 0^+$. Portanto, $0 \in S$. Observe ainda que o axioma P_4 garante que se dois números naturais são diferentes, seus sucessores serão diferentes; daí, se $n \in S$, $n \neq n^+$, logo, $n^+ \neq (n^+)^+$; ou seja, uma vez que $n \in S$, $n^+ \in S$. O axioma P_5 conclui que $S = \mathbb{N}$. Portanto, para todo $n \in \mathbb{N}$, $n^+ \neq n$.

■

Proposição 4.2. *Se $m \in \mathbb{N}$ e $m \neq 0$, então existe $n \in \mathbb{N}$ tal que $n^+ = m$.*

Demonstração: Definimos $S = \{0\} \cup \{n \in \mathbb{N} \ / \ n \neq 0$ e $m^+ = n$ para algum $m \in \mathbb{N}\}$. Por construção, $0 \in S$. Agora, se $m \in S$ e $m \neq 0$, então $m = n^+$ para algum $n \in \mathbb{N}$. Daí, $m^+ = (n^+)^+$ e, portanto $m^+ \in S$. Novamente o axioma P_5 garante que $S = \mathbb{N}$ e, portanto, a proposição é verdadeira.

■

A seguir apresentamos uma proposição que caracteriza o Princípio da Indução Finita via uma propriedade $P(n)$ sob o conjunto dos números naturais.

Proposição 4.3. *Suponhamos que a todo número natural n esteja associada uma afirmação $P(n)$ tal que:*

(i) $P(0)$ é verdadeira;

(ii) Se $P(n)$ é verdadeira, então $P(n^+)$ é verdadeira.

Se $P(n)$ satisfaz os itens citados, então $P(n)$ é verdadeira para todo $n \in \mathbb{N}$.

Demonstração: Definimos $S = \{n \in \mathbb{N} \ / \ P(n)$ é verdadeira$\}$. Pelo item *(i)* veja que $0 \in S$ e, dado $n \in S$, temos pelo item *(ii)* que $n^+ \in S$. Logo, estão satisfeitas as hipóteses do axioma P_5. Portanto, $S = \mathbb{N}$, ou seja, $P(n)$ é verdadeira para todo $n \in \mathbb{N}$.

■

Observação 4.4. Agora vamos exibir a representação de alguns números naturais.

Via o axioma P_1 denotamos por 0 aquele elemento de $\mathbb{N}$ que não é sucessor de nenhum outro elemento de $\mathbb{N}$.

Pela propriedade P_4 podemos afirmar que cada número natural n tem um único sucessor $n^+ \in \mathbb{N}$, uma vez que:

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

Este último fato permite que estabeleçamos a seguinte notação:

$$1 := 0^+;$$
$$2 := 1^+;$$
$$3 := 2^+;$$
$$\vdots$$

e assim por diante.

Com isto, podemos escrever o conjunto dos números naturais $\mathbb{N}$ explicitamente como o seguinte conjunto:

$$\mathbb{N} = \{0, 1, 2, 3, \cdots\}.$$

4.2 Adição em $\mathbb{N}$

A seguir vamos definir a adição em $\mathbb{N}$ e trataremos de algumas propriedades dessa operação binária.

Definição 4.5. *Definimos a adição como a operação binária em* $\mathbb{N}$

$$\begin{array}{rccc} + : & \mathbb{N}\times\mathbb{N} & \longrightarrow & \mathbb{N} \\ & (n,m) & \longmapsto & n+m \end{array}$$

via as seguintes condições:

- $n + 0 = n$;
- $n + m^+ = (n + m)^+$.

Observação 4.6. Note que desse fato, para qualquer $n \in \mathbb{N}$, $n^+ = (n+0)^+ = n+0^+ = n+1$.

Proposição 4.7. *A operação binária + tem as seguintes propriedades:*

A_1. *Associativa:* $\forall m, n, p \in \mathbb{N}$, $m + (n + p) = (m + n) + p$.

A_2. *Elemento Neutro: existe um único elemento* $0 \in \mathbb{N}$ *tal que* $m + 0 = m = 0 + m$ *para todo* $m \in \mathbb{N}$.

A_3. *Comutativa:* $\forall m, n \in \mathbb{N}$, $m + n = n + m$.

A_4. *Lei do cancelamento:* $\forall m, n, p \in \mathbb{N}$, $m + n = m + p \Rightarrow n = p$.

A_5. *Soma resultando em* 0*: se* $m, n \in \mathbb{N}$ *são tais que* $m + n = 0$, *então* $m = n = 0$.

Demonstração: Demonstremos cada propriedade da adição, usando, quando possível, a proposição 4.3.

A_1. *Associativa:*

Consideremos

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

Observe que $P(0)$ é verdadeira, pois:

$$m + (n + 0) = m + n = (m + n) + 0.$$

Vamos supor, por hipótese de indução, que para algum $p \in \mathbb{N}$, $P(p)$ seja verdadeira, ou seja, $(m + n) + p = m + (n + p)$.

Provemos que $P(p^+)$ também será verdadeira.

$$(m + n) + p^+ = [(m + n) + p]^+ = [m + (n + p)]^+ = m + (n + p)^+ = m + (n + p^+).$$

Portanto, segue o resultado pelo Princípio da Indução Finita.

A_2. *Elemento Neutro:*

Note que, da definição 4.5, já sabemos que dado $n \in \mathbb{N}$, $n + 0 = n$. Basta verificar que $0 + n = n$.

Consideremos

$$P(n) = \{n \in \mathbb{N} \ / \ 0 + n = n\}.$$

Observe que $P(0)$ é verdadeira, pois:

$$0 + 0 = 0.$$

Vamos supor, por hipótese de indução, que para algum $n \in \mathbb{N}$, $P(n)$ seja verdadeira, ou seja, $0 + n = n$.

Provemos que $P(n^+)$ também será verdadeira.

$$0 + n^+ = (0 + n)^+ = n^+.$$

Portanto, segue o resultado pelo Princípio da Indução Finita.

A_3. *Comutativa:*

Consideremos

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

Observe que $P(0)$ é verdadeira, pois:

$$m + 0 = m = 0 + m.$$

Para mostrar que $P(1)$ é verdadeira, consideremos

$$Q(p) = \{p \in \mathbb{N} \ / \ p + 1 = 1 + p\}.$$

Observe que $Q(0)$ é verdadeira, pois:

$$0 + 1 = 1 = 1 + 0.$$

Vamos supor, por hipótese de indução, que para algum $p \in \mathbb{N}$, $Q(p)$ é verdadeira, ou seja, $p + 1 = 1 + p$.

Provemos que $Q(p^+)$ também será verdadeira.

$$p^+ + 1 = (p + 1) + 1 = (1 + p) + 1 = 1 + (p + 1) = 1 + p^+.$$

Portanto, pelo Princípio da Indução Finita (proposição 4.3), segue que para qualquer $p \in \mathbb{N}$, $p + 1 = 1 + p$.

Portanto, $P(1)$ é verdadeira.

Vamos supor, por hipótese de indução, que para algum $n \in \mathbb{N}$ $P(n)$ seja verdadeira, ou seja, $m + n = n + m$, para todo $m \in \mathbb{N}$.

Provemos que $P(n^+)$ também será verdadeira.

$$m + n^+ = (m + n)^+ = (m + n) + 1 = (n + m) + 1 = n + (m + 1) = n + (1 + m) = (n + 1) + m = n^+ + m.$$

Portanto, segue o resultado pelo Princípio da Indução Finita.

A_4. *Lei do cancelamento:*

Consideremos

$$P(m) = \{m \in \mathbb{N} \ / \ m + n = m + p \Rightarrow n = p, \forall n, p \in \mathbb{N}\}.$$

Observe que $P(0)$ é verdadeira, pois, suponhamos $0 + n = 0 + p$, então, como 0 é o elemento neutro, segue que

$$n = 0 + n = 0 + p = p.$$

Vamos supor, por hipótese de indução, que para algum $m \in \mathbb{N}$, $P(m)$ seja verdadeira, ou seja, $m + n = m + p \Rightarrow n = p$.

Provemos que $P(m^+)$ também será verdadeira.

Suponhamos $m^+ + n = m^+ + p$, então, segue que $(m + n)^+ = (m + p)^+$.

Lembre-se que o axioma P_4 garante que $m + n = m + p$, que, por hipótese de indução, implica em $n = p$.

Portanto, segue o resultado pelo Princípio da Indução Finita.

A_5. *Soma resultando em* 0*:*

Vamos supor, sem perda de generalidade, $n, m \in \mathbb{N}, n + m = 0$ com $m \neq 0$. Então , existe algum $p \in \mathbb{N}$ tal que $m = p^+$. Daí,

$$0 = m + n = n + m = n + p^+ = (n + p)^+,$$

ou seja, que 0 é sucessor de algum número natural, o que é absurdo.

Portanto, $m = n = 0$.

■

4.3 Multiplicação em $\mathbb{N}$

A seguir vamos definir a multiplicação em $\mathbb{N}$ e trataremos de algumas propriedades dessa operação binária.

Definição 4.8. *Definimos a multiplicação como a relação binária*

$$\begin{array}{rccc} \cdot : & \mathbb{N} \times \mathbb{N} & \longrightarrow & \mathbb{N} \\ & (n, m) & \longmapsto & n \cdot m \end{array}$$

via as seguintes propriedades:

- $n \cdot 0 = 0$*;*
- $n \cdot m^+ = n \cdot m + n$*.*

Proposição 4.9. *A operação binária* $\cdot$ *tem as seguintes propriedades:*

M_1. *Multiplicação por zero:* $0 \cdot m = 0$ *para qualquer* $m \in \mathbb{N}$*.*

M_2. *Elemento Identidade:* $1 \cdot m = m$ *para qualquer* $m \in \mathbb{N}$*.*

M_3. *Distributiva em relação à adição: para quaisquer* $m, n, p \in \mathbb{N}$*, temos que* $(m + n) \cdot p = m \cdot p + n \cdot p$*.*

M_4. *Associativa: para quaisquer* $m, n, p \in \mathbb{N}, m \cdot (n \cdot p) = (m \cdot n) \cdot p$.

M_5. *Comutativa: para quaisquer* $m, n \in \mathbb{N}, m \cdot n = n \cdot m$.

M_6. *Lei do anulamento: dados* $m, n \in \mathbb{N}$, *se* $m \cdot n = 0$, *então* $m = 0$ *ou* $n = 0$.

M_7. *Lei do cancelamento: dados* $m, n, p \in \mathbb{N}$, *se* $m \cdot p = n \cdot p$ *e* $p \neq 0$, *então* $m = n$.

M_8. *Multiplicação resultando em* 1*: dados* $m, n \in \mathbb{N}$, *se* $m \cdot n = 1$, *então* $m = 1$ *e* $n = 1$.

Demonstração: Demonstremos cada propriedade da multiplicação, usando, quando possível, a proposição 4.3.

M_1. *Multiplicação por zero:*

Consideremos

$$P(m) = \{m \in \mathbb{N} \ / \ 0 \cdot m = 0\}.$$

Note que se $m = 0$ o resultado vem imediatamente da definição dada acima.

Supomos, por hipótese de indução, que $P(m)$ é verdadeira, ou seja, que $0 \cdot m = 0$. Mostremos que a afirmação também será válida no caso de $P(m^+)$, ou seja, que $0 \cdot m^+ = 0$.

Por definição, $0 \cdot m^+ = 0 \cdot m + 0$. Já sabemos que $0 \cdot m = 0$, segue que $0 \cdot m^+ = 0 + 0 = 0$.

Portanto, pelo Princípio da Indução Finita, $0 \cdot m = 0$ para qualquer $m \in \mathbb{N}$, como queríamos demonstrar.

M_2. *Elemento Identidade:*

Consideremos

$$P(m) = \{m \in \mathbb{N} \ / \ 1 \cdot m = m\}.$$

Note que se $m = 0$ o resultado segue da definição dada para a multiplicação.

Supomos, por hipótese de indução, que $1 \cdot m = m$, ou seja, que $P(m)$ é verdadeira. Mostremos que a afirmação também será válida no caso de $P(m^+)$, ou seja, que $1 \cdot m^+ = m^+$.

Por definição, $1 \cdot m^+ = 1 \cdot m + 1$ e já sabemos que $1 \cdot m = m$.

Segue que $1 \cdot m^+ = m + 1 = m + 0^+ = (m + 0)^+ = m^+$.

Portanto, pelo Princípio da Indução Finita, $1 \cdot m = m$ para qualquer $m \in \mathbb{N}$, como queríamos demonstrar.

M_3. *Distributiva em relação à adição:*

Consideremos

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

Note que $P(0)$ é verdadeira:

$$(m+n)\cdot 0 = 0 = 0+0 = m\cdot 0 + n\cdot 0.$$

Supomos, por hipótese de indução, que para quaisquer $m,n \in \mathbb{N}$,

$(m+n)\cdot p = m\cdot p + n\cdot p$, ou seja, que $P(p)$ é verdadeira. Mostremos que a afirmação também será válida no caso de $P(p^+)$, ou seja, que para quaisquer $m,n \in \mathbb{N}$, $(m+n)\cdot p^+ = m\cdot p^+ + n\cdot p^+$.

Por definição, $(m+n)\cdot p^+ = (m+n)\cdot p + (m+n)$. Já sabemos que $(m+n)\cdot p = m\cdot p + n\cdot p$, segue, usando as propriedades associativa e comutativa da soma, que:

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

Portanto, pelo Princípio da Indução Finita, $(m+n)\cdot p = m\cdot p + n\cdot p$ para quaisquer $m,n,p \in \mathbb{N}$, como queríamos demonstrar.

M_4. *Associativa:*

Consideremos

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

Note que $P(0)$ é verdadeira:

$$0\cdot(n\cdot p) = 0 = 0\cdot n = (0\cdot n)\cdot p.$$

Supomos, por hipótese de indução, que para quaisquer $n,p \in \mathbb{N}$, $m\cdot(n\cdot p) = (m\cdot n)\cdot p$, ou seja, que $P(m)$ é verdadeira. Mostremos que a afirmação também será válida no caso de $P(m^+)$, ou seja, que para quaisquer $n,p \in \mathbb{N}$, $m^+\cdot(n\cdot p) = (m^+\cdot n)\cdot p$.

Observe que:

$$m^+\cdot(n\cdot p) = (m+1)\cdot(n\cdot p) = m\cdot(n\cdot p) + 1\cdot(n\cdot p) =$$
$$= (m\cdot n)\cdot p + n\cdot p = (m\cdot n + n)\cdot p = ((m+1)\cdot n)\cdot p = (m^+\cdot n)\cdot p.$$

Portanto, pelo Princípio da Indução Finita, $m\cdot(n\cdot p) = (m\cdot n)\cdot p$, para quaisquer $m,n,p \in \mathbb{N}$, como queríamos demonstrar.

M_5. *Comutativa:*

Consideremos

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

Note que $P(0)$ é verdadeiro:

$$0 \cdot n = 0 = n \cdot 0, \ \forall n \in \mathbb{N}.$$

Supomos, por hipótese de indução, que para qualquer $n \in \mathbb{N}$, $m \cdot n = n \cdot m$, ou seja, que $P(m)$ é verdadeira. Mostremos que a afirmação também será válida no caso de $P(m^+)$, ou seja, que para qualquer $n \in \mathbb{N}$, $m^+ \cdot n = n \cdot m^+$.

Observe que:

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

Portanto, pelo Princípio da Indução Finita, $m \cdot n = n \cdot m$, para quaisquer $m, n \in \mathbb{N}$, como queríamos demonstrar.

M_6. *Lei do anulamento:*

Suponha, sem perda de generalidade, que $m \neq 0$. Logo, existe $p \in \mathbb{N}$ tal que $p^+ = m$. Daí, $m \cdot n = p^+ \cdot n = n \cdot p^+ = n \cdot p + n$.

Sendo $m \cdot n = 0$, temos que $n \cdot p + n = 0$. Pela propriedade A_5 (proposição 4.7), segue que $n \cdot p = 0$ e $n = 0$. Portanto, $n = 0$.

M_7. *Lei do cancelamento:*

Consideremos

$$P(p) = \{p \in \mathbb{N}, \ p \neq 0 \ / \ m \cdot p = n \cdot p \Rightarrow m = n, \forall m, n \in \mathbb{N}\}.$$

Note que $P(1)$ é verdadeira, pois:

$$m \cdot 1 = n \cdot 1 \Leftrightarrow m = n.$$

Supomos, por hipótese de indução, que se $m \cdot p = n \cdot p$, então $m = n$, para quaisquer $m, n \in \mathbb{N}$. Mostremos que a afirmação também será válida no caso de p^+, ou seja, que se $m \cdot p^+ = n \cdot p^+$, então $m = n$.

Da hipótese de indução, sabemos, pela contrapositiva, que:

$$m \neq n \Rightarrow m \cdot p + m \neq m \cdot p + n.$$

Por outro lado,

$$m \neq n \Rightarrow m \cdot p \neq n \cdot p \Rightarrow m \cdot p + n \neq n \cdot p + n.$$

Das afirmativas acima, concluímos que:

$$n \cdot p + n \neq m \cdot p + n \neq m \cdot p + m.$$

Ou seja,

$$n \cdot p + n \neq m \cdot p + m.$$

Segue que:

$$n \cdot p^+ \neq m \cdot p^+.$$

Observe que concluímos que dados m, n e $p \in \mathbb{N}$, $p \neq 0$, se $m \neq n$, então $m \cdot p^+ \neq n \cdot p^+$, cuja contrapositiva nos garante que se $m \cdot p^+ = n \cdot p^+$, então $m = n$.

Portanto, pelo Princípio da Indução Finita, dados $m, n, p \in \mathbb{N}$, se $m \cdot p = n \cdot p$ e $p \neq 0$, então $m = n$, como queríamos demonstrar.

M_8. *Multiplicação resultando em* 1*:*

Seja $m \cdot n = 1$. Observe que devemos ter $m \neq 0$ e $n \neq 0$, pois, da definição 4.8 e da propriedade M_1 da proposiçao 4.9, sabemos que:

$$\text{se } m = 0,\ m \cdot n = 0 \cdot n = 0 \neq 1;$$
$$\text{se } n = 0,\ m \cdot n = m \cdot 0 = 0 \neq 1.$$

Sendo $m \neq 0$ e $n \neq 0$, segundo a proposição 4.1, existem números naturais p e q, tais que $m = p^+$ e $n = q^+$.

Daí,

$$m \cdot n = p^+ \cdot q^+ = (p+1) \cdot (q+1) = (p+1) \cdot q + (p+1) \cdot 1 = p \cdot q + q + p + 1.$$

Como $m \cdot n = 1$, devemos ter

$$p \cdot q + q + p + 1 = 1 = 1 + 0.$$

Então, segundo A_4 (proposição 4.7),

$$p \cdot q + q + p = 0 \Rightarrow p \cdot q + (q + p) = 0.$$

O que implica, segundo A_5 (proposição 4.7), que

$$p \cdot q = q + p = 0 \text{ e } q = p = 0.$$

Logo,

$$m = p^+ = 0^+ = 1 \text{ e } n = q^+ = 0^+ = 1.$$

■

Observamos que a partir da operação de multiplicação é possível estabelecer a noção de divisibilidade em $\mathbb{N}$, como veremos a seguir.

Definição 4.10. *Dados m e n elementos quaisquer de $\mathbb{N}$, dizemos que m é divisível por n quando existir $k \in \mathbb{N}$ tal que $m = k \cdot n$.*

Denotamos k por $\dfrac{m}{n}$.

Definição 4.11. *Considerando o conjunto*

$$\mathcal{D}_{\mathbb{N}} = \{(m, n) \in \mathbb{N} \times \mathbb{N}^* \ / \ m = k \cdot n \text{ para algum } k \in \mathbb{N}\}$$

podemos definir a aplicação, que chamaremos de divisão, dada por:

$$\begin{array}{rccc} \div : & \mathcal{D}_{\mathbb{N}} & \longrightarrow & \mathbb{N} \\ & (m, n) & \longmapsto & m \div n \end{array}$$

em que:

$$m \div n := \frac{m}{n} = k.$$

Aos números m e n denominamos, respectivamente, numerador e denominador.

Note que esta operação não está definida para quaisquer $(m, n) \in \mathbb{N} \times \mathbb{N}$.

Exemplo 4.12. A seguir, alguns casos do conjunto dos números naturais onde a operação divisão está definida:

4 é divisível por 2, bastando considerar que $4 = 2 \cdot 2$, ou seja, $\dfrac{4}{2} = 2$;

16 é divisível por 4, bastando considerar que $16 = 4 \cdot 4$, ou seja, $\dfrac{16}{4} = 4$;

15 é divisível por 5, bastando considerar que $15 = 3 \cdot 5$, ou seja, $\dfrac{15}{5} = 3$.

Exemplo 4.13. A seguir, alguns casos do conjunto dos números naturais onde a operação divisão não está definida:

$\dfrac{5}{3}$ não está definido em $\mathbb{N}$, pois $(5, 3) \notin \mathcal{D}_{\mathbb{N}}$.

$\dfrac{7}{2}$ não está definido em $\mathbb{N}$, pois $(7, 2) \notin \mathcal{D}_{\mathbb{N}}$.

$\dfrac{10}{4}$ não está definido em $\mathbb{N}$, pois $(10, 4) \notin \mathcal{D}_{\mathbb{N}}$.

4.4 Subtração e relação de ordem em $\mathbb{N}$

Uma vez definida a adição no conjunto dos números naturais, conseguimos definir a operação $\leq$ (menor ou igual que) e a operação $-$ (subtração). A partir dessas definições, é possível explorarmos algumas propriedades.

Definição 4.14. *A relação $\leq$ (menor ou igual que) será definida do seguinte modo:*

Se $m, n \in \mathbb{N}$ dizemos que $m \leq n$ se, e somente se, $n = m + u$ para algum $u \in \mathbb{N}$.

Denotamos u por $n - m$ e chamaremos n de minuendo e m de subtraendo.

Definição 4.15. *Podemos definir a operação subtração*

$$\begin{array}{rccc} - : & \mathcal{M} & \longrightarrow & \mathbb{N} \\ & (m,n) & \longmapsto & n-m \end{array}$$

em que $\mathcal{M} = \{(m,n) \ / \ m \leq n\} \subset \mathbb{N} \times \mathbb{N}$.

Observe que esta operação não está definida para qualquer par $(m,n) \in \mathbb{N} \times \mathbb{N}$. Por exemplo, $3 - 5$ não está definida, pois $(5,3) \notin \mathcal{M}$.

No que segue, dados $m, n \in \mathbb{N}$ usamos $m < n$ para representar que $m \leq n$ com $m \neq n$.

Proposição 4.16. *A relação de ordem tem as seguintes propriedades:*

O_1. *Dados $m, n \in \mathbb{N}$, $(n - m) + m = n$, sempre que $m \leq n$.*

O_2. *Dados $m, n, p \in \mathbb{N}$, se $m \leq p$, então $(p + n) - m = (p - m) + n$.*

O_3. *Dados $m, n, p \in \mathbb{N}$, se $n + m \leq p$, então $p - (n + m) = (p - n) - m$.*

O_4. *Dados $m, n, p, q \in \mathbb{N}$, se $m \leq n$ e $p \leq q$, então $(n - m) + (q - p) = (n + q) - (m + p)$.*

O_5. *Reflexiva: para qualquer $m \in \mathbb{N}$, $m \leq m$.*

O_6. *Antissimétrica: para quaisquer $m, n \in \mathbb{N}$, se $m \leq n$ e $n \leq m$, então $m = n$.*

O_7. *Transitiva: para quaisquer $m, n, p \in \mathbb{N}$, se $m \leq n$ e $n \leq p$, então $m \leq p$.*

O_8. *Para quaisquer $m, n \in \mathbb{N}$, $m \leq n$ ou $n \leq m$.*

O_9. *Compatibilidade com a adição: para quaisquer $m, n, p \in \mathbb{N}$, se $m \leq n$, então $m + p \leq n + p$.*

O_{10}. *Compatibilidade com a multiplicação: para quaisquer $m, n, p \in \mathbb{N}$, se $m \leq n$, então $m \cdot p \leq n \cdot p$.*

O_{11}. *Para quaisquer $m, n \in \mathbb{N}$, se $m < n$, então $m + 1 \leq n$.*

O_{12}. *Princípio do menor número natural: para qualquer que seja o subconjunto não vazio* $S \subset \mathbb{N}$, S *possui mínimo.*

Demonstração: Façamos as demonstrações de cada propriedade da relação de ordem:

O_1. Basta observar que se $n - m = u$, com $u \in \mathbb{N}$, então $n = m + u = m + (n - m)$.

