



**INSTITUTO LATINO-AMERICANO DE CIÊNCIAS
DA VIDA E DA NATUREZA (ILACVN)**

MATEMÁTICA – LICENCIATURA

CONSTRUÇÃO DOS CONJUNTOS NUMÉRICOS: \mathbb{N} , \mathbb{Z} , \mathbb{Q} E \mathbb{R}

MATHEUS GRAEFF

Foz do Iguaçu
2023



**INSTITUTO LATINO-AMERICANO DE CIÊNCIAS
DA VIDA E DA NATUREZA (ILACVN)**

MATEMÁTICA – LICENCIATURA

CONSTRUÇÃO DOS CONJUNTOS NUMÉRICOS: \mathbb{N} , \mathbb{Z} , \mathbb{Q} E \mathbb{R}

MATHEUS GRAEFF

Trabalho de Conclusão de Curso apresentado ao Instituto Latino-Americano de Ciências da Vida e da Natureza da Universidade Federal da Integração Latino-Americana, como requisito parcial à obtenção do título de Licenciado em Matemática

Orientador(a): Prof. Dr. Víctor Arturo Martínez León

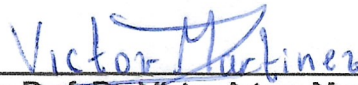
Foz do Iguaçu
2023


MATHEUS GRAEFF


CONSTRUÇÃO DOS CONJUNTOS NUMÉRICOS: N, Z, Q, E, R

Trabalho de Conclusão de Curso apresentado ao Instituto Latino-Americano de Ciências da Vida e da Natureza da Universidade Federal da Integração Latino-Americana, como requisito parcial à obtenção do título de Licenciado em Matemática.

BANCA EXAMINADORA


Orientador: Prof. Dr. Víctor Arturo Martínez León
(UNILA)


Prof. Dr. Rodrigo Bloor
(UNILA)


Prof. Dr. Newton Mayer Solórzano Chávez
(UNILA)

Foz do Iguaçu, 14 de junho de 2023.

TERMO DE SUBMISSÃO DE TRABALHOS ACADÊMICOS

Nome completo do autor(a): Matheus Graeff

Curso: Matemática – Licenciatura

Tipo de Documento

- | | |
|---|--|
| <input checked="" type="checkbox"/> graduação | <input type="checkbox"/> artigo |
| <input type="checkbox"/> especialização | <input checked="" type="checkbox"/> trabalho de conclusão de curso |
| <input type="checkbox"/> mestrado | <input type="checkbox"/> monografia |
| <input type="checkbox"/> doutorado | <input type="checkbox"/> dissertação |
| | <input type="checkbox"/> tese |
| | <input type="checkbox"/> CD/DVD – obras audiovisuais |
| | <input type="checkbox"/> |

Título do trabalho acadêmico: Construção dos Conjuntos Numéricos: \mathbb{N} , \mathbb{Z} , \mathbb{Q} e \mathbb{R}

Nome do orientador(a): Víctor Arturo Martínez León

Data da Defesa: 14/06/2023

Licença não-exclusiva de Distribuição

O referido autor(a):

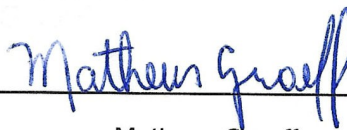
a) Declara que o documento entregue é seu trabalho original, e que o detém o direito de conceder os direitos contidos nesta licença. Declara também que a entrega do documento não infringe, tanto quanto lhe é possível saber, os direitos de qualquer outra pessoa ou entidade.

b) Se o documento entregue contém material do qual não detém os direitos de autor, declara que obteve autorização do detentor dos direitos de autor para conceder à UNILA – Universidade Federal da Integração Latino-Americana os direitos requeridos por esta licença, e que esse material cujos direitos são de terceiros está claramente identificado e reconhecido no texto ou conteúdo do documento entregue.

Se o documento entregue é baseado em trabalho financiado ou apoiado por outra instituição que não a Universidade Federal da Integração Latino-Americana, declara que cumpriu quaisquer obrigações exigidas pelo respectivo contrato ou acordo.

Na qualidade de titular dos direitos do conteúdo supracitado, o autor autoriza a Biblioteca Latino-Americana – BIUNILA a disponibilizar a obra, gratuitamente e de acordo com a licença pública *Creative Commons Licença 3.0 Unported*.

Foz do Iguaçu, 19 de junho de 2023.



Matheus Graeff

Dedico este trabalho aos meus pais.

AGRADECIMENTOS

Dedico primeiramente a Deus por sempre estar ao meu lado nos momentos de dificuldade, me dando forças nessa jornada para não desistir.

Dedico este trabalho aos meus pais Salete Silva e Moacir Graeff, que sempre me apoiaram e incentivaram em cada passo da minha jornada acadêmica. Agradeço por todo o amor, paciência e suporte incondicional ao longo desses anos. Sem vocês, nada disso seria possível.

Também dedico este trabalho aos meus professores que se fizeram presentes em todas as etapas da graduação, aos professores da banca, mas em especial ao meu orientador Dr. Víctor León, que me guiou e compartilhou seus conhecimentos durante essa caminhada. Agradeço por sua dedicação e paciência em me ajudar a expandir meus horizontes em todas as fases desse projeto.

Aos meus amigos, que enfrentaram desafios semelhantes e estiveram ao meu lado, compartilhando risadas, momentos de estudo e superação.

A todos que mencionei e a todos aqueles que contribuíram de alguma forma para minha trajetória acadêmica, meu sincero agradecimento.

Os números são a criação livre da mente humana.
Richard Dedekind

RESUMO

Neste trabalho, foram estudadas a construção dos conjuntos dos números naturais (\mathbb{N}), dos números inteiros (\mathbb{Z}), dos números racionais (\mathbb{Q}) e dos números reais (\mathbb{R}). A construção dos números naturais foi realizada por meio dos axiomas de Dedekind. A construção dos números inteiros foi feita por classes de equivalência em $\mathbb{N} \times \mathbb{N}$. A construção dos números racionais foi realizada por classes de equivalência de elementos admissíveis em $\mathbb{Z} \times \mathbb{Z}$. Finalmente, a construção do conjunto dos números reais foi realizado através dos chamados *cortes de Dedekind*, partindo do conjunto dos números racionais.

Palavras-chaves: números naturais; números inteiros; números racionais; números reais.

RESUMEN

En este trabajo, fueron estudiadas la construcción de los conjuntos de los números naturales (\mathbb{N}), de los números enteros (\mathbb{Z}), de los números racionales (\mathbb{Q}) y de los números reales (\mathbb{R}). La construcción de los números naturales fue realizada por medio de los axiomas de Dedekind. La construcción de los números enteros fue hecha por clases de equivalencia en $\mathbb{N} \times \mathbb{N}$. La construcción de los números racionales fue realizada por clases de equivalencia de elementos admisibles en $\mathbb{Z} \times \mathbb{Z}$. Finalmente, la construcción del conjunto de los números reales fue realizado a través de los llamados *cortes de Dedekind*, partiendo del conjunto de los números racionales.

Palabras clave: números naturales; números enteros; números racionales; números racionales.

ABSTRACT

In this work, was studied the construction of the sets of the natural numbers (\mathbb{N}), the integers (\mathbb{Z}), the rational numbers (\mathbb{Q}), and the real numbers (\mathbb{R}). The construction of the natural numbers was carried out through the Dedekind's axioms. The construction of the integers was done by equivalence classes in $\mathbb{N} \times \mathbb{N}$. The construction of the rational numbers was carried out by equivalence classes of admissible elements in $\mathbb{Z} \times \mathbb{Z}$. Finally, the construction of set of real numbers was carried out through the so-called *Dedekind cuts*, starting from the set of rational numbers.

Keywords: natural numbers; integers; rational numbers; real numbers.

SUMÁRIO

1	INTRODUÇÃO	11
2	TEORIA DE CONJUNTOS, RELAÇÕES E FUNÇÕES	15
2.1	TEORIA DE CONJUNTOS	15
2.2	RELAÇÕES, FUNÇÕES E OPERAÇÕES BINÁRIAS	21
3	CONSTRUÇÃO DOS NÚMEROS NATURAIS	28
3.1	ADIÇÃO E MULTIPLICAÇÃO EM \mathbb{N}	31
3.2	GRUPOS E SEMIGRUPOS	39
3.3	ORDEM EM \mathbb{N}	40
4	CONSTRUÇÃO DOS NÚMEROS INTEIROS	48
4.1	ADIÇÃO EM \mathbb{Z}	49
4.2	MULTIPLICAÇÃO EM \mathbb{Z}	54
4.3	ANÉIS	57
4.4	ORDEM EM \mathbb{Z}	58
4.5	IMERSÕES	64
4.6	ISOMORFISMO	66
5	CONSTRUÇÃO DOS NÚMEROS RACIONAIS	69
5.1	ADIÇÃO E MULTIPLICAÇÃO EM \mathbb{Q}	70
5.2	ORDEM EM \mathbb{Q}	75
5.3	IMERSÕES	77
6	CONSTRUÇÃO DOS NÚMEROS REAIS	79
6.1	CORTES DE DEDEKIND	79
7	CONSIDERAÇÕES FINAIS	105
	REFERÊNCIAS	107

1 INTRODUÇÃO

Neste trabalho, é tratada a construção formal dos conjuntos numéricos, sendo eles: o conjunto dos números naturais, conjunto dos números inteiros, conjunto dos números racionais e em especial o conjunto dos números reais por cortes de Dedekind, respectivamente.

É feito um pequeno contexto histórico na busca da construção desses conjuntos numéricos, com o objetivo de entendermos a origem de cada um deles, mas somente para a compreensão do seu surgimento, sem tirar o foco do que realmente está sendo proposto neste trabalho.

Segundo (GUNDLACH, 1992), a criação e desenvolvimento do conceito de números naturais possuem indícios desde a pré-história, mas não existe uma datação específica, pois desde os tempos mais remotos a humanidade teve a necessidade de contar e quantificar os objetos, seja ovelhas, alimentos, etc. No entanto, a noção dos números naturais como uma sequência ordenada de elementos e símbolos surgiu mais tarde em diferentes culturas e períodos históricos. Segundo (BOYER, 2012), na Mesopotâmia, por volta de 2000 antes de Cristo, surgiram as primeiras tábuas cuneiformes contendo registros numéricos, o sistema de numeração era sexagesimal (base 60). Outro exemplo no antigo Império Romano, o sistema era baseado em algarismos romanos.

A princípio, os números naturais por muito tempo aparentavam ser suficientes para as necessidades de contar e quantificar objetos, mas na decorrência de novas situações, surgiu a necessidade de uma nova representação. Segundo (BOYER, 2012), as primeiras datações foram encontradas na Babilônia e no Egito, onde se utilizava as representações fracionárias em registros comerciais e medições de terra. Segundo (IFRAH, 1989), por volta de 3000 antes de Cristo, durante a época de cheias o rio Nilo submergia, deixando o solo com muitos nutrientes, onde as terras eram aptas para o cultivo na agricultura. Quando as águas baixavam, os agricultores demarcavam igualmente as terras para que ninguém tivesse mais terra que o outro, fazendo essa repartição igualmente. Eles perceberam que essas divisões não tornava números exatos e dessa forma, o noção de fração começou a ser entendida como uma parte de um inteiro.

Na Grécia antiga, segundo (BOYER, 2012) os matemáticos perceberam que os conjunto dos números naturais e racionais não abrangiam a totalidade dos números que conhecemos hoje. Foi na Grécia antiga, que os matemáticos começaram a investigar e aprofundar a compreensão dos números reais. Pitágoras e seus seguidores, estabeleceram que todos os números poderiam ser expressos como uma razão de dois números, conhecido como a fração. No entanto, perceberam a existência de um número que não poderia ser escrito dessa maneira, assim, descobriram propriedades interessantes, e a criação de números que não eram racionais estava ligeiramente ligada aos fatores de natureza geométrica e aritmética. O problema mais conhecido é o comprimento da diagonal do quadrado. Para um quadrado de comprimento 1, a diagonal não podia ser expressa como uma fração simples. Usando os argumentos geométricos e o Teorema de Pitágoras, eles descobriram que o comprimento da diagonal é a raiz quadrada de 2. Essa descoberta abriu portas para o estudo dos números irracionais e levou um avanço significativo na compreensão dos números reais.

Ao pensar no conjunto dos números inteiros introduzimos quantidades negativas, mas que por muito tempo foi-se discutido e não tão fácil de se enquadrar a ideia de quantidades negativas, por exemplo um vendedor tinha sete maçãs e vendeu três maçãs, seu estoque diminuiria, mas a ideia de -3 maçãs não era possível, aí a ideia dos números inteiros surge como uma extensão dos números naturais. Ao contrário dos números naturais, que representa a contagem de objetos, os números inteiros foram introduzidos para lidar com a ideia de falta ou dívida, bem como quantidade negativas. Neste trabalho, faremos uma apresentação não pela ordem cronológica, mas sim de uma maneira mais elegante, para que tenha coerência no entendimento.

A Análise Real que em sua forma mais básica é o estudo rigoroso das ideias do cálculo ocorre no contexto dos números reais, porque os números reais têm as propriedades necessárias para permitir que coisas como derivadas e integrais funcionem. Uma vez que tenhamos construído os números reais verificando o *axioma do supremo* e aceitando as notações usuais, é possível a partir disso provar resultados do Análise Real que conhecemos nos cursos de graduação.

Um estudo rigoroso de derivadas e integrais requer um tratamento rigoroso das propriedades fundamentais dos números reais, e esse é o tópico deste trabalho de conclusão de curso. Sabemos que dentro do conjunto dos números reais (que

intuitivamente formam a “linha numérica completa”) existem três conjuntos familiares de números: os números naturais (intuitivamente $1, 2, 3, \dots$), os inteiros (intuitivamente $\dots, -3, -2, -1, 0, 1, 2, 3, \dots$) e os números racionais (as frações). Usamos os símbolos padrão \mathbb{N} , \mathbb{Z} , \mathbb{Q} e \mathbb{R} para denotar os números naturais, os inteiros, os números racionais e os números reais, respectivamente. Esses conjuntos são subconjuntos um do outro na ordem

$$\mathbb{N} \subset \mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R}, \quad (*)$$

onde cada conjunto é um subconjunto próprio do próximo. Acontece é que isto é a maneira intuitiva e usual de trabalhar com esses conjuntos. Mas a construção formal e axiomática destes conjuntos não verifica (*). Na verdade, nesta construção conseguimos “encaixar” estes conjuntos e por um abuso da linguagem podemos considerar (*) como válida.

A metodologia que utilizamos nesse trabalho é a bibliográfica. Tendo como fundamentação à análise e leitura de livros que abordam o tema da construção dos números naturais, os números inteiros, os números racionais e sobretudo os números reais. Mais especificamente, as principais referências são (COHEN; EHRLICH, 1963) e (MOREIRA; CABRAL, 2021).

Os objetivos principais são compreender a construção dos conjuntos dos números naturais, dos números inteiros, dos números racionais e dos números reais. Os objetivos específicos são entender a importância dos conceitos prévios da teoria dos conjuntos, das relações, funções e operações binárias.

Neste trabalho, iniciamos no segundo capítulo introduzindo a teoria axiomática de conjuntos, bem como relações, funções e operações binárias, utilizando os axiomas fundamentais da matemática. Faremos um destaque ao conceito de relação de equivalência para com isto introduzir o conceito de conjunto quociente, par ordenado e produto cartesiano. Dando continuidade, no terceiro capítulo, vamos construir o conjunto dos números naturais por meio dos Axiomas de Dedekind e verificando as aplicações de adição e multiplicação do conjunto dos números naturais, além disso definiremos grupos e semigrupos. No quarto capítulo, construímos os números inteiros, esta construção é realizada por meio das classes de equivalência entre pares ordenados, utilizando a nossa base do conjunto dos números naturais. No quinto capítulo, é feita a construção dos números racionais, seguindo o mesmo raciocínio dos números

inteiros, utilizando a classe de equivalência, e no sexto capítulo é feita a construção do conjunto dos números reais via cortes de Dedekind. Finalmente no sétimo capítulo, são feitas as conclusões obtidas nesse trabalho.

2 TEORIA DE CONJUNTOS, RELAÇÕES E FUNÇÕES

Neste capítulo colocaremos algumas preliminares necessárias para uma maior compreensão do trabalho. Antes de começar a construir os conjunto numéricos, vamos introduzir a teoria axiomática dos conjuntos e suas propriedades, bem como as relações, funções e operações binárias. A bibliografia usada como base é (COHEN; EHRLICH, 1963).

2.1 Teoria de conjuntos

Um *conjunto* é uma coleção de objetos. Um conjunto será caracterizado aqui com letras maiúsculas, e os objetos, também chamados de *elementos*, serão denotados por letras minúsculas.

A relação básica entre um objeto e um conjunto é a de pertinência. Caso um objeto x pertença a um conjunto A , então denotaremos por $x \in A$, se esse objeto não pertence ao conjunto, denotaremos por $x \notin A$.

Axioma 1 (Axioma de existência) Existe um conjunto.

Axioma 2 (Axioma de identidade) Se A e B são conjuntos tais que todo elemento de A é um elemento de B , e todo elemento de B é elemento de A , então A e B são o mesmo conjunto.

Denotaremos por $A = B$, se A e B são os mesmos conjuntos, também usaremos a mesma notação para conjuntos onde se repetem os mesmos elementos, por exemplo, $\{a, a, b, b\}$, $\{a, a, b\}$, $\{a, b\}$ denotam os mesmos conjuntos. Por outro lado, quando possuem pelo menos um elemento distinto, dizemos que $A \neq B$.

Definição 2.1 Dizemos que o conjunto B é um *subconjunto* de A , denotado por $B \subset A$ (ou $A \supset B$), se $b \in A$, para todo $b \in B$. Se $B \subset A$ e $B \neq A$ então dizemos que B é um *subconjunto próprio* de A e denotamos como $B \subsetneq A$ (ou $A \supsetneq B$).

Não é difícil verificar as seguintes propriedades:

1. Se A é um conjunto, então $A \subset A$.

2. Se A e B são conjuntos, então $A = B$ se, e só se, $A \subset B$ e $B \subset A$.
3. Se A , B e C são conjuntos tais que $A \subset B$ e $B \subset C$, então $A \subset C$.

Axioma 3 (Axioma de especificação) Se A é um conjunto e $Q(x)$ é uma condição, então existe um subconjunto B de A , cujos elementos são exatamente os elementos $x \in A$ para os quais a condição $Q(x)$ é satisfeita.

Observação 2.1

1. O subconjunto B do Axioma 3 é chamado *determinado* (ou *especificado*) pela condição $Q(x)$.
2. Pelo Axioma de identidade, se B e B' são subconjunto de A determinados pela condição $Q(x)$, então $B = B'$. Dizemos então *um único subconjunto B de A é determinado pela condição $Q(x)$* e escrevemos $B = \{x \in A; Q(x)\}$.

Teorema 2.1 [Teorema 0.1 em (COHEN; EHRLICH, 1963)] Existe um conjunto que não tem elementos.

Demonstração. Pelo Axioma de existência, existe um conjunto A . Seja $Q(x)$ a condição: $x \notin A$. Pelo Axioma de especificação, existe um subconjunto E de A consistindo de todos os elementos $x \in A$ que satisfazem a condição $x \notin A$. Como nenhum elemento de A satisfaz $Q(x)$, então E não tem elementos. ■

Observação 2.2 Qualquer conjunto que não possua elementos é chamado *de conjunto vazio*.

Teorema 2.2 [Teorema 0.2 em (COHEN; EHRLICH, 1963)] Se E e E' são conjuntos vazios, então $E = E'$.

Demonstração. Suponhamos que $E \neq E'$. Então uma das seguintes afirmações é verdadeira:

1. Existe um elemento $x \in E$ tal que $x \notin E'$.
2. Existe um elemento $x \in E'$ tal que $x \notin E$.

Ambas essas afirmações são falsas, pois nem E nem E' possuem quaisquer elementos. Consequentemente, $E = E'$. ■

Observação 2.3 Em vista do Teorema 2.2, dizemos *o conjunto vazio*. Denotamos esse conjunto por \emptyset .

Axioma 4 (Axioma de reuniões) Se C é um conjunto de conjuntos, então existe um conjunto B tal que $x \in B$, se $x \in A$ para algum $A \in C$.

Observação 2.4

1. O Axioma 4 afirma que para toda coleção de conjuntos existe um conjunto que contém todos os elementos que pertencem a pelo menos um conjunto da coleção dada.
2. O *paradoxo de Russel* afirma que não pode existir o conjunto C de todos os conjuntos. De fato, a condição $Q(x) : x$ é um conjunto em C tal que $x \notin x$, determina (pelo Axioma de Especificação), um subconjunto D de C cujos elementos x não se contém como elementos. Mas, se $D \in D$, então $D \notin D$ e se $D \notin D$, então $D \in D$. Esta contradição é inevitável se um conjunto de todos os conjuntos existisse.

Teorema 2.3 [Teorema 0.3 em (COHEN; EHRLICH, 1963)] Se C é um conjunto de conjuntos, então existe um único conjunto Σ tal que $x \in \Sigma$ se, e só se, $x \in A$ para algum $A \in C$.

Demonstração. Pelo Axioma de Reuniões 4, existe um conjunto B tal que $x \in B$ se $x \in A$ para algum $A \in C$. Pelo Axioma de especificação 3 existe um único subconjunto Σ de B determinado pela condição $x \in A$ para algum $A \in C$. ■

Observação 2.5 Σ não depende da escolha de B .

Definição 2.2 O conjunto Σ do Teorema 2.3 é chamado a *reunião dos conjuntos* A de C . Escrevemos, $\bigcup_{A \in C} A$ em vez de Σ .

Se A e B são conjuntos, ainda não temos informações que nos digam se existe um conjunto com A e B como elementos. Isso é constrangedor se quisermos considerar a união de A e B . O seguinte axioma nos permite fazê-lo.

Axioma 5 (Axioma de pares) Se A e B são conjuntos, existe um conjunto C tal que $A \in C$ e $B \in C$.

Agora, pelo Axioma de especificação, existe um subconjunto de C que consiste precisamente de A e B . Esse conjunto $\{A, B\}$ é chamado de *um par*. Se $A = B$, então o par $\{A, B\} = \{A, A\} = \{A\}$ é chamado de *unitário* A .

Pelo Axioma de Reuniões (4) e o Axioma de pares (5), temos:

Proposição 2.1 [Exercício 0.5 em (COHEN; EHRLICH, 1963)] Se A e B são conjuntos, então existe um conjunto que é a *união* de A e B . Denotamos a união de A e B pelo símbolo: $A \cup B$.

Se verificam as seguintes propriedades:

1. Se A e B são conjuntos então $A \cup B = B \cup A$.
2. Se A , B e C são conjuntos então $A \cup (B \cup C) = (A \cup B) \cup C$.

Teorema 2.4 [Teorema 0.4 em (COHEN; EHRLICH, 1963)] Se C é um conjunto de conjuntos, então existe um único conjunto Π tal que $x \in \Pi$ se, e só se, $x \in A$, para todo $A \in C$.

Demonstração. Pelo Axioma de especificação 3, a condição $Q(x) : x \in A$ para todo $A \in C$, determina um único subconjunto de $\bigcup_{A \in C} A$. Esse é o conjunto exigido Π . ■

Definição 2.3 O conjunto Π do Teorema 2.4 é chamado *interseção dos conjuntos* A de C . Escrevemos $\bigcap_{A \in C} A$ em vez de Π .

Proposição 2.2 [Exercício 0.9 em (COHEN; EHRLICH, 1963)] Se A e B são conjuntos, então existe um conjunto que é a *interseção* de A e B .

Demonstração. Pelo Axioma de Especificação (3) e pelo Axioma de Reuniões (4), existe um conjunto $\{x \in A \cup B; x \in A \text{ e } x \in B\}$, e será único pelo Teorema 2.4. ■

Denotamos a interseção de A e B pelo símbolo $A \cap B$. Se $A \cap B = \emptyset$, dizemos que A e B são conjuntos *disjuntos*.

A interseção satisfaz as seguintes propriedades: Se A , B e C são conjuntos tem-se

1. $A \cap B = B \cap A$.
2. $A \cap (B \cap C) = (A \cap B) \cap C$.
3. $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$ e $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$.

Usaremos $A - B$ para denotar $\{x; x \in A \text{ e } x \notin B\}$. Se verifica as seguintes propriedades:

- (a) $A - B = A - (A \cap B)$.
- (b) $A - B = \emptyset$ se, e só se, $A \subset B$.

Axioma 6 (Axioma das Potências) Se A é um conjunto, existe um conjunto $\mathcal{P}(A)$ (chamado *conjunto potência* de A), cujos elementos são os subconjuntos de A .

Por exemplo, o conjunto das potências do conjunto cujos elementos são a, b, c é o conjunto cujos elementos são:

$$\{\emptyset, \{a\}, \{b\}, \{c\}, \{a, b\}, \{a, c\}, \{b, c\}, \{a, b, c\}\}.$$

O conjunto das potências de um conjunto com n elementos contém 2^n elementos.

Se $a \in A$, então um dos subconjuntos de A é o conjunto unitário $\{a\}$. Observamos que se $a \in A$, então $\{a\} \subset A$ e $\{a\} \in \mathcal{P}(A)$. Se $a \in A$ e $b \in B$, então o par $\{a, b\}$ é um subconjunto de $A \cup B$ e um elemento de $\mathcal{P}(A \cup B)$.

Um conceito muito útil é o de *par ordenado*. As coordenadas (x, y) de um ponto no plano, por exemplo, formam um par ordenado. Para especificar um ponto P no plano, é suficiente declarar quais dois números servirão como as coordenadas de P e qual desses dois números será a coordenada x . No símbolo $(3, 2)$, a coordenada x é destacada por ser escrita primeiro. Uma definição de *par ordenado* que utiliza a ideia de destacar um dos elementos do par sem pressupor qualquer noção de “primeiro” ou “segundo” foi dada por Norbert Wiener:

Definição 2.4 Se $a \in A$ e $b \in B$, então o *par ordenado* (a, b) é definido como o conjunto $\{\{a\}, \{a, b\}\}$.

Observação 2.6 Notamos que se $a = b$ então

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

Essa definição tem a vantagem de pressupor apenas os axiomas dos conjuntos para que conceitos como ordem e função possam ser definidos posteriormente em termos de par ordenado sem perigo de circularidade.

O fato mais importante sobre a Definição 2.4 é que os pares ordenados assim definidos se comportam exatamente como os pares ordenados deveriam:

Teorema 2.5 [Teorema 0.5 em (COHEN; EHRLICH, 1963)] Dois pares ordenados (a, b) e (a', b') são iguais se, e só se, $a = a'$ e $b = b'$.

Demonstração. Se $a = a'$ e $b = b'$, então, pelo Axioma de identidade (2),

$$\{\{a\}, \{a, b\}\} = \{\{a'\}, \{a', b'\}\}. \quad (2.1)$$

Reciprocamente, suponhamos que (2.1) é verdadeira. Se $a = b$, então, de acordo com a Definição 2.4 e a notação da Observação 2.6, temos

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

Pelo Axioma da identidade, temos $a = a' = b'$. Como $a = b$, temos $a = a'$ e $b = b'$. Se $a \neq b$, então, pelo Axioma da identidade, $\{a, b\} \neq \{a'\}$. Portanto, $\{a, b\} = \{a', b'\}$, e $\{a\} = \{a'\}$. Mas, então $a = a'$ e $b = b'$. ■

Teorema 2.6 [Teorema 0.6 em (COHEN; EHRLICH, 1963)] Se A e B são conjuntos não vazios, então existe um conjunto C que consiste de todos os pares ordenados (a, b) com $a \in A$ e $b \in B$.

Demonstração. Cada par ordenado de $(a, b) = \{\{a\}, \{a, b\}\}$ é um subconjunto de $\mathcal{P}(A \cup B)$. Pelo Axioma de especificação (3), a condição “ x é um par ordenado (a, b) com $a \in A$ e $b \in B$ ” determina um subconjunto C de $\mathcal{P}(\mathcal{P}(A \cup B))$. O conjunto C consiste de todos os pares ordenados (a, b) com $a \in A$ e $b \in B$. ■

Definição 2.5 O conjunto C do Teorema 2.6 é chamado *produto cartesiano* de A e B , o qual será denotado por $A \times B$.

Se verifica a seguinte propriedade: Se A , B e C são conjuntos não vazios então

$$A \times (B \cup C) = (A \times B) \cup (A \times C).$$

2.2 Relações, funções e operações binárias

Se A e B são conjuntos, então uma condição $Q(x)$ determina, pelo Axioma da especificação (3), um subconjunto R de $A \times B$ que consiste em todos os pares ordenados $x = (a, b)$ para os quais a condição é verdadeira. Tal condição expressa o que, na linguagem comum, é chamado de relação entre a e b . Exemplos disso são “ a é menor que b ”, “ a é igual a b ”, “ a divide b ”, etc. Em matemática, é conveniente identificar o conjunto R como uma relação. De fato, se R é qualquer subconjunto de $A \times B$, pode-se pensar na condição $Q(x)$: “ $x \in R$ ” como sendo uma relação entre a e b , onde $x = (a, b)$.

Definição 2.6 Uma *relação binária* é um subconjunto R do produto cartesiano $A \times B$. Se $R \subset A \times A$, chamamos R uma *relação binária em A* . Se $(a, b) \in R$ podemos escrever aRb .

Definição 2.7 Seja R uma relação binária definida em um conjunto A . Dizemos que

1. R é *reflexivo* se aRa é verdadeiro para todo $a \in A$.
2. R é *simétrico* se bRa vale, sempre que aRb vale para $a, b \in A$.
3. R é *transitivo* se aRc vale, sempre que aRb e bRc valem para $a, b, c \in A$.
4. R é *antissimétrico* se $a = b$ sempre que aRb e bRa valem para $a, b \in A$.
5. R satisfaz a *lei da tricotomia* se, para qualquer $a, b \in A$, exatamente uma das seguintes afirmações é verdadeira: aRb , bRa ou $a = b$.

Definição 2.8 Se uma relação binária R em um conjunto A é reflexiva, simétrica e transitiva então ela é chamada de *relação de equivalência em A* .

Exemplo 2.1 No conjunto A de todos os números inteiros, podemos definir uma relação binária R de forma que aRb seja verdadeira se, e só se, 3 for um divisor de $b - a$.

1. Como 3 é um divisor de $a - a$ para todo $a \in A$, R é reflexiva.
2. Se 3 é um divisor de $a - b$, então 3 é um divisor de $b - a$. Portanto, R é simétrica.
3. Suponha que 3 seja um divisor de $b - a$ e também de $c - b$. Então, 3 é um divisor de $(b - a) + (c - b) = c - a$. Assim, R é transitiva.

Portanto, R é uma relação de equivalência em A . Se aRb é verdadeira para dois números inteiros a e b , dizemos que a é congruente a b módulo 3 e escrevemos $a = b \pmod{3}$. Para qualquer número inteiro não nulo m , uma relação de equivalência *congruência módulo m* pode ser definida de forma similar.

Definição 2.9 Se R é uma relação de equivalência definida em um conjunto A e se $a \in A$, então o conjunto $C_a = \{x \in A; xRa\}$ denomina-se *classe de equivalência* de a com respeito à relação R .

Exemplo 2.2 Vamos determinar as classes de equivalência no conjunto A de todos os números inteiros em relação à *congruência módulo 3*. Os inteiros congruentes a 0 módulo 3 formam uma classe de equivalência. Os elementos dessa classe são os múltiplos de 3, ou seja, os números inteiros da forma $3k$ para algum inteiro k . Os inteiros congruentes a 1 módulo 3 formam outra classe de equivalência. Essa classe consiste em todos os inteiros da forma como $3k + 1$ para algum inteiro k . Os inteiros congruentes a 2 módulo 3 formam uma terceira classe de equivalência. Essa classe consiste em todos os inteiros da forma $3k + 2$ para algum inteiro k . No entanto, todo inteiro pode ser expresso na forma $3k$, $3k + 1$ ou $3k + 2$ para algum inteiro k . Portanto, as três classes que listamos contêm todos os inteiros, e o conjunto A , em relação à *congruência módulo 3*, é a união de três classes de equivalência, onde nenhuma das classes tem elementos em comum. Isso ilustra um princípio geral muito importante.

Teorema 2.7 [Teorema 0.7 em (COHEN; EHRLICH, 1963)] Se R é uma relação de equivalência em um conjunto A , então A é uma união de classes de equivalência disjuntas dois a dois.

Demonstração. Mostremos primeiro que o conjunto A é a união de todas as suas classes de equivalências. Se $a \in A$, então $a \in C_a$ desde que aRa por conta da reflexividade de R . Mas, então A é um subconjunto de $\bigcup_{a \in A} C_a$ que, por sua vez, é um subconjunto de A . Portanto, $A = \bigcup_{a \in A} C_a$.

Mostraremos a seguir que para $a, b \in A$, as classes de equivalências C_a e C_b são disjuntas ou iguais. Se $C_a \cap C_b \neq \emptyset$, existe $x \in A$ satisfazendo xRa e xRb . Mas, como R é simétrica, aRx , e portanto, aRb desde que R é transitivo. Agora, se

$a' \in C_a$ então $a'Ra$ e como aRb , pela transitividade de R , temos $a'Rb$. Portanto, $C_a \subset C_b$. Analogamente, se $b' \in C_b$ então $b'Rb$ e como bRa (pois R é simétrica e aRb), pela transitividade de R , temos $b'Ra$. Portanto, $C_b \subset C_a$. Concluimos, $C_a = C_b$. Segue-se que A é a união de classes de equivalências mutuamente disjuntas. ■

As classes de equivalência com respeito a uma relação R formam um subconjunto do conjunto de potências de A .

Definição 2.10 Se R é uma relação de equivalência em um conjunto A , o conjunto A/R de todas as classes de equivalências com respeito a R é chamado *conjunto quociente de A módulo R* .

Definição 2.11 Se uma relação binária em um conjunto A é reflexiva, antissimétrica e transitiva, ela é chamada de *relação de ordem parcial*.

Definição 2.12 Uma relação binária R em um conjunto A é chamada de *relação de ordem em A* se for transitiva e satisfaz a lei da tricotomia. Um conjunto no qual é definida uma relação de ordem é chamado *conjunto ordenado*.

Um tipo especial importante de relação binária é chamado de *função*.

Definição 2.13 Se A e B são conjuntos não vazios, então uma *função F* de A em B , o que denotamos $F : A \rightarrow B$, é uma relação binária de A em B satisfazendo as condições:

- (1) Para cada $a \in A$, $(a, b) \in F$ para algum $b \in B$.
- (2) Se $(a, b) \in F$ e $(a, b') \in F$, então $b = b'$.

Observação 2.7 Seja $F : A \rightarrow B$.

1. Os conjuntos A e B são respectivamente chamados, *domínio* e *contradomínio* de F .
2. O conjunto $F(A) := \{b \in B; (a, b) \in F\}$ é chamada a *imagem* de F .
3. Se $(a, b) \in F$, escrevemos $b = F(a)$. Então para todo $a \in A$ existe exatamente um $b \in B$ tal que $b = F(a)$. Por outro lado, se para todo elemento $a \in A$, associamos de alguma maneira exatamente um elemento $F(a) \in B$, então o conjunto $\{(a, F(a)); a \in A\}$ é uma função de A em B .

Definição 2.14 Seja $F : A \rightarrow B$.

1. Dizemos que F é *injetiva* se $(a, b) \in F$ e $(a', b) \in F$ então $a = a'$.
2. Dizemos que F é *sobrejetiva* se $F(A) = B$.
3. Dizemos que F é *bijetiva* se, e só se, F é injetiva e sobrejetiva.

Teorema 2.8 [Teorema 0.8 em (COHEN; EHRLICH, 1963)] Duas funções $F, G : A \rightarrow B$ são iguais se, e só se, $F(a) = G(a)$, para todo $a \in A$.

Demonstração. Suponha que $F = G$. Seja $a \in A$ logo $(a, F(a)) \in F$ então $(a, F(a)) \in G$. Mas, então desde que $(a, G(a)) \in G$, temos que $F(a) = G(a)$. (Note que até agora, usamos apenas a inclusão $F \subset G$).

Por outro lado, se $F(a) = G(a)$ para todo $a \in A$, então para cada $(a, F(a)) \in F$, temos

$$(a, F(a)) = (a, G(a)) \in G$$

de modo que $F \subset G$. Da mesma forma, $G \subset F$. Portanto, $F = G$. ■

Teorema 2.9 [Teorema 0.9 em (COHEN; EHRLICH, 1963)] Sejam $F : A \rightarrow B$ e $G : B \rightarrow C$. Então existe uma única $H : A \rightarrow C$ tal que $H(a) = G(F(a))$, para todo $a \in A$.

Demonstração. Seja $H = \{(a, c); c = G(F(a)) \text{ para algum } a \in A\}$. Então, $H \subset A \times C$. Se $a \in A$, então $c = G(F(a)) \in C$, uma vez que F e G satisfazem (1) da Definição 2.13. Se $(a, c) \in H$ e $(a, c') \in H$, então $c = G(F(a)) = c'$, uma vez que F e G satisfazem (2) da Definição 2.13. Portanto, H é uma função de A em C . A condição " $c = G(F(a))$ para algum $a \in A$ " especifica um subconjunto único de $A \times C$. Assim, H é a única função com as propriedades requeridas. ■

Definição 2.15 Se $F : A \rightarrow B$ e $G : B \rightarrow C$, então a função $H : A \rightarrow C$ definida por $H(a) = G(F(a))$, para todo $a \in A$ é chamada a *composição* de F e G , a qual é denotada por GF .

Teorema 2.10 [Teorema 0.10 em (COHEN; EHRLICH, 1963)] A composição de funções é associativa, isto é, se $F : A \rightarrow B$, $G : B \rightarrow C$ e $H : C \rightarrow D$ então $(HG)F = H(GF)$.

Demonstração. Para todo $a \in A$,

$$[(HG)F](a) = (HG)(F(a)) = H(G(F(a))).$$

Também, para todo $a \in A$,

$$[H(GF)](a) = H((GF)(a)) = H(G(F(a))).$$

Portanto, pelo Teorema 2.8, $(HG)F = H(GF)$. ■

Definição 2.16 Se $F : A \rightarrow B$ e $G : B \rightarrow A$ então G é chamada a *função inversa* para F se $(GF)(x) = G(F(x)) = x$, para todo $x \in A$ e $(FG)(y) = F(G(y)) = y$, para todo $y \in B$.

Teorema 2.11 [Teorema 0.11 em (COHEN; EHRLICH, 1963)] Se $F : A \rightarrow B$ é bijetiva então F tem uma única função inversa.

Demonstração. Considere o seguinte conjunto

$$G = \{(b, a); (a, b) \in F\}. \quad (2.2)$$

Então, $G \subset B \times A$. Se $b \in B$, então, como F é uma função sobrejetiva, $(a, b) \in F$ para algum $a \in A$. Portanto, $(b, a) \in G$. Se $(b, a) \in G$ e $(b, a') \in G$, então $(a, b) \in F$ e $(a', b) \in F$. Como F é injetiva, $a = a'$. Portanto, G é uma função de B em A . Por (2.2),

$$GF(a) = G(F(a)) = a, \text{ para todo } a \in A,$$

e

$$FG(b) = F(G(b)) = b, \text{ para todo } b \in B.$$

Assim, G é uma função inversa para F . Agora, seja G' qualquer função inversa para F . Então, para todo $b \in B$, pela Definição 2.16 e pelo Teorema 2.10, tem-se

$$G'(b) = G'((FG)(b)) = [G'(FG)](b) = [(G'F)G](b) = (G'F)(G(b)) = G(b).$$

Portanto, $G' = G$. ■

Proposição 2.3 [Exercício 0.20 em (COHEN; EHRLICH, 1963)]

1. Se $F : A \rightarrow B$ é bijetiva então a função inversa $G : B \rightarrow A$ de F é bijetiva.

2. Se $F : A \rightarrow B$ é bijetiva e $G : B \rightarrow C$ é bijetiva então $GF : A \rightarrow C$ é bijetiva.

Demonstração.

1. Como G é uma aplicação inversa para F temos que $(GF)(x) = x$, para todo $x \in A$ e $(FG)(y) = y$, para todo $y \in B$.

G é injetiva: sejam $y_1, y_2 \in B$ tal que $G(y_1) = G(y_2)$. Como F é sobrejetiva e $y_1, y_2 \in B$ então existem $x_1, x_2 \in A$ tal que $y_1 = F(x_1)$ e $y_2 = F(x_2)$. Daí temos

$$x_1 = (GF)(x_1) = G(F(x_1)) = G(y_1) = G(y_2) = G(F(x_2)) = (GF)(x_2) = x_2$$

assim $y_1 = F(x_1) = F(x_2) = y_2$. Portanto, G é injetiva.

G é sobrejetiva: dado $x \in A$ temos que $G(F(x)) = (GF)(x) = x$ com $F(x) \in B$. O que mostra que G é sobrejetiva.

Concluimos que G é uma aplicação bijetiva de B em A .

2. Devemos mostrar que $GF : A \rightarrow C$ é bijetiva.

GF é injetiva: sejam $x_1, x_2 \in A$ tal que $(GF)(x_1) = (GF)(x_2)$. Agora como

$$G(F(x_1)) = (GF)(x_1) = (GF)(x_2) = G(F(x_2))$$

e G é injetiva então $F(x_1) = F(x_2)$ e como F é injetiva temos que $x_1 = x_2$. Assim, GF é injetiva.

GF é sobrejetiva: dado $z \in C$ e como $G : B \rightarrow C$ é sobrejetiva existe $y \in B$ tal que $z = G(y)$. Agora, como $y \in B$ e $F : A \rightarrow B$ é sobrejetiva então existe $x \in A$ tal que $y = F(x)$. Logo

$$z = G(y) = G(F(x)) = (GF)(x), \text{ com } x \in A.$$

Daí GF é sobrejetiva. ■

Algumas operações usuais da matemática, como adição e multiplicação de números, adição de vetores e multiplicação de vetores por escalares, podem ser interpretadas como funções cujo domínio é o produto cartesiano de dois conjuntos.

Definição 2.17 Se A , B e C são conjuntos, então qualquer função de um subconjunto não vazio de $A \times B$ em C é chamada *operação binária* de $A \times B$ para C . Em particular,

se $A = B = C$, então qualquer função de um subconjunto não vazio de $A \times A$ em A é chamada *operação binária em A* . Uma operação binária cujo domínio é todo $A \times A$ é chamada *operação binária sobre A* .

Uma operação binária $\circ : A \times B \rightarrow C$ associa a cada par ordenado $(a, b) \in A \times B$ um único elemento $a \circ b \in C$. Uma operação binária \circ em A associa a cada par ordenado (a, a') em um subconjunto de $A \times A$ um único elemento $a \circ a'$.

Exemplo 2.3 Se A é o conjunto de todas as funções de P em Q , e B é o conjunto de todas as funções de Q em T , então a composição de funções é uma operação binária de $B \times A$ para C , onde C é o conjunto de todas as funções de P em T .

Exemplo 2.4 Se C é um conjunto de conjuntos tal que, para A e B em C , $A \cup B$ e $A \cap B$ também pertencem a C , então \cup e \cap são operações binárias em C . Em particular, se $P(A)$ é o conjunto de todos os subconjuntos de um dado conjunto A , então \cup e \cap são operações binárias em $P(A)$.

Definição 2.18 Uma operação binária \circ sobre A é

- (a) *associativa* se, $a \circ (b \circ c) = (a \circ b) \circ c$, para todo $a, b, c \in A$,
- (b) *comutativa* se, $a \circ b = b \circ a$, para todo $a, b \in A$.

Definição 2.19 Se A é um conjunto, e, \circ, \circ' são operações binárias sobre A , então \circ' é

1. *distributiva à esquerda sobre \circ* se $a \circ' (b \circ c) = (a \circ' b) \circ (a \circ' c)$, para todo $a, b, c \in A$,
2. *distributiva à direita sobre \circ* se $(b \circ c) \circ' a = (b \circ' a) \circ (c \circ' a)$, para todo $a, b, c \in A$,
3. *distributiva sobre \circ* se for distributiva à esquerda e à direita sobre \circ .

Neste capítulo abordamos os seis axiomas fundamentais da teoria dos conjuntos: axioma de existência, de identidade, de especificação, de reuniões, de pares e das potências. Através de uma condição $Q(x)$, mostramos as relações binárias, denominadas como relações de equivalências, além disso, definimos as classes de equivalência onde será fundamental para a construção dos conjuntos números \mathbb{N} , \mathbb{Z} , \mathbb{Q} . E por último, não menos importante, abordamos sobre as funções injetivas, sobrejetivas e bijetivas.

3 CONSTRUÇÃO DOS NÚMEROS NATURAIS

Neste capítulo, apresentaremos a construção do conjuntos dos números naturais por meio dos axiomas de Dedekind. Além disso, introduziremos os conceitos de grupoide, semigrupo, semigrupo comutativo e semigrupo ordenado que será importante para simplificar as nomenclaturas das propriedades que verificam os números naturais. Mostramos também um importante resultado, o princípio da boa ordenação que será utilizado no sexto capítulo. A principal referência utilizada foi (COHEN; EHRLICH, 1963).

Iniciaremos nosso estudo com um conjunto \mathbb{N} e uma função $S : \mathbb{N} \rightarrow \mathbb{N}$. Os elementos de \mathbb{N} serão chamados *números naturais* e intuitivamente representamos $\mathbb{N} = \{1, 2, 3, 4, 5, \dots\}$. Para cada $n \in \mathbb{N}$, $S(n)$ será chamado o *sucessor* de n . Impomos sobre \mathbb{N} e S as seguintes condições:

(A1) S é injetiva.

(A2) $S(\mathbb{N}) \neq \mathbb{N}$.

(A3) Se $u \in \mathbb{N} - S(\mathbb{N})$ e M é um subconjunto de \mathbb{N} tal que:

(i) $u \in M$,

(ii) $S(n) \in M$ se $n \in M$,

então $M = \mathbb{N}$ (*Axioma de Indução*).

Os axiomas (A1), (A2) e (A3) formam um ligeira modificação dos axiomas geralmente associados ao nome Peano, mas na verdade foram introduzidos por Dedekind (1888).

Teorema 3.1 [Teorema 1.1 em (COHEN; EHRLICH, 1963)] Existe exatamente um número natural que não é sucessor de nenhum número natural.

Demonstração. Pelo Axioma (A2) existe um número natural $u \notin S(\mathbb{N})$. Seja $M = \{u\} \cup S(\mathbb{N})$. Então $u \in M$ e se $n \in M$ temos que $S(n) \in S(\mathbb{N})$ logo $S(n) \in M$. Pelo Axioma (A3), $M = \mathbb{N}$, isto é, $\mathbb{N} = \{u\} \cup S(\mathbb{N})$ e portanto todo número natural $n \neq u$ pertence a $S(\mathbb{N})$, isto é, todo número natural, exceto u , é o sucessor de algum número natural. ■

Observação 3.1 Usaremos o símbolo familiar 1 para denotar o único não sucessor em \mathbb{N} .

Definição 3.1 Um subconjunto M de \mathbb{N} é chamado *conjunto indutivo* se $S(n) \in M$ sempre que $n \in M$.

Observação 3.2 Podemos agora reescrever o Axioma (A3) na forma “se M é um conjunto indutivo contendo 1 então $M = \mathbb{N}$ ”.

Exemplo 3.1 Temos que $S(n) \neq n$, para todo $n \in \mathbb{N}$.

De fato, considere $M = \{n \in \mathbb{N}; S(n) \neq n\}$. Claramente $S(1) \neq 1$ pois $1 \notin S(\mathbb{N})$ e $S(1) \in S(\mathbb{N})$, isto é, $1 \in M$. Suponhamos que $n \in M$, então $S(n) \neq n$. Se $S(S(n)) = S(n)$ pelo Axioma (A1) temos que $S(n) = n$ o que é uma contradição. Logo, $S(S(n)) \neq S(n)$ assim $S(n) \in M$. Então pelo Axioma (A3), temos que $M = \mathbb{N}$.

Teorema 3.2 [Teorema de recursão, Teorema 1.2 em (COHEN; EHRLICH, 1963)] Seja A um conjunto não vazio. Se $G : A \rightarrow A$ e $a \in A$, então existe exatamente uma função $F : \mathbb{N} \rightarrow A$ tal que

$$F(1) = a \quad \text{e} \quad F(S(n)) = G(F(n)), \quad \text{para todo } n \in \mathbb{N}.$$

Demonstração.

Existência: Seja $C = \{T \subset \mathbb{N} \times A; (1, a) \in T \text{ e } (S(n), G(b)) \in T, \text{ se } (n, b) \in T\}$. Note que $(1, a) \in \mathbb{N} \times A$ e se $(n, b) \in \mathbb{N} \times A$ temos que $n \in \mathbb{N}$ e $b \in A$ logo $(S(n), G(b)) \in \mathbb{N} \times A$ assim $\mathbb{N} \times A \in C$, portanto C é não vazio. Agora, defina

$$F = \bigcap_{T \in C} T. \quad (3.1)$$

Claramente, $F \in C$ e por (3.1), temos que $F \subset T$, para todo $T \in C$. Mostraremos que F é a função procurada. Seja $M = \{n \in \mathbb{N}; (n, b) \in F \text{ para exatamente um } b \in A\}$.

Afirmção 3.1 $1 \in M$.

De fato, como $F \in C$ temos que $(1, a) \in F$. Suponhamos que $(1, b) \in F$ com $b \neq a$. Seja $F_b = F - \{(1, b)\}$, como $(1, b) \neq (1, a)$ e $(1, a) \in F$, então $(1, a) \in F_b$. Se $(n, c) \in F_b$ temos que $(S(n), G(c)) \neq (1, b)$ logo $(S(n), G(c)) \in F_b$. Portanto, $F_b \in C$ e por (3.1) tem-se que $F \subset F_b = F - \{(1, b)\}$ que é uma contradição por ser um subconjunto próprio de F . Segue-se que $1 \in M$.

Afirmção 3.2 M é um conjunto indutivo.

De fato, se $n \in M$ então existe exatamente um $b \in A$ tal que $(n, b) \in F$. Como $F \in C$ então $(S(n), G(b)) \in F$. Suponhamos que $(S(n), c) \in F$ para algum $c \neq G(b)$ e seja $F_c = F - \{(S(n), c)\}$. Como $(S(n), c) \neq (1, a) \in F$ então $(1, a) \in F_c$. Se $(m, d) \in F_c$ vamos mostrar que $(S(m), G(d)) \in F_c$, pois se supomos o contrário teríamos que $S(m) = S(n)$ e $G(d) = c \neq G(b)$ então pelo Axioma (A1) temos que $m = n$ e $d \neq b$, daí $(n, d), (n, b) \in F$ contrariando a suposição de $n \in M$. Então, efetivamente $(S(m), G(d)) \neq (S(n), c)$ logo $(S(m), G(d)) \in F_c$ assim $F_c \in C$ e $F \subset F_c = F - \{(S(m), c)\}$ o que é uma contradição. Portanto, $S(n) \in M$, isto é, M é um conjunto indutivo que contem 1.

Agora, pela Afirmção 3.1 e Afirmção 3.2 verificamos o Axioma (A3) então $M = \mathbb{N}$, isto é, para cada $n \in \mathbb{N}$ existe exatamente um $b \in A$ tal que $(n, b) \in F$, logo F é uma função de \mathbb{N} em A . Desde que $F \in C$ temos que $(1, a) \in F$, isto é, $F(1) = a$ e também temos que $(n, b) \in F$ se, e só se, $(S(n), G(b)) \in F$. Portanto, $F(S(n)) = G(F(n))$, para todo $n \in \mathbb{N}$.

Unicidade: Suponhamos que existe outra função $\bar{F} : \mathbb{N} \rightarrow A$ tal que $\bar{F}(1) = a$ e $\bar{F}(S(n)) = G(\bar{F}(n))$ para todo $n \in \mathbb{N}$. Claramente temos que $\bar{F}(1) = a = F(1)$. Suponha que $\bar{F}(n) = F(n)$ então

$$\bar{F}(S(n)) = G(\bar{F}(n)) = G(F(n)) = F(S(n)).$$

Pelo Axioma (A3),

$$\bar{F} = \{(n, \bar{F}(n)); n \in \mathbb{N}\} = \{(n, F(n)); n \in \mathbb{N}\} = F.$$

Assim F é a única função de \mathbb{N} em A com as propriedades descritas. ■

Exemplo 3.2 Sejam $A = \mathbb{N} - \{1\}$, $G : A \rightarrow A$ definido por $G(n) = S(S(n))$ e $a = S(1) \in A$ então pelo Teorema 3.2 existe uma única função $F : \mathbb{N} \rightarrow A$ tal que $F(1) = S(1)$ e $F(S(n)) = G(F(n))$, para todo $n \in \mathbb{N}$.

Se os números naturais

$$1, S(1), S(S(1)), S(S(S(1))), \dots$$

são identificados como os números

$$1, 2, 3, 4, \dots$$

então as condições proposta no Exemplo 3.2 constituem uma definição recursiva da sequência $2, 4, 6, 8, \dots$ de todos os números pares.

3.1 Adição e multiplicação em \mathbb{N}

Teorema 3.3 [Teorema 1.3 em (COHEN; EHRLICH, 1963)] Existe exatamente uma função $F : \mathbb{N} \times \mathbb{N} \rightarrow \mathbb{N}$ tal que

$$\begin{aligned} F(m, 1) &= S(m), \text{ para todo } m \in \mathbb{N} \text{ e} \\ F(m, S(n)) &= S(F(m, n)), \text{ para todo } m, n \in \mathbb{N}. \end{aligned} \quad (3.2)$$

Demonstração.

Existência: Seja $m \in \mathbb{N}$ qualquer. Pelo Teorema 3.2, considerando $A = \mathbb{N}$, $a = S(m)$ e $G = S$, existe exatamente uma função $F_m : \mathbb{N} \rightarrow \mathbb{N}$ tal que

$$F_m(1) = S(m), \quad (3.3)$$

$$F_m(S(n)) = S(F_m(n)), \text{ para todo } n \in \mathbb{N}. \quad (3.4)$$

O conjunto $F = \{(m, n), F_m(n)\}; (m, n) \in \mathbb{N} \times \mathbb{N}\}$ é uma função de $\mathbb{N} \times \mathbb{N}$ em \mathbb{N} . Para todo $(m, n) \in \mathbb{N} \times \mathbb{N}$, $F(m, n) = F_m(n)$. Por (3.3),

$$F(m, 1) = F_m(1) = S(m), \text{ para todo } m \in \mathbb{N}.$$

Por (3.4),

$$F(m, S(n)) = F_m(S(n)) = S(F_m(n)) = S(F(m, n)), \text{ para todo } m, n \in \mathbb{N}.$$

Assim, F satisfaz (3.2).

Unicidade: Se \bar{F} é uma função de $\mathbb{N} \times \mathbb{N}$ satisfazendo (3.2), então

$$\bar{F}(m, 1) = S(m) = F(m, 1), \text{ para todo } m \in \mathbb{N}.$$

Para todo $(m, n) \in \mathbb{N} \times \mathbb{N}$ tal que $\bar{F}(m, n) = F(m, n)$, temos que

$$\bar{F}(m, S(n)) = S(\bar{F}(m, n)) = S(F(m, n)) = F(m, S(n)).$$

Mas então para cada $m \in \mathbb{N}$, o conjunto $M_m = \{n \in \mathbb{N}; \bar{F}(m, n) = F(m, n)\}$ é igual a \mathbb{N} desde que M_m é um conjunto indutivo contendo 1. Portanto, $\bar{F}(m, n) = F(m, n)$ para todo $(m, n) \in \mathbb{N} \times \mathbb{N}$. Assim, $\bar{F} = F$. ■

Observação 3.3 Desde que F é uma função de $\mathbb{N} \times \mathbb{N}$ em \mathbb{N} , do Teorema 3.3, é uma operação binária em \mathbb{N} (Definição 2.17).

Definição 3.2 Escrevemos $m + n$ em vez de $F(m, n)$, onde F é a função do Teorema 3.3, e usamos o nome familiar *adição* para a operação binária $+$.

Podemos agora reformular o Teorema 3.3:

Teorema 3.4 [Teorema 3.4⁺ em (COHEN; EHRLICH, 1963)] Existe uma única operação binária sobre \mathbb{N} (chamada de *adição*) tal que

$$m + 1 = S(m), \text{ para todo } m \in \mathbb{N}, \quad (3.5)$$

$$m + S(n) = S(m + n), \text{ para todo } m, n \in \mathbb{N}. \quad (3.6)$$

Exemplo 3.3 Se $m, n, p \in \mathbb{N}$, e $m + p = n + p$, então $m = n$ (*Lei do cancelamento para a adição*).

De fato, sejam $m, n \in \mathbb{N}$ e consideremos o conjunto $M_{m,n} = \{p \in \mathbb{N}; m + p = n + p \Rightarrow m = n\}$.

Afirmção 3.3 $1 \in M_{m,n}$.

Se $m + 1 = n + 1$ por (3.5) temos que $S(m) = S(n)$ e pelo Axioma (A1) S é injetiva logo $m = n$. Daí, $1 \in M_{m,n}$.

Afirmção 3.4 $M_{m,n}$ é um conjunto indutivo.

Suponhamos que $p \in M_{m,n}$, isto é, se $m + p = n + p$ então $m = n$ (hipótese indutiva). Se $m + S(p) = n + S(p)$ por (3.6) tem-se que $S(m + p) = S(n + p)$ e pelo Axioma (A1) S é injetiva obtemos $m + p = n + p$. Logo, pela hipótese indutiva resulta que $m = n$. Daí, $S(p) \in M_{m,n}$.

Portanto, pela Afirmção 3.3 e Afirmção 3.4, $M_{m,n}$ é um conjunto indutivo contendo 1. Consequentemente, $M_{m,n} = \mathbb{N}$.

Exemplo 3.4 Para $m, n \in \mathbb{N}$, $m + n \neq n$.

De fato, para cada $m \in \mathbb{N}$ considere o conjunto $M_m = \{n \in \mathbb{N}; m + n \neq n\}$.

Afirmção 3.5 $1 \in M_m$.

Como $m + 1 = S(m)$ e pelo Teorema 3.1 $S(m) \neq 1$ então $m + 1 \neq 1$. Daí, $1 \in M_m$.

Afirmção 3.6 M_m é um conjunto indutivo.

Suponhamos que $n \in M_m$, isto é, $m + n \neq n$ (hipótese indutiva). Se $m + S(n) = S(n)$ então por (3.6) tem-se que $S(m + n) = S(n)$ e pelo Axioma (A1) S é injetiva obtemos $m + n = n$ o que contradiz a hipótese indutiva. Daí, $m + S(n) \neq S(n)$. Logo, $S(n) \in M_m$. Portanto, pela Afirmção 3.5 e Afirmção 3.6, M_m é um conjunto indutivo contendo 1. Consequentemente, $M_m = \mathbb{N}$.