O_2. Seja $p - m = u$, com $u \in \mathbb{N}$, então $p = m + u$ e, portanto, $p + n = (m + u) + n = m + (u + n)$. Daí, $(p + n) - m = (m + (u + n)) - m = ((u + n) + m) - m = (u + n) + (m - m) = (u + n) + 0 = u + n = (p - m) + n$.

O_3. Seja $p - (n + m) = u$, com $u \in \mathbb{N}$, tal que $p = (n + m) + u$.

Observe que $p = (n + m) + u \Rightarrow p = n + (m + u) \Rightarrow p - n = m + u$.

Por outro lado, $(p - n) - m = v$, com $v \in \mathbb{N}$ tal que $p - n = m + v$.

Daí, segue que $m + u = m + v$, que pela propriedade A_4 (proposição 4.7), implica em $u = v$.

Ou seja, $p - (n + m) = (p - n) - m$.

O_4. Sejam $n - m = u$, com $u \in \mathbb{N}$, tal que $n = m + u$ e $q - p = v$, com $v \in \mathbb{N}$, tal que $q = p + v$.

Observe que: $n + q = (m + u) + (p + v) = (m + p) + (u + v)$.

Ou seja, $(n + q) - (m + p) = u + v$.

Segue que $(n + q) - (m + p) = u + v = (n - m) + (q - p)$.

O_5. *Reflexiva:*

Basta observar que $m = m + 0$.

O_6. *Antissimétrica:*

Por hipótese, $m \leq n$, ou seja, $n = m + u$ para algum $u \in \mathbb{N}$; e $n \leq m$, ou seja, $m = n + v$ para algum $v \in \mathbb{N}$.

Daí, $m = n + v = (m + u) + v = m + (u + v)$.

De A_4 (proposição 4.7), segue que $u + v = 0$; e de A_5 (proposição 4.7), segue que $u = v = 0$. Portanto, $m = n$.

O_7. *Transitiva:*

Por hipótese, $m \leq n$, ou seja, $n = m + u$ para algum $u \in \mathbb{N}$; e $n \leq p$, ou seja, $p = n + v$ para algum $v \in \mathbb{N}$.

Daí, $p = n + v = (m + u) + v = m + (u + v)$, ou seja, $m \leq p$.

O_8. Para cada $n \in \mathbb{N}$, seja S_n o subconjunto de $\mathbb{N}$ formado pelos elementos p para os quais, ao menos uma das opções é válida:

(i) existe $u \in \mathbb{N}$ tal que $n = p + u$;

(ii) existe $v \in \mathbb{N}$ tal que $p = n + v$.

Observe que, quando $p = 0$, o item (i) é válido com $u = n$, logo, $0 \in S_n$.

Seja $r \in S_n$. Se $r = n$, então $r^+ = n^+ = n + 1$ e, portanto, $r^+ \in S_n$, pois satisfaz o item (ii).

Suponhamos agora $n = r + u$, $u \neq 0$; daí, $u = v^+ = v + 1$ para algum $v \in \mathbb{N}$; logo, $n = r + (v + 1) = r + (1 + v) = (r + 1) + v = r^+ + v$, ou seja, r^+ satisfaz o item (i) e, portanto, $r^+ \in S_n$.

Se $r = n + v$, $v \neq 0$, então $r^+ = (n + v)^+ = n + v^+$, o que significa que $r^+ \in S_n$, pois satisfaz o item (ii).

Segue que $S_n = \mathbb{N}$ e, para todo $n \in \mathbb{N}$, qualquer que seja $m \in \mathbb{N}$, ou $n = m + u$ ou $m = n + v$ com $u, v \in \mathbb{N}$. Ou seja, $m \leq n$ ou $n \leq m$.

O_9. *Compatibilidade com a adição:*

Por hipótese, $m \leq n$, ou seja, $n = m + u$ para algum $u \in \mathbb{N}$.

Veja que $n + p = (m + u) + p = m + (u + p) = m + (p + u) = (m + p) + u$. Portanto, $m + p \leq n + p$.

O_{10}. *Compatibilidade com a multiplicação:*

Por hipótese, $m \leq n$, ou seja, $n = m + u$ para algum $u \in \mathbb{N}$.

Veja que $n \cdot p = (m + u) \cdot p = m \cdot p + u \cdot p$. Portanto, $m \cdot p \leq n \cdot p$.

O_{11}. Sendo $m < n$, sabemos que $m \leq n$ e $m \neq n$. Então, existe $u \in \mathbb{N}$, $u \neq 0$ tal que $n = m + u$. Como $u \neq 0$, $u = v+$ para algum $v \in \mathbb{N}$, ou seja, $u = v + 1$. Daí, $n = m + u = m + (v + 1) = (m + 1) + v$. Segue que $m + 1 \leq n$.

O_{12}. *Princípio do menor número natural:*

Seja $S \subset \mathbb{N}$ um conjunto não vazio. Define-se $H = \{n \in \mathbb{N} \mid n \leq x, \forall x \in S\}$. Como $0 \leq m$, $\forall m \in S$, então $0 \in H$.

Tomemos $m \in S$, o que é possível, pois $S \neq \varnothing$. Observando que $m < m+1$, pode-se afirmar que $m + 1 \notin H$ e, portanto, $H \neq \mathbb{N}$.

Levando P_5 em consideração, necessariamente existe um elemento $p \in \mathbb{N}$ tal que $p \in H$ e $p + 1 \notin H$. Mostremos que p é o menor elemento de S. De fato:

- Como $p \in H$, então $p \leq x$, $\forall x \in S$.
- Vamos supor que $p \notin S$. Então $p < x$, para todo $x \in S$, e daí $p + 1 \leq x$, também para todo $x \in S$, o que implica $p + 1 \in H$. Mas isto é impossível. Esta contradição nos leva a concluir que $p \in S$.

■

As propriedades O_5, O_6, O_7, O_8, O_9 e O_{10}, comprovam que a relação de ordem total $\leq$ sobre $\mathbb{N}$ é compatível com as operações adição e multiplicação definidas em $\mathbb{N}$.

Como vimos anteriormente, quando $a \leq b$ é possível definir a operação subtração. Entretanto, sabemos que esta operação não se estende ao conjunto de todos os números naturais.

Veremos, no próximo capítulo, como definir um conjunto de forma que seja possível estabelecer a operação subtração para todos os números naturais.

5 Números Inteiros

Buscamos agora dar sentido matemático a todas as expressões do tipo $n - m$, para quaisquer $m, n \in \mathbb{N}$, e não apenas para os casos em que $m \leq n$.

Para tanto, faz-se necessário definir um novo conjunto de forma que a extensão da definição de subtração em $\mathbb{N} \times \mathbb{N}$ seja uma operação binária para este novo conjunto. Como veremos, este novo conjunto é denominado conjunto dos números inteiros e é denotado por $\mathbb{Z}$, o qual definimos na sequência.

Vale ressaltar que para esse capítulo também usamos como referência básica a obra de Domingues, H. H. *Fundamentos de Aritmética*, [3].

5.1 Construção do Conjunto $\mathbb{Z}$

Primeiramente observe que dados quaisquer $m, n, p, q \in \mathbb{N}$, tais que $m \leq n$ e $p \leq q$, temos:

$$n - m = q - p \Leftrightarrow n + p = m + q$$

Definição 5.1. *No conjunto* $\mathbb{N} \times \mathbb{N}$ *definimos a seguinte relação binária* $\sim$*:*

$$\forall (m, n), (p, q) \in \mathbb{N} \times \mathbb{N} : (m, n) \sim (p, q) \Leftrightarrow m + q = n + p.$$

Proposição 5.2. *A relação* $\sim$ *é uma relação de equivalência em* $\mathbb{N} \times \mathbb{N}$.

Demonstração: Para a relação $\sim$ valem as propriedades:

(i) Reflexiva: para todo $(m, n) \in \mathbb{N} \times \mathbb{N}$, sabemos pela propriedade A_2 (proposição 4.7) que $m + n = n + m$, então $(m, n) \sim (m, n)$.

(ii) Simétrica: para todo $(m, n), (p, q) \in \mathbb{N} \times \mathbb{N}$, se $(m, n) \sim (p, q)$, então $m + q = n + p$. Sabemos pela propriedade A_2 (proposição 4.7) que:

$$m + q = q + m$$

e

$$n + p = p + n.$$

Logo,

$$q + m = p + n \Leftrightarrow p + n = q + m.$$

Então $(p, q) \sim (m, n)$.

Portanto, se $(m, n) \sim (p, q)$ então $(p, q) \sim (m, n)$.

(iii) Transitiva: para todo $(m, n), (p, q), (r, s) \in \mathbb{N} \times \mathbb{N}$, sabemos que:

$$\text{se } (m, n) \sim (p, q) \text{ então } m + q = n + p$$

e

$$\text{se } (p, q) \sim (r, s) \text{ então } p + s = q + r.$$

Daí,

$$m + q = n + p \Leftrightarrow m + q + s = n + p + s$$

e

$$p + s = q + r \Leftrightarrow p + s + n = q + r + n.$$

O que implica que:

$$m + q + s = q + r + n \Leftrightarrow q + (m + s) = q + (r + n) \Leftrightarrow m + s = r + n.$$

Logo, $(m, n) \sim (r, s)$.

Ou seja, se $(m, n) \sim (p, q)$ e $(p, q) \sim (r, s)$ então $(m, n) \sim (r, s)$.

■

Sendo $\sim$ uma relação de equivalência em $\mathbb{N} \times \mathbb{N}$, esta determina uma partição neste conjunto por classes de equivalência.

Indicaremos por $\overline{(m, n)}$ a classe de equivalência determinada por $(m, n) \in \mathbb{N} \times \mathbb{N}$, a saber,

$$\overline{(m, n)} = \{(x, y) \in \mathbb{N} \times \mathbb{N} \ / \ (x, y) \sim (m, n)\} = \{(x, y) \in \mathbb{N} \times \mathbb{N} \ / \ x + n = y + m\}.$$

Exemplo 5.3. Vejamos algumas classes de equivalência:

$$\overline{(1, 0)} = \{(2, 1); (3, 2); (4, 3); (5; 4); \cdots\};$$
$$\overline{(2, 0)} = \{(3, 1); (4, 2); (5, 3); (6; 4); \cdots\};$$
$$\overline{(0, 1)} = \{(1, 2); (2, 3); (3, 4); (4; 5); \cdots\};$$
$$\overline{(4, 2)} = \{(2, 0); (3, 1); (4, 2); (5; 3); \cdots\}.$$

Definição 5.4. *O conjunto quociente de $\mathbb{N}\times\mathbb{N}$ por $\sim$, ou seja, o conjunto de todas as classes $\overline{(m,n)}$, para qualquer $(m,n)\in\mathbb{N}\times\mathbb{N}$, será indicado por $\mathbb{Z}$ e denominamos o conjunto dos números inteiros.*

Isto é,

$$\mathbb{Z} := \frac{\mathbb{N}\times\mathbb{N}}{\sim} = \{\overline{(m,n)} \;/\; (m,n)\in\mathbb{N}\times\mathbb{N}\}.$$

Observação 5.5. Vale ressaltar que

$$\overline{(m,n)} = \overline{(p,q)} \Leftrightarrow (m,n)\sim(p,q) \Leftrightarrow m+q = n+p.$$

Proposição 5.6. *Em particular, temos que:*

(i) se $n\leq m$, então $\overline{(m,n)} = \overline{(m-n,0)}$;

(ii) se $m\leq n$, então $\overline{(m,n)} = \overline{(0,n-m)}$;

(iii) se $m=n$, então $\overline{(m,n)} = \overline{(0,0)}$.

Demonstração: De fato:

(i) Basta verificar que $m+0 = n+(m-n)$.

Como $n\leq m$, existe $u\in\mathbb{N}$ tal que $m = n+u$ e, como visto anteriormente, indicamos u por $m-n$, ou seja,

$$m+0 = m = n+u = n+(m-n)$$

Segue que se $n\leq m$ então $\overline{(m,n)} = \overline{(m-n,0)}$.

(ii) Basta verificar que $m+(n-m) = n+0$.

Como $m\leq n$, existe $u\in\mathbb{N}$ tal que $n = m+u$ e, como visto anteriormente, indicamos u por $n-m$, ou seja,

$$n+0 = n = m+u = m+(n-m)$$

Segue que se $m\leq n$ então $\overline{(m,n)} = \overline{(0,n-m)}$.

(iii) Se $m=n$, então $\overline{(m,n)} = \overline{(m,m)}$.

Para provar que $\overline{(m,m)} = \overline{(0,0)}$ basta observar que $m+0 = m+0$, ou seja, que $m=m$.

Segue que se $m=n$ então $\overline{(m,n)} = \overline{(0,0)}$.

■

Exemplo 5.7. Note que: $\overline{(1,3)} = \overline{(0,2)}$ e $\overline{(4,2)} = \overline{(2,0)}$.

Observação 5.8. Sendo $a \in \mathbb{Z}$, $a = \overline{(m,n)}$, denotaremos por $(-a)$ a classe $\overline{(n,m)}$.

Mais ainda, observe que se $a \in \mathbb{Z}$, então $a = \overline{(m,0)}$, $a = \overline{(0,m)}$ ou $a = \overline{(0,0)}$, para algum $m \in \mathbb{N}$, segundo a proposição 5.6. Sendo assim, podemos denotar

$$\begin{gathered}\overline{(0,0)} = 0\\ \overline{(1,0)} = 1 \text{ e } \overline{(0,1)} = -1;\\ \overline{(2,0)} = 2 \text{ e } \overline{(0,2)} = -2;\\ \overline{(3,0)} = 3 \text{ e } \overline{(0,3)} = -3;\\ .\\ .\\ .\end{gathered}$$

Podemos então exibir o conjunto $\mathbb{Z}$ de números inteiros da seguinte forma:

$$\mathbb{Z} = \{\cdots, -3, -2, -1, 0, 1, 2, 3, \cdots\}.$$

Também podemos escrever o conjunto dos números inteiros positivos $\mathbb{Z}_+ = \{0, 1, 2, 3, \cdots\}$ e o conjunto dos números inteiros negativos $\mathbb{Z}_- = \{\cdots, -3, -2, -1, 0\}$.

Observe que temos ainda o conjunto dos números inteiros que são estritamente positivos $\mathbb{Z}_+^* = \{1, 2, 3, \cdots\}$ e o conjunto dos números inteiros que são estritamente negativos $\mathbb{Z}_-^* = \{\cdots, -3, -2, -1\}$.

Proposição 5.9. *$a \in \mathbb{Z}_+$ (ou $\mathbb{Z}_+^*$) se, e somente se, $(-a) \in \mathbb{Z}_-$ (ou $\mathbb{Z}_-^*$).*

Demonstração: De fato, se $a \in \mathbb{Z}_+$ (ou $\mathbb{Z}_+^*$), $a = \overline{(m,0)}$ para algum $m \in \mathbb{N}$. Logo, $(-a) = \overline{(0,m)}$, que pertence a $\mathbb{Z}_-$ (ou $\mathbb{Z}_-^*$). ■

5.2 Adição em $\mathbb{Z}$

A fim de entendermos melhor a definição que segue, considere o seguinte exemplo:

Exemplo 5.10. Se os números naturais 4 e 5 são escritos da forma: $5 = 6-1$ e $4 = 9-5$, então:

$$5 + 4 = (6 - 1) + (9 - 5) = (6 + 9) - (1 + 5) = 15 - 6 = 9.$$

Definição 5.11. *Dados $a = \overline{(m,n)}$ e $b = \overline{(p,q)}$ elementos quaisquer de $\mathbb{Z}$, definimos a aplicação binária, que chamaremos de adição, dada por:*

$$\begin{array}{rccc} + : & \mathbb{Z} \times \mathbb{Z} & \longrightarrow & \mathbb{Z} \\ & (a,b) & \longmapsto & a + b \end{array}$$

em que

$$a + b := \overline{(m + p, n + q)}.$$

Lema 5.12. *A aplicação anterior está bem definida.*

Demonstração: Sejam $\overline{(m,n)} = \overline{(m_1,n_1)}$ e $\overline{(p,q)} = \overline{(p_1,q_1)}$ elementos em $\mathbb{Z}$. Mostremos que

$$\overline{(m,n)} + \overline{(p,q)} = \overline{(m_1,n_1)} + \overline{(p_1,q_1)}.$$

Veja que, por definição de +,

$$\overline{(m,n)} + \overline{(p,q)} = \overline{(m+p,n+q)}$$
$$\text{e}$$
$$\overline{(m_1,n_1)} + \overline{(p_1,q_1)} = \overline{(m_1+p_1,n_1+q_1)}.$$

Porém $(m,n) \sim (m_1,n_1)$ e $(p,q) \sim (p_1,q_1)$, logo

$$m + n_1 = n + m_1$$
$$\text{e}$$
$$p + q_1 = q + p_1.$$

Somando membro a membro as igualdades anteriores, obtemos:

$$(m + n_1) + (p + q_1) = (q + p_1) + (n + m_1)$$
$$\text{e}$$
$$(m + p) + (n_1 + q_1) = (n + q) + (m_1 + p_1)$$

Consequentemente,

$$\overline{(m+p,n+q)} = \overline{(m_1+p_1,n_1+q_1)},$$

ou seja,

$$\overline{(m,n)} + \overline{(p,q)} = \overline{(m_1,n_1)} + \overline{(p_1,q_1)}.$$

■

A seguir, trataremos de propriedades da adição no conjunto dos números inteiros.

Proposição 5.13. *Para a adição em* $\mathbb{Z}$ *valem as seguintes propriedades:*

A_1. *Associativa: dados* $a,b,c \in \mathbb{Z}$ *temos* $(a + b) + c = a + (b + c)$.

A_2. *Comutativa: dados* $a,b \in \mathbb{Z}$ *temos* $a + b = b + a$.

A_3. *Elemento neutro: para qualquer* $a \in \mathbb{Z}$ *temos que* $a + 0 = a$.

A_4. *Simétrico aditivo: para todo* $a \in \mathbb{Z}$, *existe* $(-a) \in \mathbb{Z}$ *de modo que* $a + (-a) = 0$.

A_5. *Lei do cancelamento: dados* $a,b,c \in \mathbb{Z}$, $a + c = b + c \Leftrightarrow a = b$.

Demonstração: Usando a definição 5.11 e a proposição 4.7, faremos as demonstrações de cada propriedade acima.

A_1. *Associativa:*

Sejam $a, b, c \in \mathbb{Z}$ tais que $a = \overline{(m,n)}$, $b = \overline{(p,q)}$ e $c = \overline{(r,s)}$. Daí,

$$\begin{gathered}(a+b)+c = (\overline{(m,n)} + \overline{(p,q)}) + \overline{(r,s)} = \overline{(m+p, n+q)} + \overline{(r,s)} = \\ \overline{((m+p)+r, (n+q)+s)} = \overline{(m+(p+r), n+(q+s))} = \overline{(m,n)} + \overline{(p+r, q+s)} = \\ \overline{(m,n)} + (\overline{(p,q)} + \overline{(r,s)}) = a + (b+c).\end{gathered}$$

A_2. *Comutativa:*

Sejam $a, b, \in \mathbb{Z}$ tais que $a = \overline{(m,n)}$ e $b = \overline{(p,q)}$. Daí,

$$a + b = \overline{(m,n)} + \overline{(p,q)} = \overline{(m+p, n+q)} = \overline{(p+m, q+n)} = \overline{(p,q)} + \overline{(m,n)} = b + a.$$

A_3. *Elemento neutro:*

Seja $a \in \mathbb{Z}$ tal que $a = \overline{(m,n)}$, segue que:

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

A_4. *Simétrico aditivo:*

Pela observação 5.8, dado $a = \overline{(m,n)}$, então $(-a) = \overline{(n,m)}$.

Logo, $a + (-a) = \overline{(m,n)} + \overline{(n,m)} = \overline{(m+n, n+m)} = \overline{(m+n, m+n)}$.

Pela proposição 5.6, temos que $\overline{(m+n, m+n)} = \overline{(0,0)}$.

Portanto, $a + (-a) = 0$.

A_5. *Lei do cancelamento:*

Seja $a, b, c \in \mathbb{Z}$ e $a + c = b + c$, segue que:

$$a = a + 0 = a + (c + (-c)) = (a + c) + (-c) = (b + c) + (-c) = b + (c + (-c)) = b + 0 = b.$$

■

Lema 5.14. *Das propriedades anteriores,*

(i) O elemento neutro é único;

(ii) Dado $a \in \mathbb{Z}$ existe um único $(-a) \in \mathbb{Z}$ tal que $a + (-a) = 0$.

Demonstração: Provemos tais itens:

(i) Vamos supor que exista $k \in \mathbb{Z}$ tal que $a + k = a$, para qualquer $a \in \mathbb{Z}$. Mostremos que $k = 0$.

Observe que $a+k = a = a+0$, ou seja, $a+k = a+0$. Segue, pela lei do cancelamento, que $k = 0$.

(ii) Vamos supor que exista $k \in \mathbb{Z}$ tal que $a + k = 0$, para qualquer $a \in \mathbb{Z}$. Mostremos que $k = (-a)$.

Observe que $a + k = 0 = a + (-a)$, ou seja, $a + k = a + (-a)$. Segue, pela lei do cancelamento, que $k = (-a)$.

■

Observação 5.15. Para quaisquer $a, b \in \mathbb{Z}$ temos que:

(i) $(-a) + (-b)$ é o simétrico aditivo de $a + b$. De fato:

$$(a + b) + ((-a) + (-b)) = (a + (-a)) + (b + (-b)) = 0 + 0 = 0.$$

(ii) $(a + (-b)) + b = a$. Pois:

$$(a + (-b)) + b = a + ((-b) + b) = a + 0 = a.$$

5.3 Subtração em $\mathbb{Z}$

Chamaremos diferença entre a e b e indicaremos por $a - b$ o elemento $a + (-b) \in \mathbb{Z}$. Ou seja,

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

Note que, pela propriedade A_4 da proposição 5.13, é possível definir $a - b \in \mathbb{Z}$ para quaisquer $a, b \in \mathbb{Z}$.

Definição 5.16. *Dados a, b elementos quaisquer de $\mathbb{Z}$, definimos a seguinte aplicação binária, que nomearemos de subtração em $\mathbb{Z}$, dada por:*

$$\begin{array}{rccc} - : & \mathbb{Z} \times \mathbb{Z} & \longrightarrow & \mathbb{Z} \\ & (a, b) & \longmapsto & a - b. \end{array}$$

Observemos que a subtração não é associativa, nem comutativa e nem admite elemento neutro.

Em particular, pela observação 5.15 veja que $(-a) + (-b) = -(a + b) = -a - b$.

Exemplo 5.17. A subtração não é associativa.

Sejam $a, b, c \in \mathbb{Z}$ dados por $a = \overline{(1, 2)}$, $b = \overline{(2, 0)}$ e $c = \overline{(4, 7)}$. Daí,

$$a-(b-c)=a-(b+(-c))=\overline{(1,2)}-(\overline{(2,0)}+\overline{(7,4)})=\overline{(1,2)}-\overline{(2+7,0+4)}=$$
$$\overline{(1,2)}-\overline{(9,4)}=\overline{(1,2)}+\overline{(4,9)}=\overline{(1+4,2+9)}=\overline{(5,11)}$$
e
$$(a-b)-c=(a+(-b))+(-c)=(\overline{(1,2)}+\overline{(0,2)})+\overline{(7,4)}=\overline{(1+0,2+2)}+\overline{(7,4)}=$$
$$\overline{(1,4)}+\overline{(7,4)}=\overline{(1+7,4+4)}=\overline{(8,8)}.$$

Note que $\overline{(5,11)}\neq\overline{(8,8)}$, pois $5+8\neq 11+8$.

Exemplo 5.18. A subtração não é comutativa.

Sejam $a,b\in\mathbb{Z}$ dados por $a=\overline{(3,5)}$ e $b=\overline{(1,2)}$. Daí,

$$a-b=a+(-b)=\overline{(3,5)}+\overline{(2,1)}=\overline{(3+2,5+1)}=\overline{(5,6)}$$
e
$$b-a=b+(-a)=\overline{(1,2)}+\overline{(5,3)}=\overline{(1+5,2+3)}=\overline{(6,5)}.$$

Note que $\overline{(5,6)}\neq\overline{(6,5)}$, pois $5+5\neq 6+6$.