Teorema 3.5 [Teorema 1.4 e Teorema 1.5 em (COHEN; EHRLICH, 1963)]

1. A adição em \mathbb{N} é associativa, isto é, $(m + n) + p = m + (n + p)$, para todo $m, n, p \in \mathbb{N}$.
2. A adição em \mathbb{N} é comutativa, isto é, $m + n = n + m$, para todo $m, n, \in \mathbb{N}$.

Demonstração.

1. Considere o conjunto $P = \{p \in \mathbb{N}; (m + n) + p = m + (n + p), \text{ para todo } m, n \in \mathbb{N}\}$.

Afirmção 3.7 $1 \in P$.

Por (3.5) e (3.6), temos que

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

Daí, $1 \in P$.

Afirmção 3.8 P é um conjunto indutivo.

Suponhamos que $p \in P$, isto é, $(m + n) + p = m + (n + p)$ para todo $m, n \in \mathbb{N}$ (hipótese indutiva). Agora por (3.6) e pela hipótese indutiva obtemos

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

Daí, $S(p) \in P$.

Portanto, pela Afirmção 3.7 e Afirmção 3.8, P é um conjunto indutivo contendo

1. Consequentemente, $P = \mathbb{N}$.

2. Primeiro mostremos que

$$m + 1 = 1 + m \text{ para todo } m \in \mathbb{N}. \quad (3.7)$$

Considere o conjunto $M = \{m \in \mathbb{N}; m + 1 = 1 + m\}$.

Afirmção 3.9 $1 \in M$.

Como $1 + 1 = 1 + 1$, temos que $1 \in M$.

Afirmção 3.10 M é um conjunto indutivo.

Suponhamos que $m \in M$, isto é, $m + 1 = 1 + m$ (hipótese indutiva). Agora por (3.5), pela hipótese indutiva e pelo item 1 obtemos

$$S(m) + 1 = (m + 1) + 1 = (1 + m) + 1 = 1 + (m + 1) = 1 + S(m).$$

Daí, $S(m) \in M$.

Portanto, pela Afirmção 3.9 e Afirmção 3.10, M é um conjunto indutivo contendo 1. Consequentemente, $M = \mathbb{N}$.

Agora, considere o conjunto $P = \{n \in \mathbb{N}; m + n = n + m, \text{ para todo } m \in \mathbb{N}\}$.

Afirmção 3.11 $1 \in P$.

Por (3.7) temos que $1 \in P$.

Afirmção 3.12 P é um conjunto indutivo.

Suponhamos que $n \in P$, isto é, $m + n = n + m$ para todo $m \in \mathbb{N}$ (hipótese indutiva).

Agora por (3.5), (3.7), pela hipótese indutiva e pelo item 1 obtemos

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

Daí, $S(n) \in P$.

Portanto, pela Afirmção 3.11 e Afirmção 3.12, P é um conjunto indutivo contendo 1. Consequentemente, $P = \mathbb{N}$. ■

Observação 3.4 A propriedade associativa da adição foi obtida antes e foi usada para estabelecer a propriedade comutativa. Isso não é acidental, uma vez que a associatividade foi incorporada à operação de adição impondo as condições (3.5) e (3.6), de modo que

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

Teorema 3.6 [Teorema 1.6 em (COHEN; EHRLICH, 1963)] Existe exatamente uma função $K : \mathbb{N} \times \mathbb{N} \rightarrow \mathbb{N}$ tal que

$$\begin{aligned} K(m, 1) &= m, \text{ para todo } m \in \mathbb{N} \text{ e} \\ K(m, S(n)) &= K(m, n) + m, \text{ para todo } m, n \in \mathbb{N}. \end{aligned} \quad (3.8)$$

Demonstração.

Existência: Seja $m \in \mathbb{N}$ qualquer. Pelo Teorema 3.2, considerando $A = \mathbb{N}$, $a = m$ e $G(k) = k + m$, para todo $k \in \mathbb{N}$, existe exatamente uma função $K_m : \mathbb{N} \rightarrow \mathbb{N}$ tal que

$$K_m(1) = m, \quad (3.9)$$

$$K_m(S(n)) = K_m(n) + m, \text{ para todo } n \in \mathbb{N}. \quad (3.10)$$

O conjunto $K = \{(m, n), K_m(n)\}; (m, n) \in \mathbb{N} \times \mathbb{N}\}$ é uma função de $\mathbb{N} \times \mathbb{N}$ em \mathbb{N} . Para todo $(m, n) \in \mathbb{N} \times \mathbb{N}$, $K(m, n) = K_m(n)$. Por (3.9),

$$K(m, 1) = K_m(1) = m, \text{ para todo } m \in \mathbb{N}.$$

Por (3.10),

$$K(m, S(n)) = K_m(S(n)) = K_m(n) + m = K(m, n) + m, \text{ para todo } m, n \in \mathbb{N}.$$

Assim, K satisfaz (3.8).

Unicidade: Se \bar{K} é uma função de $\mathbb{N} \times \mathbb{N}$ satisfazendo (3.8), então

$$\bar{K}(m, 1) = m = K(m, 1), \text{ para todo } m \in \mathbb{N}.$$

Para todo $(m, n) \in \mathbb{N} \times \mathbb{N}$ tal que $\bar{K}(m, n) = K(m, n)$, temos que

$$\bar{K}(m, S(n)) = \bar{K}(m, n) + m = K(m, n) + m = K(m, S(n)).$$

Mas então, para cada $m \in \mathbb{N}$, o conjunto $N_m = \{n \in \mathbb{N}; \bar{K}(m, n) = K(m, n)\}$ é igual a \mathbb{N} desde que N_m é um conjunto indutivo contendo 1. Daí, $\bar{K}(m, n) = K(m, n)$ para todo $(m, n) \in \mathbb{N} \times \mathbb{N}$. Assim, $\bar{K} = K$. ■

Observação 3.5 Desde que K é uma função de $\mathbb{N} \times \mathbb{N}$ em \mathbb{N} , do Teorema 3.6, é uma operação binária em \mathbb{N} (Definição 2.17).

Definição 3.3 Escrevemos $m \cdot n$ ou mn em vez de $K(m, n)$, onde K é a função do Teorema 3.6, e usamos o nome familiar *multiplicação* para a operação binária “ \cdot ”.

Podemos agora reformular o Teorema 3.6:

Teorema 3.7 [Teorema 1.6 em (COHEN; EHRLICH, 1963)] Existe uma única operação binária sobre \mathbb{N} (chamada de *multiplicação*) tal que

$$m \cdot 1 = m, \text{ para todo } m \in \mathbb{N}, \quad (3.11)$$

$$m \cdot S(n) = m \cdot n + m, \text{ para todo } m, n \in \mathbb{N}. \quad (3.12)$$

Teorema 3.8 [Teorema 1.7, Teorema 1.8, Teorema 1.9 e Teorema 1.10 em (COHEN; EHRLICH, 1963)]

1. A multiplicação em \mathbb{N} é distributiva à esquerda sobre a adição, isto é, $m(n + p) = mn + mp$, para todo $m, n, p \in \mathbb{N}$.
2. A multiplicação em \mathbb{N} é associativa, isto é, $(mn)p = m(np)$, para todo $m, n, p \in \mathbb{N}$.
3. A multiplicação em \mathbb{N} é distributiva à direita sobre a adição, isto é, $(m + n)p = mp + np$, para todo $m, n, p \in \mathbb{N}$.
4. A multiplicação em \mathbb{N} é comutativa, isto é, $mn = nm$, para todo $m, n \in \mathbb{N}$.

Demonstração.

1. Considere o conjunto $P = \{p \in \mathbb{N}; m(n + p) = mn + mp, \text{ para todo } m, n \in \mathbb{N}\}$.

Afirmção 3.13 $1 \in P$.

Por (3.11) e (3.12), temos que

$$m(n + 1) = m \cdot S(n) = mn + m = mn + m \cdot 1.$$

Daí, $1 \in P$.

Afirmção 3.14 P é um conjunto indutivo.

Suponhamos que $p \in P$, isto é, $m(n+p) = mn + mp$ para todo $m, n \in \mathbb{N}$ (hipótese indutiva). Agora por (3.6), (3.12) e pela hipótese indutiva obtemos

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

Daí, $S(p) \in P$.

Portanto, pela Afirmação 3.13 e Afirmação 3.14, P é um conjunto indutivo contendo 1. Consequentemente, $P = \mathbb{N}$.

2. Considere o conjunto $P = \{p \in \mathbb{N}; (mn)p = m(np), \text{ para todo } m, n \in \mathbb{N}\}$.

Afirmação 3.15 $1 \in P$.

Por (3.11) temos

$$(mn) \cdot 1 = mn = m(n \cdot 1)$$

logo $1 \in P$.

Afirmação 3.16 P é um conjunto indutivo.

Suponhamos que $p \in P$, isto é, $(mn)p = m(np)$ para todo $m, n \in \mathbb{N}$ (hipótese indutiva). Agora por (3.12), (3.6), pela hipótese indutiva e pelo item 1 obtemos

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

Daí, $S(p) \in P$.

Portanto, pela Afirmação 3.15 e Afirmação 3.16, P é um conjunto indutivo contendo 1. Consequentemente, $P = \mathbb{N}$.

3. Considere o conjunto $P = \{p \in \mathbb{N}; (m+n)p = mp + np, \text{ para todo } m, n \in \mathbb{N}\}$.

Afirmação 3.17 $1 \in P$.

Por (3.11), temos que

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

Daí, $1 \in P$.

Afirmção 3.18 P é um conjunto indutivo.

Suponhamos que $p \in P$, isto é, $(m + n)p = mp + np$ para todo $m, n \in \mathbb{N}$ (hipótese indutiva). Agora por (3.6), (3.12), pelo Teorema 3.5 e pela hipótese indutiva obtemos

$$\begin{aligned} (m + n) \cdot S(p) &= (m + n)p + (m + n) = (mp + np) + (m + n) \\ &= mp + [np + (m + n)] = mp + [(m + n) + np] \\ &= [mp + (m + n)] + np = [(mp + m) + n] + np \\ &= (m \cdot S(p) + n) + np = m \cdot S(p) + (n + np) \\ &= m \cdot S(p) + (np + n) = m \cdot S(p) + n \cdot S(p). \end{aligned}$$

Daí, $S(p) \in P$.

Portanto, pela Afirmção 3.17 e Afirmção 3.18, P é um conjunto indutivo contendo 1. Consequentemente, $P = \mathbb{N}$.

4. Primeiro mostremos que

$$m \cdot 1 = 1 \cdot m \text{ para todo } m \in \mathbb{N}. \quad (3.13)$$

Considere o conjunto $M = \{m \in \mathbb{N}; m \cdot 1 = 1 \cdot m\}$.

Afirmção 3.19 $1 \in M$.

Como $1 \cdot 1 = 1 \cdot 1$, temos que $1 \in M$.

Afirmção 3.20 M é um conjunto indutivo.

Suponhamos que $m \in M$, isto é, $m \cdot 1 = 1 \cdot m$ (hipótese indutiva). Agora por (3.11), (3.12), (3.5) e pela hipótese indutiva obtemos

$$1 \cdot S(m) = 1 \cdot m + 1 = m \cdot 1 + 1 = m + 1 = S(m) = S(m) \cdot 1.$$

Daí, $S(m) \in M$.

Portanto, pela Afirmção 3.19 e Afirmção 3.20, M é um conjunto indutivo contendo 1. Consequentemente, $M = \mathbb{N}$.

Agora, considere o conjunto $P = \{n \in \mathbb{N}; m \cdot n = n \cdot m, \text{ para todo } m \in \mathbb{N}\}$.

Afirmção 3.21 $1 \in P$.

Por (3.13) temos que $1 \in P$.

Afirmção 3.22 P é um conjunto indutivo.

Suponhamos que $n \in P$, isto é, $m \cdot n = n \cdot m$ para todo $m \in \mathbb{N}$ (hipótese indutiva).

Agora por (3.11), (3.12), pela hipótese indutiva e pelo item 3 obtemos

$$\begin{aligned} m \cdot S(n) &= mn + m = nm + m \\ &= nm + m \cdot 1 = nm + 1 \cdot m \\ &= (n + 1)m = S(n) \cdot m. \end{aligned}$$

Daí, $S(n) \in P$.

Portanto, pela Afirmção 3.21 e Afirmção 3.22, P é um conjunto indutivo contendo 1. Consequentemente, $P = \mathbb{N}$. ■

3.2 Grupos e semigrupos

O conjunto \mathbb{N} de todos os números naturais, junto com a adição e a multiplicação, serve para ilustrar certas estruturas matemáticas abstratas que agora definimos.

Definição 3.4

1. Se \circ é uma operação binária sobre um conjunto G , então o par $\langle G, \circ \rangle$ é chamado de *grupoide*.
2. O grupoide $\langle G, \circ \rangle$ é chamado um *semigrupo* se a operação \circ é associativa.
3. Um semigrupo cuja operação é comutativa é chamado de *semigrupo comutativo*.

Os resultados do Teorema 3.5, item 2 e item 4 do Teorema 3.8 podem ser resumidos brevemente:

Teorema 3.9 [Teorema 1.11 em (COHEN; EHRLICH, 1963)] $\langle \mathbb{N}, + \rangle$ e $\langle \mathbb{N}, \cdot \rangle$ são semigrupos comutativos.

Definição 3.5 Se $\langle G, \circ \rangle$ é um grupoide e $e \in G$, então

1. e é chamado *identidade à esquerda* relativo a \circ , se $e \circ x = x$, para todo $x \in G$,
2. e é chamado *identidade à direita* relativo a \circ , se $x \circ e = x$, para todo $x \in G$,
3. e é uma *identidade (ambos os lados)* relativo a \circ , se $e \circ x = x \circ e = x$, para todo $x \in G$.

Como $1 \cdot n = n \cdot 1 = n$, para todo $n \in \mathbb{N}$, o número natural 1 serve como identidade relativa à multiplicação no semigrupo $\langle \mathbb{N}, \cdot \rangle$. No semigrupo $\langle \mathbb{N}, + \rangle$ não há identidade relativa à adição, pois $m + n \neq n$, para todo $m, n \in \mathbb{N}$ (Exemplo 3.4).

Teorema 3.10 [Teorema 1.12 em (COHEN; EHRLICH, 1963)] Um grupoide $\langle G, \circ \rangle$ contém no máximo uma identidade relativa a \circ .

Demonstração. Se e e f são identidades relativas a \circ , então $e = e \circ f = f$. ■

Usaremos este teorema em varias oportunidades para mostrar que um grupoide tem apenas uma identidade. O teorema implica, por exemplo, que não existe número natural $f \neq 1$ tal que $fn = nf = n$, para todo $n \in \mathbb{N}$.

3.3 Ordem em \mathbb{N}

Teorema 3.11 [Teorema 1.13 em (COHEN; EHRLICH, 1963)] Se $T = \{(m, n) \in \mathbb{N} \times \mathbb{N}; m + p = n \text{ para algum } p \in \mathbb{N}\}$ então T é um relação de ordem.

Demonstração. Desde que $T \subset \mathbb{N} \times \mathbb{N}$ é uma relação binária em \mathbb{N} . Para mostrar que T é uma relação de ordem mostramos que:

(1) Se $m, n \in \mathbb{N}$, então uma e apenas uma das afirmações:

- $m = n$,
- $(m, n) \in T$,
- $(n, m) \in T$,

é verdadeira (chamada *tricotomia*).

(2) Se $(m, n) \in T$ e $(n, p) \in T$, então $(m, p) \in T$ (chamada *transitividade*).

Para cada $m \in \mathbb{N}$, seja $M_m = \{n \in \mathbb{N}; \text{uma das afirmações em (1) é verdadeira}\}$.

Mostraremos que $M_m = \mathbb{N}$ para todo $m \in \mathbb{N}$.

Afirmção 3.23 $1 \in M_m$.

Pelo Teorema 3.1, ou $m = 1$ ou $m = p + 1$ para algum $p \in \mathbb{N}$. Daí, ou $m = 1$ ou $(1, m) \in T$. Em ambos os casos $1 \in M_m$.

Afirmção 3.24 M_m é um conjunto indutivo.

Suponhamos que $n \in M_m$, isto é, ou $m = n$, ou $(m, n) \in T$ ou $(n, m) \in T$ (hipótese indutiva).

- Se $m = n$, então por (3.5) tem-se $m + 1 = n + 1 = S(n)$. Daí, $(m, S(n)) \in T$ segue-se $S(n) \in M_m$.
- Se $(m, n) \in T$ então $m + p = n$ para algum $p \in \mathbb{N}$. Logo, por (3.6) temos

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

assim $(m, S(n)) \in T$. Daí, $S(n) \in M_m$

- Se $(n, m) \in T$ então $n + q = m$ para algum $q \in \mathbb{N}$. Como $p \in \mathbb{N}$, pelo Teorema 3.1, ou $q = 1$ ou $q = S(r)$ para algum $r \in \mathbb{N}$.
 - Se $q = 1$ então $S(n) = n + 1 = m$ logo $(n, S(n)) \in T$. Daí, $S(n) \in M_m$.
 - Se $q = S(r)$ então por (3.5) e pelo Teorema 3.5 tem-se

$$S(n) + r = (n + 1) + r = n + (1 + r) = n + (q + 1) = n + S(r) = n + q = m.$$

Logo, $(S(n), m) \in T$. Daí, $n \in M_m$.

Portanto, pela Afirmação 3.23 e Afirmação 3.24, M_m é um conjunto indutivo contendo 1. Consequentemente, $M_m = \mathbb{N}$ para todo $m \in \mathbb{N}$.

Agora, se $m, n \in \mathbb{N}$, então $n \in M_m$ e pelos menos uma das afirmações de (1) é verdadeira.

Resta mostrar que para $m, n \in \mathbb{N}$ não mais do que uma das afirmações de (1) é verdadeira.

- Se $m = n$ e $(m, n) \in T$, então $m + p = n = m$ para algum $p \in \mathbb{N}$.
- Se $m = n$ e $(n, m) \in T$, então $n + q = m = n$ para algum $q \in \mathbb{N}$.
- Se $(m, n) \in T$ e $(n, m) \in T$ então $m + p = n$ e $n + q = m$ para alguns $p, q \in \mathbb{N}$. Daí, pelo item 1 do Teorema 3.5

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

Em cada caso, temos uma contradição, desde que $m + t \neq m$, para todo $m, t \in \mathbb{N}$ (item 2 do Teorema 3.5 e o Exemplo 3.4). Isso completa a prova de (1).

Por outro lado, pela hipótese (2), existem $r, s \in \mathbb{N}$ tal que $m + r = n$ e $n + s = p$. Daí, pelo item 1 do Teorema 3.5 tem-se

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

Logo, $(m, p) \in T$. Isto prova (2). ■

Definição 3.6 Escrevemos $m < n$ ($n > m$) em vez de $(m, n) \in T$, onde T é a relação de ordem do Teorema 3.11, e lemos *m é menor que n* (*n é maior do que m*). Se $n = m + p$, escrevemos $p := n - m$ e note que $n - m$ é definido para $m, n \in \mathbb{N}$ só se $m < n$.

Podemos agora reinterpretar o Teorema 3.11:

Teorema 3.12

1. Se $m, n \in \mathbb{N}$, então apenas um de $m = n$, $m < n$, $n < m$ ($m = n$, $n > m$, $m > n$) é verdadeira (tricotomia).
2. Se $m < n$ e $n < p$ então $m < p$ (se $n > m$ e $p > n$ então $p > m$) (transitividade).

Teorema 3.13 [Exercício 1.8 e Exercício 1.9 em (COHEN; EHRLICH, 1963)] Para $m, n, p \in \mathbb{N}$. São satisfeitas:

1. Se $mp = np$ então $m = n$ (lei do cancelamento).
2. $m < n$ se, e só se, $m + p < n + p$.
3. $mp < np$ se, e só se, $m < n$.
4. $m < mp$ ou $m = mp$.

Demonstração.

1. Por hipótese temos $mp = np$. Suponhamos que $m \neq n$, pelo item 1 do Teorema 3.12, ou $n < m$ ou $m < n$.

- Se $n < m$ então existe $q \in \mathbb{N}$ tal que $n + q = m$ logo pelo item 3 do Teorema 3.8 tem-se

$$np + qp = (n + q)p = mp = np.$$

- Se $m < n$ então existe $q \in \mathbb{N}$ tal que $m + q = n$ logo pelo item 3 do Teorema 3.8 tem-se

$$mp = np = (m + q)p = mp + qp.$$

Em qualquer caso, temos uma contradição, desde que $m + t \neq m$, para todo $m, t \in \mathbb{N}$ (item 2 do Teorema 3.5 e o Exemplo 3.4). Portanto, $m = n$.

2. Se $m < n$ então existe $q \in \mathbb{N}$ tal que $m + q = n$. Logo, pelo Teorema 3.5 tem-se

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

Daí, $m + p < n + p$. Reciprocamente, se $m + p < n + p$ então existe $q \in \mathbb{N}$ tal que $(m + p) + q = n + p$. Logo, pelo Teorema 3.5 tem-se

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

Daí, pelo Exemplo 3.3, $m + q = n$ logo $m < n$.

3. Se $mp < np$ então existe $q \in \mathbb{N}$ tal que $mp + q = np$. Pelo item 1 do Teorema 3.12, ou $n = m$, ou $n < m$, ou $m < n$.

- Se $n = m$ então temos $mp + q = mp$.
- Se $n < m$ então existe $r \in \mathbb{N}$ tal que $n + r = m$. Logo, pelo item 1 do Teorema 3.5 e pelo item 3 do Teorema 3.8 tem-se

$$np + (rp + q) = (np + rp) + q = (n + r)p + q = mp + q = np.$$

Em qualquer caso, temos uma contradição, desde que $m + t \neq m$, para todo $m, t \in \mathbb{N}$ (item 2 do Teorema 3.5 e o Exemplo 3.4). Isso mostra que $m < n$. Reciprocamente, se $m < n$ então existe $q \in \mathbb{N}$ tal que $m + q = n$. Logo, pelo item 3 do Teorema 3.8 temos

$$mp + qp = (m + q)p = np.$$

Daí, $mp < np$.

4. Como $m, mp \in \mathbb{N}$ pelo item 1 do Teorema 3.12, ou $m = mp$, ou $m < mp$, ou $m > mp$. Observemos que essa última possibilidade não acontece. De fato, se $m > mp$ pelo item 3 temos que $p < 1$ o que contradiz o Teorema 3.1. ■

Observação 3.6 Note que de acordo com os itens 2 e 3 do Teorema 3.13, a ordem em \mathbb{N} não é alterada por nenhuma das operações binárias em \mathbb{N} .

Definição 3.7 Um triplo $\langle A, \circ, < \rangle$ tal que

1. $\langle A, \circ \rangle$ é um semigrupo,
2. $<$ é uma relação de ordem em A , e
3. se $a < b$ em A , então $a \circ c < b \circ c$, para todo $c \in A$,

é chamado um *semigrupo ordenado*.

Os resultados do item 1 do Teorema 3.5, item 2 do Teorema 3.8 e item 2 e 3 do Teorema 3.13 são resumidos brevemente:

Teorema 3.14 [Teorema 1.14 em (COHEN; EHRLICH, 1963)] $\langle \mathbb{N}, +, < \rangle$ e $\langle \mathbb{N}, \cdot, < \rangle$ são semigrupos ordenados.

Observação 3.7 A ordem em \mathbb{N} pode ser usada para definir subconjuntos de \mathbb{N} . Por exemplos, $M = \{n \in \mathbb{N}; S(1) < n\}$ e $P = \{n \in \mathbb{N}; n < S(m) \text{ para algum } m \in \mathbb{N}\}$.

É conveniente introduzir uma notação para enunciar definições: Denotaremos

1. $m \leq n$ para $m < n$ ou $m = n$,
2. $m < n < p$ para $m < n$ e $n < p$,
3. $m \leq n < p$ para $m \leq n$ e $n < p$,
4. $m < n \leq p$ para $m < n$ e $n \leq p$,
5. $m \leq n \leq p$ para $m \leq n$ e $n \leq p$.

Definição 3.8 Se $M \subset \mathbb{N}$ e existe algum $p \in M$ tal que $p \leq m$, para todo $m \in M$. Então p é chamado um *primeiro elemento (menor elemento)* de M .

Teorema 3.15 [Exercício 1.11 em (COHEN; EHRLICH, 1963)] Se $M \subset \mathbb{N}$ e p, q são primeiros elementos de M então $p = q$.

Demonstração. Como p e q são primeiros elementos de M , temos que $p \leq q \leq p$. Daí, $p = q$. ■

Se M tem um primeiro elemento então ele é único. Falaremos portanto do primeiro elemento de M .

Teorema 3.16 [Teorema 1.15 em (COHEN; EHRLICH, 1963)] 1 é o primeiro elemento de \mathbb{N} .

Demonstração. Se $n \in \mathbb{N}$, pelo Teorema 3.1, $m = 1$ ou $m = S(p) = p + 1$ para algum $p \in \mathbb{N}$. Se $m = p + 1$ então pela Definição 3.6 $1 < m$. Daí, $1 \leq m$ para todo $m \in \mathbb{N}$. Logo, pela Definição 3.8 e o Teorema 3.15, 1 é o único primeiro elemento de \mathbb{N} . ■

Corolário 1 [Corolário do Teorema 1.15 em (COHEN; EHRLICH, 1963)] Se $M \subset \mathbb{N}$ tal que $1 \in M$, então 1 é o primeiro elemento de M .

Teorema 3.17 [Teorema 1.16 em (COHEN; EHRLICH, 1963)] Se $n \in \mathbb{N}$, então $\{m \in \mathbb{N}; n < m < S(n)\} = \emptyset$.

Demonstração. Suponha por absurdo que existe $m \in \mathbb{N}$ tal que $n < m < S(n)$. Então, como $n < m$ existe $p \in \mathbb{N}$ tal que $n + p = m$. Pelo Teorema 3.1, $p = 1$ ou $p = S(q) = q + 1$ para algum $q \in \mathbb{N}$.

- Se $p = 1$ então $m = n + 1 = S(n)$ e $m < S(n)$ é falso pela Tricotomia.
- Se $p = S(q)$ então pelo Teorema 3.5 tem-se

$$m = n + (q + 1) = n + (1 + q) = (n + 1) + q = S(n) + q$$

logo $S(n) < m$. Assim, novamente pela tricotomia, $m < S(n)$ é falso.

Portanto, o conjunto de todos os $m \in \mathbb{N}$ tal que $n < m < S(n)$ é vazio. ■

Definição 3.9 Para $n \in \mathbb{N}$, o *segmento inicial* I_n é o conjunto de todos os $m \in \mathbb{N}$ tal que $m \leq n$.

Teorema 3.18 [Segundo Princípio de Indução, Teorema 1.17 em (COHEN; EHRLICH, 1963)] Se $M \subset \mathbb{N}$ tal que

$$(1) I_1 \subset M$$

$$(2) S(n) \in M \text{ sempre que } I_n \subset M,$$

então $M = \mathbb{N}$.

Demonstração. Consideremos o conjunto $P = \{n \in \mathbb{N}; I_n \subset M\}$. Por (1) temos que $1 \in P$. Agora, suponha que $n \in P$ logo $I_n \subset M$ daí por (2) temos que $S(n) \in M$. Pela Definição de I_n e o Teorema 3.17, $I_{S(n)} = I_n \cup \{S(n)\}$. Daí, $I_{S(n)} \subset M$. Logo, $(S(n)) \in P$. Portanto, pelo Axioma de Indução $P = \mathbb{N}$. Assim, dado $n \in \mathbb{N}$ tem-se que $n \in P$ daí $n \in I_n \subset M$ logo $n \in M$. Consequentemente, $\mathbb{N} \subset M$ e como $M \subset \mathbb{N}$, concluímos, $M = \mathbb{N}$. ■

Observação 3.8 Uma vez que a hipótese de (2) no Teorema 3.18 afirma “mais” do que a hipótese “ $n \in M$ ” de (ii) no Axioma de Indução (A3), a hipótese (1) e (2) do Teorema 3.18 afirma “menos” do que a hipótese do Axioma de Indução. Mas a conclusão “ $M = \mathbb{N}$ ” do Teorema 3.18 é também a conclusão do Axioma de Indução. Nesse sentido, o Teorema 3.8 é “mais forte” que o Axioma de Indução.

Teorema 3.19 [Princípio da Boa Ordenação, Teorema 1.18 em (COHEN; EHRLICH, 1963)] Todo subconjunto não-vazio de \mathbb{N} contém um primeiro elemento.

Demonstração. Provaremos a afirmação equivalente: “Se $M \subset \mathbb{N}$ e M não contém o primeiro elemento, então M é vazio”. Seja $P = \{n \in \mathbb{N}; n \notin M\}$.

Afirmção 3.25 $I_1 \subset P$.

Pelo Teorema 3.16, $1 \leq n$ para todo $n \in \mathbb{N}$ e como M não contém primeiro elemento temos que $1 \notin M$ assim $1 \in P$. Daí, $I_1 \subset P$.

Afirmção 3.26 Se $I_n \subset P$ então $S(n) \in P$.

Dado $p \in M$ temos que $p \notin I_n$, desde que $I_n \subset P$. Daí, $n < p$ e, pelo Teorema 3.17, $S(n) \leq p$. Desde que M não contém o primeiro elemento, $S(n) \notin M$. Portanto, $S(n) \in P$.

Agora, pela Afirmção 3.25 e Afirmção 3.26, e pelo Segundo Princípio de Indução (Teorema 3.17), $P = \mathbb{N}$. Concluímos que $M = \emptyset$. ■

Para esse capítulo, construímos o conjunto dos números naturais pelos Axioma de Dedekind, definindo o primeiro elemento dos \mathbb{N} . Construímos e definimos

as operações de adição e multiplicação sobretudo suas propriedades distributiva, associativa e comutativa, além disso, que \mathbb{N} é um conjunto bem ordenado. Para o próximo capítulo, faremos a construção do conjunto dos números inteiros e representaremos por \mathbb{Z} .

4 CONSTRUÇÃO DOS NÚMEROS INTEIROS

Neste capítulo, construiremos o conjunto dos números inteiros por classes de equivalência em $\mathbb{N} \times \mathbb{N}$. Ainda, introduziremos os conceitos de grupo, anel, anel comutativo, anel com identidade e domínio integral ordenado, que será importante para simplificar as nomenclaturas das propriedades que verificam os números inteiros. A referência base utilizada é (COHEN; EHRLICH, 1963).

O sistema $\langle \mathbb{N}, +, \cdot, < \rangle$, onde \mathbb{N} é o conjunto de todos os números naturais, reflete as propriedades dos números inteiros positivos em relação à adição, multiplicação e ordem. Como $m + p \neq m$ para todo $m, p \in \mathbb{N}$, não há números naturais correspondentes a zero ou aos inteiros negativos. Construiremos a partir de \mathbb{N} um conjunto \mathbb{Z} cujos elementos chamados inteiros e definiremos em \mathbb{Z} uma adição, $(+_{\mathbb{Z}})$, uma multiplicação $(\cdot_{\mathbb{Z}})$ e um ordem $(<_{\mathbb{Z}})$ de tal forma que \mathbb{Z} refletirá as propriedades dos conhecidos números inteiros positivos, zero e negativos. O sistema resultante $\langle \mathbb{Z}, +_{\mathbb{Z}}, \cdot_{\mathbb{Z}}, <_{\mathbb{Z}} \rangle$ será uma extensão de $\langle \mathbb{N}, +, \cdot, < \rangle$ no sentido que existe uma função injetiva de \mathbb{N} em \mathbb{Z} que “preserva” a adição, multiplicação e ordem. Os números inteiros corresponderão aos “números inteiros com sinal”.

Observamos que todo número inteiro com sinal pode ser representado de várias maneiras com uma diferença de dois números naturais (por exemplo, $+3 = 4 - 1 = 10 - 7 = 12 - 9$; $-2 = 1 - 3 = 5 - 7 = 18 - 20$), e que duas dessas diferenças são iguais quando suas “somas cruzadas” são iguais (por exemplo, $4 + 7 = 10 + 1$; $1 + 7 = 5 + 3$). Para refletir essas propriedades dos números inteiros com sinal, definimos um inteiro como uma classe de equivalência de pares ordenados de números naturais (correspondentes às diferenças de números inteiros positivos), tal que (m, n) e (p, q) são equivalentes se as “somas cruzadas” $m + q$ e $p + n$ são iguais.

Teorema 4.1 [Teorema 2.1 em (COHEN; EHRLICH, 1963)] Existe uma relação de equivalência Q em $\mathbb{N} \times \mathbb{N}$ tal que $(m, n)Q(p, q)$ vale sempre que $m + q = p + n$ em \mathbb{N} .

Demonstração. Desde que o conjunto

$$Q = \{((m, n), (p, q)) \in (\mathbb{N} \times \mathbb{N}) \times (\mathbb{N} \times \mathbb{N}); m + q = p + n, m, n, p, q \in \mathbb{N}\}$$

é um subconjunto de $(\mathbb{N} \times \mathbb{N}) \times (\mathbb{N} \times \mathbb{N})$, Q é uma relação binária em $\mathbb{N} \times \mathbb{N}$. Vejamos que Q é uma relação de equivalência:

- Reflexiva: Pelo item 2 do Teorema 3.5 temos que $m+n = n+m$ logo $((m, n), (m, n)) \in Q$.
- Simétrica: Se $((m, n), (p, q)) \in Q$ então $m + q = p + n$. Daí, $p + n = m + q$ então $((p, q), (m, n)) \in Q$.
- Transitiva: Se $((m, n), (p, q)) \in Q$ e $((p, q), (r, s)) \in Q$ então $m + q = p + n$ e $p + s = r + q$. Logo, pelo Teorema 3.5 tem-se

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

e, pela Lei de cancelação em \mathbb{N} (Exemplo 3.3), temos $m + s = r + n$, logo $((m, n), (r, s)) \in Q$.

Portanto, Q é uma relação de equivalência. ■

Definição 4.1 Escrevemos $(m, n) \sim (p, q)$ em vez de $(m, n)Q(p, q)$ e lemos “ \sim ” como é *equivalente a*. Para cada $(m, n) \in \mathbb{N} \times \mathbb{N}$, denotamos

$$C_{(m,n)} = \{(p, q) \in \mathbb{N} \times \mathbb{N}; (p, q) \sim (m, n)\}.$$

Um *inteiro* é uma classe de equivalência $C_{(m,n)}$. Denotamos por \mathbb{Z} ao conjunto de todos os inteiros e a, b, c, \dots sendo os elementos de \mathbb{Z} .

O conjunto \mathbb{Z} de todos os inteiros é o conjunto quociente $\mathbb{N} \times \mathbb{N}/Q$, onde Q é um subconjunto de $(\mathbb{N} \times \mathbb{N}) \times (\mathbb{N} \times \mathbb{N})$ definido no Teorema 4.1.

4.1 Adição em \mathbb{Z}

Os pare ordenados de números naturais que constituem um número inteiro correspondem às diferenças de números inteiros positivos associados a um número inteiro positivo com sinal. A adição por termo a termo de diferenças a dois números com sinal fornece uma diferença associada à sua soma, por exemplo

$$+3 + (-2) = (4 - 1) + (1 - 3) = (4 + 1) - (1 + 3).$$

Isso sugere que a adição por componentes de pares ordenados pertencentes a dois inteiros deve dar um par ordenado pertencente à soma dos inteiros, ou seja, que a soma de $a = C_{(m,n)}$ e $b = C_{(p,q)}$ deve ser o inteiro $c = C_{(m+p,n+q)}$. Mostraremos que c é independente da escolha de $(m, n) \in a$ e $(p, q) \in b$.

Teorema 4.2 [Teorema 2.2 em (COHEN; EHRLICH, 1963)] Se $(m', n') \sim (m, n)$ e $(p', q') \sim (p, q)$ então $(m + p, n + q) \sim (m' + p', n' + q')$.

Demonstração. Pela hipótese e a Definição 4.1, $m' + n = m + n'$ e $p' + q = p + q'$. Daí, pelo Teorema 3.5 temos que

$$\begin{aligned} (m + p) + (n' + q') &= (m + n') + (p + q') \\ &= (m' + n) + (p' + q) = (m' + p') + (n + q) \end{aligned}$$

e, pela Definição 4.1, $(m + p, n + q) \sim (m' + p', n' + q')$. ■

Teorema 4.3 [Teorema 2.3 em (COHEN; EHRLICH, 1963)] Existe uma operação binária F em \mathbb{Z} tal que $F(a, b) = C_{(m+p,n+q)}$ se $(m, n) \in a$ e $(p, q) \in b$.

Demonstração. O conjunto

$$F = \{((a, b), C_{(m+p,n+q)}); (m, n) \in a, (p, q) \in b, a, b \in \mathbb{Z}\}$$

é um subconjunto de $(\mathbb{Z} \times \mathbb{Z}) \times \mathbb{Z}$. Para cada $(a, b) \in \mathbb{Z} \times \mathbb{Z}$ existem $(m, n) \in a$, $(p, q) \in b$ e $c = C_{(m+p,n+q)}$ tal que $((a, b), c) \in F$. Se $(m', n') \in a$, $(p', q') \in b$ e $c' = C_{(m'+p',n'+q')}$ então $(m', n') \sim (m, n)$ e $(p', q') \sim (p, q)$ e, pelo Teorema 4.2, $c' = c$ então F é uma função de $\mathbb{Z} \times \mathbb{Z}$ em \mathbb{Z} (Definição 2.13). Agora, pela Definição 2.17, F é uma operação binária em \mathbb{Z} e $F(a, b) = c$. ■

Definição 4.2 Nós chamamos a operação binária F do Teorema 4.3 de *adição* em \mathbb{Z} e escrevemos

$$a +_{\mathbb{Z}} b = F(a, b), \text{ para todo } a, b \in \mathbb{Z}.$$

Nós omitimos o subscrito e escrevemos $a + b$ se não houver confusão no contexto.

Teorema 4.4 [Teorema 2.4 em (COHEN; EHRLICH, 1963)] $\langle \mathbb{Z}, +_{\mathbb{Z}} \rangle$ é um semigrupo comutativo com identidade.

Demonstração.

1. Adição em \mathbb{Z} é associativa.

Se $a, b, c \in \mathbb{Z}$, então $a = C_{(m,n)}$, $b = C_{(p,q)}$, $c = C_{(r,t)}$ para alguns $m, n, p, q, r, t \in \mathbb{N}$.

Pela Definição 4.2, Teorema 4.3 e pelo item 1 do Teorema 3.5,

$$\begin{aligned} a +_{\mathbb{Z}} (b +_{\mathbb{Z}} c) &= C_{(m,n)} +_{\mathbb{Z}} C_{(p+r,q+t)} \\ &= C_{(m+(p+r),n+(q+t))} \\ &= C_{((m+p)+r,(n+q)+t)} \\ &= C_{(m+p,n+q)} + C_{(r,t)} \\ &= (a +_{\mathbb{Z}} b) +_{\mathbb{Z}} c. \end{aligned}$$

2. Adição em \mathbb{Z} é comutativa.

Se $a, b \in \mathbb{Z}$, então $a = C_{(m,n)}$ e $b = C_{(p,q)}$ para alguns $m, n, p, q \in \mathbb{N}$. Pela Definição 4.2, Teorema 4.3 e pelo item 2 do Teorema 3.5,

$$\begin{aligned} a +_{\mathbb{Z}} b &= F(a, b) = C_{(m+p,n+q)} \\ &= C_{(p+m,q+n)} \\ &= F(b, a) = b +_{\mathbb{Z}} a. \end{aligned}$$

3. \mathbb{Z} contém uma única identidade para a adição.

Se $a = C_{(m,n)}$ é qualquer elemento de \mathbb{Z} , então

$$a +_{\mathbb{Z}} C_{(1,1)} = C_{(m+1,n+1)}.$$

Desde que pelo item 1 do Teorema 3.5 $(m+1) + n = m + (n+1)$ logo temos $(m+1, n+1) \sim (m, n)$. Daí, pela Definição 4.1,

$$C_{(m+1,n+1)} = C_{(m,n)}$$

logo

$$a +_{\mathbb{Z}} C_{(1,1)} = a.$$

Portanto, $C_{(1,1)}$ é uma identidade para \mathbb{Z} . Pelo Teorema 3.10, existe uma única identidade. ■

Observação 4.1 Escrevemos 0 para denotar a identidade para a adição em \mathbb{Z} e lemos zero.

Teorema 4.5 [Teorema 2.5 em (COHEN; EHRLICH, 1963)] Se $a \in \mathbb{Z}$, então existe um único $a' \in \mathbb{Z}$ tal que $a +_{\mathbb{Z}} a' = a' +_{\mathbb{Z}} a = 0$.

Demonstração. Se $a = C_{(m,n)} \in \mathbb{Z}$ e $a' = C_{(n,m)}$ então pelo item 2 do Teorema 3.5 tem-se

$$a +_{\mathbb{Z}} a' = C_{(m+n,n+m)} = C_{(m+n,m+n)}.$$

Desde que $(q, q) \sim (1, 1)$ para todo $q \in \mathbb{N}$, segue-se da Definição 4.1 que $C_{(m+n,m+n)} = C_{(1,1)}$. Daí, $a +_{\mathbb{Z}} a' = a' +_{\mathbb{Z}} a = 0$.

Se a'' é outro elemento de \mathbb{Z} tal que $a +_{\mathbb{Z}} a'' = a'' +_{\mathbb{Z}} a = 0$, então pelo Teorema 4.4 temos que

$$\begin{aligned} a' &= a' +_{\mathbb{Z}} 0 = a' +_{\mathbb{Z}} (a +_{\mathbb{Z}} a'') \\ &= (a' +_{\mathbb{Z}} a) +_{\mathbb{Z}} a'' = 0 +_{\mathbb{Z}} a'' = a''. \end{aligned}$$

Portanto, $a' = a''$. ■

Observação 4.2 Escrevemos $-a$, para denotar o único elemento a' do Teorema 4.5.

Teorema 4.6 [Exercício 2.1 em (COHEN; EHRLICH, 1963)]

1. Para $a, b \in \mathbb{Z}$ existe um único $c \in \mathbb{Z}$ tal que $a = b + c$ em \mathbb{Z} .
2. Se $a + c = b + c$ em \mathbb{Z} então $a = b$ (lei do cancelamento para a adição em \mathbb{Z}).

Demonstração.

1. Se $a, b \in \mathbb{Z}$, então $a = C_{(m,n)}$ e $b = C_{(p,q)}$ para alguns $m, n, p, q \in \mathbb{N}$. Consideremos $c = C_{(m+q,p+n)}$,

$$\begin{aligned} b + c &= C_{(p,q)} + C_{(m+q,p+n)} \\ &= C_{(p+(m+q),q+(p+n))}. \end{aligned}$$

Por outro lado, pelo Teorema 3.5 temos

$$[p+(m+q)]+n = n+[p+(m+q)] = (n+p)+(m+q) = (m+q)+(p+n) = m+[q+(p+n)]$$

logo $(p + (m + q), q + (p + n)) \sim (m, n)$, segue-se que da Definição 4.1 que $C_{(p+(m+q),q+(p+n))} = C_{(m,n)}$. Daí, $a = b + c$.

Se c' é outro elemento de \mathbb{Z} tal que $a = b + c'$, então pelo Teorema 4.4 e Teorema 4.5 temos que

$$\begin{aligned} c &= 0 + c = [(-b) + b] + c \\ &= (-b) + (b + c) = (-b) + (b + c') \\ &= [(-b) + b] + c' = 0 + c' = c'. \end{aligned}$$

2. Pelo Teorema 4.4 e Teorema 4.5 tem-se

$$\begin{aligned} a &= a + 0 = a + [c + (-c)] \\ &= (a + c) + (-c) = (b + c) + (-c) \\ &= b + [c + (-c)] = b + 0 = b. \end{aligned}$$

Portanto, $a = b$. ■

Observação 4.3 Escrevemos $a - b$ para o único elemento c tal que $a = b + c$ em \mathbb{Z} .

Definição 4.3 Se $\langle A, \circ \rangle$ é um semigrupo, e identidade à direita, identidade à esquerda ou ambos os lados para \circ , $e, x, y \in A$, então y é chamado uma

1. *inversa à esquerda de x relativa para e se $y \circ x = e$,*
2. *inversa à direita de x relativa para e se $x \circ y = e$,*
3. *inversa (ambos os lados) de x relativa para e se $x \circ y = y \circ x = e$.*

Observação 4.4 O elemento a' do Teorema 4.5 é uma inversa de a relativa a identidade e . A prova dada acima para a unicidade do inverso aplica-se em semigrupos arbitrários.

Teorema 4.7 [Teorema 2.6 em (COHEN; EHRLICH, 1963)] Em um semigrupo $\langle A, \circ \rangle$ com identidade (ambos os lados) e , um elemento x tem no máximo uma inversa relativa para e .

Demonstração. Se x' e x'' são ambos inversos de x , então

$$x'' = x'' \circ e = x'' \circ (x \circ x') = (x'' \circ x) \circ x' = e \circ x' = x'.$$

Portanto, $x'' = x'$. ■

Usaremos este teorema repetidamente para provar a unicidade das inversas.

Definição 4.4 Se $\langle A, \circ \rangle$ é um semigrupo com identidade e tal que todo elemento de A tem uma inversa relativa para e , então $\langle A, \circ \rangle$ é chamado de *grupo*.

Portanto, $\langle \mathbb{Z}, +_{\mathbb{Z}} \rangle$ é um grupo, enquanto $\langle \mathbb{N}, + \rangle$ não é um grupo. O objetivo da nossa construção de \mathbb{Z} foi incorporar o semigrupo $\langle \mathbb{N}, + \rangle$ no grupo $\langle \mathbb{Z}, +_{\mathbb{Z}} \rangle$.

4.2 Multiplicação em \mathbb{Z}

Nossa definição de multiplicação em \mathbb{Z} é padronizada no comportamento das diferenças de números inteiros positivos com sinal sob multiplicação:

$$(+2)(-3) = (4 - 2)(3 - 6) = (4 \cdot 3 + 2 \cdot 6) - (2 \cdot 3 + 4 \cdot 6).$$

Isso sugere que o produto de $a = C_{(m,n)}$ e $b = C_{(p,q)}$ deve ser $c = C_{(mp+nq, mq+np)}$, desde que c seja independente da escolha de $(m, n) \in a$ e $(p, q) \in b$.

Teorema 4.8 [Teorema 2.7 em (COHEN; EHRLICH, 1963)] Se $(m, n) \sim (m', n')$ e $(p, q) \sim (p', q')$ então $(mp + nq, mq + np) \sim (m'p' + n'q', m'q' + n'p')$.

Demonstração. A conclusão do teorema segue de

$$(mp + nq, mq + np) \sim (m'p + n'q, m'q + n'p) \quad (4.1)$$

e

$$(m'p + n'q, m'q + n'p) \sim (m'p' + n'q', m'q' + n'p') \quad (4.2)$$

pela transitividade da relação de equivalência (Teorema 4.1).

Da hipótese, $m + n' = m' + n$. Daí, pelo Teorema 3.5 e item 3 do Teorema 3.8 temos

$$\begin{aligned} (mp + nq) + (m'q + n'p) &= (mp + nq) + (n'p + m'q) = [(mp + nq) + n'p] + m'q \\ &= [mp + (nq + n'p)] + m'q = [mp + (n'p + nq)] + m'q \\ &= [(mp + n'p) + nq] + m'q = [(m + n')p + nq] + m'q \\ &= (m + n')p + (nq + m'q) = (m' + n)p + (n + m')q \\ &= (m' + n)p + (m' + n)q = (m' + n)(p + q) \end{aligned}$$

e

$$\begin{aligned} (m'p + n'q) + (mq + np) &= (m'p + n'q) + (np + mq) = [(m'p + n'q) + np] + mq \\ &= [m'p + (n'q + np)] + mq = [m'p + (np + n'q)] + mq \\ &= [(m'p + np) + n'q] + mq = [(m' + n)p + n'q] + mq \\ &= (m' + n)p + (n'q + mq) = (m' + n)p + (n' + m)q \\ &= (m + n')p + (m + n')q = (m + n')(p + q). \end{aligned}$$

Portanto, pela Definição 4.1, (4.1) é provado.

Da hipótese, $p + q' = p' + q$. Daí, pelo Teorema 3.5 e item 1 do Teorema

3.8 temos

$$\begin{aligned}
 (m'p + n'q) + (m'q' + n'p') &= [(m'p + n'q) + m'q'] + n'p' = [m'p + (n'q + m'q')] + n'p' \\
 &= [m'p + (m'q' + n'q)] + n'p' = [(m'p + m'q') + n'q] + n'p' \\
 &= (m'p + m'q') + (n'q + n'p') = m'(p + q') + n'(q + p') \\
 &= m'(p + q') + n'(p' + q) = m'(p + q') + n'(p + q') \\
 &= (m' + n')(p + q')
 \end{aligned}$$

e

$$\begin{aligned}
 (m'p' + n'q') + (m'q + n'p) &= [(m'p' + n'q') + m'q] + n'p = [m'p' + (n'q' + m'q)] + n'p \\
 &= [m'p' + (m'q + n'q')] + n'p = [(m'p' + m'q) + n'q'] + n'p \\
 &= (m'p' + m'q) + (n'q' + n'p) = m'(p' + q) + n'(q' + p) \\
 &= m'(p + q') + n'(p + q') = (m' + n')(p + q').
 \end{aligned}$$

Portanto, pela Definição 4.1, (4.2) é provado. ■

Teorema 4.9 [Teorema 2.8 em (COHEN; EHRLICH, 1963)] Existe uma operação binária G em \mathbb{Z} tal que $G(a, b) = C_{(mp+nq, mq+np)}$ se $(m, n) \in a$ e $(p, q) \in b$.

Demonstração. O conjunto

$$G = \{((a, b), C_{(mp+nq, mq+np)}); (m, n) \in a, (p, q) \in b, a, b \in \mathbb{Z}\}$$

é um subconjunto de $(\mathbb{Z} \times \mathbb{Z}) \times \mathbb{Z}$. Para cada $(a, b) \in \mathbb{Z} \times \mathbb{Z}$ existem $(m, n) \in a$, $(p, q) \in b$ e $c = C_{(mp+nq, mq+np)}$ tal que $((a, b), c) \in G$. Se $(m', n') \in a$, $(p', q') \in b$ e $c' = C_{(m'p'+n'q', m'q'+n'p')}$ então $(m', n') \sim (m, n)$, $(p', q') \sim (p, q)$ e, pelo Teorema 4.8,

$$(mp + nq, mq + np) \sim (m'p' + n'q', m'q' + n'p').$$

Daí, pela Definição 4.1 $c' = c$. Mas então G é uma função de $\mathbb{Z} \times \mathbb{Z}$ em \mathbb{Z} (Definição 2.13). Agora, pela Definição 2.17, G é uma operação binária em \mathbb{Z} e $G(a, b) = c$. ■

Definição 4.5 Chamamos a operação binária G do Teorema 4.9 de *multiplicação* em \mathbb{Z} e escrevemos

$$a \cdot_{\mathbb{Z}} b = G(a, b), \text{ para todo } a, b \in \mathbb{Z}.$$

(Nós omitimos o subscrito e escrevemos $a \cdot b$ ou ab se não houver confusão no contexto.)

Teorema 4.10 [Teorema 2.9 em (COHEN; EHRLICH, 1963)] $\langle \mathbb{Z}, \cdot_{\mathbb{Z}} \rangle$ é um semigrupo comutativo com identidade.

Demonstração.

1. Multiplicação em \mathbb{Z} é associativa.

Se $a, b, c \in \mathbb{Z}$, então $a = C_{(m,n)}$, $b = C_{(p,q)}$, $c = C_{(r,t)}$ para alguns $m, n, p, q, r, t \in \mathbb{N}$.

Pela Definição 4.5, Teorema 4.9, Teorema 3.5 e Teorema 3.8,

$$\begin{aligned} a \cdot_{\mathbb{Z}} (b \cdot_{\mathbb{Z}} c) &= C_{(m,n)} \cdot_{\mathbb{Z}} C_{(pr+qt,pt+qr)} \\ &= C_{(m(pr+qt)+n(pt+qr),m(pt+qr)+n(pr+qt))} \\ &= C_{(mp+nq)r+(mq+np)t,(mp+nq)t+(mq+np)r} \\ &= C_{(mp+nq,mq+np)} \cdot_{\mathbb{Z}} C_{(r,t)} \\ &= (a \cdot_{\mathbb{Z}} b) \cdot_{\mathbb{Z}} c. \end{aligned}$$

2. Multiplicação em \mathbb{Z} é comutativa.

Se $a, b \in \mathbb{Z}$, então $a = C_{(m,n)}$ e $b = C_{(p,q)}$ para alguns $m, n, p, q \in \mathbb{N}$. Pela Definição 4.5, Teorema 4.9, pelo item 2 do Teorema 3.5 e pelo item 2 do Teorema 3.8,

$$\begin{aligned} a \cdot_{\mathbb{Z}} b &= G(a, b) = C_{(mp+nq,mq+np)} \\ &= C_{(pm+qn,pn+qm)} \\ &= G(b, a) = b \cdot_{\mathbb{Z}} a. \end{aligned}$$

3. \mathbb{Z} contém uma única identidade para a multiplicação.

Se $a = C_{(m,n)}$ é qualquer elemento de \mathbb{Z} , então

$$\begin{aligned} a \cdot_{\mathbb{Z}} C_{(1+1,1)} &= C_{(m,n)} \cdot_{\mathbb{Z}} C_{(1+1,1)} = C_{(m(1+1)+n,m+n(1+1))} \\ &= C_{(m+m+n,m+n+n)} = C_{(2m+n,m+2n)}. \end{aligned}$$

Desde que pelo Teorema 3.5

$$(2m+n)+n = 2m+(n+n) = 2m+2n = (m+m)+2n = m+(m+2n) = (m+2n)+m$$

logo temos $(2m+n, m+2n) \sim (m, n)$. Daí, pela Definição 4.1,

$$C_{(2m+n,m+2n)} = C_{(m,n)}$$

logo

$$a \cdot_{\mathbb{Z}} C_{(1+1,1)} = a.$$

Portanto, $C_{(1+1,1)}$ é uma identidade para a multiplicação em \mathbb{Z} . Pelo Teorema 3.10, existe uma única identidade. ■

Observação 4.5 Escrevemos $1_{\mathbb{Z}}$ para identidade da multiplicação. (Se não houver confusão com $1_{\mathbb{Z}}$ em \mathbb{N} , é provável que omitamos o subscrito e escrevamos 1.)

Teorema 4.11 [Teorema 2.10 em (COHEN; EHRLICH, 1963)] A multiplicação em \mathbb{Z} é distributiva em relação à adição.

Demonstração.

1. A multiplicação em \mathbb{Z} é distributiva à esquerda sobre a adição. Se $a, b, c \in \mathbb{Z}$, então $a = C_{(m,n)}$, $b = C_{(p,q)}$, $c = C_{(r,t)}$ para alguns $m, n, p, q, r, t \in \mathbb{N}$. Pela Definição 4.5, Definição 4.2, Teorema 4.9, Teorema 4.3, pelo item 1 do Teorema 3.8 e pelo item 1 do Teorema 3.5,

$$\begin{aligned} a \cdot_{\mathbb{Z}} (b +_{\mathbb{Z}} c) &= C_{(m,n)} \cdot_{\mathbb{Z}} C_{(p+r,q+t)} \\ &= C_{(m(p+r)+n(q+t), m(q+t)+n(p+r))} \\ &= C_{((mp+nq)+(mr+nt), (mq+np)+(mt+nr))} \\ &= C_{(mp+nq, mq+np)} +_{\mathbb{Z}} C_{(mr+nt, mt+nr)} \\ &= a \cdot_{\mathbb{Z}} b +_{\mathbb{Z}} a \cdot_{\mathbb{Z}} c. \end{aligned}$$

2. A multiplicação em \mathbb{Z} é distributiva à direita sobre a adição. Se $a, b, c \in \mathbb{Z}$, então $a = C_{(m,n)}$, $b = C_{(p,q)}$, $c = C_{(r,t)}$ para alguns $m, n, p, q, r, t \in \mathbb{N}$. Pela Definição 4.5, Definição 4.2, Teorema 4.9, Teorema 4.3, pelo item 3 do Teorema 3.8 e pelo item 1 do Teorema 3.5,

$$\begin{aligned} (a +_{\mathbb{Z}} b) \cdot_{\mathbb{Z}} c &= C_{(m+p,n+q)} \cdot_{\mathbb{Z}} C_{(r,t)} \\ &= C_{((m+p)r+(n+q)t, (m+p)t+(n+q)r)} \\ &= C_{((mr+nt)+(pr+qt), (mt+nr)+(pt+qr))} \\ &= C_{(mr+nt, mt+nr)} +_{\mathbb{Z}} C_{(pr+qt, pt+qr)} \\ &= a \cdot_{\mathbb{Z}} c +_{\mathbb{Z}} b \cdot_{\mathbb{Z}} c. \end{aligned}$$

Portanto, a multiplicação em \mathbb{Z} é distributiva em relação à adição. ■

4.3 Anéis

Definição 4.6 Um triplo $\langle A, +, \cdot \rangle$ é chamado de *anel* se:

1. $\langle A, + \rangle$ é um grupo comutativo,

2. $\langle A, \cdot \rangle$ é um semigrupo, e
3. \cdot é distributiva à esquerda e à direita sobre $+$.

Um anel $\langle A, +, \cdot \rangle$ é chamado de *comutativo* se o semigrupo $\langle A, \cdot \rangle$ for comutativo, e é chamado de *anel com identidade* se o semigrupo $\langle A, \cdot \rangle$ tiver uma identidade.

Algumas vezes nos referimos a um anel $\langle A, +, \cdot \rangle$ brevemente como *o anel* A e à identidade de $\langle A, + \rangle$ como 0_A .

Teorema 4.12 [Teorema 2.11 em (COHEN; EHRLICH, 1963)] O triplo $\langle \mathbb{Z}, +_{\mathbb{Z}}, \cdot_{\mathbb{Z}} \rangle$ é um anel comutativo com identidade.