5.4 Multiplicação em $\mathbb{Z}$

A fim de entendermos melhor a definição que segue, considere o seguinte exemplo:

Exemplo 5.19. Se os números naturais 4 e 5 são escritos da forma: $5=6-1$ e $4=9-5$, então:

$$5\cdot 4=(6-1)\cdot(9-5)=(6\cdot 9+1\cdot 5)-(6\cdot 5+1\cdot 9)=(54+5)-(30+9)=59-39=20.$$

Definição 5.20. *Sejam $a=\overline{(m,n)}$ e $b=\overline{(p,q)}$ elementos quaisquer de $\mathbb{Z}$, definimos a aplicação binária, que chamaremos de multiplicação, dada por:*

$$\begin{array}{rccc}\cdot: & \mathbb{Z}\times\mathbb{Z} & \longrightarrow & \mathbb{Z}\\ & (a,b) & \longmapsto & a\cdot b\end{array}$$

em que:

$$a\cdot b:=\overline{(m\cdot p+n\cdot q,m\cdot q+n\cdot p)}.$$

Lema 5.21. *A operação acima está bem definida.*

Demonstração: Sejam $\overline{(m,n)}=\overline{(m_1,n_1)}$ e $\overline{(p,q)}=\overline{(p_1,q_1)}$ elementos de $\mathbb{Z}$.

Mostremos que:

$$\overline{(m,n)}\cdot\overline{(p,q)}=\overline{(m_1,n_1)}\cdot\overline{(p_1,q_1)}.$$

Note que:

$$\overline{(m,n)} \cdot \overline{(p,q)} = \overline{(m \cdot p + n \cdot q, m \cdot q + n \cdot p)}$$
e
$$\overline{(m_1,n_1)} \cdot \overline{(p_1,q_1)} = \overline{(m_1 \cdot p_1 + n_1 \cdot q_1, m_1 \cdot q_1 + n_1 \cdot p_1)}.$$

Entretanto $(m,n) \sim (m_1,n_1)$ e $(p,q) \sim (p_1,q_1)$, assim

$$m + n_1 = n + m_1$$
e
$$p + q_1 = q + p_1.$$

Obtemos:

$$p \cdot (m + n_1) = p \cdot (n + m_1);$$
$$m_1 \cdot (p + q_1) = m_1 \cdot (q + p_1);$$
$$q \cdot (n + m_1) = q \cdot (m + n_1) \text{ e}$$
$$n_1 \cdot (q + p_1) = n_1 \cdot (p + q_1).$$

Desenvolvendo os produtos acima e somando-os membro a membro, segue que:

$$p \cdot m + p \cdot n_1 + m_1 \cdot p + m_1 \cdot q_1 + q \cdot n + q \cdot m_1 + n_1 \cdot q + n_1 \cdot p_1 =$$
$$p \cdot n + p \cdot m_1 + m_1 \cdot q + m_1 \cdot p_1 + q \cdot m + q \cdot n_1 + n_1 \cdot p + n_1 \cdot q_1.$$

Pela lei do cancelamento (proposição 4.7),

$$(m \cdot p + n \cdot q) + (m_1 \cdot q_1 + n_1 \cdot p_1) = (n \cdot p + m \cdot q) + (m_1 \cdot p_1 + n_1 \cdot q_1),$$

e por fim,

$$\overline{(m \cdot p + n \cdot q, m \cdot q + n \cdot p)} = \overline{(m_1 \cdot p_1 + n_1 \cdot q_1, m_1 \cdot q_1 + n_1 \cdot p_1)}.$$

Ou seja,

$$\overline{(m,n)} \cdot \overline{(p,q)} = \overline{(m_1,n_1)} \cdot \overline{(p_1,q_1)}.$$

■

A seguir, algumas propriedades da multiplicação no conjunto dos números inteiros.

Proposição 5.22. *Para a multiplicação em* $\mathbb{Z}$ *valem as seguintes propriedades:*

M_1. *Associativa: dados* $a,b,c \in \mathbb{Z}$, $(a \cdot b) \cdot c = a \cdot (b \cdot c)$.

M_2. *Comutativa: dados* $a,b \in \mathbb{Z}$, $a \cdot b = b \cdot a$.

M_3. *Elemento identidade: para qualquer* $a \in \mathbb{Z}$, $a \cdot 1 = a$.

M_4. *Lei do anulamento do produto: para todo* $a,b \in \mathbb{Z}$, *se* $a \cdot b = 0$, *então* $a = 0$ *ou* $b = 0$.

M_5. *Distributiva: dados* $a,b,c \in \mathbb{Z}$, $a \cdot (b + c) = a \cdot b + a \cdot c$.

Demonstração: As demonstrações de cada propriedade da multiplicação em $\mathbb{Z}$ seguem usando a definição 5.20 e a proposição 4.9, de fato:

M_1. *Associativa:*

Sejam $a, b, c \in \mathbb{Z}$ tais que $a = \overline{(m,n)}$, $b = \overline{(p,q)}$ e $c = \overline{(r,s)}$. Daí,

$$\begin{gathered}(a \cdot b) \cdot c = (\overline{(m,n)} \cdot \overline{(p,q)}) \cdot \overline{(r,s)} = \overline{(m \cdot p + n \cdot q, m \cdot q + n \cdot p)(r,s)} = \\ \overline{((m \cdot p + n \cdot q) \cdot r + (m \cdot q + n \cdot p) \cdot s, (m \cdot p + n \cdot q) \cdot s + (m \cdot q + n \cdot p) \cdot r)} = \\ \overline{(m \cdot p \cdot r + n \cdot q \cdot r + m \cdot q \cdot s + n \cdot p \cdot s, m \cdot p \cdot s + n \cdot q \cdot s + m \cdot q \cdot r + n \cdot p \cdot r)} = \\ \overline{(m \cdot p \cdot r + m \cdot q \cdot s + n \cdot q \cdot r + n \cdot p \cdot s, m \cdot p \cdot s + m \cdot q \cdot r + n \cdot q \cdot s + n \cdot p \cdot r)} = \\ \overline{(m \cdot (p \cdot r + q \cdot s) + n \cdot (q \cdot r + p \cdot s), m \cdot (p \cdot s + q \cdot r) + n \cdot (q \cdot s + p \cdot r))} = \\ \overline{(m,n)} \cdot (\overline{(p,q)} \cdot \overline{(r,s)}) = a \cdot (b \cdot c).\end{gathered}$$

M_2. *Comutativa:*

Sejam $a, b, \in \mathbb{Z}$ tais que $a = \overline{(m,n)}$ e $b = \overline{(p,q)}$. Daí,

$$\begin{gathered}a \cdot b = \overline{(m,n)} \cdot \overline{(p,q)} = \overline{(m \cdot p + n \cdot q, m \cdot q + n \cdot p)} = \overline{(p \cdot m + q \cdot n, q \cdot m + p \cdot n)} = \\ \overline{(p,q)} \cdot \overline{(m,n)} = b \cdot a.\end{gathered}$$

M_3. *Elemento identidade:*

Seja $a \in \mathbb{Z}$ tal que $a = \overline{(m,n)}$. Daí,

$$a \cdot 1 = \overline{(m,n)} \cdot \overline{(1,0)} = \overline{(m \cdot 1 + n \cdot 0, m \cdot 0 + n \cdot 1)} = \overline{(m+0, 0+n)} = \overline{(m,n)} = a.$$

M_4. *Lei do anulamento do produto:*

Como já observamos anteirormente na proposição 5.6, todo elemento de $\mathbb{Z}$ pode ser representado como $\overline{(0,m)}, \overline{(m,0)}$ ou $\overline{(0,0)}$ para algum $m \in \mathbb{N}$.

Note que, para os casos em que a ou b são iguais a $\overline{(0,0)}$, o resultado já está satisfeito. Além desses casos, teremos quatro possíveis combinações para efetuar $a \cdot b$:

1^o **caso:** Sejam $a = \overline{(m,0)}$ e $b = \overline{(n,0)}$, logo:

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

Para que $\overline{(m \cdot n, 0)} = \overline{(0,0)}$, devemos ter $m \cdot n + 0 = 0 + 0$, ou seja, $m \cdot n = 0$. Daí, $m = 0$ ou $n = 0$. Ou seja, $a = \overline{(0,0)}$ ou $b = \overline{(0,0)}$.

2^o **caso:** Sejam $a = \overline{(0,m)}$ e $b = \overline{(0,n)}$, logo:

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

Para que $\overline{(m\cdot n,0)} = \overline{(0,0)}$, devemos ter $m\cdot n+0 = 0+0$, ou seja, $m\cdot n = 0$. Daí, $m = 0$ ou $n = 0$. Ou seja, $a = \overline{(0,0)}$ ou $b = \overline{(0,0)}$.

3^o **caso:** Sejam $a = \overline{(0,m)}$ e $b = \overline{(n,0)}$, logo:

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

Para que $\overline{(0,m\cdot n)} = \overline{(0,0)}$, devemos ter $0+0 = m\cdot n$, ou seja, $m\cdot n = 0$. Daí, $m = 0$ ou $n = 0$. Ou seja, $a = \overline{(0,0)}$ ou $b = \overline{(0,0)}$.

4^o **caso:** Sejam $a = \overline{(m,0)}$ e $b = \overline{(0,n)}$, logo:

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

Para que $\overline{(0,m\cdot n)} = \overline{(0,0)}$, devemos ter $0+0 = m\cdot n$, ou seja, $m\cdot n = 0$. Daí, $m = 0$ ou $n = 0$. Ou seja, $a = \overline{(0,0)}$ ou $b = \overline{(0,0)}$.

M_5. *Distributiva:*

Sejam $a,b,c\in\mathbb{Z}$ tais que $a = \overline{(m,n)}$, $b = \overline{(p,q)}$ e $c = \overline{(r,s)}$. Daí,

$$\begin{gathered}
a\cdot(b+c) = \overline{(m,n)}\cdot(\overline{(p,q)}+\overline{(r,s)}) = \overline{(m,n)}\cdot\overline{(p+r,q+s)} = \\
\overline{((m\cdot(p+r)+n\cdot(q+s), m\cdot(q+s)+n\cdot(p+r))} = \\
\overline{(m\cdot p+m\cdot r+n\cdot q+n\cdot s, m\cdot q+m\cdot s+n\cdot p+n\cdot r)} = \\
\overline{(m\cdot p+n\cdot q, m\cdot q+n\cdot p)}+\overline{(m\cdot r+n\cdot s, m\cdot s+n\cdot r)} = \\
\overline{(m,n)}\cdot\overline{(p,q)}+\overline{(m,n)}\cdot\overline{(r,s)} = a\cdot b+a\cdot c.
\end{gathered}$$

■

Definição 5.23. *Dado um conjunto A munido de uma operação binária $\cdot$ e com a propriedade do elemento identidade $\boldsymbol{e}$ (ou seja, existe $\boldsymbol{e}\in A$ tal que $a\cdot\boldsymbol{e} = a = \boldsymbol{e}\cdot a$, para qualquer $a\in A$), dizemos que $b\in A$ é o elemento inverso de um elemento $a\in A$ se $a\cdot b = \boldsymbol{e} = b\cdot a$.*

Observação 5.24. Veja que para o conjunto dos números inteiros temos que os únicos elementos que possuem a propriedade do elemento inverso são $a_1 = \overline{(1,0)}$ e $a_2 = \overline{(0,1)}$, pois:

$$a_1\cdot a_1 = \overline{(1,0)}\cdot\overline{(1,0)} = \overline{(1\cdot 1+0\cdot 0, 1\cdot 0+0\cdot 1)} = \overline{(1,0)} = 1$$

e

$$a_2\cdot a_2 = \overline{(0,1)}\cdot\overline{(0,1)} = \overline{(0\cdot 0+1\cdot 1, 0\cdot 1+1\cdot 0)} = \overline{(1,0)} = 1.$$

Logo,

$$a_1\cdot a_1 = 1 \text{ e } a_2\cdot a_2 = 1.$$

Ou seja, o próprio a_1 é o elemento inverso de a_1 e o próprio a_2 é o elemento inverso de a_2.

5.5 Relação de ordem em $\mathbb{Z}$

Definição 5.25. *Sejam $a, b \in \mathbb{Z}$. Dizemos que a é menor ou igual a b e denotamos $a \leq b$, se para algum $r \in \mathbb{Z}_+$, $b = a + r$. Também podemos escrever b é maior ou igual a a e, neste caso, denotamos $b \geq a$.*

Caso $r \in \mathbb{Z}_+^*$, então dizemos que a é menor que b e denotamos $a < b$. Também podemos escrever b é maior que a e denotamos $b > a$.

Proposição 5.26. *Observemos que:*

(i) Dado $r \in \mathbb{Z}_+$, $0 \leq r$;

(ii) Dado $s \in \mathbb{Z}_-$, $s \leq 0$.

Demonstração: De fato,

(i) Dado $r \in \mathbb{Z}_+$, $r = 0 + r$.

(ii) Dado $s \in \mathbb{Z}_-$, $0 = s + (-s)$, com $(-s) \in \mathbb{Z}_+$.

■

A seguir veremos algumas propriedades acerca da relação de ordem.

Proposição 5.27. *A relação de ordem tem as seguintes propriedades:*

O_1. *Reflexiva: para qualquer $a \in \mathbb{Z}$, $a \leq a$.*

O_2. *Antissimétrica: para quaisquer $a, b \in \mathbb{Z}$, se $a \leq b$ e $b \leq a$, então $a = b$.*

O_3. *Transitiva: para quaisquer $a, b, c \in \mathbb{Z}$, se $a \leq b$ e $b \leq c$, então $a \leq c$.*

O_4. *Para quaisquer $a, b \in \mathbb{Z}$, $a \leq b$ ou $b \leq a$.*

O_5. *Compatibilidade com a adição: para quaisquer $a, b, c \in \mathbb{Z}$, se $a \leq b$, então $a + c \leq b + c$.*

O_6. *Compatibilidade com a multiplicação: para quaisquer $a, b, c \in \mathbb{Z}$ e $0 \leq c$, se $a \leq b$, então $a \cdot c \leq b \cdot c$.*

Demonstração: Façamos as demonstrações de cada propriedade da relação de ordem usando as proposições 4.7, 4.9, 5.13 e 5.22.

O_1. *Reflexiva:*

Basta observar que $a = a + 0$ e $0 \in \mathbb{Z}_+$.

O_2. *Antissimétrica:*

Por hipótese, $a \leq b$, ou seja, $b = a + r_1$ para algum $r_1 \in \mathbb{Z}_+$ e $b \leq a$, ou seja, $a = b + r_2$ para algum $r_2 \in \mathbb{Z}_+$. Sendo $r_1 \in \mathbb{Z}_+$ e $r_2 \in \mathbb{Z}_+$, podemos escrever $r_1 = \overline{(k,0)}$ e $r_2 = \overline{(l,0)}$, com $k, l \in \mathbb{N}$.

Daí, $a = b + r_2 = (a + r_1) + r_2 = a + (r_1 + r_2) = a + \overline{(k+l,0)}$.

O que implica, pela lei do cancelamento da adição, que $\overline{(k+l,0)} = \overline{(0,0)}$.

Logo, $k + l = 0$ e, portanto, pela proposição 4.7, $k = 0 = l$.

O_3. *Transitiva:*

Por hipótese, $a \leq b$ e $b \leq c$, ou seja, $b = a + r_1$ para algum $r_1 \in \mathbb{Z}_+$ e $c = b + r_2$ para algum $r_2 \in \mathbb{Z}_+$.

Daí, $c = b + r_2 = (a + r_1) + r_2 = a + (r_1 + r_2)$.

Note que se $r_1 \in \mathbb{Z}_+$ e $r_2 \in \mathbb{Z}_+$, $r_1 = \overline{(m,0)}$ para algum $m \in \mathbb{N}$ e $r_2 = \overline{(n,0)}$ para algum $n \in \mathbb{N}$. Segue que $r_1 + r_2 = \overline{(m,0)} + \overline{(n,0)} = \overline{(m+n,0)}$ e $\overline{(m+n,0)} \in \mathbb{Z}_+$.

Logo, $c = a + (r_1 + r_2)$ com $r_1 + r_2 \in \mathbb{Z}_+$.

Portanto, $a \leq c$.

O_4. Essa demonstração é feita considerando todas as possibilidades para elementos não nulos do conjunto dos números inteiros. Note que o caso de $a = 0$ ou $b = 0$ está contemplado na proposição 5.26.

1^o **caso:** $a = \overline{(m,0)}$ para algum $m \in \mathbb{N}$ e $b = \overline{(n,0)}$ para algum $n \in \mathbb{N}$.

Se $m \leq n$, então $n = m + l$ para algum $l \in \mathbb{N}$ e, portanto,

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

Como $\overline{(l,0)} \in \mathbb{Z}_+$, segue que $a \leq b$.

Se $n \leq m$, então $m = n + k$ para algum $k \in \mathbb{N}$ e, portanto,

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

Como $\overline{(k,0)} \in \mathbb{Z}_+$, segue que $b \leq a$.

2^o **caso:** $a = \overline{(0,m)}$ para algum $m \in \mathbb{N}$ e $b = \overline{(0,n)}$ para algum $n \in \mathbb{N}$.

Se $m \leq n$, então $n = m + l$ para algum $l \in \mathbb{N}$ e, portanto,

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

Daí,

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

Como $\overline{(l,0)} \in \mathbb{Z}_+$, segue que $b \leq a$.

Se $n \leq m$, então $m = n + k$ para algum $k \in \mathbb{N}$ e, portanto,

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

Daí,

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

Como $\overline{(k,0)} \in \mathbb{Z}_+$, segue que $a \leq b$.

3^o **caso:** $a = \overline{(m,0)}$ para algum $m \in \mathbb{N}$ e $b = \overline{(0,n)}$ para algum $n \in \mathbb{N}$.

Daí,

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

Como $\overline{(m+n,0)} \in \mathbb{Z}_+$, segue que $b \leq a$.

Portanto, para quaisquer $a, b \in \mathbb{Z}$, $a \leq b$ ou $b \leq a$.

O_5. *Compatibilidade com a adição:*

Se $a \leq b$, segue que $b = a + r$ para algum $r \in \mathbb{Z}_+$. Assim, para todo $c \in \mathbb{Z}$ temos que:

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

Daí, $a + c \leq b + c$.

Portanto, dados $a, b, c \in \mathbb{Z}$, se $a \leq b$, então $a + c \leq b + c$.

O_6. *Compatibilidade com a multiplicação:*

Por hipótese, $a \leq b$, ou seja, $b = a + r$ para algum $r \in \mathbb{Z}_+$, e com isso $r = \overline{(k,0)}$ para algum $k \in \mathbb{N}$.

Seja $0 \leq c$, então $c \in \mathbb{Z}_+$, e $c = \overline{(m,0)}$ para algum $m \in \mathbb{N}$.

Segue que:

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

Note que, dado $c = \overline{(m,0)}$ e $r = \overline{(k,0)}$, temos $c \cdot r \in \mathbb{Z}_+$, pois:

$$c \cdot r = \overline{(m,0)} \cdot \overline{(k,0)} = \overline{(m \cdot k + 0 \cdot 0, m \cdot 0 + 0 \cdot k)} = \overline{(m \cdot k, 0)}.$$

Ou seja, $b \cdot c = a \cdot c + c \cdot r$ com $c \cdot r \in \mathbb{Z}_+$.

Logo, $a \cdot c \leq b \cdot c$.

■

5.6 Divisibilidade em $\mathbb{Z}$

Definição 5.28. *Sejam a e b elementos quaisquer de $\mathbb{Z}$. Considere o conjunto $\mathcal{D}_{\mathbb{Z}} = \{(a,b) \in \mathbb{Z}\times\mathbb{Z} \mid a = k\cdot b \text{ para algum } k \in \mathbb{Z}\}$. Definimos a aplicação, que chamaremos de divisão, dada por:*

$$\begin{array}{rccc} \div : & \mathcal{D}_{\mathbb{Z}} & \longrightarrow & \mathbb{Z} \\ & (a,b) & \longmapsto & a \div b \end{array}$$

em que:

$$a \div b := \frac{a}{b} = k.$$

Ao número $k = \dfrac{a}{b}$ denominamos fração ordinária.

Assim como no conjunto dos números naturais, ao número a e ao número b denominamos, respectivamente, numerador e denominador.

Notemos que não é possível estender a operação divisão a todos os elementos de $\mathbb{Z}\times\mathbb{Z}$.

Exemplo 5.29. A seguir, alguns casos do conjunto dos números inteiros onde a operação divisão está definida:

4 é divisível por -2, bastando considerar que $4 = (-2)\cdot(-2)$, ou seja, $\dfrac{4}{-2} = -2$;

-16 é divisível por -4, bastando considerar que $-16 = 4\cdot(-4)$, ou seja, $\dfrac{-16}{-4} = 4$;

15 é divisível por 3, bastando considerar que $15 = 5\cdot 3$, ou seja, $\dfrac{15}{3} = 5$.

Exemplo 5.30. A seguir, alguns casos do conjunto dos números inteiros onde a operação divisão não está definida:

$\dfrac{5}{-2}$ não está definido em $\mathbb{Z}$, pois $(5,-2) \notin \mathcal{D}_{\mathbb{Z}}$.

$\dfrac{-7}{-3}$ não está definido em $\mathbb{Z}$, pois $(-7,-3) \notin \mathcal{D}_{\mathbb{Z}}$.

$\dfrac{11}{5}$ não está definido em $\mathbb{Z}$, pois $(11,5) \notin \mathcal{D}_{\mathbb{Z}}$.

Definição 5.31. *Sejam a e b elementos quaisquer de $\mathbb{Z}$. Um elemento $d \in \mathbb{Z}$ se diz máximo divisor comum de a e b se satisfaz as seguintes condições:*

(i) $d \geq 0$;

(ii) $(a,d) \in \mathcal{D}_{\mathbb{Z}}$ *e* $(b,d) \in \mathcal{D}_{\mathbb{Z}}$;

(iii) Se $d' \in \mathbb{Z}$ *é tal que* $(a,d') \in \mathcal{D}_{\mathbb{Z}}$ *e* $(b,d') \in \mathcal{D}_{\mathbb{Z}}$, *então* $(d,d') \in \mathcal{D}_{\mathbb{Z}}$.

Usaremos a notação $d = mdc(a,b)$.

Exemplo 5.32. No caso de $a = 10$ e $b = 8$, o número 2 é o único inteiro que satisfaz as condições da definição 5.31. Segue que:

$$mdc(10,8) = 2.$$

Definição 5.33. *Dada a fração ordinária* $\frac{a}{b}$, *se* $mdc(a,b) = 1$ *dizemos que a fração é irredutível.*

Notemos que as únicas frações irredutíveis no conjunto dos números inteiros são aquelas cujo denominador é 1 ou -1.

No próximo capítulo trataremos do conjunto dos números racionais, para o qual veremos que a aplicação divisão é uma operação binária.

Veremos ainda que esse fato está intrinsecamente relacionado com a propriedade do elemento inverso, a qual será válida para qualquer número racional não nulo.

Para finalizarmos esse capítulo, abordamos a imersão do conjunto dos números naturais no conjunto dos números inteiros.

5.7 Imersão de $\mathbb{N}$ em $\mathbb{Z}$

Neste momento, a partir das construções do conjunto dos números naturais e do conjunto dos números inteiros, veremos como considerar $\mathbb{N}$ como sendo parte de $\mathbb{Z}$.

Para tanto, seja a função f definida por:

$$\begin{array}{rccc} f: & \mathbb{N} & \longrightarrow & \mathbb{Z} \\ & n & \longmapsto & \overline{(n,0)} \end{array}$$

para todo $n \in \mathbb{N}$.

Ou seja,

$$\begin{aligned} f(0) &= \overline{(0,0)} = 0 \\ f(1) &= \overline{(1,0)} = 1 \\ f(2) &= \overline{(2,0)} = 2 \\ f(3) &= \overline{(3,0)} = 3 \\ &\vdots \end{aligned}$$

A função f considerada é chamada de *imersão* de $\mathbb{N}$ em $\mathbb{Z}$.

Observação 5.34. $Im(f) = \{f(n) \ / \ n \in \mathbb{N}\} = \mathbb{Z}_+ = \{0,1,2,3,\cdots\}$.