Demonstração. Pelo Teorema 4.4 e Teorema 4.5, $\langle \mathbb{Z}, +_{\mathbb{Z}} \rangle$ é um grupo comutativo. Pelo Teorema 4.10 $\langle \mathbb{Z}, \cdot_{\mathbb{Z}} \rangle$ é um semigrupo comutativo com $1_{\mathbb{Z}}$ como a única identidade. Também, pelo Teorema 4.11, $\langle \mathbb{Z}, \cdot_{\mathbb{Z}} \rangle$ é distributiva à esquerda e à direita em relação à adição. Portanto, $\langle \mathbb{Z}, +_{\mathbb{Z}}, \cdot_{\mathbb{Z}} \rangle$ é um anel comutativo com identidade. ■

4.4 Ordem em \mathbb{Z}

Os inteiros familiares são positivos, negativos ou zero. Um inteiro b excede um inteiro a se a diferença $b - a$ for positiva. Isso sugere introduzir em \mathbb{Z} um conjunto de elementos positivos e usa-ló para definir ordem.

Definição 4.7 Um inteiro a é chamado *positivo* se $(m, n) \in a$ para algum m, n tal que $n < m$ em \mathbb{N} .

Para mostrar que, de acordo com essa definição, um inteiro é positivo não importa qual par ordenado de números naturais seja usado para representá-lo, provamos:

Teorema 4.13 [Teorema 2.12 em (COHEN; EHRLICH, 1963)] Se $n < m$ em \mathbb{N} e $(p, q) \sim (m, n)$ em $\mathbb{N} \times \mathbb{N}$ então $q < p$ em \mathbb{N} .

Demonstração. Da hipótese, $n + h = m$ para algum $h \in \mathbb{N}$. Também, por hipótese, $n + p = q + m$. Daí, $n + p = q + (n + h)$ e, pelo Teorema 3.5 tem-se

$$n + p = (q + n) + h = (n + q) + h = n + (q + h)$$

e pela lei da cancelação para a adição (Exemplo 3.3), $p + q + h$. Segue-se que $q < p$ em \mathbb{N} . ■

Corolário 2 [Corolário do Teorema 2.12 em (COHEN; EHRLICH, 1963)] Um inteiro a , é positivo se, e só se, $n < m$ para todo $(m, n) \in a$.

Teorema 4.14 [Teorema 2.13 em (COHEN; EHRLICH, 1963)] Se $a \in \mathbb{Z}$, então uma e somente uma das seguintes afirmações é verdadeira:

- (i) a é positivo, (ii) $a = 0$, (iii) $-a$ é positivo.

Demonstração. Suponha $a = C_{(m,n)}$. Pela Definição 4.7 e o Teorema 4.13, a é positivo se, e só se, $n < m$. Desde que $C_{(1,1)} = 0$, $a = 0$ se, e só se, $m = n$. Desde que $C_{(n,m)} = -C_{(m,n)}$, $-a$ é positivo se, e só se, $m < n$. Pela tricotomia da ordem em \mathbb{N} (Teorema 3.11), exatamente um de $m < n$, $m = n$, $n < m$ é verdadeiro. Daí, exatamente uma de (i), (ii) e (iii) é verdadeira. ■

Teorema 4.15 [Exercício 2.10 em (COHEN; EHRLICH, 1963)] Se a, b são positivos em \mathbb{Z} então $a + b$ é positivo.

Demonstração. Seja $(r, t) \in a + b$. Como a, b inteiros positivos, pela Definição 4.7, existem m, n, p, q tais que $(m, n) \in a$ com $n < m$ e $(p, q) \in b$ com $q < p$. Logo, pela Definição 4.2 e o Teorema 4.3, tem-se

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

Agora, como $(r, t) \in a + b$, pela Definição 4.1, $(m+p, n+q) \sim (r, t)$. Note que $n+q < m+p$ daí, pelo Teorema 4.13, $t < r$ e portanto pelo Corolário 2, $a + b$ é positivo. ■

Teorema 4.16 [Teorema 2.14 em (COHEN; EHRLICH, 1963)] Se $T = \{(a, b) \in \mathbb{Z} \times \mathbb{Z}; b - a \text{ é positivo}\}$ então T é uma relação de ordem em \mathbb{Z} .

Demonstração. Desde que $T \subset \mathbb{Z} \times \mathbb{Z}$ é uma relação binária em \mathbb{Z} . Para mostrar que T é uma relação de ordem mostramos que:

- (1) Se $a, b \in \mathbb{Z}$, então uma e apenas uma das afirmações:

- $a = b,$
- $(a, b) \in T,$
- $(b, a) \in T,$

é verdadeira (chamada *tricotomia*).

(2) Se $(a, b) \in T$ e $(b, c) \in T$, então $(a, c) \in T$ (chamada *transitividade*).

Se $a, b \in \mathbb{Z}$, então $b - a \in \mathbb{Z}$ e, pelo Teorema 4.14, apenas um dos, $a - b = 0$, $a - b$ é positivo, $b - a$ é positivo é verdadeiro. Daí, apenas um dos $a = b$, $(a, b) \in T$, $(b, a) \in T$ é verdadeiro. Portanto, T tem a propriedade da Tricotomia.

Se $(a, b) \in T$ e $(b, c) \in T$, então $b - a$ e $c - b$ são positivos e, pelo Teorema 4.15,

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

é positivo. Logo, $(a, c) \in T$. Daí, T é transitivo. Pela Definição 2.12, T é uma relação de ordem em \mathbb{Z} . ■

Observação 4.6 Escrevemos $a <_{\mathbb{Z}} b$ ou $b >_{\mathbb{Z}} a$ (leia-se a é menor que b em \mathbb{Z} ou b é maior que a em \mathbb{Z}) se $b - a$ é positivo, isto é, se $(a, b) \in T$, onde T é a relação de ordem do Teorema 4.16. Normalmente omitimos o subscrito e escrevemos $a < b$ ou $b > a$.

Denotamos por \mathbb{Z}^+ ao conjunto de todos os inteiros positivos.

Teorema 4.17 [Teorema 2.15 em (COHEN; EHRLICH, 1963)] $\mathbb{Z}^+ = \{C_{(S(n),1)}; n \in \mathbb{N}\}$.

Demonstração. Devemos provar que

$$\{C_{(S(n),1)}; n \in \mathbb{N}\} \subset \mathbb{Z}^+ \quad (4.3)$$

e

$$\mathbb{Z}^+ \subset \{C_{(S(n),1)}; n \in \mathbb{N}\}. \quad (4.4)$$

Como, $1 < S(n)$ para todo $n \in \mathbb{N}$. Daí, $C_{(S(n),1)} \in \mathbb{Z}^+$, para todo $n \in \mathbb{N}$. Portanto, (4.3) é satisfeito. Seja $a = C_{(p,q)} \in \mathbb{Z}^+$, então $q < p$ em \mathbb{N} .

- Se $q = 1$, então $p > 1$ daí, $p = S(n)$ para algum $n \in \mathbb{N}$. Logo, $a = C_{(S(n),1)}$.
- Se $1 < q < p$, então $q = 1 + m$ e $p = 1 + m + n$ para alguns $m, n \in \mathbb{N}$. Logo, como $1 + m + n + 1 = 1 + m + S(n)$ então $(p, q) = (1 + m + m, 1 + m) \sim (S(n), 1)$ daí $a = C_{(S(n),1)}$.

Em qualquer caso (4.4) é provado.

A igualdade segue de (4.3) e (4.4). ■

Teorema 4.18 [Teorema 2.16 em (COHEN; EHRLICH, 1963)] Para $a, b \in \mathbb{Z}^+$ então $a \cdot b \in \mathbb{Z}^+$.

Demonstração. Se $a, b \in \mathbb{Z}^+$. Pelo Teorema 4.17, $a = C_{(S(n),1)}$ e $b = C_{(S(m),1)}$ para alguns $m, n \in \mathbb{N}$. Daí,

$$\begin{aligned} a \cdot b &= C_{(S(n),1)} \cdot_{\mathbb{Z}} C_{(S(m),1)} = C_{(mn+m+n+1+1, n+1+m+1)} \\ &= C_{(mn+1,1)} = C_{(S(mn),1)} \in \mathbb{Z}^+. \end{aligned}$$

Portanto, $a \cdot b \in \mathbb{Z}^+$. ■

Teorema 4.19 [Exercício 2.12 em (COHEN; EHRLICH, 1963)] Se $a \neq 0$ e $b \neq 0$ em \mathbb{Z} , então $a \cdot b \neq 0$ em \mathbb{Z} .

Demonstração. Como $a \neq 0, b \neq 0$ em \mathbb{Z} , pelo Teorema 4.16, ou $a > 0$ ou $-a > 0$ e, ou $b > 0$ ou $-b > 0$ em \mathbb{Z} .

- Se $a > 0$ e $b > 0$, pelo Teorema 4.18, $a \cdot b > 0$.
- Se $a > 0$ e $-b > 0$, pelo Teorema 4.18, $-(a \cdot b) = a \cdot (-b) > 0$. Logo, $a \cdot b < 0$.
- Se $-a > 0$ e $-b > 0$, pelo Teorema 4.18, $a \cdot b = (-a) \cdot (-b) > 0$. Logo, $a \cdot b > 0$.
- Se $-a > 0$ e $b > 0$, pelo Teorema 4.18, $-(a \cdot b) = (-a) \cdot b > 0$. Logo, $a \cdot b < 0$.

Em qualquer caso, mostramos que $a \cdot b \neq 0$ em \mathbb{Z} . ■

Definição 4.8 Se $\langle A, +, \cdot \rangle$ é uma anel comutativo com identidade $1_A \neq 0_A$ tal que para $a, b \in A$, $a \cdot b = 0_A$, só se, $a = 0_A$ ou $b = 0_A$, então $\langle A, +, \cdot \rangle$ é chamado um *domínio integral*.

Como uma consequência imediata do Teorema 4.19 temos:

Teorema 4.20 [Teorema 2.17 em (COHEN; EHRLICH, 1963)] $\langle \mathbb{Z}, +, \cdot \rangle$ é um domínio integral.

A adição de um elemento, ou a multiplicação por um elemento positivo, não altera as desigualdades em \mathbb{Z} , assim como o cancelamento de termos em somas, ou de fatores positivos em produtos. Mais precisamente, temos:

Teorema 4.21 [Exercício 2.14 em (COHEN; EHRLICH, 1963)] Para $a, b \in \mathbb{Z}$, $a < b$ se, e só se,

- (1) $a + c < b + c$, para todo $c \in \mathbb{Z}$, e
- (2) $ac < bc$, para todo $c \in \mathbb{Z}^+$.

Demonstração.

1. Se $a < b$ em \mathbb{Z} então $b - a \in \mathbb{Z}^+$ e, como $(b + c) - (a + c) = b - a \in \mathbb{Z}^+$. Daí, $a + c < b + c$ em \mathbb{Z} . Reciprocamente, se $a + c < b + c$ em \mathbb{Z} então $b - a = (b + c) - (a + c) \in \mathbb{Z}^+$. Daí, $a < b$ em \mathbb{Z} .
2. Se $a < b$ em \mathbb{Z} e $c \in \mathbb{Z}^+$. Logo, $b - a \in \mathbb{Z}^+$ e pelo Teorema 4.18 $(b - a)c \in \mathbb{Z}^+$. Assim, pelo Teorema 4.11, tem-se

$$bc - ac = (b - a)c \in \mathbb{Z}^+.$$

Daí, $ac < bc$ em \mathbb{Z} . Reciprocamente, se $ac < bc$ em \mathbb{Z} . Pelo Teorema 4.14, ou $a = b$, ou $b < a$ ou $a < b$.

- Se $a = b$ então $0 = ac - bc \in \mathbb{Z}^+$ logo $0 < 0$ o que é um absurdo.
- Se $b < a$ então $a - b \in \mathbb{Z}^+$ e como $c \in \mathbb{Z}^+$, pelo Teorema 4.18, tem-se

$$ac - bc = (a - b)c \in \mathbb{Z}^+$$

logo $bc < ac$ o que contradiz a hipótese.

Portanto, $a < b$ em \mathbb{Z} . ■

Definição 4.9 Se $<$ denota uma relação de ordem em um domínio integral $\langle A, +, \cdot \rangle$ tal que

- (i) para $a < b$ em A , $a + c < b + c$, para todo $c \in A$, e
- (ii) para $a < b$ em A , $a \cdot c < b \cdot c$, para todo $c > 0_A$ em A ,

então o sistema $\langle A, +, \cdot, < \rangle$ é chamada um *domínio integral ordenado*.

Pelo Teorema 4.20 e o Teorema 4.21 temos

Teorema 4.22 [Teorema 2.18 em (COHEN; EHRLICH, 1963)] $\langle \mathbb{Z}, +, \cdot, < \rangle$ é um domínio integral ordenado.

Definição 4.10 Se $\langle A, +, \cdot \rangle$ é um domínio integral, então o subconjunto A^+ de A é chamado o *conjunto de elementos positivos* de A se:

- (i) $a + b \in A^+$, para todo $a, b \in A^+$,
- (ii) $a \cdot b \in A^+$, para todo $a, b \in A^+$,
- (iii) para cada $a \in A$, exatamente uma das seguintes é válido: $a \in A^+$, $a = 0_A$, $-a \in A^+$.

Teorema 4.23 [Teorema 2.19 em (COHEN; EHRLICH, 1963)] Se $\langle A, +, \cdot \rangle$ é um domínio integral e A^+ é um conjunto de elementos positivos de A , então

1. $T = \{(a, b) \in A \times A; b - a \in A^+\}$ é uma relação de ordem em A .
2. Se escrevemos $a < b$ (ou $b > a$) para $(a, b) \in T$, então $\langle A, +, \cdot, < \rangle$ é um domínio integral ordenado.
3. $A^+ = \{a; a > 0_A\}$.

Demonstração. Se $(a, b), (b, c) \in T$, então $b - a, c - b \in A^+$. Daí, pelo item (i) da Definição 4.10,

$$c - a = (c - b) + (b - a) \in A^+.$$

Portanto, $(a, c) \in T$. Logo, T é transitiva. Agora, para $a, b \in A$, pelo item (iii) da Definição 4.10, exatamente uma das

$$b - a \in A^+, \quad b - a = 0, \quad -(b - a) = a - b \in A^+$$

é válida. Portanto, T é tricotomia. Segue-se que T é uma relação de ordem em A .

Se $(a, b) \in T$, então, para qualquer $c \in A$,

$$(b + c) - (a + c) = b - a \in A^+.$$

Daí, $(a + c, b + c) \in T$. Além disso, se $(a, b) \in T$ e $c \in A^+$, então, pelo item (ii) da Definição 4.10,

$$bc - ac = (b - a)c \in A^+.$$

Daí, $(ac, bc) \in T$.

Assim, de $a < b$ e $c \in A^+$, segue-se $a + c < b + c$, e de $a < b$ e $c \in A^+$ segue $ac < bc$, de modo que $\langle A, +, \cdot, < \rangle$ é um domínio integral ordenado.

Finalmente, se $a \in A^+$ temos que $a - 0_A = a \in A^+$, logo $(0_A, a) \in T$, daí $0_A < a$.

Reciprocamente, se $a > 0_A$ então $(0_A, a) \in T$, daí $a = a - 0_A \in A^+$. ■

4.5 Imersões

Os elementos $C_{(S(n),1)} \in \mathbb{Z}^+$ se comportam, em relação a $+_{\mathbb{Z}}, \cdot_{\mathbb{Z}}, <_{\mathbb{Z}}$, exatamente como os números naturais n se comportam, em relação a $+, \cdot, <$, no sentido do seguinte teorema:

Teorema 4.24 [Teorema 2.20 em (COHEN; EHRLICH, 1963)] A aplicação $E := E_{\mathbb{N}}^{\mathbb{Z}}$ de \mathbb{N} em \mathbb{Z} definido por $E(n) = C_{(S(n),1)}$ para $n \in \mathbb{N}$ é uma função injetiva, com imagem \mathbb{Z}^+ , tal que

- (1) $E(m + n) = E(m) +_{\mathbb{Z}} E(n)$,
- (2) $E(m \cdot n) = E(m) \cdot_{\mathbb{Z}} E(n)$,
- (3) $E(m) <_{\mathbb{Z}} E(n)$ se, e só se, $m < n$ em \mathbb{N} .

Demonstração. Se $m, n \in \mathbb{N}$, então

$$\begin{aligned} E(m) +_{\mathbb{Z}} E(n) &= C_{(S(m),1)} +_{\mathbb{Z}} C_{(S(n),1)} = C_{(S(m)+S(n),1+1)} \\ &= C_{(S(mn),1)} = E(m + n) \end{aligned}$$

e (1) é provado. Também,

$$\begin{aligned} E(m) \cdot_{\mathbb{Z}} E(n) &= C_{(S(m),1)} \cdot_{\mathbb{Z}} C_{(S(n),1)} \\ &= C_{(S(m) \cdot S(n)+1, S(m)+S(n))} \\ &= C_{(mn+m+n+1+1, m+n+1+1)} = C_{(S(mn),1)} \\ &= E(m \cdot n) \end{aligned}$$

e (2) é provado. Finalmente,

$$E(m) = C_{(S(m),1)} <_{\mathbb{Z}} C_{(S(n),1)} = E(n)$$

se, e só se,

$$C_{(S(n),1)} - C_{(S(m),1)} = C_{(S(n),1)} + C_{(1,S(m))} = C_{(S(S(n)), S(S(m)))}$$

é positivo. Daí, $E(m) <_{\mathbb{Z}} E(n)$ se, e só se, $S(S(m)) < S(S(n))$ em \mathbb{N} se, e só se, $m < n$ em \mathbb{N} . Portanto, (3) é provado. ■

Corolário 3 [Exercício 2.22 em (COHEN; EHRLICH, 1963)] $E_{\mathbb{N}}^{\mathbb{Z}}(1) = 1_{\mathbb{Z}}$.

Demonstração. Pelo item (2) do Teorema 4.24 temos que $E(m) = E(m \cdot 1) = E(m) \cdot_{\mathbb{Z}} E(1)$ e como $E(m) \in \mathbb{Z}^+$ pelo item (2) do Teorema 4.21 tem-se $E(1) = 1_{\mathbb{Z}}$.

Teorema 4.25 [Exercício 2.17 em (COHEN; EHRLICH, 1963)] Se $\langle A, +, \cdot, < \rangle$ é um domínio integral ordenado, então o conjunto $A^+ = \{a \in A; a > 0_A\}$ é um conjunto dos elementos positivos para A e a relação de ordem $T = \{(a, b); b - a \in A^+\}$ é a ordem dada em $\langle A, +, \cdot, < \rangle$.

Demonstração. Vejamos que A^+ é um conjunto de elementos positivos. Se $a, b \in A^+$ então $a > 0_A$ e $b > 0_A$. Como $\langle A, +, \cdot, < \rangle$ é um domínio integral ordenado, tem-se

$$0_A < b = 0_A + b < a + b.$$

Daí, $a + b \in A^+$. Também,

$$0_A = 0_A \cdot b < a \cdot b.$$

Logo, $a \cdot b \in A^+$. Agora, se $a \in A$, como $<$ é uma relação de ordem em A ele verifica a tricotomia, logo exatamente um das seguintes $a = 0_A$, $a > 0_A$, $a < 0_A$ é válida. Equivalentemente, temos que exatamente um das seguintes $a = 0_A$, $a > 0_A$, $a + (-a) < 0_A + (-a) = -a$ é válida. Portanto, exatamente um das seguintes $a = 0_A$, $a \in A^+$, $-a \in A^+$ é válida. Concluimos que A^+ é um conjunto de elemento positivos de A e pelo Teorema 4.23 segue-se a última parte. ■

Teorema 4.26 [Exercício 2.18 em (COHEN; EHRLICH, 1963)]

1. Se $\langle a, +, \cdot, < \rangle$ é um domínio integral ordenado, então para $a \neq 0_A$, $a \cdot a$ é positivo em A , a identidade multiplicativa 1_A é positivo.
2. No domínio ordenado \mathbb{Z} de inteiros, $ab = 1$ se, e só se, $a = b = \pm 1$ (isto é, $a = b = 1$ ou $a = b = -1$).

Demonstração.

1. Se $a \neq 0_A$ logo pelo Teorema 4.25, ou $a \in A^+$ ou $-a \in A^+$.

- Se $a \in A^+$ logo $a \cdot a \in A^+$.
- Se $-a \in A^+$ logo, $a \cdot a = (-a) \cdot (-a) \in A^+$.

Em qualquer caso, $a \cdot a \in A^+$, isto é, $a \cdot a$ é positivo. Em particular, $1_A = 1_A \cdot 1_A \in A^+$. Logo, 1_A é positivo.

2. Se $ab = 1$ em \mathbb{Z} . Então $a, b > 0$ ou $a, b < 0$. Suponha que $a \neq b$.

- (i) Se $0 < a < b$ então $0 < a \cdot a < ab = 1$. Como $a \cdot a \in \mathbb{Z}^+$ e como, pelo Teorema 4.24, $E : \mathbb{N} \rightarrow \mathbb{Z}^+$ é uma bijeção temos que existe $n \in \mathbb{N}$ tal que $E(n) = a \cdot a$ e como $E(1) = 1$ temos que $E(n) < E(1)$ logo, pelo item (3) do Teorema 4.24, $n < 1$ em \mathbb{N} o que é absurdo.
- (ii) Se $0 < b < a$ então $0 < b \cdot b < ab = 1$. Como $b \cdot b \in \mathbb{Z}^+$ e como, pelo Teorema 4.24, $E : \mathbb{N} \rightarrow \mathbb{Z}^+$ é uma bijeção temos que existe $m \in \mathbb{N}$ tal que $E(m) = b \cdot b$ e como $E(1) = 1$ temos que $E(m) < E(1)$ logo, pelo item (3) do Teorema 4.24, $m < 1$ em \mathbb{N} o que é absurdo.
- (iii) Se $a < b < 0$ então $0 < -b < -a$ logo $0 < b \cdot b = (-b)(-b) < (-a)(-b) = ab = 1$. Analogamente, como no subitem (ii), chegamos a um absurdo.
- (iv) Se $b < a < 0$ então $0 < -a < -b$ logo $0 < a \cdot a = (-a)(-a) < (-a)(-b) = ab = 1$. Analogamente, como no subitem (i), chegamos a um absurdo.

Em qualquer caso, $a = b$. Daí, temos que $a \cdot a = 1$, assim $(a-1)(a+1) = a \cdot a - 1 = 0$ e como, pelo Teorema 4.20, $\langle \mathbb{Z}, +, \cdot \rangle$ é um domínio integral, temos que $a - 1 = 0$ ou $a + 1 = 0$, logo $a = b = \pm 1$.

Reciprocamente, se $a = b = \pm 1$ temos

$$a \cdot b = (\pm 1) \cdot (\pm 1) = 1 \cdot 1 = 1.$$

Portanto, $a \cdot b = 1$. ■

4.6 Isomorfismo

Definição 4.11

- (1) Se \circ é uma operação binária em um conjunto A , e \circ' é uma operação binária em um conjunto A' então uma função injetiva (bijetiva) F de A em A' é chamada um (\circ, \circ') –*isomorfismo injetivo (isomorfismo bijetivo)* de A em A' se,

$$F(a \circ b) = F(a) \circ' F(b), \text{ para todo } a, b \in A.$$

- (2) Se T é uma relação binária em A , e T' é uma relação binária em A' , então uma função injetiva F de A em A' (bijetiva) é chamada um (T, T') –*isomorfismo injetivo* de A em A' (*isomorfismo bijetivo*) se para $a, b \in A$,

$$aTb \text{ é verdade se, e só se, } F(a)T'F(b) \text{ é verdade.}$$

Observamos que a condição em (1) também pode ser escrita como

$$F(\circ(a, b)) = \circ'(F(a), F(b)).$$

Se as relações T e T' em (2) são funções de A em A e A' em A' , respectivamente, então a condição em (2) pode ser escrita

$$F(T(a)) = T'(F(a)), \text{ para cada } a \in A.$$

De acordo com a Definição 4.11, a função $E_{\mathbb{N}}^{\mathbb{Z}}$ do Teorema 4.24 é um $(+, +_{\mathbb{Z}})$ –, $(\cdot, \cdot_{\mathbb{Z}})$ – e $(<, <_{\mathbb{Z}})$ –isomorfismos injetivos de \mathbb{N} em \mathbb{Z} (bijetivos de \mathbb{N} em \mathbb{Z}^+). Diremos simplesmente que E é um isomorfismo injetivo de \mathbb{N} em \mathbb{Z} preservando adição, multiplicação e ordem, ou que \mathbb{N} é isomorfa a \mathbb{Z}^+ em relação à adição, multiplicação e ordem.

Observação 4.7 Tendo em vista o isomorfismo injetivo $E_{\mathbb{N}}^{\mathbb{Z}}$ e o Corolário 3, usamos alternadamente os símbolos

$$C_{(S(n),1)} \text{ e } n,$$

$$1_{\mathbb{Z}} \text{ e } 1.$$

Definição 4.12 Se existe um isomorfismo injetivo de A em A' em relação a um par de operações ou relações (α, α') , então A' é chamada uma *extensão* de A em relação a (α, α') . Se A' é uma extensão de A em relação a (α, α') , dizemos que A pode ser *isomorficamente imerso* em A' em relação a (α, α') .

Assim, \mathbb{Z} é uma extensão de \mathbb{N} em relação a $(+, +_{\mathbb{Z}})$, $(\cdot, \cdot_{\mathbb{Z}})$, e $(<, <_{\mathbb{Z}})$, ou seja, em relação à adição, multiplicação e ordem.

Neste capítulo construímos o conjunto \mathbb{Z} via classes de equivalências por pares, e observando uma imersão de \mathbb{N} em \mathbb{Z} . Para adição mostramos que \mathbb{Z} possui identidade e ela é única, sendo o número zero essa identidade, e, que para cada elemento em \mathbb{Z} há um inverso. Para a multiplicação em \mathbb{Z} também obtemos uma única identidade, sendo o número um. Para o próximo capítulo, faremos a construção do conjunto dos números racionais e são representados por \mathbb{Q} .

5 CONSTRUÇÃO DOS NÚMEROS RACIONAIS

Neste capítulo, construiremos o conjunto dos números racionais por classes de equivalência de elementos admissíveis em $\mathbb{Z} \times \mathbb{Z}$. Veremos que este conjunto é um corpo ordenado. A referência base utilizada é (COHEN; EHRLICH, 1963).

O conjunto $\mathbb{Z}^* = \mathbb{Z} - \{0\}$ forma um semigrupo sob a multiplicação. Este semigrupo não é um grupo, pois, pelo item (2) do Teorema 4.26, nenhum inteiro diferente de ± 1 tem um inverso multiplicativo relativo à identidade 1. Construiremos agora a partir de \mathbb{Z} um conjunto, \mathbb{Q} , cujos elementos chamamos de *números racionais*, e definimos em \mathbb{Q} uma adição ($+$ _{\mathbb{Q}}), uma multiplicação (\cdot _{\mathbb{Q}}) e uma ordem ($<$ _{\mathbb{Q}}), de tal maneira que o sistema $\langle \mathbb{Q}, +_{\mathbb{Q}}, \cdot_{\mathbb{Q}}, <_{\mathbb{Q}} \rangle$ reflete as propriedades familiares das frações. Este sistema será uma extensão de $\langle \mathbb{Z}, +_{\mathbb{Z}}, \cdot_{\mathbb{Z}}, <_{\mathbb{Z}} \rangle$ em relação à adição, multiplicação e ordem. Se excluirmos de \mathbb{Q} a identidade aditiva $0_{\mathbb{Q}}$, obtemos um conjunto \mathbb{Q}^* , que forma um grupo sob a multiplicação.

Nossa definição de números racionais será baseada em propriedades familiares das frações. Observamos que duas frações (por exemplo, $\frac{2}{4}$ e $\frac{-3}{6}$) são iguais quando seus *produtos cruzados* são iguais $2(-6) = (-3)4$. Definiremos um número racional como uma classe de equivalência de pares ordenados de inteiros, onde a relação de equivalência é dada pela igualdade de produtos cruzados.

Definição 5.1 Um par ordenado (a, b) de inteiros é chamado *admissível* se $b \neq 0$ em \mathbb{Z} . Denotemos $A = \{(a, b) \in \mathbb{Z} \times \mathbb{Z}; (a, b) \text{ é admissível}\}$.

Teorema 5.1 [Teorema 3.1 em (COHEN; EHRLICH, 1963)] Existe uma relação de equivalência R em A tal que $(a, b)R(c, d)$ sempre que $ad = bc$.

Demonstração. O conjunto $R = \{((a, b), (c, d)); ad = cb \text{ em } \mathbb{Z}\}$ é um subconjunto de $A \times A$. Pela Definição 2.6, R é uma relação binária em A . Desde que $ab = ab$, temos que $((a, b), (a, b)) \in R$, para todo $(a, b) \in A$. Daí a relação R é reflexiva. Se $((a, b), (c, d)) \in R$, então $ad = cb$, equivalentemente, $cb = ad$, logo $((c, d), (a, b)) \in R$. Assim, temos que R é simétrica. Finalmente se $((a, b), (c, d)) \in R$ e $((c, d), (e, f)) \in R$, então $ad = cb$ e $cf = ed$. Pelas propriedades da multiplicação em \mathbb{Z} ,

$$adf = cbf = cfb = edb \Rightarrow afd = ebd,$$

e, desde que $d \neq 0$, tem-se $af = eb$. Daí, $((a, b), (e, f)) \in R$. Daí, a relação R , é transitiva. Portanto, pela Definição 2.8, R é uma relação de equivalência em A . ■

Definição 5.2 Escrevemos $(a, b) \sim (c, d)$ para $((a, b), (c, d)) \in R$ e lemos \sim como é *equivalente* à. Para cada $(a, b) \in A$, a classe de equivalência $C_{(a,b)}$ é o conjunto de todos os $(c, d) \in A$ tal que $(c, d) \sim (a, b)$. Um *número racional* é uma classe de equivalência $C_{(a,b)}$. Escrevemos \mathbb{Q} para o conjunto de todos os números racionais e x, y, z, \dots para os elementos de \mathbb{Q} .

Se A e R são os conjuntos definidos no Teorema 5.1, então o conjunto quociente

$$\mathbb{Q} = A/R = \{C_{(a,b)}; (a, b) \in A\},$$

é o conjunto de todos os números racionais.

5.1 Adição e Multiplicação em \mathbb{Q} .

Nossas definições de adição e multiplicação em \mathbb{Q} espelham as propriedades familiares da adição e multiplicação de frações. A unicidade de somas e produtos será uma consequência do teorema a seguir:

Teorema 5.2 Se $(a, b) \sim (a', b')$ e $(c, d) \sim (c', d')$, então

1. $(ad + cb, bd) \sim (a'd' + c'b', b'd')$;
2. $(ac, bd) \sim (a'c', b'd')$.

Demonstração. Por hipótese, $ab' = a'b$ e $cd' = c'd$. Daí, temos, pelas propriedades da adição e multiplicação em \mathbb{Z} ,

$$\begin{aligned} (ad + cb)(b'd') &= (ad)(b'd') + (cb)(b'd') \\ &= (ab')(dd') + (cd')(bb') \\ &= (a'b)(dd') + (c'd)(bb') \\ &= (a'd')(bd) + (c'b')(bd) \\ &= (a'd' + c'b')(bd). \end{aligned}$$

Desde que $bd \neq 0$ e $b'd' \neq 0$, tem-se pela Definição 5.2 $(ad + cb, bd) \sim (a'd' + c'b', b'd')$.

Também,

$$(ac)(b'd') = (ab')(cd') = (a'b)(c'd) = (a'c')(bd),$$

e, desde que $bd \neq 0$ e $b'd' \neq 0$, assim temos $(ac, bd) \sim (a'c', b'd')$. ■

Teorema 5.3 [Teorema 3.3 em (COHEN; EHRLICH, 1963)] Existem operações binárias F e G tal que se $(a, b) \in x$ e $(c, d) \in y$ então

$$(1) F(x, y) = C_{(ad+cb, bd)},$$

$$(2) G(x, y) = C_{(ac, bd)}.$$

Demonstração. Os conjuntos

$$F = \{((x, y), C_{(ad+cb, bd)}); (a, b) \in x, (c, d) \in y; x, y \in \mathbb{Q}\}$$

e

$$G = \{((x, y), C_{(ac, bd)}); (a, b) \in x, (c, d) \in y; x, y \in \mathbb{Q}\}$$

são subconjuntos de $(\mathbb{Q} \times \mathbb{Q}) \times \mathbb{Q}$. Desde que (a, b) e (c, d) pertencem a A , $(ad + cb, bd)$ e (ac, bd) pertencem a A . Para cada $(x, y) \in \mathbb{Q} \times \mathbb{Q}$, existem $(a, b) \in x$, $(c, d) \in y$ e $z = C_{(ad+cb, bd)}$ tal que $((x, y), z) \in F$. Se $(a', b') \in x$, $(c', d') \in y$, e $z' = C_{(a'd'+c'b', b'd')}$, então, como $(a', b') \sim (a, b)$, $(c', d') \sim (c, d)$, e pelo Teorema 5.2, segue-se que $(ad + cb, bd) \sim (a'd' + c'b', b'd')$. Daí, pela Definição 5.2, $z' = z$. Consequentemente, F é uma função de $\mathbb{Q} \times \mathbb{Q}$ em \mathbb{Q} , e pela Definição 2.13, e pela Definição 2.17, F é uma operação binária em \mathbb{Q} .

Para cada $(x, y) \in \mathbb{Q} \times \mathbb{Q}$, existem $(a, b) \in x$, $(c, d) \in y$ e $z = C_{(ac, bd)}$, tal que $((x, y), z) \in G$. Se $(a', b') \in x$, $(c', d') \in y$ e $z' = C_{(a'c', b'd')}$, então $(a', b') \sim (a, b)$, $(c', d') \sim (c, d)$, e pelo Teorema 5.2, $(ac, bd) \sim (a'c', b'd')$. Daí, pela Definição 5.2, $z = z'$. Portanto G é uma função de $\mathbb{Q} \times \mathbb{Q}$ em \mathbb{Q} . Pela Definição 2.17, G é uma operação binária em \mathbb{Q} . ■

Definição 5.3 Referimos-nos as operações binárias F e G do Teorema 5.3, respectivamente, como adição e multiplicação em \mathbb{Q} , e escrevemos

$$x +_{\mathbb{Q}} y = F(x, y) \quad \text{e} \quad x \cdot_{\mathbb{Q}} y = G(x, y).$$

Observação 5.1 Omitimos o subscrito \mathbb{Q} e até mesmo \cdot , se o contexto deixar claro que as operações estão em \mathbb{Q} .

Teorema 5.4 [Teorema 3.4 em (COHEN; EHRLICH, 1963)] $\langle \mathbb{Q}, +_{\mathbb{Q}} \rangle$ é um grupo comutativo.

Demonstração.

1. Adição em \mathbb{Q} é comutativo.

Se $x, y \in \mathbb{Q}$, então $x = C_{(a,b)}$, $y = C_{(c,d)}$, para alguns (a, b) , (c, d) admissíveis. Pela Definição 5.3, pelo Teorema 5.3, e as propriedades de adição e multiplicação em \mathbb{Z} , tem-se

$$\begin{aligned} x +_{\mathbb{Q}} y = F(x, y) &= C_{(ad+cb, bd)} \\ &= C_{(cb+ad, db)} = F(y, x) = y +_{\mathbb{Q}} x. \end{aligned}$$

2. Adição em \mathbb{Q} é associativo.

Se $x, y, z \in \mathbb{Q}$, então $x = C_{(a,b)}$, $y = C_{(c,d)}$ e $z = C_{(e,f)}$ para alguns (a, b) , (c, d) e (e, f) admissíveis. Agora, pela Definição 5.3, pelo Teorema 5.3, e as propriedades de adição e multiplicação em \mathbb{Z} , temos

$$\left\{ \begin{array}{l} (ad + cb, bd) \in x +_{\mathbb{Q}} y, \\ ((ad + cb)f + e(bd), (bd)f) \in (x +_{\mathbb{Q}} y) +_{\mathbb{Q}} z, \end{array} \right. \quad (5.1)$$

$$\left\{ \begin{array}{l} (cf + ed, df) \in y +_{\mathbb{Q}} z, \\ (a(df) + (cf + ed)b, b(df)) \in x +_{\mathbb{Q}} (y +_{\mathbb{Q}} z). \end{array} \right. \quad (5.2)$$

Desde que, em \mathbb{Z} ,

$$(ad + cb)f + e(bd) = a(df) + (cf + ed)b \quad \text{e} \quad (bd)f = b(fd),$$

segue-se de (5.1) e (5.2) que as classes de equivalência $(x +_{\mathbb{Q}} y) +_{\mathbb{Q}} z$ e $x +_{\mathbb{Q}} (y +_{\mathbb{Q}} z)$ têm um elemento em comum. Daí,

$$x +_{\mathbb{Q}} (y +_{\mathbb{Q}} z) = (x +_{\mathbb{Q}} y) +_{\mathbb{Q}} z.$$

3. \mathbb{Q} contém uma única identidade para adição.

Se $x = C_{(a,b)}$ é qualquer elemento de \mathbb{Q} , então

$$x +_{\mathbb{Q}} C_{(0,1)} = C_{a \cdot 1 + 0 \cdot b, b \cdot 1} = C_{(a,b)} = x.$$

Portanto, $C_{(0,1)}$ é uma identidade para a adição. Pelo Teorema 3.10 há apenas uma identidade.

4. Todo elemento de \mathbb{Q} tem um único inverso em relação a adição.

Se $x = C_{(a,b)} \in \mathbb{Q}$ e $x' = C_{(-a,b)}$, então

$$x +_{\mathbb{Q}} x' = C_{(ab+(-a)b,b^2)} = C_{(0,b^2)} = C_{(0,1)},$$

desde que $(0, b^2) \sim (0, 1)$. Daí, x' é o único inverso para x . Pelo Teorema 4.7, x' é o único inverso. ■

Observação 5.2 Escrevemos $0_{\mathbb{Q}}$ para a identidade $C_{(0,1)}$, $-x$ para a inversa de x , e $x - y$ para o elemento z tal que $x = y + z$ em $\langle \mathbb{Q}, +_{\mathbb{Q}} \rangle$.

Teorema 5.5 [Teorema 3.5 em (COHEN; EHRLICH, 1963)] $\langle \mathbb{Q}, \cdot_{\mathbb{Q}} \rangle$ é um semigrupo comutativo com identidade.

Demonstração.

1. Multiplicação em \mathbb{Q} é associativa.

Se $x, y, z \in \mathbb{Q}$, então $x = C_{(a,b)}$, $y = C_{(c,d)}$, $z = C_{(e,f)}$ para alguns $a, b, c, d, e, f \in \mathbb{Z}$.

Pela Definição 5.3, Teorema 5.3, e pelas propriedades da multiplicação em \mathbb{Z} , tem-se

$$\begin{aligned} x \cdot_{\mathbb{Q}} (y \cdot_{\mathbb{Q}} z) &= C_{(a,b)} \cdot_{\mathbb{Q}} C_{(ce,df)} \\ &= C_{(a(ce),b(df))} \\ &= C_{((ac)e,(bd)f)} \\ &= C_{(ac,bd)} \cdot_{\mathbb{Q}} C_{(e,f)} \\ &= (x \cdot_{\mathbb{Q}} y) \cdot_{\mathbb{Q}} z. \end{aligned}$$

2. Multiplicação em \mathbb{Q} é comutativa.

Se $x, y \in \mathbb{Q}$, então $x = C_{(a,b)}$ e $y = C_{(c,d)}$ para alguns $a, b, c, d \in \mathbb{Z}$. Pela Definição 5.3, Teorema 5.3, e pelas propriedades da multiplicação em \mathbb{Z} , tem-se

$$\begin{aligned} x \cdot_{\mathbb{Q}} y &= G(x, y) = C_{(ac,bd)} \\ &= C_{(ca,db)} = G(y, x) \\ &= y \cdot_{\mathbb{Q}} x. \end{aligned}$$

3. \mathbb{Q} contém uma única identidade para a multiplicação.

Se $x = C_{(a,b)}$ é qualquer elemento de \mathbb{Q} , então

$$\begin{aligned} x \cdot_{\mathbb{Q}} C_{(1,1)} &= C_{(a,b)} \cdot_{\mathbb{Q}} C_{(1,1)} = C_{(a \cdot 1, b \cdot 1)} \\ &= C_{(a,b)} = x. \end{aligned}$$

Portanto, $\langle \mathbb{Q}, \cdot_{\mathbb{Q}} \rangle$ é um semigrupo com identidade. ■

Observação 5.3 Escrevemos $1_{\mathbb{Q}}$ para a identidade $C_{(1,1)}$.

Teorema 5.6 [Teorema 3.6 em (COHEN; EHRLICH, 1963)] $\langle \mathbb{Q}, +_{\mathbb{Q}}, \cdot_{\mathbb{Q}} \rangle$ é um anel comutativo com identidade.

Demonstração. Desde que $\langle \mathbb{Q}, +_{\mathbb{Q}} \rangle$ é um grupo comutativo e $\langle \mathbb{Q}, \cdot_{\mathbb{Q}} \rangle$ é um semigrupo comutativo com identidade, resta apenas mostrar que a multiplicação em \mathbb{Q} distribui sobre a adição.

Se $x = C_{(a,b)}$, $y = C_{(c,d)}$ e $z = C_{(e,f)}$, então

$$\begin{aligned} x \cdot_{\mathbb{Q}} y +_{\mathbb{Q}} x \cdot_{\mathbb{Q}} z &= C_{(ac,bd)} +_{\mathbb{Q}} C_{(ae,bf)} \\ &= C_{(acb+aebd,b^2df)} \\ &= C_{(acf+aed,bdf)} \\ &= C_{(a(cf+ed),b(df))} \\ &= C_{(a,b)} \cdot_{\mathbb{Q}} (C_{(c,d)} +_{\mathbb{Q}} C_{(e,f)}) \\ &= x \cdot_{\mathbb{Q}} (y +_{\mathbb{Q}} z) \end{aligned}$$

desde que $b \neq 0$ em \mathbb{Z} . ■

Teorema 5.7 [Teorema 3.7 em (COHEN; EHRLICH, 1963)] Todo elemento x em \mathbb{Q} diferente de 0 tem uma única inversa em relação à multiplicação.

Demonstração. Se $x = C_{(a,b)} \in \mathbb{Q}$ e $x \neq 0_{\mathbb{Q}} = C_{(0,1)}$, então $a \neq 0$, desde que $(0, b) \sim (0, 1)$, para todo $b \neq 0$ em \mathbb{Z} . Se $a \neq 0$, então $x' = C_{(b,a)} \in \mathbb{Q}$ e

$$x \cdot_{\mathbb{Q}} x' = G(x, x') = C_{(ab,ba)} = C_{(1,1)} = 1_{\mathbb{Q}}.$$

Daí, x' é uma inversa para x com respeito à multiplicação em \mathbb{Q} . Pelo Teorema 4.7 x' é o único inverso de x . ■

Corolário 4 [Corolário do Teorema 5.7 em (COHEN; EHRLICH, 1963)] O conjunto $\mathbb{Q}^* = \mathbb{Q} - \{0_{\mathbb{Q}}\}$ é um grupo em relação à multiplicação em \mathbb{Q} .

Definição 5.4 Um triplo $\langle A, +, \cdot \rangle$ é chamado um *corpo* se:

1. $\langle A, +, \cdot \rangle$ é um anel comutativo

2. $\langle A^*, \cdot^* \rangle$ é um grupo, onde $A^* = A - \{0_A\}$, onde 0_A denota a identidade da operação $+$, e, \cdot^* denota a restrição da operação \cdot para o conjunto A^* .

Assim, do Teorema 5.6 e do Corolário 4, obtemos o seguinte teorema.

Teorema 5.8 [Teorema 3.8 em (COHEN; EHRLICH, 1963)] $\langle \mathbb{Q}, +_{\mathbb{Q}}, \cdot_{\mathbb{Q}} \rangle$ é um corpo.

5.2 Ordem em \mathbb{Q}

Como no caso de \mathbb{Z} , começamos introduzindo um conjunto de elementos positivos.

Denotemos $\mathbb{Q}^+ = \{x; ab >_{\mathbb{Z}} 0_{\mathbb{Z}}; \text{ para algum } (a, b) \in x\}$.

Teorema 5.9 [Teorema 3.9 em (COHEN; EHRLICH, 1963)] Se $ab >_{\mathbb{Z}} 0_{\mathbb{Z}}$ e $(a, b) \sim (c, d)$, então $cd >_{\mathbb{Z}} 0_{\mathbb{Z}}$.

Demonstração. De $ad = cb$, temos $(cb)(ad) = (cb)(cb)$. Daí $(ab)(cd) = (cb)(cb)$. Pelo Teorema 4.26, $(cb)(cb) >_{\mathbb{Z}} 0_{\mathbb{Z}}$ em \mathbb{Z} . Mas então $(ab)(cd) >_{\mathbb{Z}} 0_{\mathbb{Z}}$ em \mathbb{Z} , e, desde que $ab >_{\mathbb{Z}} 0_{\mathbb{Z}}$ em \mathbb{Z} , tem-se $cd >_{\mathbb{Z}} 0_{\mathbb{Z}}$ em \mathbb{Z} (Teorema 4.21). ■

Corolário 5 [Corolário do Teorema 3.9 em (COHEN; EHRLICH, 1963)] $\mathbb{Q}^+ = \{x; ab >_{\mathbb{Z}} 0_{\mathbb{Z}}, \text{ para todo } (a, b) \in x\}$.

Teorema 5.10 [Teorema 3.10 em (COHEN; EHRLICH, 1963)] \mathbb{Q}^+ é um conjunto de elementos positivos em \mathbb{Q} .

Demonstração. Mostraremos que \mathbb{Q}^+ satisfaz (i), (ii) e (iii) da Definição 4.10.

Se $x, y \in \mathbb{Q}^+$, então $x = C_{(a,b)}$, $y = C_{(c,d)}$, onde $a, b, c, d \in \mathbb{Z}$, e

$$ab >_{\mathbb{Z}} 0_{\mathbb{Z}} \text{ e } cd >_{\mathbb{Z}} 0_{\mathbb{Z}}. \quad (5.3)$$

Daí,

$$x +_{\mathbb{Q}} y = C_{(a,b)} +_{\mathbb{Q}} C_{(c,d)} = C_{(ad+cb, bd)}.$$

Por (5.3), Teorema 4.18 e Teorema 4.15, tem-se

$$(ad + cb)bd = (ab)(dd) + (cd)(bb) >_{\mathbb{Z}} 0_{\mathbb{Z}}.$$

Assim, $x +_{\mathbb{Q}} y \in \mathbb{Q}^+$, e por (i) da Definição 4.10 é satisfeita.

Também,

$$x \cdot_{\mathbb{Q}} y = C_{(a,b)} \cdot_{\mathbb{Q}} C_{(c,d)} = C_{(ac,bd)},$$

e por (5.3) tem-se

$$(ac)(bd) = (ab)(cd) >_{\mathbb{Z}} 0_{\mathbb{Z}},$$

de modo que $x \cdot_{\mathbb{Q}} y \in \mathbb{Q}^+$, assim (ii) da Definição 4.10 é satisfeita.

Finalmente, se $x = C_{(a,b)}$, então, pela propriedade da tricotomia da ordem em \mathbb{Z} , exatamente um dos

$$ab >_{\mathbb{Z}} 0_{\mathbb{Z}}, \quad ab = 0_{\mathbb{Z}}, \quad -ab >_{\mathbb{Z}} 0_{\mathbb{Z}}$$

deve ser válido. Mas, pelo Teorema 5.9

$$ab >_{\mathbb{Z}} 0_{\mathbb{Z}} \text{ se, e só se, } x \in \mathbb{Q}^+$$

$$(-a)b = -ab >_{\mathbb{Z}} 0_{\mathbb{Z}} \text{ se, e só se, } C_{(-a,b)} = -x \in \mathbb{Q}^+$$

e, desde que $b \neq 0_{\mathbb{Z}}$ e \mathbb{Z} é um domínio integral

$$ab = 0_{\mathbb{Z}} \text{ se, e só se, } a = 0_{\mathbb{Z}}, \text{ e } x = C_{(0,b)} = 0_{\mathbb{Q}}.$$

Portanto, \mathbb{Q}^+ satisfaz (iii) da Definição 4.10. ■

Pelo item 1 do Teorema 4.23, temos:

Teorema 5.11 [Teorema 3.11 em (COHEN; EHRLICH, 1963)] O conjunto $T = \{(x, y); y - x \in \mathbb{Q}^+\}$ é uma relação de ordem em \mathbb{Q} .

Observação 5.4 Escrevemos $x <_{\mathbb{Q}} y$ (ou $y >_{\mathbb{Q}} x$) se $(x, y) \in T$. Usualmente omitimos o subscrito \mathbb{Q} .

Pelo item 2 do Teorema 4.23, tem-se:

Teorema 5.12 [Teorema 3.12 em (COHEN; EHRLICH, 1963)] $\langle \mathbb{Q}, +_{\mathbb{Q}}, \cdot_{\mathbb{Q}}, <_{\mathbb{Q}} \rangle$ é um domínio integral ordenado.

Observação 5.5 Pelo Teorema 5.12 temos que $\langle \mathbb{Q}, +_{\mathbb{Q}}, \cdot_{\mathbb{Q}}, <_{\mathbb{Q}} \rangle$ é um domínio integral ordenado e pela Definição 4.9, temos que

- (i) para $x < y$ em \mathbb{Q} então $x + z < y + z$ para todo $z \in \mathbb{Q}$ (*monotonicidade da adição em \mathbb{Q}*), e
- (ii) para $x < y$ em \mathbb{Q} então $x \cdot z < y \cdot z$ para todo $z \in \mathbb{Q}^+$ (*monotonicidade da multiplicação em \mathbb{Q}*).

Definição 5.5 Se $\langle A, +, \cdot, < \rangle$ é um domínio integral ordenado tal que $\langle A, +, \cdot \rangle$ é um corpo, então $\langle A, +, \cdot, < \rangle$ é chamado de *corpo ordenado*.

5.3 Imersões

Mostraremos agora que o corpo ordenado $\langle \mathbb{Q}, +_{\mathbb{Q}}, \cdot_{\mathbb{Q}}, <_{\mathbb{Q}} \rangle$ é uma extensão do domínio integral ordenado $\langle \mathbb{Z}, +_{\mathbb{Z}}, \cdot_{\mathbb{Z}}, <_{\mathbb{Z}} \rangle$.

Teorema 5.13 [Teorema 3.13 em (COHEN; EHRLICH, 1963)] A aplicação $E = E_{\mathbb{Z}}^{\mathbb{Q}}$ de \mathbb{Z} em \mathbb{Q} tal que, para cada $a \in \mathbb{Z}$, $E(a) = C_{(a,1)}$, é um isomorfismo injetivo de \mathbb{Z} em \mathbb{Q} preservando a adição, multiplicação, e ordem.

Demonstração. Vejamos que E é uma função injetiva de \mathbb{Z} em \mathbb{Q} . De fato, se $E(a) = E(b)$ com $a, b \in \mathbb{Z}$. Então, $C_{(a,1)} = C_{(b,1)}$, daí, $(a, 1) \sim (b, 1)$, logo $a \cdot 1 = b \cdot 1$, assim $a = b$.

Para $a, b \in \mathbb{Z}$,

$$E(a + b) = C_{(a+b,1)} = C_{(a,1)} + C_{(b,1)} = E(a) + E(b).$$

Portanto, E preserva a adição.

Para $a, b \in \mathbb{Z}$,

$$E(ab) = C_{(ab,1)} = C_{(a,1)} \cdot C_{(b,1)} = E(a) \cdot E(b).$$

Portanto, E preserva a multiplicação.

Para $a, b \in \mathbb{Z}$, $a <_{\mathbb{Z}} b$ se, e só se, $b - a \in \mathbb{Z}^+$, isto é, se, e só se,

$$C_{(b-a,1)} = C_{(b,1)} - C_{(a,1)} = E(b) - E(a) \in \mathbb{Q}^+,$$

se, e só se, $E(a) <_{\mathbb{Q}} E(b)$. Portanto, E preserva a ordem. ■

Observação 5.6 Tendo em vista os isomorfismos imersos $E_{\mathbb{N}}^{\mathbb{Z}}$ e $E_{\mathbb{Z}}^{\mathbb{Q}}$. Usaremos a partir de agora a mesma notação para elementos de \mathbb{Z} e suas imagens em \mathbb{Q} . Como usamos

anteriormente n para denotar $E_{\mathbb{N}}^{\mathbb{Z}}(n) = C_{(S(n),1)}$ em \mathbb{Z} , agora usaremos n para denotar $E_{\mathbb{Z}}^{\mathbb{Q}}(E_{\mathbb{N}}^{\mathbb{Z}}(n)) = C_{(n,1)}$ em \mathbb{Q} . Notamos que $E_{\mathbb{Z}}^{\mathbb{Q}}(E_{\mathbb{N}}^{\mathbb{Z}}(1)) = 1_{\mathbb{Q}}$, e $E_{\mathbb{Z}}^{\mathbb{Q}}(0) = 0_{\mathbb{Q}}$, de modo que estamos justificados em escrever 1 e 0 para $1_{\mathbb{Q}}$ e $0_{\mathbb{Q}}$, respectivamente. Finalmente, como para $h \in \mathbb{Z}$ e $k \neq 0$ em \mathbb{Z} ,

$$C_{(h,k)} = \frac{C_{(h,1)}}{C_{(k,1)}} = \frac{E_{\mathbb{Z}}^{\mathbb{Q}}(h)}{E_{\mathbb{Z}}^{\mathbb{Q}}(k)},$$

escrevemos $\frac{h}{k}$ para o número racional $C_{(h,k)}$. Também, usamos \mathbb{N} e \mathbb{Z} para designar, respectivamente, as imagens de \mathbb{N} e \mathbb{Z} em \mathbb{Q} .

Neste capítulo fizemos a construção do conjunto dos números racionais por meio das classes de equivalências de pares ordenados de números inteiros e mostramos que as operações de adição e multiplicação são bem consistentes, possuindo as propriedades associativas, comutativas e distributiva com os números inteiros. Notamos que ainda não temos um conjunto completo dos números, e para o último capítulo, vamos construir o conjunto dos números reais e será denotado por \mathbb{R} , faremos essa construção via cortes de Dedekind.

6 CONSTRUÇÃO DOS NÚMEROS REAIS

Neste capítulo, construiremos o conjunto dos números reais por meio dos cortes de Dedekind tomando como base o conjunto dos números racionais. Mostraremos que o conjunto dos cortes de Dedekind é um corpo ordenado, mais ainda, ele é completo, isto é, verifica o chamado *axioma do supremo* que afirma que todo subconjunto não vazio e limitado superiormente tem supremo. A principal referência utilizada foi (MOREIRA; CABRAL, 2021).

6.1 Cortes de Dedekind

Um corte de Dedekind em um conjunto ordenado consiste em dividir esse conjunto em duas partes, de tal forma que todas as entradas na primeira parte são menores do que todas as entradas na segunda parte. Essencialmente, o corte divide o conjunto em duas metades, uma que contém todos os elementos menores que um certo número e outra que contém todos os elementos maiores ou iguais a esse número.

No contexto dos números reais, os cortes de Dedekind são usados para definir os mesmos como o conjunto de todos os cortes de Dedekind nos números racionais. Cada número real é então definido como um conjunto de cortes de Dedekind.

Definição 6.1 Dizemos que $A \subset \mathbb{Q}$ é um *corte* se valem as seguintes propriedades:

- (i) $A \neq \emptyset$ e $A \neq \mathbb{Q}$.
- (ii) Se $p \in A$, $q \in \mathbb{Q}$ e $q < p$, então $q \in A$.
- (iii) Para todo $p \in A$, existe $q \in A$ tal que $p < q$.

Denotaremos o conjunto de todos os cortes por Ω .

Exemplo 6.1 Seja $r \in \mathbb{Q}$. O conjunto $Z(r) = \{p \in \mathbb{Q}; p < r\}$ é um corte.

Primeiramente vamos mostrar (i) da Definição 6.1: $Z(r) \neq \emptyset$ e $Z(r) \neq \mathbb{Q}$.

De fato, basta observar que $r - 1 \in Z(r)$ e $r + 1 \notin Z(r)$.

Agora vamos mostrar (ii) da Definição 6.1: Se $p \in Z(r)$, $q \in \mathbb{Q}$ e $q < p$, então $q \in Z(r)$. De fato, como $p \in Z(r)$ então $p < r$ e como $q < p$ por transitividade temos que $q < r$ com $q \in \mathbb{Q}$. Portanto, $q \in Z(r)$.

Finalmente, vamos mostrar (iii) da Definição 6.1: Se $p \in Z(r)$, então existe $q \in Z(r)$ tal que $p < q$. De fato, como $p \in Z(r)$ então $p < r$. Desde que $p, r \in \mathbb{Q}$, tomando $q = \frac{p+r}{2} \in \mathbb{Q}$, temos que $p < q < r$. Logo, $q \in Z(r)$ com $p < q$.

Graças ao Exemplo 6.1, definimos uma função $Z : \mathbb{Q} \rightarrow \Omega$ que associa a cada $r \in \mathbb{Q}$ o corte $Z(r)$.

Definição 6.2 Os cortes da forma $Z(r) = \{p \in \mathbb{Q}; p < r\}$, com $r \in \mathbb{Q}$, são ditos **cortes racionais**.

Teorema 6.1 [Teorema 3.3 em (MOREIRA; CABRAL, 2021)] Sejam $A, B \in \Omega$. Temos $A \subset B$ ou $B \subset A$.

Demonstração. Se $A = B$, então não temos nada a mostrar. Suponhamos, então, $A \neq B$. Assim temos, $A \not\subset B$ ou $B \not\subset A$.

- Se $A \not\subset B$, isto é, existe $q \in A$ tal que $q \notin B$. Vamos mostrar neste caso que $B \subset A$. De fato, seja $r \in B$. Suponha $q \leq r$. Se $q = r \in B$, absurdo, pois $q \notin B$. Logo, $q < r$. Como B é corte e $r \in B$, pelo item (ii) da Definição 6.1, $q \in B$, o que é um absurdo, pois $q \notin B$. Concluimos, $r < q$. Agora, como A é corte e $q \in A$, pelo item (ii) da Definição 6.1, $r \in A$. Portanto, $B \subset A$.
- Se $B \not\subset A$, isto é, existe $p \in B$ tal que $p \notin A$. Analogamente ao caso anterior vamos mostrar que $A \subset B$. De fato, seja $s \in A$. Suponha $p \leq s$. Se $p = s \in A$, absurdo, pois $p \notin A$. Logo, $p < s$. Como A é corte e $s \in A$, pelo item (ii) da Definição 6.1, $p \in A$, o que é um absurdo, pois $p \notin A$. Concluimos, $s < p$. Agora, como B é corte e $p \in B$, pelo item (ii) da Definição 6.1, $s \in B$. Portanto, $A \subset B$. ■

Seja $X \subset \mathbb{Q}$. Denotaremos $X^c = \mathbb{Q} - X$ chamado de *complementar* de X em relação a \mathbb{Q} .