Proposição 5.35. *f é injetora.*

Demonstração: Dados $m, n \in \mathbb{N}$,

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

■

Proposição 5.36. *Dados $m, n \in \mathbb{N}$, temos que:*

(i) $f(m+n) = f(m) + f(n)$;

(ii) $f(m \cdot n) = f(m) \cdot f(n)$;

(iii) *Se $m \leq n$, então $f(m) \leq f(n)$.*

Demonstração: Dados $m, n \in \mathbb{N}$,

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

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

(iii) Se $m \leq n$, então $n = m + u$ para algum $u \in \mathbb{N}$ e, portanto,

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

em que $\overline{(u,0)} \in \mathbb{Z}_+$.

O que significa que $f(m) \leq f(n)$.

■

Sobretudo, veja que pela observação 5.34 e pela proposição 5.35, ao restringir o contradomínio de f, obtemos uma bijeção entre os conjuntos $\mathbb{N}$ e $\mathbb{Z}_+$, dada por:

$$n \longmapsto \overline{(n,0)} \tag{5.1}$$

Nesse sentido, podemos identificar $\mathbb{N}$ com $\mathbb{Z}_+$.

Ainda, como $\mathbb{Z}_+ \subset \mathbb{Z}$, fazemos um abuso de notação ao considerar $\mathbb{N} \subset \mathbb{Z}$ para indicar a imersão de $\mathbb{N}$ em $\mathbb{Z}$.

Desta maneira, o número natural 0 corresponde ao inteiro $0 = \overline{(0,0)}$, o número natural 1 corresponde ao inteiro $1 = \overline{(1,0)}$, e assim por diante.

Observação 5.37. Dado $a = \overline{(m,n)} \in \mathbb{Z}$, note que

$$a = \overline{(m,n)} = \overline{(m,0)} + \overline{(0,n)} = \overline{(m,0)} + [-\overline{(n,0)}].$$

Devido à imersão em questão, concluímos que $a = m - n$. Ou seja, acabamos de concluir que todo número inteiro é uma diferença entre dois números naturais.

Note, por fim, que dados $m, n \in \mathbb{N}$,

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

Neste contexto, podemos dizer que a subtração de dois números naturais é sempre possível em $\mathbb{Z}$; fato este que foi a motivação da construção dos números inteiros.

6 Números Racionais

Buscamos neste momento dar sentido matemático a todas as expressões do tipo $\frac{a}{b}$, para quaisquer $a, b \in \mathbb{Z}$, e não apenas para os casos em que $(a, b) \in \mathcal{D}_{\mathbb{Z}}$ (vide definição 5.28).

Para tanto, faz-se necessário definir um outro conjunto de forma que a extensão da aplicação divisão em $\mathbb{Z} \times \mathbb{Z}$ seja uma operação binária para este novo conjunto. Como veremos, este novo conjunto é denominado conjunto dos números racionais $\mathbb{Q}$, o qual definimos na sequência.

Para esse capítulo ainda usamos como referência básica a obra de Domingues, H. H. *Fundamentos de Aritmética*, [3].

Definição 6.1. *Denote* $\mathbb{Z}^* = \{a \in \mathbb{Z} \ / \ a \neq 0\}$.

Para o conjunto $\mathbb{Z} \times \mathbb{Z}^* = \{(a, b) \ / \ a \in \mathbb{Z},\ b \in \mathbb{Z}^*\}$, *definimos a seguinte relação binária* $\sim$*:*

$$\forall (a, b), (c, d) \in \mathbb{Z} \times \mathbb{Z}^* : (a, b) \sim (c, d) \Leftrightarrow a \cdot d = b \cdot c.$$

Proposição 6.2. *A relação* $\sim$ *é uma relação de equivalência em* $\mathbb{Z} \times \mathbb{Z}^*$.

Demonstração: Para a relação $\sim$ valem as propriedades:

(i) Reflexiva: Para todo $(a, b) \in \mathbb{Z} \times \mathbb{Z}^*$, sabemos pela propriedade M_2 (proposição 5.22) que $a \cdot b = b \cdot a$, então $(a, b) \sim (a, b)$.

(ii) Simétrica: Para quaisquer $(a, b), (c, d) \in \mathbb{Z} \times \mathbb{Z}^*$, se $(a, b) \sim (c, d)$, então $a \cdot d = b \cdot c$. Sabemos pela propriedade M_2 (proposição 5.22) que:

$$a \cdot d = d \cdot a$$

e

$$b \cdot c = c \cdot b.$$

Logo,

$$a \cdot d = b \cdot c \Leftrightarrow d \cdot a = c \cdot b \Leftrightarrow c \cdot b = d \cdot a.$$

Então $(c,d) \sim (a,b)$.

Portanto, se $(a,b) \sim (c,d)$, então $(c,d) \sim (a,b)$.

(iii) Transitiva: Para quaisquer $(a,b),(c,d),(e,f) \in \mathbb{Z} \times \mathbb{Z}^*$, sabemos que:

$$\text{se } (a,b) \sim (c,d) \text{ então } a \cdot d = b \cdot c$$

e

$$\text{se } (c,d) \sim (e,f) \text{ então } c \cdot f = d \cdot e.$$

Daí, como a operação está bem definida no conjunto dos números inteiros, segue que:

$$a \cdot d = b \cdot c \Leftrightarrow (a \cdot d) \cdot f = (b \cdot c) \cdot f$$

e

$$c \cdot f = d \cdot e \Leftrightarrow (c \cdot f) \cdot b = (d \cdot e) \cdot b.$$

O que implica, pelas propriedades M_1 e M_2 (proposição 5.22), que:

$$(a \cdot d) \cdot f = (b \cdot c) \cdot f = (c \cdot b) \cdot f = c \cdot (b \cdot f) = c \cdot (f \cdot b) = (c \cdot f) \cdot b = (d \cdot e) \cdot b.$$

Ou seja,

$$(a \cdot d) \cdot f = (d \cdot e) \cdot b \Leftrightarrow a \cdot (d \cdot f) = d \cdot (e \cdot b) \Leftrightarrow a \cdot (f \cdot d) = d \cdot (b \cdot e) \Leftrightarrow (a \cdot f) \cdot d = (b \cdot e) \cdot d \Leftrightarrow a \cdot f = b \cdot e.$$

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

Ou seja, se $(a,b) \sim (c,d)$ e $(c,d) \sim (e,f)$, então $(a,b) \sim (e,f)$.

■

Sendo $\sim$ uma relação de equivalência em $\mathbb{Z} \times \mathbb{Z}^*$, esta determina uma partição neste conjunto por classes de equivalência.

Indicaremos por $\frac{a}{b}$ a classe de equivalência determinada por $(a,b) \in \mathbb{Z} \times \mathbb{Z}^*$, a saber,

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

Exemplo 6.3. Vejamos algumas classes de equivalência:

$\frac{1}{3} = \{(x,y) \in \mathbb{Z} \times \mathbb{Z}^* \ / \ (x,y) \sim (1,3)\} = \{(x,y) \in \mathbb{Z} \times \mathbb{Z}^* \ / \ x \cdot 3 = y \cdot 1\}.$

Ou seja, $\frac{1}{3} = \{(-2,-6),(-1,-3),(1,3),(2,6),\cdots\}$.

$\frac{2}{5} = \{(x,y) \in \mathbb{Z} \times \mathbb{Z}^* \ / \ (x,y) \sim (2,5)\} = \{(x,y) \in \mathbb{Z} \times \mathbb{Z}^* \ / \ x \cdot 5 = y \cdot 2\}.$

Isto é, $\frac{2}{5} = \{(-4,-10),(-2,-5),(2,5),(4,10),\cdots\}$.

Observação 6.4. Veja que segue da propriedade reflexiva o fato de $(a,b) \in \frac{a}{b}$ para todo $(a,b) \in \mathbb{Z} \times \mathbb{Z}^*$.

Ainda,

$$\frac{a}{b} = \frac{c}{d} \Leftrightarrow (a,b) \sim (c,d).$$

Ou seja,

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

Exemplo 6.5. $\frac{1}{3} = \frac{-1}{-3} = \frac{-2}{-6} = \frac{2}{6} = \cdots$.

Ao conjunto de todas as classes de equivalência determinadas por $\sim$ sobre $\mathbb{Z} \times \mathbb{Z}^*$ denominamos conjunto dos números racionais e denotamos por $\mathbb{Q}$.

Ou seja,

$$\mathbb{Q} = \left\{ \frac{a}{b} \ / \ (a,b) \in \mathbb{Z} \times \mathbb{Z}^* \right\}.$$

Sendo assim, cada $x \in \mathbb{Q}$ admite infinitas representações $\frac{a}{b}$ com $a \in \mathbb{Z}$ e $b \in \mathbb{Z}^*$.

Assim como no conjunto dos números naturais e no conjunto dos números inteiros, ao número a e b denominamos numerador e denominador, respectivamente.

Os elementos de $\mathbb{Q}$ são chamados números racionais.

Proposição 6.6. *Dados $x, y \in \mathbb{Q}$, sempre é possível exibir suas representações com denominadores iguais.*

Demonstração: Sejam $x, y \in \mathbb{Q}$ tais que $x = \frac{a}{b}$ e $y = \frac{c}{d}$.

Observemos que da proposição 5.22, temos que $a \cdot (b \cdot d) = b \cdot (a \cdot d)$ e $c \cdot (b \cdot d) = d \cdot (b \cdot c)$.

Da definição da relação $\sim$, concluímos que $(a,b) \sim (a \cdot d, b \cdot d)$ e $(c,d) \sim (b \cdot c, b \cdot d)$.

Por fim,

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

■

Observação 6.7. A classe de equivalência

$$\cdots = \frac{0}{-2} = \frac{0}{-1} = \frac{0}{1} = \frac{0}{2} = \cdots$$

é indicada apenas por 0. Enquanto que a classe de equivalência

$$\cdots = \frac{-2}{-2} = \frac{-1}{-1} = \frac{1}{1} = \frac{2}{2} = \cdots$$

é representada por 1.

Ainda, dado $x = \frac{a}{b} \in \mathbb{Q}$, indicamos neste conjunto o elemento $\frac{-a}{b}$ por $-x$.

Para $x = \frac{a}{b} \in \mathbb{Q}$ e $x \neq 0$, denotamos neste conjunto o elemento $\frac{b}{a}$ por x^{-1}.

Veremos mais adiante as justificativas para essas notações.

6.1 Adição em $\mathbb{Q}$

Definição 6.8. *Sejam x, y elementos quaisquer de $\mathbb{Q}$ tais que $x = \frac{a}{b}$ e $y = \frac{c}{d}$. Definimos a aplicação binária adição da seguinte forma:*

$$\begin{array}{rccc} + : & \mathbb{Q}\times\mathbb{Q} & \longrightarrow & \mathbb{Q} \\ & (x,y) & \longmapsto & x+y \end{array}$$

em que

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

Lema 6.9. *A adição no conjunto dos números racionais está bem definida.*

Demonstração: Sejam $\frac{a}{b} = \frac{a_1}{b_1}$ e $\frac{c}{d} = \frac{c_1}{d_1}$ elementos quaisquer de $\mathbb{Q}$.

Sabemos que

$$a\cdot b_1 = b\cdot a_1 \text{ e } c\cdot d_1 = d\cdot c_1.$$

Ainda, pela proposição 5.22, segue que

$$a\cdot b_1 = b\cdot a_1 \Leftrightarrow (a\cdot b_1)\cdot(d\cdot d_1) = (b\cdot a_1)\cdot(d\cdot d_1)$$
e
$$c\cdot d_1 = d\cdot c_1 \Leftrightarrow (c\cdot d_1)\cdot(b\cdot b_1) = (d\cdot c_1)\cdot(b\cdot b_1)$$

Somando as igualdades termo a termo, obtemos:

$$a\cdot b_1\cdot d\cdot d_1 + c\cdot d_1\cdot b\cdot b_1 = b\cdot a_1\cdot d\cdot d_1 + d\cdot c_1\cdot b\cdot b_1.$$

Ou seja,

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

Portanto, segue da definição que

$$\frac{a\cdot d + c\cdot b}{b\cdot d} = \frac{a_1\cdot d_1 + c_1\cdot b_1}{b_1\cdot d_1}.$$

Consequentemente,

$$\frac{a}{b} + \frac{c}{d} = \frac{a_1}{b_1} + \frac{c_1}{d_1}.$$

■

A seguir, trataremos de propriedades da adição no conjunto dos números racionais.

Proposição 6.10. *Para a adição em $\mathbb{Q}$ valem as seguintes propriedades:*

A_1. *Associativa: dados $x, y, z \in \mathbb{Q}$, temos $(x + y) + z = x + (y + z)$.*

A_2. *Comutativa: dados $x, y \in \mathbb{Q}$, temos $x + y = y + x$.*

A_3. *Elemento neutro: para qualquer* $x \in \mathbb{Q}$, *temos que* $x + 0 = x$.

A_4. *Simétrico aditivo: para todo* $x \in \mathbb{Q}$, *existe* $(-x) \in \mathbb{Q}$ *de modo que* $x + (-x) = 0$.

Demonstração: Vejamos a demonstração de cada propriedade da adição em $\mathbb{Q}$. Observe que usaremos as propriedades já demonstradas para o conjunto dos números inteiros (proposição 5.13 e proposição 5.22) e a definição da adição no conjunto dos números racionais (definição 6.8).

A_1. *Associativa:*

Sejam $x, y, z \in \mathbb{Q}$ tais que $x = \frac{a}{b}$, $y = \frac{c}{d}$ e $z = \frac{e}{f}$. Daí,

$$(x+y)+z = \left(\frac{a}{b}+\frac{c}{d}\right)+\frac{e}{f} = \frac{a\cdot d+b\cdot c}{b\cdot d}+\frac{e}{f} = \frac{(a\cdot d+b\cdot c)\cdot f+(b\cdot d)\cdot e}{(b\cdot d)\cdot f} =$$
$$\frac{(a\cdot d)\cdot f+(b\cdot c)\cdot f+(b\cdot d)\cdot e}{(b\cdot d)\cdot f} = \frac{a\cdot(d\cdot f)+b\cdot(c\cdot f)+b\cdot(d\cdot e)}{b\cdot(d\cdot f)} =$$
$$\frac{a\cdot(d\cdot f)+b\cdot(c\cdot f+d\cdot e)}{b\cdot(d\cdot f)} = \frac{a}{b}+\frac{c\cdot f+d\cdot e}{d\cdot f} = \frac{a}{b}+\left(\frac{c}{d}+\frac{e}{f}\right) = x+(y+z).$$

A_2. *Comutativa:*

Sejam $x, y \in \mathbb{Q}$ tais que $x = \frac{a}{b}$ e $y = \frac{c}{d}$. Então,

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

A_3. *Elemento neutro:* O elemento neutro é a classe de equivalência do zero, ou seja,

$$0 = \cdots = \frac{0}{-2} = \frac{0}{-1} = \frac{0}{1} = \frac{0}{2} = \cdots.$$

Uma vez que a adição está bem definida no conjunto dos números racionais, usaremos a fração ordinária $\frac{0}{1}$ para a demonstração desse item.

Seja $x \in \mathbb{Q}$ tal que $x = \frac{a}{b}$. Daí,

$$x+0 = \frac{a}{b}+\frac{0}{1} = \frac{a\cdot 1+0\cdot b}{b\cdot 1} = \frac{a}{b} = x.$$

Portanto, para qualquer $x \in \mathbb{Q}$, temos que $x + 0 = x$

A_4. *Simétrico aditivo:*

Já ressaltamos anteriormente que, dado $x \in \mathbb{Q}$ tal que $x = \frac{a}{b}$, indicamos $(-x) = \frac{-a}{b}$.

Agora a notação é justificada, considerando que:

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

■

Definição 6.11. *Sejam x, y elementos quaisquer de $\mathbb{Q}$. Definimos a aplicação binária subtração entre x e y, que indicamos por $x-y$, da seguinte forma:*

$$\begin{array}{rccc} -: & \mathbb{Q}\times\mathbb{Q} & \longrightarrow & \mathbb{Q} \\ & (x,y) & \longmapsto & x-y \end{array}$$

em que

$$x-y=x+(-y)$$

A seguir veremos algumas propriedades sobre a subtração no conjunto dos números racionais.

Proposição 6.12. *Dados $x, y, z \in \mathbb{Q}$, as seguintes propriedades são válidas:*

(i) $-(x+y)=-x-y$;

(ii) $(x-y)+y=x$;

(iii) $x+z=y \Leftrightarrow z=y-x$;

(iv) $x+y=x+z \Leftrightarrow y=z$.

Demonstração: A seguir, a demonstração de cada item da proposição acima.

(i) Dados $x, y \in \mathbb{Q}$, observe que:

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

Ou seja,

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

(ii) Dados $x, y \in \mathbb{Q}$, temos que:

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

(iii) Sejam $x, y, z \in \mathbb{Q}$ tais que $x+z=y$. Então,

$$x+z=y \Leftrightarrow (-x)+(x+z)=(-x)+y \Leftrightarrow ((-x)+x)+z=y+(-x) \Leftrightarrow$$
$$0+z=y-x \Leftrightarrow z=y-x.$$

(iv) Sejam $x, y, z \in \mathbb{Q}$ tais que $x+y=x+z$. Segue que:

$$x+y=x+z \Leftrightarrow (-x)+(x+y)=(-x)+(x+z) \Leftrightarrow$$
$$((-x)+x)+y=((-x)+x)+z \Leftrightarrow 0+y=0+z \Leftrightarrow y=z.$$

■

6.2 Multiplicação em $\mathbb{Q}$

Definição 6.13. *Sejam x, y elementos quaisquer de $\mathbb{Q}$ tais que $x = \frac{a}{b}$ e $y = \frac{c}{d}$. Definimos a aplicação binária multiplicação da seguinte forma:*

$$\begin{array}{rccc} \cdot : & \mathbb{Q}\times\mathbb{Q} & \longrightarrow & \mathbb{Q} \\ & (x,y) & \longmapsto & x\cdot y \end{array}$$

em que

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

Lema 6.14. *A operação acima está bem definida.*

Demonstração: Sejam $\frac{a}{b} = \frac{a_1}{b_1}$ e $\frac{c}{d} = \frac{c_1}{d_1}$ elementos quaisquer de $\mathbb{Q}$.

Sabemos que

$$\frac{a}{b} = \frac{a_1}{b_1} \Leftrightarrow a\cdot b_1 = b\cdot a_1$$
$$\text{e}$$
$$\frac{c}{d} = \frac{c_1}{d_1} \Leftrightarrow c\cdot d_1 = d\cdot c_1.$$

Multiplicando as igualdades, segue que

$$(a\cdot b_1)\cdot(c\cdot d_1) = (b\cdot a_1)\cdot(d\cdot c_1) \Leftrightarrow (a\cdot c)\cdot(b_1\cdot d_1) = (b\cdot d)\cdot(a_1\cdot c_1) \Leftrightarrow \frac{a\cdot c}{b\cdot d} = \frac{a_1\cdot c_1}{b_1\cdot d_1}.$$

Consequentemente,

$$\frac{a}{b}\cdot\frac{c}{d} = \frac{a_1}{b_1}\cdot\frac{c_1}{d_1}.$$

■

Observação 6.15. Note que se $x = \frac{a}{b}$ e $y = \frac{c}{b}$, ou seja, ambos tem o mesmo denominador, temos:

$$x+y = \frac{a}{b}+\frac{c}{b} = \frac{a\cdot b + b\cdot c}{b\cdot b} = \frac{b\cdot(a+c)}{b\cdot b} = \frac{b}{b}\cdot\frac{a+c}{b} = 1\cdot\frac{a+c}{b} = \frac{a+c}{b}.$$

Logo,

$$\frac{a}{b}+\frac{c}{b} = \frac{a+c}{b}.$$

A seguir, algumas propriedades da multiplicação no conjunto dos números racionais.

Proposição 6.16. *Para a multiplicação em $\mathbb{Q}$ valem as seguintes propriedades:*

M_1. *Associativa: dados $x, y, z \in \mathbb{Q}$, $(x\cdot y)\cdot z = x\cdot(y\cdot z)$.*

M_2. *Comutativa: dados $x, y \in \mathbb{Q}$, $x\cdot y = y\cdot x$.*

M_3. *Elemento identidade: para qualquer $x \in \mathbb{Q}$, $x\cdot 1 = x$.*

M_4. *Inverso multiplicativo: para qualquer* $x \in \mathbb{Q}$, $x \neq 0$, *existe* x^{-1} *tal que* $x \cdot x^{-1} = 1$.

M_5. *Distributiva: dados* $x, y, z \in \mathbb{Q}$, $x \cdot (y + z) = x \cdot y + x \cdot z$.

Demonstração: As demonstrações de cada propriedade da multiplicação em $\mathbb{Q}$ seguem usando a definição 6.13 e a proposição 5.22.

M_1. *Associativa:*

Sejam $x, y, z \in \mathbb{Q}$ tais que $x = \frac{a}{b}$, $y = \frac{c}{d}$ e $z = \frac{e}{f}$. Daí,

$$\left(\frac{a}{b} \cdot \frac{c}{d}\right) \cdot \frac{e}{f} = \frac{a \cdot c}{b \cdot d} \cdot \frac{e}{f} = \frac{(a \cdot c) \cdot e}{(b \cdot d) \cdot f} = \frac{a \cdot (c \cdot e)}{b \cdot (d \cdot f)} = \frac{a}{b} \cdot \frac{c \cdot e}{d \cdot f} = \frac{a}{b} \cdot \left(\frac{c}{d} \cdot \frac{e}{f}\right).$$

Portanto,

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

M_2. *Comutativa:*

Sejam $x, y \in \mathbb{Q}$ tais que $x = \frac{a}{b}$ e $y = \frac{c}{d}$. Então,

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

M_3. *Elemento identidade:*

O elemento identidade é a classe de equivalência do um, ou seja,

$$1 = \cdots = \frac{-2}{-2} = \frac{-1}{-1} = \frac{1}{1} = \frac{2}{2} = \cdots.$$

Uma vez que a adição está bem definida no conjunto dos números racionais, usaremos a fração ordinária $\frac{1}{1}$ para a demonstração desse item.

Seja $x \in \mathbb{Q}$ tal que $x = \frac{a}{b}$. Daí,

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

Portanto, para qualquer $x \in \mathbb{Q}$, temos que $x \cdot 1 = x$

M_4. *Inverso multiplicativo:*

Seja $x \in \mathbb{Q}$ tal que $x = \frac{a}{b}$. Sendo $x \neq 0$, temos que $a \neq 0$. Sendo assim, $\frac{b}{a} \in \mathbb{Q}$.

Definimos o inverso de x como $x^{-1} = \frac{b}{a}$.

Daí,

$$x \cdot x^{-1} = \frac{a}{b} \cdot \frac{b}{a} = \frac{a \cdot b}{b \cdot a} = \frac{a \cdot b}{a \cdot b} = 1.$$

M_5. *Distributiva:*

Sejam $x, y, z \in \mathbb{Q}$ tais que $x = \frac{a}{b}, y = \frac{c}{d}$ e $z = \frac{e}{f}$.

Para essa demonstração, faremos uso da observação 6.15.

$$x \cdot (y + z) = \frac{a}{b} \cdot (\frac{c}{d} + \frac{e}{f}) = \frac{a}{b} \cdot (\frac{c \cdot f + d \cdot e}{d \cdot f}) = \frac{a \cdot (c \cdot f + d \cdot e)}{b \cdot (d \cdot f)} = \frac{a \cdot c \cdot f + a \cdot d \cdot e}{b \cdot d \cdot f} =$$
$$\frac{a \cdot c \cdot f}{b \cdot d \cdot f} + \frac{a \cdot d \cdot e}{b \cdot d \cdot f} = \frac{a \cdot c}{b \cdot d} \cdot \frac{f}{f} + \frac{a \cdot e}{b \cdot f} \cdot \frac{d}{d} = \frac{a \cdot c}{b \cdot d} \cdot 1 + \frac{a \cdot e}{b \cdot f} \cdot 1 = \frac{a \cdot c}{b \cdot d} + \frac{a \cdot e}{b \cdot f} = \frac{a}{b} \cdot \frac{c}{d} + \frac{a}{b} \cdot \frac{e}{f}$$

■

Por fim, no próximo capítulo faremos uso da definição que segue.

Definição 6.17. *Dados $u \in \mathbb{Q}$ e $n \in \mathbb{N}$, definimos u^n como sendo a multiplicação $u \cdot u \cdot u \cdots u$ com n fatores u. Ou seja,*

$$u^n = u \cdot u \cdot u \cdots u, \text{ com } n \text{ fatores } u.$$

6.3 Relação de ordem em $\mathbb{Q}$

No intuito de estabelecer uma relação de ordem no conjunto dos números racionais, sempre é possível considerar uma representação em que o denominador seja maior que zero.

Primeiramente observamos que, sendo $x \in \mathbb{Q}$, se $x = \frac{a}{b}$ é uma representação, temos:

$$\frac{a}{b} = \frac{-a}{-b}.$$

Daí, se $b > 0$, $-(b) < 0$.

Por exemplo, $\frac{-3}{-4} = \frac{3}{4}$ e $\frac{7}{-3} = \frac{-7}{3}$.

Definição 6.18. *Sejam $x, y \in \mathbb{Q}$ tais que $x = \frac{a}{b}$ e $y = \frac{c}{d}$, cujos denominadores são maiores que zero. Dizemos que x é menor ou igual a y e denotamos $x \leq y$, se $a \cdot d \leq b \cdot c$. Também podemos escrever y é maior ou igual a x e, nesse caso, denotamos $y \geq x$.*

Dizemos ainda que x é menor que y e denotamos $x < y$ se $a \cdot d < b \cdot c$. Também podemos escrever y é maior que x e denotamos $y > x$.

Exemplo 6.19. $\frac{-1}{5} < \frac{1}{3}$, pois $(-1) \cdot 3 < 5 \cdot 1$.

A seguir veremos algumas propriedades acerca da relação de ordem no conjunto dos números racionais.

Proposição 6.20. *A relação de ordem tem as seguintes propriedades:*

O_1. *Reflexiva: para qualquer $x \in \mathbb{Q}$, $x \leq x$.*

O_2. *Antissimétrica: para quaisquer $x, y \in \mathbb{Q}$, se $x \leq y$ e $y \leq x$, então $x = y$.*

O_3. *Transitiva: para quaisquer $x, y, z \in \mathbb{Q}$, se $x \leq y$ e $y \leq z$, então $x \leq z$.*

O_4. *Para quaisquer $x, y \in \mathbb{Q}$, $x \leq y$ ou $y \leq x$.*

O_5. *Compatibilidade com a adição: para quaisquer $x, y, z \in \mathbb{Q}$, se $x \leq y$, então $x + z \leq y + z$.*

O_6. *Compatibilidade com a multiplicação: para quaisquer $x, y, z \in \mathbb{Z}$ e $0 \leq z$, se $x \leq y$, então $x \cdot z \leq y \cdot z$.*

Demonstração: Façamos as demonstrações de cada propriedade da relação de ordem usando as proposições 4.7, 4.9, 5.13 e 5.22.

O_1. *Reflexiva:*

Seja $x \in \mathbb{Q}$, $x = \dfrac{a}{b}$. Basta observar que $a \cdot b \leq b \cdot a$ (item O_1 da proposição 5.27).

Segue que $x \leq x$.

O_2. *Antissimétrica:*

Sejam $x, y \in \mathbb{Q}$ quaisquer. Suponha que $x = \dfrac{a}{b}$ e $y = \dfrac{c}{d}$.

Se $x \leq y$, então $a \cdot d \leq b \cdot c$. Analogamente, se $y \leq x$, então $c \cdot b \leq d \cdot a$.

Daí, $a \cdot d = b \cdot c$ (item O_2 da proposição 5.27). O que implica que $\dfrac{a}{b} = \dfrac{c}{d}$.

Portanto, se $x \leq y$ e $y \leq x$, segue que $x = y$.

O_3. *Transitiva:*

Sejam $x, y, z \in \mathbb{Q}$ e suponha $x = \dfrac{a}{b}$, $y = \dfrac{c}{d}$ e $z = \dfrac{e}{f}$.

Se $x \leq y$, então $a \cdot d \leq b \cdot c$. Analogamente, se $y \leq z$, então $c \cdot f \leq d \cdot e$.

Uma vez que $a \cdot d \leq b \cdot c$, ao multiplicarmos a desigualdade por $f > 0$, temos que $a \cdot d \cdot f \leq b \cdot c \cdot f$.

Da mesma forma, tendo $c \cdot f \leq d \cdot e$, ao multiplicarmos a desigualdade por $b > 0$, temos que $c \cdot f \cdot b \leq d \cdot e \cdot b$. Ou seja,

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

Segue pelo item O_3 da proposição 5.27 que $a \cdot d \cdot f \leq d \cdot e \cdot b$.

Sendo $d > 0$, temos que $a \cdot f \leq e \cdot b$.

Portanto, $\frac{a}{b} \leq \frac{c}{d}$.

Assim, se $x \leq y$ e $y \leq z$, então $x \leq z$.

O_4. Sejam $x, y \in \mathbb{Q}$ tais que $x = \frac{a}{b}$ e $y = \frac{c}{d}$. Observe que

$$a \cdot d \leq b \cdot c \text{ ou } c \cdot b \leq d \cdot a.$$

Ou seja,

$$\frac{a}{b} \leq \frac{c}{d} \text{ ou } \frac{c}{d} \leq \frac{a}{b}.$$

Portanto,

$$x \leq y \text{ ou } y \leq x.$$

O_5. *Compatibilidade com a adição:*

Sejam $x, y, z \in \mathbb{Q}$ tais que $x \leq y$. Considere $x = \frac{a}{b}$, $y = \frac{c}{d}$ e $z = \frac{e}{f}$.

Como $x \leq y$, temos que $\frac{a}{b} \leq \frac{c}{d}$. Daí,

$$\frac{a}{b} \leq \frac{c}{d} \Leftrightarrow a \cdot d \leq b \cdot c \Leftrightarrow a \cdot d \cdot f \cdot f \leq b \cdot c \cdot f \cdot f \Leftrightarrow a \cdot f \cdot d \cdot f \leq b \cdot f \cdot c \cdot f \Leftrightarrow$$
$$a \cdot f \cdot d \cdot f + b \cdot e \cdot d \cdot f \leq b \cdot f \cdot c \cdot f + b \cdot e \cdot d \cdot f \Leftrightarrow a \cdot f \cdot d \cdot f + b \cdot e \cdot d \cdot f \leq b \cdot f \cdot c \cdot f + b \cdot f \cdot d \cdot e \Leftrightarrow$$
$$(a \cdot f + b \cdot e) \cdot d \cdot f \leq b \cdot f \cdot (c \cdot f + \cdot d \cdot e) \Leftrightarrow \frac{a \cdot f + b \cdot e}{b \cdot f} \leq \frac{c \cdot f + \cdot d \cdot e}{d \cdot f} \Leftrightarrow \frac{a}{b} + \frac{e}{f} \leq \frac{c}{d} + \frac{e}{f}.$$

Ou seja,

$$x + z \leq y + z.$$

O_6. *Compatibilidade com a multiplicação:*

Sejam $x, y, z \in \mathbb{Q}$ tais que $0 \leq z$ e $x \leq y$. Suponha que $x = \frac{a}{b}$, $y = \frac{c}{d}$ e $z = \frac{e}{f}$ são tais que b, d e f são maiores que zero.

Uma vez que $0 \leq z = \frac{e}{f}$, então $0 \leq e \cdot f$.

Como $x \leq y$, temos que $\frac{a}{b} \leq \frac{c}{d}$.

Daí,

$$\frac{a}{b} \leq \frac{c}{d} \Leftrightarrow a \cdot d \leq b \cdot c \Leftrightarrow (a \cdot d) \cdot (e \cdot f) \leq (b \cdot c) \cdot (e \cdot f) \Leftrightarrow a \cdot d \cdot e \cdot f \leq b \cdot c \cdot e \cdot f \Leftrightarrow$$
$$a \cdot e \cdot d \cdot f \leq b \cdot f \cdot c \cdot e \Leftrightarrow \frac{a \cdot e}{b \cdot f} \leq \frac{c \cdot e}{d \cdot f} \Leftrightarrow \frac{a}{b} \cdot \frac{e}{f} \leq \frac{c}{d} \cdot \frac{e}{f}.$$

Ou seja,

$$x \cdot z \leq y \cdot z.$$

■

6.4 Imersão de $\mathbb{Z}$ em $\mathbb{Q}$

Vejamos a seguir como estabelecer uma imersão de $\mathbb{Z}$ em $\mathbb{Q}$. Desejamos, por exemplo, que o elemento 2 no conjunto dos números inteiros e o elemento $\frac{6}{3} = \{(-4,-2);(-2,-1);(2,1);(4,2);\cdots\}$ no conjunto dos números racionais sejam identificados.

Para tanto, seja f a função definida por:

$$\begin{array}{rccc} f: & \mathbb{Z} & \longrightarrow & \mathbb{Q} \\ & a & \longmapsto & \dfrac{a}{1} \end{array}$$

para todo $a \in \mathbb{Z}$.

Ou seja,

$$\vdots$$
$$f(-3) = \frac{-3}{1}$$
$$f(-2) = \frac{-2}{1}$$
$$f(-1) = \frac{-1}{1}$$
$$f(0) = \frac{0}{1}$$
$$f(1) = \frac{1}{1}$$
$$f(2) = \frac{2}{1}$$
$$f(3) = \frac{3}{1}$$
$$\vdots$$

A função f considerada é chamada de imersão de $\mathbb{Z}$ em $\mathbb{Q}$.

Proposição 6.21. *f é injetora.*

Demonstração: Dados $a, b \in \mathbb{Z}$,

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

■

Proposição 6.22. *Dados $a, b \in \mathbb{Z}$, temos que:*

(i) $f(a+b) = f(a) + f(b)$;

(ii) $f(a \cdot b) = f(a) \cdot f(b)$;

(iii) *Se $a \leq b$, então $f(a) \leq f(b)$.*

Demonstração: Dados $a, b \in \mathbb{Z}$,

(i) $f(a+b) = \dfrac{a+b}{1} = \dfrac{a \cdot 1 + 1 \cdot b}{1 \cdot 1} = \dfrac{a}{1} + \dfrac{b}{1} = f(a) + f(b)$.

(ii) $f(a \cdot b) = \dfrac{a \cdot b}{1} = \dfrac{a \cdot b}{1 \cdot 1} = \dfrac{a}{1} \cdot \dfrac{b}{1} = f(a) \cdot f(b)$.

(iii) Se $a \leq b$, então $a \cdot 1 \leq b \cdot 1$ e, daí, $\dfrac{a}{1} \leq \dfrac{b}{1}$. Portanto, $f(a) \leq f(b)$.

■

Note que, das proposições acima, a imagem de $\mathbb{Z}$ pela função f, ou seja,

$$Im(f) = \left\{ \frac{a}{1} \;/\; a \in \mathbb{Z} \right\}$$

pode ser vista como uma cópia de $\mathbb{Z}$.

Nesse sentido, podemos identificar $\mathbb{Z}$ com $Im(f)$. Como $Im(f) \subset \mathbb{Q}$, então fazendo um abuso de notação, consideramos $\mathbb{Z} \subset \mathbb{Q}$ para indicar a imersão de $\mathbb{Z}$ em $\mathbb{Q}$.

Desta maneira, o número inteiro -1 corresponde ao racional $\dfrac{-1}{1}$, o número inteiro 0 corresponde ao racional $\dfrac{0}{1}$, o número natural 1 corresponde ao inteiro $\dfrac{1}{1}$, o número natural 2 corresponde ao inteiro $\dfrac{2}{1}$ e assim por diante.

Observação 6.23. Dados $a, b \in \mathbb{Z}$, $b \neq 0$, note que

$$a \div b = \frac{a}{1} \div \frac{b}{1} = \frac{a}{1} \cdot \frac{1}{b} = \frac{a \cdot 1}{1 \cdot b} = \frac{a}{b} \in \mathbb{Q}.$$

E ainda, dado $\dfrac{a}{b} \in \mathbb{Q}$ qualquer, temos que:

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

Neste contexto, podemos dizer que a divisão de dois números inteiros é sempre possível em $\mathbb{Q}$ (considerando o denominador não nulo); fato este que foi a motivação da construção dos números racionais.

Como podemos perceber, o conjunto dos números racionais tem uma boa estrutura algébrica, no seguinte sentido: as operações adição, multiplicação, subtração e divisão estão bem definidas para todo $(x, y) \in \mathbb{Q} \times \mathbb{Q}$.

Entretanto, $\mathbb{Q}$ ainda não é um conjunto tão completo assim.

Veremos no próximo capítulo que em $\mathbb{Q}$ existem subconjuntos não vazios limitados superiormente que não admitem *"menor cota superior"* (que chamaremos de supremo do subconjunto em $\mathbb{Q}$).

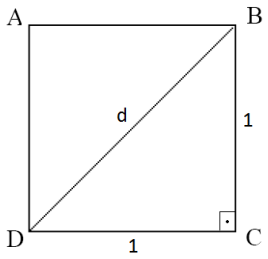
No intuito de estabelecer um conjunto em que as operações adição, multiplicação, subtração e divisão estejam bem definidas e que todo subconjunto não vazio limitado superiormente possua menor cota superior é que surge o conjunto dos números reais $\mathbb{R}$. Em outras palavras, o conjunto dos números reais é uma extensão do conjunto dos números racionais, construída para preencher as lacunas causadas pela ausência desses supremos no conjunto dos números racionais, como veremos no próximo capítulo.

7 Números Reais

Neste momento veremos que existem números além dos números racionais, o que será uma motivação para a construção de um conjunto mais completo. Faremos uso de um teorema bastante conhecido na matemática e também de algumas propriedades sem antes demonstrar sua validade, uma vez que isso não é de fato importante dentro dessa dissertação.

Seja o quadrado $ABCD$ de lado 1. Queremos, a partir dele, mostrar que a medida de sua diagonal não será um número racional.

Para tanto, tracemos a diagonal desse quadrado.



Observe que BCD forma um triângulo retângulo em C cujos catetos medem 1.

Aplicando o teorema de Pitágoras, temos:

$$d^2 = 1^2 + 1^2 \Rightarrow d^2 = 1 + 1 \Rightarrow d^2 = 2.$$

Vamos supor que d seja um número racional; logo existem $p, q \in \mathbb{Z}$, $q \neq 0$, tais que d será a fração irredutível $\frac{p}{q}$. Segue que:

$$d^2 = 2 \Rightarrow \left(\frac{p}{q}\right)^2 = 2 \Rightarrow \frac{p^2}{q^2} = 2 \Rightarrow p^2 = 2 \cdot q^2.$$

Isso nos mostra que p^2 é par, o que implica que p também é par. Sendo p um número par, $p = 2 \cdot r$ com $r \in \mathbb{Z}$. Daí,

$$p^2 = 2 \cdot q^2 \Rightarrow (2 \cdot r)^2 = 2 \cdot q^2 \Rightarrow 4 \cdot r^2 = 2 \cdot q^2 \Rightarrow 2 \cdot r^2 = q^2.$$

Concluímos que q^2 é par, o que implica que q também é par.

Agora, veja que supomos $\frac{p}{q}$ como sendo uma fração irredutível e acabamos mostrando que tanto p quanto q são números pares (divisíveis por 2).

O absurdo está em supor que d, nestas condições, é um número racional.

Portanto, fica demonstrado que d não é um número racional.

No que segue, definiremos uma extensão do conjunto dos números racionais que comporta o número d acima, qual seja, o conjunto dos números reais, $\mathbb{R}$.

Estabeleceremos neste conjunto as operações adição e multiplicação e, ainda, mostraremos que todo conjunto limitado superiormente possui menor cota superior.

Ao longo desse capítulo, usamos como referência básica a referência [6].

Definição 7.1. *Seja X um conjunto totalmente ordenado e $A \subset X$, $A \neq \varnothing$. Um elemento $a \in A$ é chamado mínimo de A se $a \leq x$, para todo $x \in A$. Denotamos $a = min\ A$.*

Observação 7.2. A propriedade antissimétrica da relação de ordem garante que um subconjunto não vazio $A \subset X$ não pode ter mais que um mínimo. Pois, se x e y são mínimos de um conjunto A, temos $x \leq y$ e $y \leq x$, logo, conforme a definição de relação de ordem total, $x = y$.

Exemplo 7.3. Se $A = \mathbb{N}$, então $0 = min\ A$.

Exemplo 7.4. Se $A = \mathbb{Z}$, então A não tem mínimo.

Basta observar que $a - 1 < a$, $\forall a \in \mathbb{Z}$, pois, $a = (a-1) + 1$ com $1 \in \mathbb{Z}_+$.

Proposição 7.5. *Se $x, y \in \mathbb{Q}$ e $x < y$, então $x < \frac{1}{2} \cdot (x + y) < y$.*

Demonstração: Primeiramente, considere que dado $x \in \mathbb{Q}$, $x + x = 2 \cdot x$. Pois, usando as propriedades da proposição 6.16, temos que:

$$x + x = 1 \cdot x + 1 \cdot x = (1 + 1) \cdot x = 2 \cdot x.$$

Veja também que dado $x \in \mathbb{Q}$, $\frac{1}{2} \cdot (2 \cdot x) = x$. Pois, também usando as propriedades da proposição 6.16, temos que:

$$\frac{1}{2} \cdot (2 \cdot x) = (\frac{1}{2} \cdot 2) \cdot x = (\frac{1}{2} \cdot \frac{2}{1}) \cdot x = \frac{1 \cdot 2}{2 \cdot 1} \cdot x = \frac{2}{2} \cdot x = 1 \cdot x = x.$$

Agora, para a demonstração da proposição, vamos separar em dois itens:

(i) $x < \frac{1}{2} \cdot (x + y)$:

Uma vez que $x < y$ e , pela proposição 6.20, $x \leq x$, temos que:

$$x \leq x \text{ e } x < y \Rightarrow x + x < x + y \Rightarrow 2 \cdot x < x + y.$$

Multiplicando a desigualdade por $\frac{1}{2}$, obtemos:

$$\frac{1}{2}\cdot(2\cdot x) < \frac{1}{2}\cdot(x+y).$$

Ou seja,

$$x < \frac{1}{2}\cdot(x+y).$$

(ii) $\frac{1}{2}\cdot(x+y) < y$:

Sendo $x < y$, usando a proposição 5.27, temos que:

$$x < y \Rightarrow x+y < y+y \Rightarrow x+y < 2\cdot y.$$

Multiplicando a desigualdade por $\frac{1}{2}$, obtemos:

$$\frac{1}{2}\cdot(x+y) < \frac{1}{2}\cdot(2\cdot y).$$

Daí,

$$\frac{1}{2}\cdot(x+y) < y.$$

■

Exemplo 7.6. O conjunto $A = \{x \in \mathbb{Q} \ / \ 0 < x < 1\}$ não tem mínimo. Basta verificar que para todo $x \in \mathbb{Q}$ tal que $0 < x < 1$, temos $0 < \frac{1}{2}\cdot x < x < 1$, conforme a proposição 7.5.

Definição 7.7. *Uma cota superior de um conjunto não vazio $A \subset X$ é um elemento $k \in X$ tal que $k \geq x$, para todo $x \in A$.*

Definição 7.8. *Um conjunto não vazio $A \subset X$ é limitado superiormente em X se A admite cota superior em X.*

Definição 7.9. *Se o conjunto das cotas superiores de um conjunto não vazio $A \subset X$, tem um mínimo s, este é chamado supremo de A.*

Denotamos $s = sup\ A$.

Exemplo 7.10. Considere o conjunto $B = \{x \in \mathbb{Q} \ / \ 0 < x < 2\}$. Observe que 2 é cota superior para o conjunto B, já que para qualquer $x \in B$, temos que:

$$0 < x < 2 \Rightarrow 0 < x < \frac{1}{2}\cdot(x+2) < 2.$$

E ainda, $2 = sup\ B$. De fato, resta mostrarmos que 2 é a menor das cotas superiores.

Para isso, suponha que k seja uma cota superior para B com $k < 2$. Então,

$$k < \frac{1}{2} \cdot (k+2) < 2.$$

Sendo assim,

$$\frac{1}{2} \cdot (k+2) \in B \text{ e } \frac{1}{2} \cdot (k+2) > k.$$

O que é absurdo, uma vez que k é cota superior de B.

Logo, $2 = sup\ B$.

Veremos no próximo exemplo um subconjunto não vazio limitado superiormente que não possuí cota superior no conjunto dos números racionais.

Exemplo 7.11. Seja $X = \{x \in \mathbb{Q} \ / \ x \geq 0 \text{ e } x^2 < 2\}$. Observemos que o conjunto X não possuí elemento máximo.

Dado $x \in X$ (isto é, dado um número racional não negativo cujo quadrado é inferior a 2), tomamos um número racional $r < 1$ tal que

$$0 < r < \frac{2 - x^2}{2 \cdot x + 1}.$$

Afirmamos que $x + r$ ainda pertence a X. Com efeito de $r < 1$, segue que $r^2 < r$. Da outra desigualdade que r satisfaz, segue que $r \cdot (2 \cdot x + 1) < 2 - x^2$. Por consequência,

$$(x+r)^2 = x^2 + 2 \cdot x \cdot r + r^2 < x^2 + 2 \cdot x \cdot r + r = x^2 + r \cdot (2 \cdot x + 1) < x^2 + 2 - x^2 = 2.$$

Assim, dado qualquer $x \in X$, existe um número maior, $x + r \in X$.

7.1 Construção de $\mathbb{R}$

Para construir o conjunto dos números reais, inicialmente precisamos da definição de corte no conjunto dos números racionais.

Definição 7.12. *Dizemos que um conjunto $\alpha \subset \mathbb{Q}$ é um corte em $\mathbb{Q}$ se:*

(i) $\alpha \neq \varnothing$ *e* $\alpha \neq \mathbb{Q}$;

(ii) Se $x \in \alpha$ *e* $y < x$, *então* $y \in \alpha$;

(iii) Para todo $x \in \alpha$ *existe* $y \in \alpha$ *de maneira que* $y > x$.

Exemplo 7.13. Seja $\alpha = \{x \in \mathbb{Q} \ / \ x < 3\}$. Veja que:

(i) $\alpha \neq \varnothing$, pois $0 \in \alpha$. $\alpha \neq \mathbb{Q}$, pois $3 \in \mathbb{Q}$ e $3 \notin \alpha$.

(ii) Sejam x e y racionais quaisquer, com $x \in \alpha$ e $y < x$. Temos que:

$$x \in \alpha \Leftrightarrow x < 3.$$

Como $y < x$ e $x < 3$, segue da proposição 6.20 que $y < 3$. Portanto, $y \in \alpha$.

(iii) Para mostrar que para todo $x \in \alpha$ existe $y \in \alpha$ de maneira que $y > x$, basta tomar $y = \frac{1}{2} \cdot (x + 3)$. Fica garantido pela proposição 7.5 que:

$$x < \frac{1}{2} \cdot (x + 3) < 3.$$

Então, $y \in \alpha$ e $y > x$.

Portanto, $\alpha = \{x \in \mathbb{Q} \ / \ x < 3\}$ é um corte em $\mathbb{Q}$.

Definição 7.14. *Seja* $\mathbb{R}$ *o conjunto de todos os cortes em* $\mathbb{Q}$*. Os elementos de* $\mathbb{R}$ *são chamados de números reais e, sendo assim,* $\mathbb{R}$ *é denominado conjunto dos números reais.*

Através dessa definição, buscamos representar um número real pelo conjunto de todos os números racionais que o antecedem.

Exemplo 7.15. Seja $\alpha = \{x \in \mathbb{Q} \ / \ x < 5\}$. Veja que:

(i) $\alpha \neq \varnothing$, pois $0 \in \alpha$. $\alpha \neq \mathbb{Q}$, pois $5 \in \mathbb{Q}$ e $5 \notin \alpha$.

(ii) Sejam x e y racionais quaisquer, com $x \in \alpha$ e $y < x$. Temos que:

$$x \in \alpha \Leftrightarrow x < 5.$$

Como $y < x$ e $x < 5$, segue da proposição 6.20 que $y < 5$. Portanto, $y \in \alpha$.

(iii) Para mostrar que para todo $x \in \alpha$ existe $y \in \alpha$ de maneira que $y > x$, basta tomar $y = \frac{1}{2} \cdot (x + 5)$. Fica garantido pela proposição 7.5 que:

$$x < \frac{1}{2} \cdot (x + 5) < 5.$$

Então, $y \in \alpha$ e $y > x$.

Logo, $\alpha = \{x \in \mathbb{Q} \ / \ x < 5\}$ é um corte em $\mathbb{Q}$ e, portanto, um número real.