Proposição 6.1 [Proposição 3.4 em (MOREIRA; CABRAL, 2021)] Seja $A, B \in \Omega$. O conjunto

$$C = \{r \in \mathbb{Q}; r = p + q \text{ com } p \in A \text{ e } q \in B\}$$

é corte.

Demonstração. Primeiro vamos mostrar (i) da Definição 6.1: $C \neq \emptyset$ e $C^{\complement} \neq \emptyset$ (equivalentemente, $C \neq \mathbb{Q}$). Como A e B são cortes, por (i) da Definição 6.1, temos que $A \neq \emptyset$ e $B \neq \emptyset$, logo existem $p \in A$ e $q \in B$. Seja $r = p + q$, como $p, q \in \mathbb{Q}$ tem-se $r = p + q \in \mathbb{Q}$. Portanto, $r \in C$, assim $C \neq \emptyset$. Também, como A e B são cortes, por (i) da Definição 6.1, temos que $A^{\complement} \neq \emptyset$ e $B^{\complement} \neq \emptyset$, logo existem $p' \in A^{\complement}$ e $q' \in B^{\complement}$.

Afirmção 6.1 $p' + q' \in C^{\complement}$.

De fato, suponha por absurdo que $p' + q' \in C$, então existem $p \in A$ e $q \in B$ tal que

$$p' + q' = p + q. \quad (6.1)$$

Se $p' = p \in A$, absurdo pois, $p' \in A^{\complement}$. Se $p' < p$, como A é corte e $p \in A$, por (ii) da Definição 6.1, temos que $p' \in A$, o que é absurdo, pois $p' \in A^{\complement}$. Portanto,

$$p < p'. \quad (6.2)$$

Se $q' = q \in B$, absurdo pois $q' \in B^{\complement}$. Se $q' < q$, como B é corte e $q \in B$, logo $q' \in B$, o que é absurdo, pois $q' \in B^{\complement}$. Portanto,

$$q < q'. \quad (6.3)$$

De (6.2) e (6.3), e pela monotonicidade da adição em \mathbb{Q} , temos que $p + q < p' + q'$, o que é absurdo por (6.1). Concluimos que $p' + q' \in C^{\complement}$.

Assim, pela Afirmção 6.1, $C^{\complement} \neq \emptyset$.

Vamos mostrar agora (ii) da Definição 6.1: Se $r \in C$ e $s \in \mathbb{Q}$ com $s < r$, então $s \in C$.

De fato, como $r \in C$, existem $p \in A$ e $q \in B$ tal que $r = p + q$. Daí, $s < p + q$ então $s - q < p$. Agora, como $s - q \in \mathbb{Q}$, $p \in A$ e A é corte, por (ii) da Definição 6.1, $s - q \in A$.

Reescrevendo, $s = (s - q) + q$, com $s - q \in A$ e $q \in B$, temos que $s \in C$.

Agora, mostraremos (iii) da Definição 6.1: Se $t \in C$, então existe $r \in C$ tal que $t < r$.

De fato, como $t \in C$ existem $p \in A$ e $q \in B$ tal que $t = p + q$. Como A é corte e $p \in A$, por (iii) da Definição 6.1, existe $\alpha \in A$ tal que

$$p < \alpha. \quad (6.4)$$

Também, como B é corte e $q \in B$, por (iii) da Definição, existe $\beta \in B$ tal que

$$q < \beta. \quad (6.5)$$

De (6.4) e (6.5), e usando monotonia da adição em \mathbb{Q} , temos que $t = p + q < \alpha + \beta$. Seja $r = \alpha + \beta$, como $\alpha \in A$ e $\beta \in B$, tem-se que $r \in C$ com $t < r$.

Finalmente, concluímos que C é um corte. ■

Definição 6.3 Sejam $A, B \in \Omega$. O corte C dado na Proposição 6.1, denotado por $A \oplus B$, é chamado de *soma* ou *adição* de A e B .

Observação 6.1 Se $A, B \in \Omega$ são tais que $Z(0) \subset A \cap B$, então $Z(0) \subset A \oplus B$. De fato, se $r \in Z(0)$ logo $r < 0$ em \mathbb{Q} assim $\frac{r}{2} < 0$ em \mathbb{Q} daí $\frac{r}{2} \in Z(0) \subset A \cap B$. Agora, note que

$$r = \underbrace{\frac{r}{2}}_{\in A} + \underbrace{\frac{r}{2}}_{\in B}.$$

Portanto, $r \in A \oplus B$. Concluímos, $Z(0) \subset A \oplus B$.

Assim temos definida uma operação de adição entre cortes. Mostraremos a seguir que esta operação satisfaz algumas das propriedades da adição em um corpo.

Teorema 6.2 [Teorema 3.6 em (MOREIRA; CABRAL, 2021)] Sejam $A, B, C \in \Omega$. Temos que:

- (1) $A \oplus B = B \oplus A$;
- (2) $(A \oplus B) \oplus C = A \oplus (B \oplus C)$;
- (3) $A \oplus Z(0) = A$.

Demonstração. As demonstrações serão realizadas por dupla inclusão.

- (1) Seja $r \in A \oplus B$. Logo, existem $p \in A$ e $q \in B$ tal que $r = p + q$. Agora, pela comutatividade da soma em \mathbb{Q} , temos que $r = q + p$, com $q \in B$ e $p \in A$, assim $r \in B \oplus A$. Portanto,

$$A \oplus B \subset B \oplus A. \quad (6.6)$$

Analogamente, seja $r \in B \oplus A$. Logo, existem $q \in B$ e $p \in A$ tal que $r = q + p$. Pela comutatividade de soma em \mathbb{Q} , tem-se que $r = p + q$, com $p \in A$ e $q \in B$, daí $r \in A \oplus B$. Concluímos que

$$B \oplus A \subset A \oplus B. \quad (6.7)$$

De (6.6) e (6.7), segue-se $A \oplus B = B \oplus A$.

(2) Seja $r \in (A \oplus B) \oplus C$. Daí, existem $p \in A$, $q \in B$ e $t \in C$ tal que $r = (p + q) + t$. Pela associatividade da soma em \mathbb{Q} , temos $r = p + (q + t)$. Assim, $r \in A \oplus (B \oplus C)$. Portanto,

$$(A \oplus B) \oplus C \subset A \oplus (B \oplus C). \quad (6.8)$$

Seja $r \in A \oplus (B \oplus C)$. Logo, existem $p \in A$, $q \in B$ e $t \in C$ tal que $r = p + (q + t)$. Pela associatividade da soma em \mathbb{Q} , temos $r = (p + q) + t$. Daí, $r \in (A \oplus B) \oplus C$. Concluimos que

$$A \oplus (B \oplus C) \subset (A \oplus B) \oplus C. \quad (6.9)$$

De (6.8) e (6.9), segue-se $(A \oplus B) \oplus C = A \oplus (B \oplus C)$.

(3) Seja $r \in A \oplus Z(0)$. Logo, existem $p \in A$ e $q \in Z(0)$ tal que $r = p + q$. Como $q \in Z(0)$ tem-se $q < 0$ em \mathbb{Q} . Pela monotonicidade da adição em \mathbb{Q} , $r = p + q < p + 0 = p$. Como A é corte e $p \in A$, por (ii) da Definição 6.1, $r \in A$. Assim, concluimos que

$$A \oplus Z(0) \subset A. \quad (6.10)$$

Reciprocamente, seja $r \in A$. Como A é corte e $r \in A$, por (iii) da Definição 6.1, existe $p \in A$ tal que $r < p$ em \mathbb{Q} . Logo, $r - p < 0$ em \mathbb{Q} . Assim, $r - p \in Z(0)$. Observe que, pela comutatividade da adição em \mathbb{Q} , temos

$$r = (r - p) + p = \underbrace{p}_{\in A} + \underbrace{(r - p)}_{\in Z(0)}.$$

Daí, $r \in A \oplus Z(0)$. Logo,

$$A \subset A \oplus Z(0). \quad (6.11)$$

Portanto, de (6.10) e (6.11), obtemos $A \oplus Z(0) = A$. ■

Proposição 6.2 [Proposição 3.7 em (MOREIRA; CABRAL, 2021)] Seja $A \in \Omega$. O conjunto

$$B = \{p \in \mathbb{Q}; -p \in A^{\complement} \text{ e existe } q \in A^{\complement} \text{ tal que } q < -p\}$$

é corte.

Demonstração. Vamos mostrar (i) da Definição 6.1: $B \neq \emptyset$ e $B^{\complement} \neq \emptyset$. De fato, como A é corte, por (i) da Definição 6.1, $A^{\complement} \neq \emptyset$, logo existe $q \in A^{\complement}$.

Afirmção 6.2 $-(q + 1) \in B$.

De fato, note que $q + 1 \in A^c$, pois senão $q + 1 \in A$ e como $q < q + 1$ e A é corte, por (ii) da Definição 6.1, $q \in A$, o que contradiz $q \in A^c$. Logo, $-(-(q + 1)) = q + 1 \in A^c$ e existe $q \in A^c$ tal que $q < q + 1 = -(-(q + 1))$. Portanto, por definição de B , $-(q + 1) \in B$.

Também, como A é corte, por (i) da Definição 6.1, $A \neq \emptyset$, daí existe $p \in A$.

Afirmção 6.3 $-p \in B^c$.

De fato, se $-p \notin B^c$, então $-p \in B$. Logo, $p = -(-p) \in A^c$, mas isso contradiz $p \in A$. Portanto, $-p \in B^c$.

Concluimos, da Afirmação 6.2 e da Afirmação 6.3, $B \neq \emptyset$ e $B^c \neq \emptyset$.

Agora vamos mostrar (ii) da Definição 6.1: Se $p \in B$ e $q \in \mathbb{Q}$ com $q < p$, então $q \in B$. De fato, como $p \in B$ tem-se que $-p \in A^c$ e existe $q' \in A^c$ tal que $q' < -p$. Como $q < p$ temos $-p < -q$.

Afirmção 6.4 $-q \in A^c$.

De fato, se $-q \notin A^c$ tem-se que $-q \in A$. Agora, como A é corte e $-p < -q$, por (ii) da Definição 6.1, $-p \in A$, o que contradiz $-p \in A^c$.

Assim, pela Afirmação 6.4, $-q \in A^c$ e como $q' < -p < -q$ temos que $q' < -q$ com $q' \in A^c$, logo, por definição de B , $q \in B$.

Finalmente, vamos mostrar (iii) da Definição 6.1: Para todo $p \in B$, existe $r \in B$ tal que $p < r$. De fato, como $p \in B$, $-p \in A^c$ e existe $q \in A^c$ tal que $q < -p$. Logo, $p < -q$. Note que, pela monotonicidade da adição em \mathbb{Q} , tem-se

$$2p = p + p < p - q < -q - q = -2q \Rightarrow p < \frac{p - q}{2} < -q.$$

Considere $r = \frac{p - q}{2} \in \mathbb{Q}$. Assim, temos que $p < r < -q$.

Afirmção 6.5 $r \in B$.

De fato, como $r < -q$ tem-se que $q < -r$. Suponhamos que $-r \in A$ e como A é corte, por (ii) da Definição 6.1, $q \in A$ o que contradiz $q \in A^c$, logo $-r \notin A$. Portanto, $-r \in A^c$. Agora, $q < -r$ e $q \in A^c$, pela definição de B , $r \in B$.

Portanto, da Afirmação 6.5, $r \in B$ com $p < r$. ■

Definição 6.4 O corte B da Proposição 6.2 é denotado $\ominus A$ e chamado *oposto* de A .

Observação 6.2 Seja $A \in \Omega$, as seguintes afirmações são válidas:

1. $\ominus(\ominus A) = A$;
2. $A = Z(0) \iff \ominus A = Z(0)$;
3. $A \neq Z(0) \iff \ominus A \neq Z(0)$;
4. $A \supset Z(0) \iff \ominus A \subset Z(0)$;
5. $A \supsetneq Z(0) \iff \ominus A \subsetneq Z(0)$.

Teorema 6.3 [Teorema 3.9 em (MOREIRA; CABRAL, 2021)] Seja $A \in \Omega$. Temos que $A \oplus (\ominus A) = Z(0)$.

Demonstração. Seja $r \in A \oplus (\ominus A)$. Logo, existem $s \in A$ e $p \in \ominus A$ tal que $r = s + p$. Como $p \in \ominus A$, pela Definição 6.4 e a Proposição 6.2, temos $-p \in A^{\mathbb{C}}$ e existe $q \in A^{\mathbb{C}}$ tal que $q < -p$. Note que $s \neq q$ (pois $s \in A$ e $q \in A^{\mathbb{C}}$). Suponha $q < s$. Como A é corte e $s \in A$, por (ii) da Definição 6.1, $q \in A$, o que contradiz $q \in A^{\mathbb{C}}$, logo $s < q$. Daí, pela monotonicidade da adição em \mathbb{Q} ,

$$r = s + p < p + q < p - p = 0,$$

logo $r \in Z(0)$. Portanto,

$$A \oplus (\ominus A) \subset Z(0). \quad (6.12)$$

Reciprocamente, seja $r \in Z(0)$ logo $r < 0$. Como A é corte, por (i) da Definição 6.1, $A^{\mathbb{C}} \neq \emptyset$ daí existe $s \in A^{\mathbb{C}}$.

Afirmção 6.6 $s - r \in A^{\mathbb{C}}$.

De fato, suponha que $s - r \notin A^{\mathbb{C}}$, logo $s - r \in A$. Como A é corte e $s < s - r$, por (ii) da Definição 6.1, $s \in A$, o que contradiz $s \in A^{\mathbb{C}}$. Logo, $s - r \in A^{\mathbb{C}}$.

Por outro lado, vamos definir o seguinte conjunto

$$X = \{n \in \mathbb{N}; s - \frac{nr}{2} \in A^{\mathbb{C}}\}.$$

Pela Afirmção 6.6, $s - r \in A^{\mathbb{C}}$, logo $2 \in X$. Assim $X \neq \emptyset$. Pelo Princípio da Boa Ordenação (Teorema 3.19) existe $n_0 \in \mathbb{N}$ tal que $n_0 = \min X$, isto é, $n_0 \in X$ e $n_0 \leq n$ em \mathbb{N} para todo $n \in X$. Consideremos agora

$$p = s - \left(\frac{n_0 - 1}{2}\right)r, \quad t = s - \frac{n_0 r}{2} \quad \text{e} \quad q = s - \left(\frac{n_0 + 1}{2}\right)r.$$

Note que, como $n_0 \in X$, temos que $t \in A^{\mathbb{C}}$.

Afirmção 6.7 $p \in A$.

De fato, suponha $p \notin A$, logo $p \in A^c$, assim $s - \left(\frac{n_0-1}{2}\right)r \in A^c$, daí $n_0 - 1 \in X$, mas isso contradiz a minimalidade de X , o que é um absurdo, assim $p \in A$.

Afirmção 6.8 $q \in A^c$.

De fato, suponha $q \notin A^c$, logo $q \in A$, assim, $s - \left(\frac{n_0+1}{2}\right)r \in A$. Como A é corte e $s < s - \left(\frac{n_0+1}{2}\right)r$, por (ii) da Definição 6.1, temos que $s \in A$, mas isto contradiz $s \in A^c$. Portanto, $q \in A^c$.

Afirmção 6.9 $-q \in \ominus A$.

De fato, como $-(-q) = q \in A^c$ (Afirmção 6.8) e existe $t \in A^c$ tal que

$$t = s - \frac{n_0 r}{2} < s - \left(\frac{n_0 + 1}{2}\right)r = -(-q),$$

pela definição de $\ominus A$, $-q \in \ominus A$.

Finalmente, note que

$$\begin{aligned} p - q &= s_0 - \left(\frac{n_0-1}{2}\right)r - \left(s_0 - \left(\frac{n_0+1}{2}\right)r\right) \\ &= \frac{r}{2}(-n_0 + 1) + (n_0 + 1)r = \frac{2r}{2} = r. \end{aligned}$$

Logo, pela Afirmção 6.7 e Afirmção 6.9,

$$r = p - q = p + (-q) \in A \oplus (\ominus A).$$

Daí,

$$Z(0) \subseteq A \oplus (\ominus A). \quad (6.13)$$

De (6.11) e (6.12), temos $Z(0) = A \oplus (\ominus A)$. ■

Proposição 6.3 [Proposição 3.10 em (MOREIRA; CABRAL, 2021)] Sejam $A, B \in \Omega$ tais que $Z(0) \subset A$ e $Z(0) \subset B$. O conjunto

$$C = \{r \in \mathbb{Q}; r < 0 \text{ ou } r = p \cdot q \text{ com } p \in A, q \in B, p \geq 0 \text{ e } q \geq 0\}$$

é corte.

Demonstração. Primeiramente, vamos mostrar (i) da Definição 6.1: $C \neq \emptyset$ e $C^c \neq \emptyset$.

De fato, como $-1 \in C$, logo $C \neq \emptyset$. Agora, como A e B são cortes, então $A^c \neq \emptyset$ e $B^c \neq \emptyset$, logo existem $p' \in A^c$ e $q' \in B^c$. Como $Z(0) \subset A, B$, temos que $p', q' \notin Z(0)$, logo $p' \geq 0$ e $q' \geq 0$. Daí, $p'q' \geq 0$.

Afirmção 6.10 $p'q' \in C^c$.

De fato, suponha que $p'q' \in C$. Como $p'q' \geq 0$ temos que existem $p \in A$, $q \in B$, $p \geq 0$ e $q \geq 0$ tal que

$$p'q' = pq. \quad (6.14)$$

Se $p' = p \in A$, o que contradiz $p' \in A^c$. Logo, $p' \neq p$. Se $p' < p$, como A é corte e $p \in A$, por (ii) da Definição 6.1, $p' \in A$, o que contradiz $p' \in A^c$. Logo,

$$p < p'. \quad (6.15)$$

Se $q' = q \in B$, o que contradiz $q' \in B^c$. Daí, $q' \neq q$. Se $q' < q$, como B é corte e $q \in B$, por (ii) da Definição 6.1, $q' \in B$ o que contradiz $q' \in B^c$. Assim,

$$q < q'. \quad (6.16)$$

De (6.15), (6.16) e pela monotonicidade da multiplicação em \mathbb{Q} , tem-se

$$pq \leq p'q < p'q',$$

logo $pq < p'q'$, o que contradiz (6.14). Portanto, $p'q' \in C^c$. Consequentemente, $C^c \neq \emptyset$.

Vamos agora mostrar (ii) da Definição 6.1: Se $r \in C$, $s \in \mathbb{Q}$ e $s < r$, então $s \in C$. De fato, se $s < 0$, por definição de C , $s \in C$. Suponha agora $s \geq 0$ e, portanto, $r > 0$. Como $r \in C$, por definição de C , existem $p \in A$ e $q \in B$, tal que $r = pq$, com $p > 0$ e $q > 0$. Como $p > 0$ e $s < r = pq$, temos que $\frac{s}{p} < q$. Como B é corte, $\frac{s}{p} \in \mathbb{Q}$ e $q \in B$, por (ii) da Definição 6.1, $\frac{s}{p} \in B$. Daí, $s = p\left(\frac{s}{p}\right)$ com $p \in A$ e $\frac{s}{p} \in B$ e ainda $p > 0$ e $\frac{s}{p} > 0$, por definição de C , $s \in C$.

Finalmente, mostraremos (iii) da Definição 6.1: Para todo $r \in C$, existe $t \in C$ tal que $r < t$. De fato, se $r < 0$, tomando $t = \frac{r}{2} < 0$, tem-se $t \in C$ com $r < t$. Se $r \geq 0$, como $r \in C$ temos que $r = pq$, com $p \in A$, $q \in B$, $p \geq 0$ e $q \geq 0$. Como A é corte e $p \in A$, por (iii) da Definição 6.1, existe $\alpha \in A$ tal que

$$p < \alpha. \quad (6.17)$$

Também, como B é corte e $q \in B$, por (iii) da Definição 6.1, existe $\beta \in B$ tal que

$$q < \beta. \quad (6.18)$$

De (6.17), (6.18) e pela monotonicidade da multiplicação em \mathbb{Q} , tem-se

$$pq \leq \alpha q < \alpha\beta,$$

logo $r = pq < \alpha\beta$. Agora, tomando $t = \alpha\beta$, como $\alpha \in A$, $\beta \in B$ com $\alpha > 0$ e β , pela definição de C , $t \in C$ com $r < t$. ■

Definição 6.5 Sejam $A, B \in \Omega$ tais que $Z(0) \subset A$ e $Z(0) \subset B$. O corte C dado na Proposição 6.3 e denotado $A * B$ é chamado de **produto** ou **multiplicação** de A e B .

Observação 6.3 Da Definição 6.5 segue-se que $Z(0) \subset A$ e $Z(0) \subset B$, então $Z(0) \subset A * B$.

Definição 6.6 Dado $A \in \Omega$, o *módulo* de A , denotado por $|A|$, é definido por

$$|A| = \begin{cases} A & \text{se } Z(0) \subset A, \\ \ominus A & \text{se } A \subsetneq Z(0). \end{cases}$$

Em vista da Observação 6.2, temos que $|A| \supset Z(0)$ para todo $A \in \Omega$.

Definição 6.7 Sejam $A, B \in \Omega$. Definimos $A \odot B$ por:

$$A \odot B = \begin{cases} A * B & \text{se } Z(0) \subset A \text{ e } Z(0) \subset B, \\ \ominus(A * |B|) & \text{se } Z(0) \subset A \text{ e } B \subsetneq Z(0), \\ \ominus(|A| * B) & \text{se } A \subsetneq Z(0) \text{ e } Z(0) \subset B, \\ |A| * |B| & \text{se } A \subsetneq Z(0) \text{ e } B \subsetneq Z(0). \end{cases}$$

Teorema 6.4 [Teorema 3.14 em (MOREIRA; CABRAL, 2021)] Sejam $A, B, C \in \Omega$.

Temos que:

1. $A \odot B = B \odot A$;
2. $(A \odot B) \odot C = A \odot (B \odot C)$;
3. $A \odot Z(1) = A$, onde $Z(1) = \{p \in \mathbb{Q}; p < 1\}$ (Definição 6.2).

Demonstração. Vamos supor inicialmente que $Z(0) \subset A \cap B \cap C$.

1. Seja $r \in A * B$. Se $r < 0$, por definição de $B * A$, tem-se $r \in B * A$. Se $r \geq 0$, como $r \in A * B$ logo existem $p \in A, q \in B, p \geq 0$ e $q \geq 0$ tal que $r = pq$. Pela comutatividade do produto em \mathbb{Q} , temos $r = qp$, com $q \in B, p \in A, q \geq 0$ e $p \geq 0$. Logo, $r \in B * A$. Portanto,

$$A * B \subset B * A. \quad (6.19)$$

Analogamente, seja $r \in B * A$, se $r < 0$, por definição de $A * B$, então é imediato que $r \in A * B$. Se $r \geq 0$, como $r \in B * A$, logo existem $q \in B, p \in A, q \geq 0$ e $p \geq 0$ tal que $r = qp$. Pela comutatividade do produto em \mathbb{Q} , $r = pq$. Assim, $r \in A * B$. Consequentemente,

$$B * A \subset A * B. \quad (6.20)$$

De (6.19) e (6.20), temos que $A * B = B * A$.

2. Seja $r \in (A * B) * C$. Se $r < 0$, por definição de $A * (B * C)$, é imediato que $r \in A * (B * C)$. Se $r \geq 0$, como $r \in (A * B) * C$ existem $m \in A * B, t \in C, m \geq 0$ e $t \geq 0$ tal que $r = mt$. Como $m \in A * B$ e $m \geq 0$, existem $p \in A, q \in B, p \geq 0$ e $q \geq 0$ tal que $m = pq$. Daí, $r = mt = (pq)t$. Pela associatividade de produto em \mathbb{Q} , temos $r = p(qt)$, com $p \in A, q \in B, t \in C, p \geq 0, q \geq 0$ e $t \geq 0$. Assim, $r \in A * (B * C)$. Logo,

$$(A * B) * C \subset A * (B * C). \quad (6.21)$$

Analogamente, seja $r \in A * (B * C)$. Se $r < 0$, por definição de $(A * B) * C$, é imediato que $r \in (A * B) * C$. Se $r \geq 0$, como $r \in A * (B * C)$ existem $p \in A, q \in B, t \in C, p \geq 0, q \geq 0$ e $t \geq 0$ tal que $r = p(qt)$. Pela associatividade de produto em \mathbb{Q} , tem-se $r = (pq)t$. Portanto, $r \in (A * B) * C$, e daí

$$A * (B * C) \subset (A * B) * C. \quad (6.22)$$

De (6.21) e (6.22), concluímos que $(A * B) * C = A * (B * C)$.

3. Seja $r \in A * Z(1)$. Se $r < 0$ então $r \in Z(0)$ e como $Z(0) \subset A$, tem-se $r \in A$. Se $r \geq 0$. Como $r \in A * Z(1)$ existem $p \in A, q \in Z(1), p \geq 0$ e $q \geq 0$ tal que $r = pq$. Daí, como $q \in Z(1)$, temos que $0 \leq q < 1$. Se $p = 0$ então $r = 0 = p \in A$. Se $p > 0$, logo, pela monotonicidade da multiplicação em \mathbb{Q} , $r = pq < p \cdot 1 = p$. Assim, $r < p$. Como A é corte e $p \in A$, por (ii) da Definição 6.1, $r \in A$. Em qualquer caso, $r \in A$.

Portanto

$$A * Z(1) \subset A. \quad (6.23)$$

Reciprocamente, se $r \in A$. Se $r < 0$, por definição de $A * Z(1)$, $r \in A * Z(1)$. Se $r \geq 0$, como $r \in A$ e A é corte, por (iii) da Definição 6.1, existe $p \in A$ tal que $0 \leq r < p$. Logo, $\frac{r}{p} < 1$ assim $\frac{r}{p} \in Z(1)$. Agora, desde que $r = p \left(\frac{r}{p}\right)$ com $p \in A$ e $\frac{r}{p} \in Z(1)$, por definição de $A * Z(1)$, temos que $r \in A * Z(1)$. Daí,

$$A \subset A * Z(1). \quad (6.24)$$

Portanto, de (6.23) e (6.24), temos $A * Z(1) = A$.

Vamos mostrar o caso geral do item 1.

(1.a) Se $Z(0) \subset A$ e $B \subsetneq Z(0)$. Então, pela Definição 6.7, temos

$$A \odot B = \ominus(|A| * B) = \ominus(B * |A|) = B \odot A.$$

(1.b) Se $A \subsetneq Z(0)$ e $Z(0) \subset B$. Então, pela Definição 6.7, temos

$$A \odot B = \ominus(|A| * B) = \ominus(B * |A|) = B \odot A.$$

(1.c) Se $A \subsetneq Z(0)$ e $B \subsetneq Z(0)$. Então, pela Definição 6.7, temos

$$A \odot B = |A| * |B| = |B| * |A| = B \odot A.$$

Agora, mostraremos o caso geral do item 2.

(2.a) Se $Z(0) \subset A$, $B \subsetneq Z(0)$ e $Z(0) \subset C$. Então, pela Definição 6.7, temos

$$\begin{aligned} (A \odot B) \odot C &= (\ominus(A * |B|)) \odot C = \ominus(|\ominus(A * |B|)| * C) \\ &= \ominus(\ominus(\ominus(A * |B|)) * C) = \ominus((A * |B|) * C) \\ &= \ominus(A * (|B| * C)) = \ominus(A * (\ominus(\ominus(|B| * C)))) \\ &= \ominus(A * |\ominus(|B| * C)|) = A \odot (\ominus(|B| * C)) \\ &= A \odot (B \odot C). \end{aligned}$$

(2.b) Se $Z(0) \subset A$, $B \subsetneq Z(0)$ e $C \subsetneq Z(0)$. Então, pela Definição 6.7, temos

$$\begin{aligned} (A \odot B) \odot C &= (\ominus(A * |B|)) \odot C = |\ominus(A * |B|)| * |C| \\ &= (\ominus(\ominus(A * |B|))) * |C| = (A * |B|) * |C| \\ &= A * (|B| * |C|) = A \odot (|B| * |C|) \\ &= A \odot (B \odot C). \end{aligned}$$

(2.c) Se $Z(0) \subset A$, $Z(0) \subset B$ e $C \subsetneq Z(0)$. Então, pela Definição 6.7, temos

$$\begin{aligned} (A \odot B) \odot C &= (A * B) \odot C = \ominus((A * B) * |C|) \\ &= \ominus(A * (B * |C|)) = \ominus(A * (\ominus(\ominus(B * |C|)))) \\ &= \ominus(A * |\ominus(B * |C|)|) = A \odot (\ominus(B * |C|)) \\ &= A \odot (B \odot C). \end{aligned}$$

(2.d) Se $A \subsetneq Z(0)$, $Z(0) \subset B$ e $C \subsetneq Z(0)$. Então, pela Definição 6.7, temos

$$\begin{aligned} (A \odot B) \odot C &= (\ominus(|A| * B)) \odot C = |\ominus(|A| * B)| * |C| \\ &= (\ominus(\ominus(|A| * B))) * |C| = (|A| * B) * |C| \\ &= |A| * (B * |C|) = |A| * (\ominus(\ominus(B * |C|))) \\ &= |A| * |\ominus(B * |C|)| = A \odot (\ominus(B * |C|)) \\ &= A \odot (B \odot C). \end{aligned}$$

(2.e) Se $A \subsetneq Z(0)$, $Z(0) \subset B$ e $Z(0) \subset C$. Então, pela Definição 6.7, temos

$$\begin{aligned} (A \odot B) \odot C &= (\ominus(|A| * B)) \odot C = \ominus(|\ominus(|A| * B)| * C) \\ &= \ominus(\ominus(\ominus(|A| * B))) * C = \ominus((|A| * B) * C) \\ &= \ominus(|A| * (B * C)) = A \odot (B * C) \\ &= A \odot (B \odot C). \end{aligned}$$

(2.f) Se $A \subsetneq Z(0)$, $B \subsetneq Z(0)$ e $Z(0) \subset C$. Então, pela Definição 6.7, temos

$$\begin{aligned} (A \odot B) \odot C &= (|A| * |B|) \odot C = (|A| * |B|) * C \\ &= |A| * (|B| * C) = |A| * (\ominus(\ominus(|B| * C))) \\ &= |A| * |\ominus(|B| * C)| = A \odot (\ominus(|B| * C)) \\ &= A \odot (B \odot C). \end{aligned}$$

(2.g) Se $A \subsetneq Z(0)$, $B \subsetneq Z(0)$ e $C \subsetneq Z(0)$. Então, pela Definição 6.7, temos

$$\begin{aligned} (A \odot B) \odot C &= (|A| * |B|) \odot C = \ominus((|A| * |B|) * |C|) \\ &= \ominus(|A| * (|B| * |C|)) = A \odot (|B| * |C|) \\ &= A \odot (B \odot C). \end{aligned}$$

Finalmente, mostraremos o último caso do item 3. Se $A \subsetneq Z(0)$. Então, pela Definição 6.7, temos

$$A \odot Z(1) = \ominus(|A| * Z(1)) = \ominus(|A|) = \ominus(\ominus A) = A.$$

Portanto, $A \odot Z(1) = A$. ■

Proposição 6.4 [Proposição 3.5 em (MOREIRA; CABRAL, 2021)] Seja $A \in \Omega$ tal que $Z(0) \subsetneq A$. O conjunto

$$B = \{p \in \mathbb{Q}; p \leq 0 \text{ ou } p^{-1} \in A^{\mathbb{C}} \text{ e existe } q \in A^{\mathbb{C}} \text{ tal que } q < p^{-1}\}$$

é corte.