Proposição 7.16. *Para qualquer* $r \in \mathbb{Q}$*, o conjunto* $\{x \in \mathbb{Q} \ / \ x < r\}$ *é um número real.*

Demonstração: Para mostrar que o conjunto $\{x \in \mathbb{Q} \ / \ x < r\}$ é um número real, é necessário mostrar este conjunto é um corte. Para tanto, mostraremos os três itens da definição 7.12.

(i) Note que $\alpha \neq \varnothing$. Basta observar que $x - 1 < x$, $\forall x \in \mathbb{Q}$, pois, $x = (x - 1) + 1$ com $1 \in \mathbb{Q}_+$. Segue que $r - 1 \in \{x \in \mathbb{Q} \ / \ x < r\}$.

Ainda, $\alpha \neq \mathbb{Q}$, já que $r \in \mathbb{Q}$ mas $r \notin \{x \in \mathbb{Q} \ / \ x < r\}$.

(ii) Suponha que $u \in \{x \in \mathbb{Q} \;/\; x < r\}$, segue que $u < r$. Para todo número racional y tal que $y < u$ vale a relação $y < r$ (propriedade da proposição 6.20). Logo, $y \in \{x \in \mathbb{Q} \;/\; x < r\}$.

(iii) Para mostrar que para todo $u \in \{x \in \mathbb{Q} \;/\; x < r\}$ existe $y \in \{x \in \mathbb{Q} \;/\; x < r\}$ de maneira que $y > u$, basta tomar $y = \frac{1}{2} \cdot (u + r)$. Fica garantido pela proposição 7.5 que:

$$u < \frac{1}{2} \cdot (u + r) < r.$$

Então, $y \in \{x \in \mathbb{Q} \;/\; x < r\}$ e $y > u$.

Logo, $\{x \in \mathbb{Q} \;/\; x < r\}$ é um corte em $\mathbb{Q}$ e, portanto, um número real.

■

Definição 7.17. *Denotamos r' o conjunto $\{x \in \mathbb{Q} \;/\; x < r\}$ com $r \in \mathbb{Q}$.*
Ou seja, para todo $r \in \mathbb{Q}$,

$$r' = \{x \in \mathbb{Q} \;/\; x < r\}.$$

Em particular,

$$0' = \{x \in \mathbb{Q} \;/\; x < 0\}$$
$$e$$
$$1' = \{x \in \mathbb{Q} \;/\; x < 1\}.$$

7.2 Relação de ordem em $\mathbb{R}$

Definição 7.18. *Sejam α e β dois números reais. Definimos:*

(i) $\alpha \leq \beta \Leftrightarrow \alpha \subset \beta$.

(ii) $\alpha < \beta \Leftrightarrow \alpha \subset \beta$ *e* $\alpha \neq \beta$.

Proposição 7.19. *A relação $\leq$ é uma relação de ordem em $\mathbb{R}$.*

Demonstração: Basta verificar que a relação $\leq$ satisfaz as propriedades reflexiva, antissimétrica e transitiva.

(i) *Reflexiva:* Para qualquer $\alpha \in \mathbb{R}$, $\alpha \subset \alpha$. Segue da definição 7.18 que $\alpha \leq \alpha$.

(ii) *Antissimétrica:* Sejam $\alpha, \beta \in \mathbb{R}$. Sendo $\alpha \leq \beta$, segue da definição 7.18 que $\alpha \subset \beta$. Ainda, sendo $\beta \leq \alpha$, segue da mesma definição que $\beta \subset \alpha$. Uma vez que $\alpha \subset \beta$ e $\beta \subset \alpha$, segue da teoria de conjuntos que $\alpha = \beta$.

(iii) *Transitiva:* Sejam $\alpha, \beta, \gamma \in \mathbb{R}$. Se $\alpha \leq \beta$ segue da definição 7.18 que $\alpha \subset \beta$. Ainda, se $\beta \leq \gamma$, segue da mesma definição que $\beta \subset \gamma$. Uma vez que $\alpha \subset \beta$ e $\beta \subset \gamma$, segue da teoria de conjuntos que $\alpha \subset \gamma$. Daí, segue da definição 7.18 que $\alpha \leq \gamma$.

■

Lema 7.20. *Se α é um número real e y é um número racional tal que $y \notin \alpha$, então para todo $x \in \alpha$ temos $x < y$.*

Demonstração: Suponhamos, por absurdo, que exista $x \in \alpha$ que satisfaça $x \geq y$, ou seja, $y \leq x$. Veja que:

(i) Se $y = x$, como $x \in \alpha$, teremos $y \in \alpha$, contrariando a hipótese do lema.

(ii) Se $y < x$, a definição 7.12 nos garante que $y \in \alpha$, contrariando a hipótese do lema.

Portanto, se $y \notin \alpha$, então $x < y$, para todo $x \in \alpha$.

■

Proposição 7.21. *Para quaisquer $\alpha, \beta \in \mathbb{R}$, $\alpha \leq \beta$ ou $\beta \leq \alpha$.*

Demonstração: Para quaisquer $\alpha, \beta \in \mathbb{R}$, $\alpha \subset \beta$ ou $\alpha \not\subset \beta$.

Se $\alpha \subset \beta$, a definição 7.18 nos garante que $\alpha \leq \beta$.

Se $\alpha \not\subset \beta$, então existe um número racional y tal que $y \in \alpha$ e $y \notin \beta$. Seja $x \in \beta$, qualquer. Como $y \notin \beta$, segue do lema 7.20 que $x < y$. Uma vez que $y \in \alpha$ e $x < y$ para todo $x \in \beta$, segue da definição 7.12 que $x \in \alpha$. Portanto, $\beta \subset \alpha$, ou seja, $\beta \leq \alpha$.

■

7.3 Adição em $\mathbb{R}$

Proposição 7.22. *Se α e β são números reais, então*

$$\gamma = \alpha + \beta = \{x + y \ / \ x \in \alpha \ e \ y \in \beta\}$$

também é número real.

Demonstração: Para mostrar que o conjunto γ é um número real, é necessário mostrar que este é um corte no conjunto dos números racionais. Para tanto, mostraremos os três itens da definição 7.12.

(i) Como α e β são números reais, sabemos que $\alpha \neq \varnothing$ e $\beta \neq \varnothing$. Logo, existem $x \in \alpha$ e $y \in \beta$ que nos garantem que $x + y \in \alpha + \beta = \gamma$. Portanto, $\gamma \neq \varnothing$.

Ainda, como α e β são números reais, sabemos que $\alpha \neq \mathbb{Q}$ e $\beta \neq \mathbb{Q}$. Logo, existem $z, w \in \mathbb{Q}$ com $z \notin \alpha$ e $w \notin \beta$. Do lema 7.20, temos que:

$$\forall x \in \alpha,\ x < z$$

e

$$\forall y \in \beta,\ y < w.$$

Daí, pela proposição 6.20, segue que:

$$\forall x \in \alpha,\ \forall y \in \beta,\ x + y < z + w.$$

Note que $z + w \in \mathbb{Q}$, uma vez que a adição está bem definida no conjunto dos números racionais, mas $z + w \notin \alpha + \beta = \gamma$, pois, se $z + w \in \alpha + \beta = \gamma$ existiriam $x_0 \in \alpha$ e $y_0 \in \beta$ tais que $z + w = x_0 + y_0$, o que é absurdo, pois para qualquer $x \in \alpha$ e para qualquer $y \in \beta$, $x + y < z + w$.

Concluímos que $\gamma \neq \mathbb{Q}$.

(ii) Seja $t \in \gamma$ e $u \in \mathbb{Q}$ tal que $u < t$. Queremos mostrar que $u \in \gamma$. Para isso, será necessário exibir $x \in \alpha$ e $y \in \beta$ tal que $u = x + y$.

Sabemos que $t \in \gamma$, logo, existem $a \in \alpha$ e $b \in \beta$ tal que $t = a + b$.

Como $u < t$ segue que $u < a + b$. Ou seja, $u + (-a) < a + b + (-a) \to u - a < b$ (Veja que os resultados ficam garantidos pelas propriedades já demonstradas para os números racionais).

Note que uma vez que $b \in \beta$, $u - a \in \beta$ (definição 7.12).

Então, $u = a + (u - a)$, com $a \in \alpha$ e $u - a \in \beta$. Portanto $u \in \gamma$.

(iii) Seja $z \in \gamma$. Logo $z = x + y$ para algum $x \in \alpha$ e $y \in \beta$. Uma vez que α e β são números reais, satisfazem a condição de ser corte no conjunto dos números racionais. Logo, existem números racionais $t \in \alpha$ e $u \in \beta$ com $x < t$ e $y < u$. Note que $t + u \in \alpha + \beta = \gamma$ e $x + y < t + u$.

Logo, $\gamma = \alpha + \beta = \{x + y \ / \ x \in \alpha \text{ e } y \in \beta\}$ com α e β números reais é um corte em $\mathbb{Q}$ e, portanto, um número real.

■

Definição 7.23. *Sejam α e β dois números reais quaisquer. Definimos a aplicação binária adição da seguinte forma:*

$$\begin{array}{rccc} + : & \mathbb{R} \times \mathbb{R} & \longrightarrow & \mathbb{R} \\ & (\alpha, \beta) & \longmapsto & \alpha + \beta \end{array}$$

em que

$$\alpha + \beta := \{x + y \ / \ x \in \alpha \ e \ y \in \beta\}.$$

Note que pela proposição 7.22, esta operação é binária.

A seguir veremos a demonstração de dois lemas que serão utilizados na demonstração da propriedade do simétrico aditivo no conjunto dos números reais.

Lema 7.24. *Seja* α *um número real e* M_α *o conjunto dos racionais que são cotas superiores de* α*. Então,*

$$\beta = \{p \in \mathbb{Q} \ / \ -p \in M_\alpha \ e \ -p \neq min \ M_\alpha\}$$

é número real.

Demonstração: Para mostrar que $\beta = \{p \in \mathbb{Q} \ / \ -p \in M_\alpha \text{ e } -p \neq min \ M_\alpha\}$ é um número real, é necessário mostrar que esse é um corte no conjunto dos números racionais, ou seja, que ele satisfaz os itens *(i)*, *(ii)* e *(iii)* da definição 7.12.

No que segue, como α é um número real, temos que $\alpha = \{x \in \mathbb{Q} \ / \ x < a\}$ para algum $a \in \mathbb{Q}$. Observe que $M_\alpha \neq \varnothing$ já que $a \in M_\alpha$.

(i) Observe que $\beta \neq \varnothing$: seja $q \in M_\alpha$ qualquer. Uma vez que $q < q + 1$, segue que $q + 1 \in M_\alpha$. Como $q + 1 \in M_\alpha$ e $q + 1 \neq min \ M_\alpha$, segue que $-(q + 1) \in \beta$.

Note também que $\beta \neq \mathbb{Q}$: para qualquer $p \in \alpha$, temos que $p < a$. Logo, qualquer $p \in \alpha$ não é cota superior para α, ou seja, $p \notin M_\alpha$. Segue que $q = -p \notin \beta$ já que $-q = -(-p) = p \notin M_\alpha$.

(ii) Queremos mostrar que para qualquer $x \in \beta$ e $y < x$, então $y \in \beta$. Para isso, seja $x \in \beta$ e $y < x$, logo, $-x < -y$. Como $x \in \beta$, sabemos que $-x \in M_\alpha$ e $-x \neq min \ M_\alpha$. Como $-x < -y$, segue que $-y \in M_\alpha$ e $-y \neq min \ M_\alpha$ (pois $min \ M_\alpha < -x < -y$). Portanto, $y \in \beta$.

(iii) Queremos mostrar que para qualquer $x \in \beta$ existe $y \in \beta$ tal que $y > x$. Para isso seja $x \in \beta$, logo, da definição de β, $-x \in M_\alpha$ e $-x \neq min \ M_\alpha$, segue que $min \ M_\alpha < -x$.

Segundo a proposição 7.5, existe $z \in \mathbb{Q}$, $z = \dfrac{1}{2} \cdot [min \ M_\alpha + (-x)]$ tal que

$$min \ M_\alpha < \frac{1}{2} \cdot [min \ M_\alpha + (-x)] < -x.$$

Ou seja, $min \ M_\alpha < z < -x$.

Uma vez que $min \ M_\alpha < z$, temos que $z \in M_\alpha$ e $z \neq min \ M_\alpha$. Segue que $-z \in \beta$.

Note por fim que como $z < -x$, então $-z > x$.

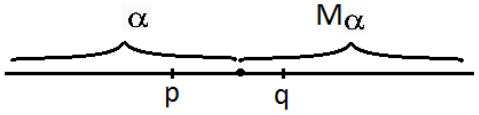
Portanto, $y = -z \in \beta$ é tal que $y > x$, como queríamos.

Logo, $\beta = \{p \in \mathbb{Q} \ / \ -p \in M_\alpha \text{ e } -p \neq min \ M_\alpha\}$ é um corte no conjunto dos números racionais e, portanto, um número real.

■

Lema 7.25. *Seja* α *um número real,* $u < 0$ *um número racional e* M_α *o conjunto das cotas superiores de* α*. Nestas condições, existem* $p \in \alpha$*,* $q \in M_\alpha$*,* $q \neq min\ M_\alpha$ *(caso* $min\ M_\alpha$ *exista), tais que* $p - q = u$*.*

Demonstração: Seja α um número real e M_α o conjunto das cotas superiores de α, onde vamos considerar $\alpha = \{x \in \mathbb{Q} \ / \ x < a\}$ para algum $a \in \mathbb{Q}$.

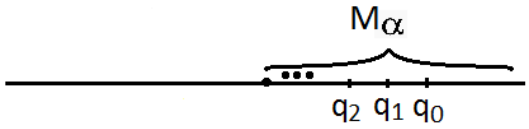


Precisamos determinar $p \in \alpha$, $q \in M_\alpha$, $q \neq min\ M_\alpha$ com $p - q = u$.

Para isso, seja o racional $s \notin \alpha$, com $s \neq min\ M_\alpha$. Para cada $n \in \mathbb{N}$, consideremos o racional

$$q_n = n \cdot u + s.$$

Observe que, da hipótese do lema, u é um número racional e $u < 0$, ou seja, $u \in \mathbb{Q}_-$.



Seja $\overline{n}$ o máximo dos naturais n para os quais $q_n \in M_\alpha$ e $q_n \neq min\ M_\alpha$.

Note que necessariamente existe $\overline{n} \in \mathbb{N}$ com essa propriedade pois, caso contrário, teríamos $a < q_n$ para qualquer $n \in \mathbb{N}$, o que produziria um absurdo, já que como $s \notin \alpha$ e $s \neq min\ M_\alpha$, sabemos que $s > a$. Logo, existe $r \in \mathbb{Q}_+$ tal que $s = a + r$. Sendo assim, da definição de q_n, temos:

$$q_n = n \cdot u + s = n \cdot u + a + r = (n \cdot u + r) + a.$$

Daí, para qualquer $n \in \mathbb{N}$, teríamos:

$$a < q_n \Rightarrow a < (n \cdot u + r) + a \Rightarrow 0 < n \cdot u + r,$$

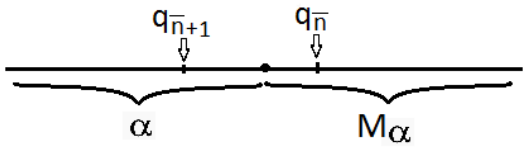
em que $n \cdot u \in \mathbb{Q}_-$ e $r \in \mathbb{Q}_+$, o que é um absurdo.

Observe que sendo $\overline{n}$ o máximo dos naturais com tal característica , então, para $\overline{n} + 1 > \overline{n}$, temos $\overline{n} + 1 \notin M_\alpha$ e, portanto, $q_{\overline{n}+1} \in \alpha$ ou $q_{\overline{n}+1} = min\ M_\alpha$.

Observe como proceder em cada um dos dois casos.

- 1º caso: $q_{\overline{n}} \in M_\alpha$ e $q_{\overline{n}+1} \in \alpha$.

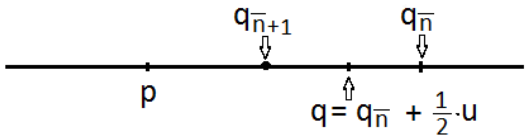
  Basta tomar $q = q_{\overline{n}}$ e $p = q_{\overline{n}+1}$, pois:



$$p - q = q_{\overline{n}+1} - q_{\overline{n}} = (\overline{n}+1)\cdot u + s - (\overline{n}\cdot u + s) = \overline{n}\cdot u + u + s - (\overline{n}\cdot u + s) = u.$$

- 2^{o} caso: $q_{\overline{n}} \in M_\alpha$ e $q_{\overline{n}+1} = min\ M_\alpha$.

  Neste caso tomaremos $q = q_{\overline{n}} + \dfrac{1}{2}\cdot u$ e $p = q_{\overline{n}+1} + \dfrac{1}{2}\cdot u$.



  Daí,

$$p - q = q_{\overline{n}+1} + \frac{1}{2}\cdot u - q_{\overline{n}} + \frac{1}{2}\cdot u = (\overline{n}+1)\cdot u + s + \frac{1}{2}\cdot u - (\overline{n}\cdot u + s + \frac{1}{2}\cdot u) =$$
$$\overline{n}\cdot u + u + s + \frac{1}{2}\cdot u - (\overline{n}\cdot u + s + \frac{1}{2}\cdot u) = u.$$

■

A seguir trataremos de algumas propriedades da adição no conjunto dos números reais.

Proposição 7.26. *Para a adição em* $\mathbb{R}$ *valem as seguintes propriedades:*

A_1. *Associativa: dados* $\alpha, \beta, \gamma \in \mathbb{R}$, *temos* $(\alpha+\beta)+\gamma = \alpha+(\beta+\gamma)$.

A_2. *Comutativa: dados* $\alpha, \beta \in \mathbb{R}$, *temos* $\alpha+\beta = \beta+\alpha$.

A_3. *Elemento neutro: para qualquer* $\alpha \in \mathbb{R}$, *temos que* $\alpha + 0' = \alpha$.

A_4. *Simétrico aditivo: para todo* $\alpha \in \mathbb{R}$, *existe* $(-\alpha) \in \mathbb{R}$ *de modo que* $\alpha + (-\alpha) = 0'$.

Demonstração: Vejamos a demonstração de cada propriedade da adição em $\mathbb{R}$.

A_1. *Associativa:*

Para mostrar que dados $\alpha, \beta, \gamma \in \mathbb{R}$, $(\alpha+\beta)+\gamma = \alpha+(\beta+\gamma)$, é necessário mostrar que $(\alpha+\beta)+\gamma \subset \alpha+(\beta+\gamma)$ e que $\alpha+(\beta+\gamma) \subset (\alpha+\beta)+\gamma$ (definição 2.13).

Sejam $\alpha, \beta, \gamma \in \mathbb{R}$. Seja $w \in (\alpha+\beta)+\gamma$, então $w = u+z$ tal que $u \in \alpha+\beta$ e $z \in \gamma$. Uma vez que $u \in \alpha+\beta$, segue que $u = x+y$ tal que $x \in \alpha$ e $y \in \beta$ (veja que $w, u, z, x, y \in \mathbb{Q}$). Daí, basta lembrar que a associativa pode ser aplicada aos números racionais, segundo a proposição 6.10:

$$w = u + z = (x + y) + z = x + (y + z) = x + v.$$

Segue que $w = x + v$ tal que $x \in \alpha$ e $v \in \beta + \gamma$. Ou seja, $w \in \alpha + (\beta + \gamma)$.

Segue que $(\alpha + \beta) + \gamma \subset \alpha + (\beta + \gamma)$.

De maneira análoga mostramos que $\alpha + (\beta + \gamma) \subset (\alpha + \beta) + \gamma$.

Portanto, para quaisquer $\alpha, \beta, \gamma \in \mathbb{R}$, segue que $(\alpha + \beta) + \gamma = \alpha + (\beta + \gamma)$.

A_2. *Comutativa:*

Para mostrar que dados $\alpha, \beta \in \mathbb{R}$, $\alpha+\beta = \beta+\alpha$, é necessário mostrar que $\alpha+\beta \subset \beta+\alpha$ e que $\beta + \alpha \subset \alpha + \beta$ (definição 2.13).

Sejam $\alpha, \beta \in \mathbb{R}$. Seja $w \in \alpha + \beta$, então $w = x + y$ tal que $x \in \alpha$ e $y \in \beta$ (veja que $w, x, y \in \mathbb{Q}$). Daí, basta lembrar que a comutativa pode ser aplicada aos números racionais, segundo a proposição 6.10:

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

Segue que $w = y + x$ tal que $y \in \beta$ e $x \in \alpha$. Ou seja, $w \in \beta + \alpha$.

Segue que $\alpha + \beta \subset \beta + \alpha$.

De maneira análoga mostramos que $\beta + \alpha \subset \alpha + \beta$.

Portanto, para quaisquer $\alpha, \beta, \in \mathbb{R}$, segue que $\alpha + \beta = \beta + \alpha$.

A_3. *Elemento neutro:* Precisamos mostrar que para qualquer $\alpha \in \mathbb{R}$, temos que

$\alpha+0' = \alpha$, ou seja, será necessário provar que $\alpha+0' \subset \alpha$ e que $\alpha \subset \alpha+0'$. Lembremos que $0' = \{x \in \mathbb{Q} \ / \ x < 0\}$.

(a) $\alpha + 0' \subset \alpha$:

Seja $w \in \alpha + 0'$. Segue que $w = x + u$ para algum $x \in \alpha$ e algum $u < 0$, $u \in \mathbb{Q}$.

Sendo $u < 0$, temos que:

$$u < 0 \Rightarrow x + u < x \Rightarrow w < x \Rightarrow w \in \alpha \text{ (definição 7.12).}$$

Portanto, $\alpha + 0' \subset \alpha$.

(b) $\alpha \subset \alpha + 0'$:

Seja $x \in \alpha$. Pela definição 7.12, existe $y \in \alpha$ tal que $x < y$. Se $x < y$, segue da proposição 6.20 que $x - y < 0$. Daí,

$$x = y + (x - y), \text{ com } y \in \alpha \text{ e } x - y < 0.$$

Segue que $x \in \alpha + 0'$. Portanto, $\alpha \subset \alpha + 0'$.

A_4. *Simétrico aditivo:*

Seja α um número real, $\alpha = \{x \in \mathbb{Q} \ / \ x < a\}$. Já sabemos pelo lema 7.24 que $\beta = \{p \in \mathbb{Q} \ / \ -p \in M_\alpha \text{ e } -p \neq min\ M_\alpha\}$ é número real.

Provemos que $\alpha + \beta = 0'$, para isso será necessário mostrar, segundo a definição 2.13 que $\alpha + \beta \subset 0'$ e que $0' \subset \alpha + \beta$.

(a) $\alpha + \beta \subset 0'$:

Seja $x \in \alpha + \beta$, então $x = a + b$ com $a \in \alpha$ e $b \in \beta$.

Se $b \in \beta$, então $-b > a$. Isso implica que $a + b < 0$, ou seja, $x < 0$.

Segue que $x \in 0'$.

Portanto, $\alpha + \beta \subset 0'$.

(b) $0' \subset \alpha + \beta$:

Seja $x \in 0'$. Precisamos mostrar que então $x = a+b$ para algum $a \in \alpha$ e algum $b \in \beta$.

Como $x \in 0'$ segue que $x < 0$. O lema 7.25 garante que existem $a \in \alpha$ e $-b \in M_\alpha$, com $-b \neq min\ M_\alpha$, tais que $x = a - (-b)$.

Assim, $x = a + b$ com $a \in \alpha$ e $b \in \beta$.

Segue que $0' \subset \alpha + \beta$.

Portanto, $\alpha + \beta = 0'$.

Indicaremos β por $-\alpha$.

■

Lema 7.27. *O elemento neutro citado acima é único.*

Demonstração: Sabemos que para qualquer $\alpha \in \mathbb{R}$, $\alpha + 0' = \alpha$.

Supomos que o elemento neutro não seja único, ou seja, existe $\beta \in \mathbb{R}$ tal que $\alpha+\beta = \alpha$ para qualquer $\alpha \in \mathbb{R}$.

Em particular, para $\alpha = 0'$, temos:

$$0' + \beta = 0' \Rightarrow \beta = 0'.$$

Portanto, o elemento neutro é único.

■

Lema 7.28. *O simétrico aditivo citado acima é único.*

Demonstração: Para todo $\alpha \in \mathbb{R}$ existe $(-\alpha) \in \mathbb{R}$ de modo que $\alpha + (-\alpha) = 0'$.

Supomos que exista outro simétrico aditivo para α, ou seja, existe $\theta \in \mathbb{R}$ tal que $\alpha + \theta = 0'$.

Sendo $\alpha + (-\alpha) = 0'$ e $\alpha + \theta = 0'$, temos que $\alpha + (-\alpha) = \alpha + \theta$. Daí, somando $(-\alpha)$ de ambos os lados da igualdade, obtemos:

$$\alpha + (-\alpha) = \alpha + \theta \to (-\alpha) + (\alpha + (-\alpha)) = (-\alpha) + (\alpha + \theta).$$

Associando as somas convenientemente e fazendo uso da propriedade do simétrico aditivo, temos que:

$$((-\alpha) + \alpha) + (-\alpha) = ((-\alpha) + \alpha) + \theta \to 0' + (-\alpha) = 0' + \theta \to (-\alpha) = \theta.$$

Portanto, o simétrico aditivo é único.

■

Proposição 7.29. *A adição e a relação de ordem são compatíveis, no seguinte sentido: dados* $\alpha, \beta \in \mathbb{R}$, $\alpha \leq \beta \Rightarrow \alpha + \gamma \leq \beta + \gamma$, $\forall \gamma \in \mathbb{R}$.

Demonstração: Sejam $\alpha, \beta, \gamma \in \mathbb{R}$ tal que $\alpha \leq \beta$. Queremos mostrar que $\alpha + \gamma \leq \beta + \gamma$. Pela definição 7.12, basta verificarmos que $\alpha + \gamma \subset \beta + \gamma$.

Seja $w \in \alpha + \gamma$. Segue que $w = x + z$ para algum $x \in \alpha$ e algum $z \in \gamma$.

Da hipótese, como $\alpha \leq \beta$, sabemos pela mesma definição já citada que $\alpha \subset \beta$. Logo, uma vez que $x \in \alpha$, temos que $x \in \beta$.

Assim, $w = x + z$ para algum $x \in \beta$ e algum $z \in \gamma$.

Portanto, $w \in \beta + \gamma$, demonstrando que $\alpha + \gamma \subset \beta + \gamma$.

Novamente pela definição 7.12, fica garantido que $\alpha + \gamma \leq \beta + \gamma$.

■

7.4 Multiplicação em $\mathbb{R}$

Proposição 7.30. *Se* α *e* β *são números reais,* $\alpha > 0'$ *e* $\beta > 0'$, *então*

$$\gamma = \alpha \cdot \beta = \mathbb{Q}_- \cup \{x \cdot y \;/\; x \in \alpha \text{ e } y \in \beta, x > 0 \text{ e } y > 0\}$$

também é número real.

Demonstração: Para mostrar que o conjunto γ é um número real, é necessário mostrar que ele é um corte no conjunto dos números racionais. Para tanto, mostraremos os três itens da definição 7.12.

Seja $\gamma = \alpha \cdot \beta = \mathbb{Q}_- \cup \{x \cdot y \;/\; x \in \alpha \text{ e } y \in \beta, x > 0 \text{ e } y > 0\}$ com α e β números reais.

(i) Observe que $\gamma \neq \varnothing$, pois $0 \in \gamma$.

Ainda, como α e β são números reais, sabemos que $\alpha \neq \mathbb{Q}$ e $\beta \neq \mathbb{Q}$. Logo, existem $z, w \in \mathbb{Q}$ com $z \notin \alpha$ e $w \notin \beta$. Do lema 7.20, temos que:

$$\forall x \in \alpha,\ 0 < x < z$$

e

$$\forall y \in \beta,\ 0 < y < w.$$

Daí, pela proposição 6.20, segue que:

$$\forall x \in \alpha,\ \forall y \in \beta,\ 0 < x \cdot y < z \cdot w.$$

Uma vez que $0 < z \cdot w$, temos que $z \cdot w \notin \mathbb{Q}_-$. Assim, para que $z \cdot w \in \gamma$ necessariamente teríamos que ter $x_0 \in \alpha$ e $y_0 \in \beta$, com $x_0 > 0$ e $y_0 > 0$ tais que $z \cdot w = x_0 \cdot y_0$, o que é absurdo, pois para qualquer $x \in \alpha$, $x > 0$, e para qualquer $y \in \beta$, $y > 0$, temos que $x \cdot y < z \cdot w$.

Portanto, $z \cdot w \in \mathbb{Q}$, uma vez que a multiplicação está bem definida no conjunto dos números racionais, mas $z \cdot w \notin \alpha \cdot \beta = \gamma$.

Concluímos que $\gamma \neq \mathbb{Q}$.

(ii) Seja $t \in \gamma$ e $u \in \mathbb{Q}$ tal que $u < t$. Queremos mostrar que $u \in \gamma$. Para isso, considere os casos possíveis para $u < t$:

- 1º caso: Se $t \leq 0$ e $u < 0$, temos que $u \in \gamma$ pela construção do conjunto γ.
- 2º caso: Se $t > 0$ e $u \leq 0$, temos que $u \in \gamma$ pela construção do conjunto γ.
- 3º caso: Se $t > 0$ e $u > 0$, temos que $t = x \cdot y$ para algum $x \in \alpha$, algum $y \in \beta$, com $x > 0$ e $y > 0$.
  Sendo $0 < u < t = x \cdot y$, temos que $u < x \cdot y$, ou seja, $\frac{1}{x} \cdot u < \frac{1}{x} \cdot (x \cdot y)$.
  Concluímos que $\frac{1}{x} \cdot u < y$. Segue da definição 7.12 que $\frac{1}{x} \cdot u \in \beta$ com $\frac{1}{x} \cdot u > 0$.
  Note que $u = x \cdot \left(\frac{1}{x} \cdot u\right)$ com $x \in \alpha$ e $\frac{1}{x} \cdot u \in \beta$, com $a > 0$ e $\frac{1}{x} \cdot u > 0$.
  Portanto, $u \in \gamma$.

(iii) Seja $t \in \gamma$, $t > 0$. Note que $t = x \cdot y$ para algum $x \in \alpha$, $x > 0$ e algum $y \in \beta$, $y > 0$. Uma vez que α e β são números reais, satisfazem a condição de ser corte no conjunto dos números racionais. Logo, existem números racionais $z \in \alpha$ e $w \in \beta$ com $x < z$ e $y < w$. Segue que $z \cdot w \in \alpha \cdot \beta = \gamma$ e $x \cdot y < z \cdot w$ (proposição 6.20).

Logo, $\gamma = \alpha \cdot \beta = \mathbb{Q}_- \cup \{x \cdot y \ / \ x \in \alpha \text{ e } y \in \beta, x > 0 \text{ e } y > 0\}$ com α e β números reais é um corte em $\mathbb{Q}$ e, portanto, um número real.

■

A seguir, estabelecemos entre os números reais a operação multiplicação, a qual é definida caso a caso, mediante análise dos números reais envolvidos.

Definição 7.31. *Sejam α e β dois números reais quaisquer. Definimos a aplicação binária multiplicação da seguinte forma:*

$$\begin{array}{rccc} \cdot : & \mathbb{R} \times \mathbb{R} & \longrightarrow & \mathbb{R} \\ & (\alpha, \beta) & \longmapsto & \alpha \cdot \beta \end{array}$$

em que

$$\alpha \cdot \beta := \begin{cases} \mathbb{Q}_- \cup \{x \cdot y \ / \ x \in \alpha, x > 0; y \in \beta, y > 0\}, & se \quad \alpha > 0' \quad e \quad \beta > 0'; \\ 0, & se \quad \alpha = 0' \quad ou \quad \beta = 0'; \\ (-\alpha) \cdot (-\beta), & se \quad \alpha < 0' \quad e \quad \beta < 0'; \\ -[(-\alpha) \cdot \beta], & se \quad \alpha < 0' \quad e \quad \beta \geq 0'; \\ -[\alpha \cdot (-\beta)], & se \quad \alpha \geq 0' \quad e \quad \beta < 0'. \end{cases}$$

A multiplicação no conjunto dos números reais está bem definida, segundo a proposição 7.30.

A seguir veremos a demonstração de dois lemas que serão utilizados na demonstração da propriedade do inverso multiplicativo no conjunto dos números reais.

Lema 7.32. *Seja* α *um número real e* M_α *o conjunto dos racionais que são cotas superiores de* α*. Então,*

$$\beta = \mathbb{Q}_- \cup \left\{ p \in \mathbb{Q} \ / \ p > 0, \frac{1}{p} \in M_\alpha, \frac{1}{p} \neq min \ M_\alpha \right\}$$

é número real.

Demonstração: Para mostrar que $\beta = \mathbb{Q}_- \cup \left\{ p \in \mathbb{Q} \ / \ p > 0, \frac{1}{p} \in M_\alpha, \frac{1}{p} \neq min \ M_\alpha \right\}$ é um número real, é necessário mostrar que este é um corte no conjunto dos números racionais, ou seja, que ele satisfaz os itens *(i)*, *(ii)* e *(iii)* da definição 7.12.

No que segue, como α é um número real, temos que
$\alpha = \{x \in \mathbb{Q} \ / \ x < a\}$ para algum $a \in \mathbb{Q}$. Observe que $M_\alpha \neq \varnothing$ já que $a \in M_\alpha$.

(i) Observe que $\beta \neq \varnothing$: $-1 < 0$ e, então, $-1 \in \mathbb{Q}_-$. Segue que $-1 \in \beta$.

Note ainda que $\beta \neq \mathbb{Q}$: para qualquer $x \in \alpha$, temos que $x < a$. Logo, x não é cota superior para α, ou seja, $x \notin M_\alpha$. Seque que $y = \frac{1}{x} \notin \beta$, já que $\frac{1}{\frac{1}{x}} = x \notin M_\alpha$.

(ii) Queremos mostrar que se $x \in \beta$ e $y < x$, então $y \in \beta$.

Seja $x \in \beta$ e $y < x$. Pela definição do conjunto β, se $y \leq 0$, segue que $y \in \mathbb{Q}_-$ e, portanto, $y \in \beta$.

Suponhamos $y > 0$, logo, $x > y > 0$. Note que se $x > y$, então $\frac{1}{x} < \frac{1}{y}$.

Como $x \in \beta$ e $x > 0$, sabemos que $\frac{1}{x} \in M_\alpha$ com $\frac{1}{x} \neq min \ M_\alpha$.

Uma vez que $\frac{1}{y} > \frac{1}{x} \neq min \ M_\alpha$, segue que $\frac{1}{y} \in M_\alpha$ com $\frac{1}{y} \neq min \ M_\alpha$.

Portanto, $y \in \beta$.

(iii) Queremos mostrar que para todo $x \in \beta$, existe $y \in \beta$ tal que $y > x$. Para isso, seja $x \in \beta$. Da definição de β, $x > 0$, $\frac{1}{x} \in M_\alpha$ e $\frac{1}{x} \neq min \ M_\alpha$. Segue que $min \ M_\alpha < \frac{1}{x}$.

Segundo a proposição 7.5, existe $z \in \mathbb{Q}$,

$$z = \frac{1}{2} \cdot \left[min\ M_\alpha + \frac{1}{x} \right],$$

tal que

$$min\ M_\alpha < \frac{1}{2} \cdot \left[min\ M_\alpha + \frac{1}{x} \right] < \frac{1}{x}.$$

Ou seja, $min\ M_\alpha < z < \frac{1}{x}$.

Uma vez que $min\ M_\alpha < z$, temos que $z \in M_\alpha$ e $z \neq min\ M_\alpha$.

Segue que $y = \frac{1}{z} \in \beta$.

Note, por fim, que $z < \frac{1}{x} \Rightarrow y = \frac{1}{z} > x$.

Portanto, $y = \frac{1}{z} \in \beta$ tal que $y > x$, como queríamos mostrar.

Logo, $\beta = \mathbb{Q}_- \cup \left\{ p \in \mathbb{Q} \ / \ p > 0, \frac{1}{p} \in M_\alpha, \frac{1}{p} \neq min\ M_\alpha \right\}$ é um corte no conjunto dos números racionais e, portanto, um número real.

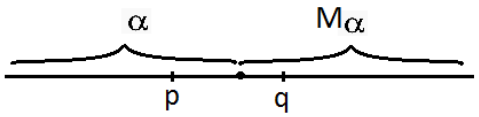
■

Para a demonstração do próximo lema, será necessário o uso de duas definições, a definição 6.17 e a que segue.

Definição 7.33. *Seja* $a \in \mathbb{R}$ *tal que* $a > 0$. *Denotamos por* $\sqrt[n]{a} = a^{\frac{1}{n}}$ *ao número real* $b \in \mathbb{R}$ *tal que* $b^n = a$.

Lema 7.34. *Seja* $\alpha > 0'$ *um número real,* u *um número racional tal que* $0 < u < 1$ *e* M_α *o conjunto das cotas superiores de* α. *Nestas condições, existem* $p \in \alpha$, $q \in M_\alpha$, *com* $q \neq min\ M_\alpha$ *(caso* $min\ M_\alpha$ *exista), tais que* $\frac{p}{q} = u$.

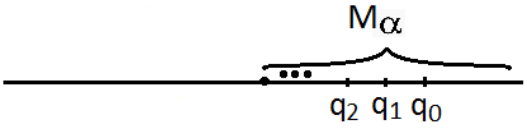
Demonstração: Seja $\alpha > 0'$ um número real e M_α o conjunto das cotas superiores de α.



Precisamos determinar $p \in \alpha$, $q \in M_\alpha$, $q \neq min\ M_\alpha$ com $\frac{p}{q} = u$.

Para isso, seja o racional $s \notin \alpha$, com $s \neq min\ M_\alpha$. Para cada $n \in \mathbb{N}$, consideremos o racional

$$q_n = s \cdot u^n.$$



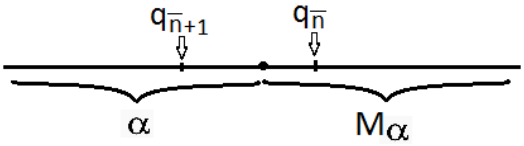
Observe que, da hipótese do lema, u é um número racional e $0 < u < 1$.

Seja $\overline{n}$ o máximo dos naturais n para os quais $q_n \in M_\alpha$ e $q_n \neq min\ M_\alpha$.

Note que necessariamente existe $\overline{n} \in \mathbb{N}$ com essa propriedade pois, caso contrário, teríamos $q_n \in M_\alpha$ para qualquer $n \in \mathbb{N}$, porém, sabemos que a partir de algum n_0 teremos $s \cdot u^n < a$ para $n > n_0$.

Observe que sendo $\overline{n}$ o máximo dos naturais com tal característica , então, para $\overline{n}+1 > \overline{n}$, temos $\overline{n}+1 \notin M_\alpha$ e, portanto, $q_{\overline{n}+1} \in \alpha$ ou $q_{\overline{n}+1} = min\ M_\alpha$.

- 1º caso: $q_{\overline{n}} \in M_\alpha$ e $q_{\overline{n}+1} \in \alpha$.

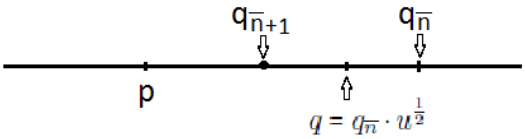


Basta tomar $q = q_{\overline{n}}$ e $p = q_{\overline{n}+1}$, pois:

$$\frac{p}{q} = \frac{q_{\overline{n}+1}}{q_{\overline{n}}} = \frac{s \cdot u^{\overline{n}+1}}{s \cdot u^{\overline{n}}} = \frac{s \cdot u^{\overline{n}} \cdot u}{s \cdot u^{\overline{n}}} = u.$$

- 2º caso: $q_{\overline{n}} \in M_\alpha$ e $q_{\overline{n}+1} = min\ M_\alpha$ (que só poderá ocorrer se $min\ M_\alpha$ existir).

Neste caso tomaremos $q = q_{\overline{n}} \cdot u^{\frac{1}{2}}$ e $p = q_{\overline{n}+1} \cdot u^{\frac{1}{2}}$.



Daí,

$$\frac{p}{q} = \frac{q_{\overline{n}+1} \cdot u^{\frac{1}{2}}}{q_{\overline{n}} \cdot u^{\frac{1}{2}}} = \frac{s \cdot u^{\overline{n}+1} \cdot u^{\frac{1}{2}}}{s \cdot u^{\overline{n}} \cdot u^{\frac{1}{2}}} = \frac{s \cdot u^{\overline{n}} \cdot u \cdot u^{\frac{1}{2}}}{s \cdot u^{\overline{n}} \cdot u^{\frac{1}{2}}} = u.$$

■

A seguir trataremos de algumas propriedades da multiplicação no conjunto dos números reais.

Proposição 7.35. *Para a multiplicação em* $\mathbb{R}$ *valem as seguintes propriedades:*

M_1. *Associativa: dados* $\alpha, \beta, \gamma \in \mathbb{R}$, $(\alpha \cdot \beta) \cdot \gamma = \alpha \cdot (\beta \cdot \gamma)$.

M_2. *Comutativa: dados* $\alpha, \beta \in \mathbb{R}$, $\alpha \cdot \beta = \beta \cdot \alpha$.

M_3. *Elemento identidade: para qualquer* $\alpha \in \mathbb{R}$, $\alpha \cdot 1' = \alpha$.

M_4. *Inverso multiplicativo: para qualquer* $\alpha \in \mathbb{R}$, $\alpha \neq 0'$, *existe* α^{-1} *tal que* $\alpha \cdot \alpha^{-1} = 1'$.

M_5. *Distributiva: dados* $\alpha, \beta, \gamma \in \mathbb{R}$, $\alpha \cdot (\beta + \gamma) = \alpha \cdot \beta + \alpha \cdot \gamma$.

Demonstração: A seguir, as demonstrações de cada propriedade da multiplicação em $\mathbb{R}$.

M_1. *Associativa:*

Para mostrar que dados $\alpha, \beta, \gamma \in \mathbb{R}$, $(\alpha \cdot \beta) \cdot \gamma = \alpha \cdot (\beta \cdot \gamma)$, é necessário mostrar que $(\alpha \cdot \beta) \cdot \gamma \subset \alpha \cdot (\beta \cdot \gamma)$ e que $\alpha \cdot (\beta \cdot \gamma) \subset (\alpha \cdot \beta) \cdot \gamma$ (definição 2.13).

Seja $w \in (\alpha \cdot \beta) \cdot \gamma$ qualquer, se $w \leq 0$, então $w \in \alpha \cdot (\beta \cdot \gamma)$ por definição; caso $w > 0$, então $w = u \cdot z$ tal que $u \in \alpha \cdot \beta$, $u > 0$ e $z \in \gamma$, $z > 0$. Uma vez que $u \in \alpha \cdot \beta$, segue que $u = x \cdot y$ tal que $x \in \alpha$ e $y \in \beta$ (veja que $w, u, z, x, y \in \mathbb{Q}$). Daí, basta lembrar que a propriedade associativa pode ser aplicada aos números racionais, segundo a proposição 6.16:

$$w = u \cdot z = (x \cdot y) \cdot z = x \cdot (y \cdot z) = x \cdot v.$$

Segue que $w = x \cdot v$ tal que $x \in \alpha$ e $v = y \cdot z \in \beta \cdot \gamma$. Ou seja, $w \in \alpha \cdot (\beta \cdot \gamma)$.

Consequentemente $(\alpha \cdot \beta) \cdot \gamma \subset \alpha \cdot (\beta \cdot \gamma)$.

De maneira análoga mostramos que $\alpha \cdot (\beta \cdot \gamma) \subset (\alpha \cdot \beta) \cdot \gamma$.

Portanto, para quaisquer $\alpha, \beta, \gamma \in \mathbb{R}$, segue que $(\alpha \cdot \beta) \cdot \gamma = \alpha \cdot (\beta \cdot \gamma)$.

M_2. *Comutativa:*

Para mostrar que dados $\alpha, \beta \in \mathbb{R}$, $\alpha \cdot \beta = \beta \cdot \alpha$, é necessário mostrar que $\alpha \cdot \beta \subset \beta \cdot \alpha$ e que $\beta \cdot \alpha \subset \alpha \cdot \beta$ (definição 2.13).

Seja $w \in \alpha \cdot \beta$ qualquer, se $w \leq 0$, então $w \in \beta \cdot \alpha$ por definição; caso $w > 0$, então $w = x \cdot y$ tal que $x \in \alpha$, $x > 0$ e $y \in \beta$, $y > 0$ (veja que $w, x, y \in \mathbb{Q}$). Daí, basta lembrar que a propriedade comutativa pode ser aplicada aos números racionais, segundo a proposição 6.16:

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

Segue que $w = y \cdot x$ tal que $y \in \beta$ e $x \in \alpha$. Ou seja, $w \in \beta \cdot \alpha$.

Logo, $\alpha \cdot \beta \subset \beta \cdot \alpha$.

De maneira análoga mostramos que $\beta \cdot \alpha \subset \alpha \cdot \beta$.

Portanto, para quaisquer $\alpha, \beta, \in \mathbb{R}$, segue que $\alpha \cdot \beta = \beta \cdot \alpha$.

M_3. *Elemento identidade:*

Suponhamos, inicialmente, $\alpha > 0'$.

Precisamos mostrar que para qualquer $\alpha \in \mathbb{R}$, temos que $\alpha \cdot 1' = \alpha$, ou seja, será necessário provar que $\alpha \cdot 1' \subset \alpha$ e que $\alpha \subset \alpha \cdot 1'$. Lembremos que $1' = \{x \in \mathbb{Q} \,/\, x < 1\}$.

(a) $\alpha \cdot 1' \subset \alpha$:

Lembramos, inicialmente, que $\alpha \cdot 1' = \mathbb{Q}_- \cup \{x \cdot y \,/\, x \in \alpha, x > 0; 0 < y < 1\}$.

Agora, se $x \in \alpha \cdot 1'$ e $x \leq 0$, temos que $x \in \alpha$. Já se $x \in \alpha \cdot 1'$ e $x > 0$, então $x = a \cdot u$, com $a \in \alpha$, $a > 0$, e $0 < u < 1$.

De $u < 1$ e $a > 0$, temos que $a \cdot u < a$ e, portanto, $x = a \cdot u \in \alpha$.

Portanto, $\alpha \cdot 1' \subset \alpha$.

(b) $\alpha \subset \alpha \cdot 1'$:

Se $x \in \alpha$ e $x \leq 0$, temos que $x \in \alpha \cdot 1'$. Já se $x \in \alpha$ e $x > 0$, então existe $a \in \alpha$ com $x < a$.

Assim, $x = a \cdot \dfrac{x}{a} \in \alpha \cdot 1'$, pois, $a \in \alpha$, $a > 0$, e $\dfrac{x}{a} < 1$, com $\dfrac{x}{a} > 0$.

Portanto $\alpha \subset \alpha \cdot 1'$.

Provamos, assim, que se $\alpha > 0'$, então $\alpha = \alpha \cdot 1'$.

Se $\alpha = 0'$, pela definição de produto, $\alpha \cdot 1' = 0' \cdot 1' = 0' = \alpha$.

Se $\alpha < 0'$, $\alpha \cdot 1' = -[(-\alpha) \cdot 1'] = -[-\alpha] = \alpha$.

M_4. *Inverso multiplicativo:*

Seja α um número real tal que $\alpha = \{x \in \mathbb{Q} \,/\, x < r\}$. Já sabemos pelo lema 7.32 que $\beta = \mathbb{Q}_- \cup \left\{p \in \mathbb{Q} \,/\, p > 0, \dfrac{1}{p} \in M_\alpha, \dfrac{1}{p} \neq min\ M_\alpha\right\}$ é um número real.

Provemos que $\alpha \cdot \beta = 1'$, para isso será necessário mostrar, segundo a definição 2.13, que $\alpha \cdot \beta \subset 1'$ e que $1' \subset \alpha \cdot \beta$.

(a) $\alpha \cdot \beta \subset 1'$:

Seja $x \in \alpha \cdot \beta$ qualquer. Se $x \leq 0$, então $x \leq 0 < 1$ e, portanto, $x \in 1'$. Se $x > 0$, então $x = a \cdot b$ com $a \in \alpha$, $a > 0$ e $b \in \beta$, $b > 0$.

Sendo $b > 0 \in \beta$, temos que $\dfrac{1}{b} \in M_\alpha, \dfrac{1}{b} \neq min\ M_\alpha$. Ou seja, $\dfrac{1}{b} > r$. Como $a \in \alpha$, $a < r$. Temos que:

$$a < r < \frac{1}{b} \Rightarrow a < \frac{1}{b}.$$

Logo, $a \cdot b < 1$. Segue que, $a \cdot b \in 1'$.

Portanto, $\alpha \cdot \beta \subset 1'$.

(b) $1' \subset \alpha \cdot \beta$:

Seja $x \in 1'$ qualquer, então, $x \in \mathbb{Q}$ tal que $x < 1$.

Se $x < 0$, $x \in \mathbb{Q}_-$ e, então, $x \in \alpha \cdot \beta$ por definição.

Se $0 < x < 1$, precisamos mostrar que $x = a \cdot b$ para algum $a \in \alpha$, $a > 0$ e algum $b \in \beta$, $b > 0$.

Como $0 < x < 1$, o lema 7.34 garante que existem $a \in \alpha$ e $\frac{1}{b} \in M_\alpha$, com $\frac{1}{b} \neq min\ M_\alpha$, tais que $x = \frac{a}{\frac{1}{b}}$.

Assim, $x = a \cdot b$ com $a \in \alpha$ e $b \in \beta$.

Segue que $1' \subset \alpha + \beta$.

Portanto, $\alpha \cdot \beta = 1'$.

Indicaremos β por α^{-1}.

M_5. *Distributiva:*

Para mostrar que dados $\alpha, \beta, \gamma \in \mathbb{R}$, $\alpha \cdot (\beta + \gamma) = \alpha \cdot \beta + \alpha \cdot \gamma$, é necessário mostrar que $\alpha \cdot (\beta + \gamma) \subset \alpha \cdot \beta + \alpha \cdot \gamma$ e que $\alpha \cdot \beta + \alpha \cdot \gamma \subset \alpha \cdot (\beta + \gamma)$ (definição 2.13).

Seja $w \in \alpha \cdot (\beta + \gamma)$ qualquer. Se $w \leq 0$, então $w \in \alpha \cdot \beta + \alpha \cdot \gamma$ por definição. Se $w > 0$, então $w = x \cdot t$ tal que $x \in \alpha$, $x > 0$ e $t \in \beta + \gamma$, $t > 0$. Uma vez que $t \in \beta + \gamma$, segue que $t = y + z$ tal que $y \in \beta$ e $z \in \gamma$ (veja que $w, x, t, y, z \in \mathbb{Q}$). Daí, basta lembrar que a distributiva pode ser aplicada aos números racionais, segundo a proposição 6.16:

$$w = x \cdot t = x \cdot (y + z) = x \cdot y + x \cdot z = u + v.$$

Segue que $w = u + v$ tal que $u \in \alpha \cdot \beta$ e $v \in \alpha \cdot \gamma$. Ou seja, $w \in \alpha \cdot \beta + \alpha \cdot \gamma$.

Segue que $\alpha \cdot (\beta + \gamma) \subset \alpha \cdot \beta + \alpha \cdot \gamma$.

Veja ainda que $\alpha \cdot \beta + \alpha \cdot \gamma \subset \alpha \cdot (\beta + \gamma)$, pois dado $x \in \alpha \cdot \beta + \alpha \cdot \gamma$ qualquer, temos que se $x \leq 0$, $x \in \alpha \cdot (\beta + \gamma)$ por definição; e caso $x > 0$, $x = u + v$ com $u \in \alpha \cdot \beta$, $u > 0$ e $v \in \alpha \cdot \gamma$, $v > 0$.

Sendo $u \in \alpha \cdot \beta$, $u > 0$, $u = a_1 \cdot b$ com $a_1 \in \alpha$, $a_1 > 0$ e $b \in \beta$, $b > 0$. Também sendo $v \in \alpha \cdot \gamma$, $v > 0$, $v = a_2 \cdot c$ com $a_2 \in \alpha$, $a_2 > 0$ e $c \in \gamma$, $c > 0$. Consideremos ainda a como sendo o maior valor entre a_1 e a_2. Daí,

$$x = u + v = a_1 \cdot b + a_2 \cdot c < a \cdot b + a \cdot c = a \cdot (b + c)$$

Note que $a \cdot (b + c) \in \alpha \cdot (\beta + \gamma)$

Da definição de corte (definição 7.12), sabemos que como $x < a \cdot (b + c)$ e $a \cdot (b + c) \in \alpha \cdot (\beta + \gamma)$, segue que $x \in \alpha \cdot (\beta + \gamma)$.

Portanto, para quaisquer $\alpha, \beta, \gamma \in \mathbb{R}$, segue que $\alpha \cdot (\beta + \gamma) = \alpha \cdot \beta + \alpha \cdot \gamma$.

■

Lema 7.36. *O elemento identidade citado acima é único.*

Demonstração: Sabemos que para qualquer $\alpha \in \mathbb{R}$, $\alpha \cdot 1' = \alpha$.

Supomos que o elemento identidade não seja único, ou seja, existe $\beta \in \mathbb{R}$ tal que $\alpha \cdot \beta = \alpha$ para qualquer $\alpha \in \mathbb{R}$.

Em particular, para $\alpha = 1'$, temos:

$$1' \cdot \beta = 1' \Rightarrow \beta = 1'.$$

Portanto, o elemento identidade é único.

■

Lema 7.37. *O inverso multiplicativo citado acima é único.*

Demonstração: Para todo $\alpha \in \mathbb{R}$ existe $\alpha^{-1} \in \mathbb{R}$ de modo que $\alpha \cdot \alpha^{-1} = 1'$.

Supomos que exista outro inverso multiplicativo para α, ou seja, existe $\theta \in \mathbb{R}$ tal que $\alpha \cdot \theta = 1'$.

Sendo $\alpha \cdot \alpha^{-1} = 1'$ e $\alpha \cdot \theta = 1'$, temos que $\alpha \cdot \alpha^{-1} = \alpha \cdot \theta$. Daí, multiplicando por α^{-1} de ambos os lados da igualdade, obtemos:

$$\alpha \cdot \alpha^{-1} = \alpha \cdot \theta \rightarrow \alpha^{-1} \cdot (\alpha \cdot \alpha^{-1}) = \alpha^{-1} \cdot (\alpha \cdot \theta).$$

Associando as multiplicações convenientemente e fazendo uso da propriedade do inverso multiplicativo, temos que:

$$\alpha^{-1} \cdot (\alpha \cdot \alpha^{-1}) = (\alpha^{-1} \cdot \alpha) \cdot \theta \rightarrow 1' \cdot \alpha^{-1} = 1' \cdot \theta \rightarrow \alpha^{-1} = \theta.$$

Portanto, o inverso multiplicativo é único.

■

Proposição 7.38. *A multiplicação e a relação de ordem são compatíveis no seguinte sentido: dados* $\alpha, \beta, \gamma \in \mathbb{R}$, $\alpha \leq \beta$ *e* $0' \leq \gamma \Rightarrow \alpha \cdot \gamma \leq \beta \cdot \gamma$.

Demonstração: Sejam $\alpha, \beta, \gamma \in \mathbb{R}$ tal que $\alpha \leq \beta$. Queremos mostrar que dado $\gamma \geq 0'$, $\alpha \cdot \gamma \leq \beta \cdot \gamma$. Pela definição 7.12, basta verificarmos que $\alpha \cdot \gamma \subset \beta \cdot \gamma$.

Seja $w \in \alpha \cdot \gamma$. Se $w \leq 0$, $w \in \beta \cdot \gamma$ por definição. Se $w > 0$, segue que $w = x \cdot z$ para algum $x \in \alpha$ e algum $z \in \gamma$, $x > 0$, $z > 0$.

Da hipótese, como $\alpha \leq \beta$, sabemos pela mesma definição já citada que $\alpha \subset \beta$. Logo, uma vez que $x \in \alpha$, temos que $x \in \beta$.

Assim, $w = x \cdot z$ para algum $x \in \beta$ e algum $z \in \gamma$.

Portanto, $w \in \beta \cdot \gamma$, demonstrando que $\alpha \cdot \gamma \subset \beta \cdot \gamma$.

Novamente pela definição 7.12, fica garantido que $\alpha \cdot \gamma \leq \beta \cdot \gamma$.

■

7.5 Teorema do Supremo

Realizadas as operações adição e multiplicação, o próximo objetivo é mostrar que todo subconjunto não vazio limitado superiormente possuí menor cota superior.

Relembre que um subconjunto A de $\mathbb{R}$ se diz limitado superiormente se existe um número real m tal que para todo $\alpha \in A$, $\alpha \leq m$.

Exemplo 7.39. O intervalo aberto $A = (-\infty, a)$ é limitado superiormente, pois existe $m = a + 1$ tal que $\alpha \leq m$ para qualquer $\alpha \in A$.

E ainda, o número real m será uma cota superior e a menor dessas cotas superiores será o supremo de A.

Lema 7.40. *Seja A um subconjunto não vazio de $\mathbb{R}$ limitado superiormente. Então, a reunião de todos os números reais pertencentes a A é um número real. Ou seja,*

$$\gamma = \cup\alpha = \{x \in \mathbb{Q} \ / \ x \in \alpha \text{ para algum } \alpha \in A\}$$

é um número real.

Demonstração: Para mostrar que o conjunto γ é um número real, é necessário mostrar que este é um corte no conjunto dos números racionais. Para tanto, mostraremos os três itens da definição 7.12.

(i) Da hipótese sabemos que $A \neq \varnothing$, logo existe $\alpha \in A$ e, como $\alpha \neq \varnothing$, temos que $\gamma \neq \varnothing$.

Sendo A limitado superiormente, existe um número real m tal que $\alpha \leq m$ para todo $\alpha \in A$. Como m é um número real, existe um número racional x, com $x \notin m$. Daí, para todo $\alpha \in A$, $x \notin \alpha$. Logo $x \notin \gamma$. Portanto $\gamma \neq \mathbb{Q}$.

(ii) Sejam p e q dois números racionais quaisquer. Vamos supor $p \in \gamma$ e $q < p$. Queremos mostrar que $q \in \gamma$.

Para isso, considere que:

$$p \in \gamma \Rightarrow p \in \alpha \text{ para algum } \alpha \in \gamma.$$

Agora, uma vez que α é um número real, $p \in \alpha$ e $q < p$, temos que $q \in \alpha$.

Por fim, se $q \in \alpha$, então $q \in \gamma$.

(iii) Seja $p \in \gamma$, logo $p \in \alpha$ para algum $\alpha \in \gamma$. Como α é um número real, existe $q \in \alpha$ tal que $q > p$. Sendo $q \in \alpha$, temos que $q \in \gamma$ com $q > p$.

Logo, γ é um corte em $\mathbb{Q}$ e, portanto, um número real.

■

Apresentamos a seguir o resultado conhecido como Teorema do Supremo.

Teorema 7.41. *Se A for um subconjunto não vazio de $\mathbb{R}$ limitado superiormente, então A admitirá supremo.*

Demonstração: Seja $\gamma = \cup\alpha$. Pelo lema anterior, já sabemos que γ é um corte em $\mathbb{Q}$ e, portanto, um número real. Vamos mostrar que $\gamma = sup\ A$.

Como γ é a reunião de todos os números reais pertencentes a A, segue que para todo $\alpha \in A$, $\alpha \subset \gamma$. Pela definição 7.18, temos que $\alpha < \gamma$. Segue que γ é cota superior de A.

Seja β uma cota superior qualquer de A, assim para todo $\alpha \in A$ temos que $\alpha < \beta$. Portanto, $\alpha \subset \beta$.

Segue que $\cup\alpha \subset \beta$, ou seja, $\gamma \subset \beta$. O que implica que $\gamma < \beta$.

Assim, γ é a menor cota superior de A. Isto é, $\gamma = sup\ A$.

■

7.6 Imersão de $\mathbb{Q}$ em $\mathbb{R}$

Vejamos a seguir como estabelecer uma imersão de $\mathbb{Q}$ em $\mathbb{R}$. Desejamos, por exemplo, que o elemento a no conjunto dos números racionais e o número real a' sejam identificados.

Para tanto, seja f a função definida por:

$$\begin{array}{rccc} f: & \mathbb{Q} & \longrightarrow & \mathbb{R} \\ & a & \longmapsto & a' \end{array}$$

para todo $a \in \mathbb{Q}$.

Alguns exemplos dessa identificação:

$$\vdots$$

$$f\left(\frac{-3}{2}\right) = \left\{x \in \mathbb{Q} \ / \ x < \frac{-3}{2}\right\}$$

$$f(-1) = \{x \in \mathbb{Q} \ / \ x < -1\}$$

$$f(0) = \{x \in \mathbb{Q} \ / \ x < 0\}$$

$$f\left(\frac{1}{2}\right) = \left\{x \in \mathbb{Q} \ / \ x < \frac{1}{2}\right\}$$

$$f(1) = \{x \in \mathbb{Q} \ / \ x < 1\}$$

$$\vdots$$

A função f considerada é chamada de imersão de $\mathbb{Q}$ em $\mathbb{R}$.

Proposição 7.42. *f é injetora.*

Demonstração: Dados $a, b \in \mathbb{Q}$, mostremos que se $a \neq b$, então $a' \neq b'$.

Sejam $a' = \{x \in \mathbb{Q} \mid x < a\}$ e $b' = \{x \in \mathbb{Q} \mid x < b\}$.

Sendo $a \neq b$, temos que $a > b$ ou $b > a$. Vamos supor, sem perda de generalidade, $b > a$.

Note que $a \in b'$, mas $a \notin a'$, o que implica que $b' \not\subset a'$.

Segue que $b' \neq a'$.

■

Proposição 7.43. *Dados $a, b \in \mathbb{Z}$, temos que:*

(i) $f(a+b) = f(a) + f(b)$;

(ii) $f(a \cdot b) = f(a) \cdot f(b)$;

(iii) *Se $a \leq b$, então $f(a) \leq f(b)$.*

Demonstração: Dados $a, b \in \mathbb{Z}$,

(i) Mostrar que f$(a+b) = f(a) + f(b)$ é equivalente a mostrar que $(a+b)' = a' + b'$. Para tanto, será necessário mostrar, segundo a definição 2.13 que $(a+b)' \subset a' + b'$ e que $a' + b' \subset (a+b)'$.

$(a+b)' \subset a' + b'$: Seja $p \in (a+b)'$, então $p < a + b$. Consideremos:

$$q = a - \frac{a+b-p}{2}$$

e

$$t = b - \frac{a+b-p}{2}.$$

Como $a + b > p$, então $a + b - p > 0$ e, consequentemente, $-(a+b-p) < 0$. Daí,

$$q = a - \frac{a+b-p}{2} < a$$

e

$$t = b - \frac{a+b-p}{2} < b.$$

Logo, $q \in a'$ e $t \in b'$. E ainda,

$$q + t = a - \frac{a+b-p}{2} + b - \frac{a+b-p}{2} = \frac{2 \cdot a - a - b + p}{2} + \frac{2 \cdot b - a - b + p}{2} = \frac{2 \cdot a - a - b + p + 2 \cdot b - a - b + p}{2} = \frac{2 \cdot p}{2} = p.$$

Portanto, $p \in a' + b'$. Segue que $(a+b)' \subset a' + b'$.

$a' + b' \subset (a+b)'$: Seja $p \in a' + b'$, então $p = q + t$ onde $q \in a'$ e $t \in b'$. Segue que $q < a$ e $t < b$. Ainda, $p = q + t < a + b$.

Logo, $p \in (a+b)'$. Portanto $a' + b' \subset (a+b)'$.

(ii) Mostrar que $f(a \cdot b) = f(a) \cdot f(b)$ é equivalente a mostrar que $(a \cdot b)' = a' \cdot b'$. Para tanto, será necessário mostrar, segundo a definição 2.13 que $(a \cdot b)' \subset a' \cdot b'$ e que $a' \cdot b' \subset (a \cdot b)'$.

$(a \cdot b)' \subset a' \cdot b'$: Seja $a \geq 0$, $b \geq 0$ tal que $0' \subset a' \cap b'$. Se $r \in (a \cdot b)'$, então $r < a \cdot b$.

Se $r < 0$, como $a \geq 0$ e $b \geq 0$ é imediato que $r \in a' \cdot b'$.

Supondo $r \geq 0$ devemos ter $a > 0$ e $b > 0$. Tomando $s = \dfrac{r + a \cdot b}{2}$, ou seja, $r < s < a \cdot b$.

Tomamos $r = a \cdot \dfrac{r}{s} \cdot b \cdot \dfrac{s}{a \cdot b}$. Veja que $r < s \Rightarrow \dfrac{r}{s} < 1$, então, $a \cdot \dfrac{r}{s} < a$. Portanto, $a \cdot \dfrac{r}{s} \in a'$.

Analogamente, como $s < a \cdot b$, segue que $\dfrac{s}{a \cdot b} < 1$, então $b \cdot \dfrac{s}{a \cdot b} < b$. Portanto, $b \cdot \dfrac{s}{a \cdot b} \in b'$.

Segue que $r \in a' \cdot b'$.

Logo, $(a \cdot b)' \subset a' \cdot b'$.

$a' \cdot b' \subset (a \cdot b)'$: Seja $r \in a' \cdot b'$, se $r < 0$, então $r \in (a \cdot b)'$. Já se $r \geq 0$, então $r = s \cdot t$ onde $s \in a'$ e $t \in b'$, $s \geq 0$ e $t \geq 0$. Segue que $s < a$ e $t < b$. Ainda, $p = s \cdot t < a \cdot b$.

Logo, $r \in (a \cdot b)'$. Portanto $a' \cdot b' \subset (a \cdot b)'$.

(iii) Dados $a, b \in \mathbb{Q}$, mostremos que se $a < b$, então $a' < b'$.

Sejam $a' = \{x \in \mathbb{Q} \;/\; x < a\}$ e $b' = \{x \in \mathbb{Q} \;/\; x < b\}$.

Para qualquer $p \in a'$, temos que $p < a$. Uma vez que $a < b$, segue que $p < b$. Logo, para qualquer $p \in a'$, teremos $p \in b'$, o que implica que $a' \subset b'$. Da definição 7.18, segue que $a' < b'$.

■

Sendo f uma função injetora, existe uma correspondência biunívoca entre $\mathbb{Q}$ e $f(\mathbb{Q})$. Daí, é válido identificar cada $a \in \mathbb{Q}$ com o corte a'. Uma vez que $f(\mathbb{Q}) \subset \mathbb{R}$, podemos fazer um abuso de notação e considerarmos $\mathbb{Q} \subset \mathbb{R}$ para indicar a imersão de $\mathbb{Q}$ em $\mathbb{R}$.

8 Conjuntos Numéricos no Ensino Médio

Ao longo desse capítulo, tratamos das observações particulares que tivemos ao observar alguns livros didáticos, bem como das leituras das referências [5], [7], [8] e [9].

Durante essa dissertação, tratamos das construções formais dos conjuntos numéricos que estudamos desde o Ensino Fundamental, partindo do conjunto dos números naturais até o conjunto dos números reais. Também pudemos vivenciar as propriedades de cada um desses conjuntos.

Após a observação de diversos materiais, pode-se verificar que tanto em livros didáticos quanto em apostilas não existe a preocupação de contar o processo de construção desses conjuntos e nem mesmo de citar os abusos de notação que acabamos cometendo após as imersões de um conjunto no outro.

Este trabalho surgiu para que pudéssemos perceber que esta inclusão não é tão óbvia quanto os autores tratam nos livros, uma vez que em cada sistema numérico temos objetos de natureza completamente diferentes dos demais.

Desde o ensino fundamental, quando são apresentados pela primeira vez, o conjunto dos números naturais é exposto como um conjunto que começa no número zero e aumenta de um em um. No ensino médio, quando reaparece, essa ideia prossegue da mesma maneira. Algumas vezes o conjunto é apresentado até mesmo fazendo uso do conjunto dos números inteiros, de maneira que os alunos acabam entendendo que os números naturais são aqueles números inteiros e positivos. Poucas referências do ensino médio que foram observadas contam aos alunos que os números naturais surgiram da necessidade de contar.

Os números inteiros negativos e suas propriedades são introduzidos para dar significado a algumas subtrações que deixam de fazer sentido quando estamos no conjunto dos números naturais. Cabe lembrar que, na verdade, a subtração nem define uma operação para os números naturais. Depois que esses números são introduzidos, há uma tentativa nada rigorosa de estender as operações, que antes eram utilizadas no conjunto dos números naturais, para o conjunto dos números inteiros.

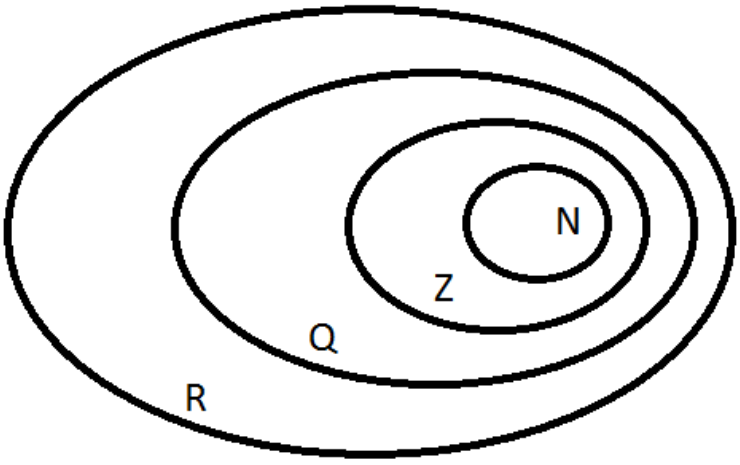
Se buscarmos fontes históricas, descobriremos que alguns matemáticos encontraram uma maneira de, partindo dos números naturais, construir os números inteiros sem

mencionar a subtração, mas trazendo sua essência, como vimos aqui nesse trabalho.

Ainda no ensino fundamental, aprende-se que números racionais são, na verdade, razões entre dois números inteiros. Razão, naquele contexto, aponta para a mesma ideia de divisão. De maneira nada rigorosa, quando se compara o número racional a uma divisão entre dois inteiros, tenta-se impor nos números inteiros uma propriedade que ele não tem, uma vez que para números inteiros só faz sentido falarmos em adição, mutiplicação ou subtração.

Na apresentação do número real ao longo do ensino, percebe-se que seu estudo não passa de uma necessidade de números que não se enquadram no conjunto dos números racionais, aos quais nomeamos números irracionais; e costuma-se associar cada número real a um ponto de uma reta. Também é muito comum tentar definir um número irracional via uma representação decimal não periódica. Finaliza-se dizendo que ao unirmos o conjunto dos números racionais com o dos números irracionais, obtém-se o conjunto dos números reais. Em nenhum momento cita-se a natureza desses novos números comparados com os anteriores.

Por fim, podemos visualizar abaixo a imagem mais clássica que vem sendo apresentada nos livros didáticos, que, de certa forma, acaba auxiliando na ideia um tanto errônea dessas inclusões.



Esperamos deixar claro que do ponto de vista rigoroso da matemática, não faz sentido apresentar tal configuração, uma vez que os elementos de cada conjunto são de natureza diferente dos demais. Na verdade apenas exibimos, a cada mudança de conjunto numérico, uma função injetora que preserva as operações do conjunto anterior, permitindo que sua imagem tenha uma cópia algébrica no novo conjunto numérico.

Referências

[1] Boyer, C. B. *História da Matemática*. Editora Edgard Blucher Ltda, 2012.

[2] Ifrah, G. *Os Números, A História de uma Grande Invenção*. Editora Globo, 2007.

[3] Domingues, H. H. *Fundamentos de Aritmética*. Editora Atual, 2009.

[4] Domingues, H. H., Iezzi, G. *Álgebra Moderna*. Editora Atual, 2003.

[5] Lima, E. L., Carvalho, P. C. P., Wagner, E., Morgado, A. C. *A Matemática do Ensino Médio*. Editora Sociedade Brasileira de Matemática, 2012.

[6] Guidorizzi, H. L., *Um Curso de Cálculo*. Editora LTC, 2001.

[7] Ferreira, J. *A construção dos números*. Editora Sociedade Brasileira de Matemática, 2013.

[8] Ripoll, C., Rangel, L., Giraldo, V. *Livro do Professor de Matemática na Educação Básica: Números Naturais*. Editora Sociedade Brasileira de Matemática, 2016.

[9] Ripoll, C., Rangel, L., Giraldo, V. *Livro do Professor de Matemática na Educação Básica: Números Inteiros*. Editora Sociedade Brasileira de Matemática, 2016.