Demonstração. Primeiramente, vamos mostrar (i) da Definição 6.1: $B \neq \emptyset$ e $B^{\mathbb{C}} \neq \emptyset$. De fato, como $-1 \in B$, daí $B \neq \emptyset$. Agora, como por hipótese $Z(0) \subsetneq A$, logo existe $q \in A$ tal que $q \notin Z(0)$, isto é, $q \in A$ com $q \geq 0$. Note também, como A é corte e $q \in A$, por (iii) da Definição 6.1, existe $p \in A$ tal que $0 \leq q < p$. Logo, $p \in A$ com $p > 0$.

Afirmção 6.11 $p^{-1} \notin B$.

De fato, se $p^{-1} \in B$, como $p^{-1} > 0$, por definição de B , temos $p = (p^{-1})^{-1} \in A^{\mathbb{C}}$, mas isso contradiz que $p \in A$. Portanto $p^{-1} \notin B$.

Logo, pela Afirmção 6.11, $p^{-1} \in B^{\mathbb{C}}$, assim temos $B^{\mathbb{C}} \neq \emptyset$.

Vamos agora mostrar (ii) da Definição 6.1: Se $p \in B$, $q \in \mathbb{Q}$ e $q < p$, então $q \in B$. De fato, se $q \leq 0$, por definição de B , é imediato que $q \in B$. Se $q > 0$, como $0 < q < p$ então $p > 0$ e $p \in B$, por definição de B , $p^{-1} \in A^{\mathbb{C}}$ e existe $r \in A^{\mathbb{C}}$ tal que $r < p^{-1}$. Como $0 < q < p$ então $p^{-1} < q^{-1}$. Suponhamos que $q^{-1} \in A$ e como A é corte, por (ii) da Definição 6.1, $p^{-1} \in A$, mas isso contradiz $p^{-1} \in A^{\mathbb{C}}$. Portanto, $q^{-1} \in A^{\mathbb{C}}$. Agora, como $r < p^{-1} < q^{-1}$ então $r < q^{-1}$ e desde que $r \in A^{\mathbb{C}}$, por definição de B , tem-se $q \in B$.

Finalmente, vamos mostrar (iii) da Definição 6.1: Para todo $p \in B$ existe $q \in B$ tal que $p < q$. Primeiramente mostremos a seguinte afirmação:

Afirmção 6.12 Existe $q \in B$ com $q > 0$.

De fato, como A é corte, por (i) da Definição 6.1, $A^{\mathbb{C}} \neq \emptyset$, logo existe $m \in A^{\mathbb{C}}$ e como $Z(0) \subsetneq A$, temos que $m \notin Z(0)$, isto é, $m \geq 0$. Logo, $m + 1 \geq 1 > 0$, daí $m + 1 > 0$. Consideremos $q = (m + 1)^{-1}$. Note que $q > 0$ e $m < m + 1 = q^{-1}$ com $m \in A^{\mathbb{C}}$. Agora, suponha que $q^{-1} \in A$, como A é corte, por (ii) da Definição 6.1, $m \in A$ o que contradiz que $m \in A^{\mathbb{C}}$. Logo, $q^{-1} \in A^{\mathbb{C}}$. Portanto, $q \in B$.

Por outro lado, seja $p \in B$. Se $p \leq 0$, pela Afirmção 6.12, existe $q \in B$ com $q > 0$, daí $q \in B$ e $p < q$. Se $p > 0$, como $p \in B$, por definição de B , $p^{-1} \in A^{\mathbb{C}}$

e existe $r \in A^{\mathbb{C}}$ tal que $r < p^{-1}$. Consideremos $s = \frac{r+p^{-1}}{2}$. Daí, pela monotonicidade da adição em \mathbb{Q} , $2r = r + r < r + p^{-1} < p^{-1} + p^{-1} = 2p^{-1}$, logo

$$r < s < p^{-1}. \quad (6.25)$$

Suponha que $s \leq 0$, logo por (6.25), $r < 0$, assim $r \in Z(0)$, e como por hipótese $Z(0) \subsetneq A$, $r \in A$ o que contradiz que $r \in A^{\mathbb{C}}$. Daí, $s > 0$. Suponhamos agora que $s \in A$. Por (6.25), $r < s$, e como A é corte, por (ii) da Definição 6.1, $r \in A$ o que contradiz novamente que $r \in A^{\mathbb{C}}$. Portanto, $s \in A^{\mathbb{C}}$ com $s > 0$. Consideremos $q = s^{-1}$, desde que $s > 0$ temos que $q > 0$. Como $s \in A^{\mathbb{C}}$ temos que $q^{-1} = s \in A^{\mathbb{C}}$. Agora, por (6.25), tem-se que $r < q^{-1}$ com $r \in A^{\mathbb{C}}$. Logo, por definição de B , $q \in B$. Também, por (6.25), $p < s^{-1} = q$. Portanto, existe $q \in B$ com $p < q$. ■

Definição 6.8 Seja $A \in \Omega$ tal que $A \neq Z(0)$. Se $Z(0) \subsetneq A$, então o corte B da Proposição 6.4 é denotado $A^{\ominus 1}$ e chamado *inverso* de A . Se $A \subsetneq Z(0)$, então definimos $A^{\ominus 1} = \ominus(|A|^{\ominus 1})$.

Teorema 6.5 [Teorema 3.17 em (MOREIRA; CABRAL, 2021)] Seja $A \in \Omega$ tal que $A \neq Z(0)$. Temos $A \odot (A^{\ominus 1}) = Z(1)$.

Demonstração. Suponhamos inicialmente que $Z(0) \subsetneq A$. Mostraremos que $A * A^{\ominus 1} = Z(1)$.

Seja $r \in A * (A^{\ominus 1})$. Se $r \leq 0$, então $r \in Z(1)$. Se $r > 0$, por definição do produto, existem $s \in A$ e $p \in A^{\ominus 1}$ com $s > 0$ e $p > 0$ tal que $r = sp$. Daí, como $p \in A^{\ominus 1}$, logo $p^{-1} \in A^{\mathbb{C}}$ e existe $q \in A^{\mathbb{C}}$ tal que $q < p^{-1}$. Como $s \in A$ e $q \in A^{\mathbb{C}}$, temos que $s \neq q$. Se $q < s$, como A é corte e $s \in A$, por (ii) da Definição 6.1, $q \in A$ o que é contradiz $q \in A^{\mathbb{C}}$. Logo, $0 < s < q$. Agora, como $q < p^{-1}$, pela monotonicidade da multiplicação em \mathbb{Q} , obtemos $p < q^{-1}$, daí $r = sp < sq^{-1}$, e sendo $q > 0$ com $s < q$ tem-se $r < \frac{s}{q} < 1$. Logo, $r < 1$, daí $r \in Z(1)$. Portanto,

$$A * A^{\ominus 1} \subset Z(1). \quad (6.26)$$

Reciprocamente, seja $r \in Z(1)$. Daí $r < 1$. Aqui temos as seguintes possibilidades:

- Se $r < 0$, por definição do produto, $r \in A * A^{\ominus 1}$.

- Se $r = 0$, como $Z(0) \subsetneq A$, existe $s \in A$, tal que $s \geq 0$. Se $s = 0$, então $0 \in A$. Se $s > 0$, como $s \in A$, $0 < s$ e A é corte, por (ii) da Definição 6.1, $0 \in A$. Logo, em qualquer caso, $0 \in A$. Note também que, por definição de $A^{\ominus 1}$, $0 \in A^{\ominus 1}$. Daí, $r = 0 \cdot 0 \in A * (A^{\ominus 1})$.
- Se $0 < r < 1$. Como já vimos no caso anterior $0 \in A$, daí como A é corte, por (iii) da Definição 6.1, existe $s \in A$ tal que $s > 0$.

Afirmção 6.13 Existe $n \in \mathbb{N}$ tal que $s(r^{-1})^n \in A^{\mathbb{C}}$.

De fato, suponha que $s(r^{-1})^n \in A$ para todo $n \in \mathbb{N}$ (hipótese auxiliar). Como A é corte, por (i) da Definição 6.1, $A^{\mathbb{C}} \neq \emptyset$, logo existe $\ell \in A^{\mathbb{C}}$. Como $0 \in A$, daí $\ell \neq 0$. Se $\ell < 0$, como A é corte e $0 \in A$, por (ii) da Definição 6.1, $\ell \in A$ o que contradiz $\ell \in A^{\mathbb{C}}$. Logo, $\ell \in A^{\mathbb{C}}$ com $\ell > 0$. Agora, desde que $0 < r < 1$ então $\lim_{n \rightarrow \infty} r^n = 0$ em \mathbb{Q} (Exemplo 6 do Capítulo 3 em (LIMA, 2014)). Assim para $\frac{s}{\ell} > 0$ em \mathbb{Q} temos que existe $m \in \mathbb{N}$ tal que $r^m < \frac{s}{\ell}$ logo $\ell < s(r^{-1})^m$ e, pela hipótese auxiliar temos que $s(r^{-1})^m \in A$. Como A é corte, por (ii) da Definição 6.1, $\ell \in A$ o que contradiz que $\ell \in A^{\mathbb{C}}$. Portanto, existe $n \in \mathbb{N}$ tal que $s(r^{-1})^n \in A^{\mathbb{C}}$.

Consideremos agora

$$X = \{p \in \mathbb{N}; s(r^{-1})^p \in A^{\mathbb{C}}\}.$$

Pela Afirmção 6.13, X é não vazio e $X \subset \mathbb{N}$. Pelo Princípio da Boa Ordenação (Teorema 3.19), existe $n_0 \in \mathbb{N}$, tal que $n_0 = \min X$. Logo, temos $t = s(r^{-1})^{n_0} \in A^{\mathbb{C}}$ e $p_1 = s(r^{-1})^{n_0-1} \in A$. Por outro lado, como A é corte, por (iii) da Definição 6.1, existe $p \in A$, tal que $p_1 < p$. Denotemos, $q = t^{-1}p^{-1}p_1$.

Afirmção 6.14 $q^{-1} \in A^{\mathbb{C}}$.

De fato, sendo $0 < p_1 < p$ temos que $1 < pp_1^{-1}$ daí $t < tpp_1^{-1} = q^{-1}$. Se $q^{-1} \in A$, como A é corte, por (ii) da Definição 6.1, $t \in A$, o que contradiz $t \in A^{\mathbb{C}}$. Logo, $q^{-1} \in A^{\mathbb{C}}$.

Note que, como $q^{-1} \in A^{\mathbb{C}}$ e $t < q^{-1}$ com $t \in A^{\mathbb{C}}$ então $q \in A^{\ominus 1}$. Assim obtemos que

$$pq = p(t^{-1}p^{-1}p_1) = t^{-1}p_1 = (s(r^{-1})^{n_0})^{-1}(s(r^{-1})^{n_0-1}) = r.$$

Como $p \in A$ e $q \in A^{\ominus 1}$, então $r \in A * A^{\ominus 1}$.

Portanto, em qualquer caso,

$$Z(1) \subset A * A^{\ominus 1} \quad (6.27)$$

De (6.26) e (6.27), temos que $A * A^{\ominus 1} = Z(1)$.

Vamos agora considerar o caso $A \subsetneq Z(0)$. Temos que, pela Definição $A^{\ominus 1}$, $Z(0) \subsetneq A^{\ominus 1}$. Assim, pela definição de produto, definição do inverso e usando o caso anterior, obtemos:

$$A \odot A^{\ominus 1} = |A| * |A^{\ominus 1}| = |A| * |\ominus(|A|^{\ominus 1})| = |A| * (\ominus(\ominus(|A|^{\ominus 1}))) = |A| * |A|^{\ominus 1} = Z(1). \blacksquare$$

Teorema 6.6 [Teorema 3.18 em (MOREIRA; CABRAL, 2021)] Sejam $A, B, C \in \Omega$. Temos que

$$(A \oplus B) \odot C = (A \odot C) \oplus (B \odot C).$$

Demonstração. Vamos supor inicialmente $Z(0) \subset A \cap B \cap C$.

Seja $r \in (A \oplus B) * C$. Se $r < 0$, então $r \in Z(0)$ e pela Observação 6.1, $r \in (A * C) \oplus (B * C)$. Se $r \geq 0$, por definição de produto, $r = pq$ com $p \in A \oplus B$, $q \in C$, $p \geq 0$ e $q \geq 0$. Agora, como $q \geq 0$ temos duas possibilidades:

- Se $q = 0$ então $0 \in C$ daí, por definição de produto, $0 \in A * C, B * C$. Logo, podemos escrever

$$r = 0 = \underbrace{0}_{\in A * C} + \underbrace{0}_{\in B * C} \in (A * C) \oplus (B * C).$$

- Se $q > 0$, como $p \in A \oplus B$ existem $m \in A$ e $n \in B$ tais que $p = m + n$, logo $r = (m + n)q$. Se $mq < 0$, por definição de produto, $mq \in A * C$. Se $mq \geq 0$, como $q > 0$ temos que $m \geq 0$, daí, obtemos $mq \in A * C$. Em qualquer caso, $mq \in A * C$. Analogamente, se $nq < 0$, por definição de produto, $nq \in B * C$. Se $nq \geq 0$, como $q > 0$ temos que $n \geq 0$, daí, obtemos $nq \in B * C$. Em qualquer caso, $nq \in B * C$. Agora, pela distributividade em \mathbb{Q} , temos

$$r = (m + n)q = \underbrace{mq}_{\in A * C} + \underbrace{nq}_{\in B * C} \in (A * C) \oplus (B * C).$$

Em qualquer caso, $r \in (A * C) \oplus (B * C)$. Portanto,

$$(A \oplus B) * C \subset (A * C) \oplus (B * C). \quad (6.28)$$

Reciprocamente, seja $r \in (A * C) \oplus (B * C)$. Se $r < 0$, por definição de produto, $r \in (A \oplus B) * C$. Suponha $r \geq 0$, como $r \in (A * C) \oplus (B * C)$ existem $m \in A * C$ e $n \in B * C$ tal que $r = m + n$.

- Se $r = 0$, logo $m = -n$.
 - Se $m < 0$ então $n > 0$. Como $n \in B * C$ existem $p \in B$, $q \in C$, $p > 0$ e $q > 0$ tais que $n = pq$. Aqui temos,

$$r = 0 = m + n = m + pq = (mq^{-1} + p)q. \quad (6.29)$$

Como $q > 0$, por (6.29), tem-se $mq^{-1} + p = 0$. Também, como $mq^{-1} < 0$ então $mq^{-1} \in Z(0) \subset A$, logo $mq^{-1} \in A$, $p \in B$ e $q \in C$, temos que

$$r = 0 = 0 \cdot q = (mq^{-1} + p)q \in (A \oplus B) * C.$$

- Se $m = 0$ então $n = 0$. Como $m \in A * C$ e $n \in B * C$ existem $a \in A$, $b \in B$, $c, d \in C$, $a, b, c, d \geq 0$ tais que $0 = m = ac$ e $0 = n = bd$. Como $ac = 0$ então $a = 0$ ou $c = 0$. Também, como $bd = 0$ então $b = 0$ ou $d = 0$.
 - * Se $c = 0$ ou $d = 0$, neste caso temos $0 \in C$, logo $r = 0 = (a + b) \cdot 0$, onde $a + b \in A \oplus B$ com $a + b \geq 0$. Daí, $r \in (A \oplus B) * C$.
 - * Se $a = b = 0$ e $c, d > 0$, neste caso, $0 \in A$ e $0 \in B$, logo temos que $r = 0 = (0 + 0)c$, com $0 + 0 \in A \oplus B$ e $c \in C$. Logo, $r \in (A \oplus B) * C$.
- Se $m > 0$ então $n < 0$. Como $m \in A * C$ existem $p \in A$, $q \in C$, $p > 0$ e $q > 0$ tais que $m = pq$. Aqui temos,

$$r = 0 = m + n = pq + n = (p + nq^{-1})q. \quad (6.30)$$

Como $q > 0$, por (6.30), tem-se $p + nq^{-1} = 0$. Também, como $nq^{-1} < 0$ então $nq^{-1} \in Z(0) \subset B$, logo $nq^{-1} \in B$, $p \in A$ e $q \in C$, temos que

$$r = 0 = 0 \cdot q = (p + nq^{-1})q \in (A \oplus B) * C.$$

- Se $r > 0$, logo $r = m + n > 0$. Aqui temos os seguintes casos.
 - Se $m < 0$ e $n < 0$. Temos que $m + n < 0$ o que contradiz $r > 0$. Este caso não acontece.

– Se $m < 0$ e $n \geq 0$. Como $n \in B * C$ existem $p \in B, q \in C, p \geq 0$ e $q \geq 0$ tais que $n = pq$.

* Se $q = 0$ então $n = 0$. Logo, $r = m < 0$, assim, pela definição de produto, $r \in (A \oplus B) * C$.

* Se $q > 0$, temos

$$r = m + n = m + pq = (mq^{-1} + p)q. \quad (6.31)$$

Agora, como $m < 0$ e $q^{-1} > 0$ temos que $mq^{-1} < 0$, portanto $mq^{-1} \in Z(0) \subset A$. Logo, $mq^{-1} \in A$. Note também, como $r > 0$ e $q > 0$, por (6.31), obtemos $mq^{-1} + p > 0$ e como $p \in B$, por (6.31) tem-se $r \in (A \oplus B) * C$.

– Se $m \geq 0$ e $n < 0$. Como $m \in A * C$ existem $p \in A, q \in C, p \geq 0$ e $q \geq 0$ tais que $m = pq$.

* Se $q = 0$ então $m = 0$. Logo, $r = n < 0$, assim, pela definição de produto, $r \in (A \oplus B) * C$.

* Se $q > 0$, temos

$$r = m + n = pq + n = (p + nq^{-1})q. \quad (6.32)$$

Agora, como $n < 0$ e $q^{-1} > 0$ temos que $nq^{-1} < 0$, portanto $nq^{-1} \in Z(0) \subset B$. Logo, $nq^{-1} \in B$. Note também, como $r > 0$ e $q > 0$, por (6.32), obtemos $p + nq^{-1} > 0$ e como $p \in A$, por (6.32) tem-se $r \in (A \oplus B) * C$.

– Se $m \geq 0$ e $n \geq 0$. Como $m \in A * C$ e $n \in B * C$ existem $a \in A, b \in B, c, d \in C, a, b, c, d \geq 0$ tais que $m = ac$ e $n = bd$.

* Se $m = 0$ e $n = 0$ então logo $r = m + n = 0$ o que contradiz $r > 0$. Este caso não acontece.

* Se $m > 0$ e $n > 0$. Logo, $a, b, c, d > 0$. Note que, $c, d > 0$ e $c, d \in C$.

• Se $c = d$ então $r = ac + bc = (a + b)c$, como $a \in A, b \in B$ e $c \in C$, então $r \in (A \oplus B) * C$.

• Se $d < c$ então $dc^{-1} < 1$, e como $b > 0$ logo $bdc^{-1} < b$. Agora, como B é corte e $b \in B$, por (ii) da Definição 6.1, $bdc^{-1} \in B$. Daí, temos

$$r = ac + bd = (a + bdc^{-1})c. \quad (6.33)$$

Note também, como $r > 0$ e $c > 0$, por (6.33), obtemos $a + bdc^{-1} > 0$. Desde que $a \in A$, $bdc^{-1} \in B$ e $q \in C$, por (6.33), tem-se que $r \in (A \oplus B) * C$.

- Se $c < d$ então $cd^{-1} < 1$, e como $a > 0$ logo $acd^{-1} < a$. Agora, como A é corte e $a \in A$, por (ii) da Definição 6.1, $acd^{-1} \in A$. Daí, temos

$$r = ac + bd = (acd^{-1} + b)d. \quad (6.34)$$

Note também, como $r > 0$ e $d > 0$, por (6.34), obtemos $acd^{-1} + b > 0$. Desde que $acd^{-1} \in A$, $b \in A$, e $d \in C$, por (6.34), tem-se que $r \in (A \oplus B) * C$.

- * Se $m > 0$ e $n = 0$. Logo, $0 \in B * C$. Agora, como $B * C$ é corte, por (iii) da Definição 6.1, existe $n' \in B * C$ tal que $0 < n'$. Note que $r = m + 0 < m + n'$ e, pelo caso anterior $m + n' \in (A \oplus B) * C$, e como $(A \oplus B) * C$ é corte, então $r \in (A \oplus B) * C$.
- * Se $m = 0$ e $n > 0$. Logo, $0 \in A * C$. Agora, como $A * C$ é corte, por (iii) da Definição 6.1, existe $m' \in A * C$ tal que $0 < m'$. Note que $r = 0 + n < m' + n$ e, pelo caso anterior $m' + n \in (A \oplus B) * C$, e como $(A \oplus B) * C$ é corte, então $r \in (A \oplus B) * C$.

Em qualquer caso, $r \in (A * C) \oplus (B * C)$. Portanto,

$$(A * C) \oplus (B * C) \subset (A \oplus B) * C. \quad (6.35)$$

De (6.28) e (6.35), temos que $(A * C) \oplus (B * C) = (A \oplus B) * C$.

Cada um dos outros casos (para os quais não vale $Z(0) \subset A$, $Z(0) \subset B$ e $Z(0) \subset C$) é tratado de maneira análoga ou é consequência deste que acabamos de demonstrar. ■

Pelo Teorema 6.2, Teorema 6.3, Teorema 6.4, Teorema 6.5 e Teorema 6.6 temos que $\langle \Omega, \oplus, \odot \rangle$ é um corpo. Além disto, a relação de inclusão \subset é uma relação de ordem em Ω .

Para concluirmos que $\langle \Omega, \oplus, \odot, \subset \rangle$ é um corpo ordenado falta estabelecer a monotonia das operações. Este é o assunto do próximo teorema.

Teorema 6.7 [Teorema 3.19 em (MOREIRA; CABRAL, 2021)] Sejam $A, B, C \in \Omega$. Temos:

1. Se $A \subset B$, então $A \oplus C \subset B \oplus C$;
2. Se $A \subset B$ e $Z(0) \subset C$, então $A \odot C \subset B \odot C$;
3. Se $A \subset B$ e $C \subset Z(0)$, então $B \odot C \subset A \odot C$.

Demonstração.

1. Seja $r \in A \oplus C$, então existem $p \in A$ e $q \in C$ tal que $r = p + q$. Como $A \subset B$ e $p \in A$, logo $p \in B$, daí $r = p + q$ com $p \in B$ e $q \in C$, assim temos $r \in B \oplus C$. Portanto, $A \oplus C \subset B \oplus C$.
2. Pelo item anterior, temos que $A \oplus (\ominus A) \subset B \oplus (\ominus A)$. Daí, pelo Teorema 6.3, $Z(0) \subset B \oplus (\ominus A)$. Da Observação 6.3 e pelo Teorema 6.6, temos

$$Z(0) \subset (B \oplus (\ominus A)) \odot C = (B \odot C) \oplus ((\ominus A) \odot C),$$

daí novamente pelo item anterior

$$Z(0) \oplus (A \odot C) \subset ((B \odot C) \oplus ((\ominus A) \odot C)) \oplus (A \odot C)$$

agora, usando o Teorema 6.6 e os itens 2 e 3 do Teorema 6.2, obtemos

$$A \odot C \subset (B \odot C) \oplus (((\ominus A) \odot C) \oplus (A \odot C)) = (B \odot C) \oplus ((\ominus A) \oplus A) \odot C.$$

Logo, pelo Teorema 6.3,

$$A \odot C \subset (B \odot C) \oplus (Z(0) \odot C)$$

e, como por definição de produto, $Z(0) \odot C = Z(0)$, obtemos

$$A \odot C \subset (B \odot C) \oplus Z(0)$$

daí, pelo item 2 do Teorema 6.2, tem-se $A \odot C \subset B \odot C$.

3. Pelo item 1, temos que $A \oplus (\ominus A) \subset B \oplus (\ominus A)$. Daí, pelo Teorema 6.3, $Z(0) \subset B \oplus (\ominus A)$. Agora, como $C \subset Z(0)$, pela Observação 6.2, $Z(0) \subset \ominus C$. Da Observação 6.3 e pelo Teorema 6.6, temos

$$Z(0) \subset (B \oplus (\ominus A)) \odot (\ominus C) = (B \odot (\ominus C)) \oplus ((\ominus A) \odot (\ominus C)),$$

novamente usando o item 1, obtemos

$$Z(0) \oplus (B \odot C) \subset ((B \odot (\ominus C)) \oplus ((\ominus A) \odot (\ominus C))) \oplus (B \odot C),$$

usando o item 1 e item 3 do Teorema 6.2, temos

$$B \odot C \subset (((\ominus A) \odot (\ominus C)) \oplus (B \odot (\ominus C))) \oplus (B \odot C),$$

daí, pelo item 2 do Teorema 6.2, tem-se

$$B \odot C \subset ((\ominus A) \odot (\ominus C)) \oplus ((B \odot (\ominus C)) \oplus (B \odot C)),$$

e, usando o item 1 do Teorema 6.4,

$$B \odot C \subset ((\ominus A) \odot (\ominus C)) \oplus (((\ominus C) \odot B) \oplus (C \odot B)),$$

assim, pelo Teorema 6.6 tem-se

$$B \odot C \subset ((\ominus A) \odot (\ominus C)) \oplus (((\ominus C) \oplus C) \odot B),$$

logo pelo Teorema 6.3,

$$B \odot C \subset ((\ominus A) \odot (\ominus C)) \oplus (Z(0) \odot B),$$

e, como por definição de produto, $Z(0) \odot B = Z(0)$ e $(\ominus A) \odot (\ominus C) = A \odot C$, temos

$$B \odot C \subset (A \odot C) \oplus Z(0),$$

daí, pelo item 3 do Teorema 6.2, obtemos $B \odot C \subset A \odot C$. ■

Proposição 6.5 [Proposição 3.20 em (MOREIRA; CABRAL, 2021)] A função Z é injetiva. Além disso Z é um **homomorfismo** de corpos ordenados, isto é, para todo $p, q \in \mathbb{Q}$, temos:

1. $p \leq q$ se, e só se, $Z(p) \subset Z(q)$;
2. $Z(p + q) = Z(p) \oplus Z(q)$;
3. $Z(p \cdot q) = Z(p) \odot Z(q)$.

Demonstração. Primeiramente vamos mostrar que Z é injetiva. Sejam $m, n \in \mathbb{Q}$ tais que $Z(m) = Z(n)$. Suponha que $m \neq n$, logo ou $m > n$ ou $m < n$. Se $n < m$, temos que

$$n < \frac{m+n}{2} < m$$

logo $\frac{m+n}{2} \in Z(m)$, mas $\frac{m+n}{2} \notin Z(n)$, daí $Z(m) \neq Z(n)$, o que contradiz $Z(m) = Z(n)$. Se $m < n$, temos que

$$m < \frac{m+n}{2} < n$$

logo $\frac{m+n}{2} \in Z(n)$, mas $\frac{m+n}{2} \notin Z(m)$, assim $Z(m) \neq Z(n)$ o que contradiz $Z(m) = Z(n)$. Portanto, $m = n$. Logo, Z é injetiva.

1. Se $p \leq q$. Seja $x \in Z(p)$ logo $x < p$ e como $p \leq q$ tem-se $x < q$ daí $x \in Z(q)$. Portanto, $Z(p) \subset Z(q)$. Reciprocamente, se $Z(p) \subset Z(q)$. Suponha, por absurdo, que $q < p$ daí $Z(q) \subset Z(p)$ e como $Z(p) \subset Z(q)$ temos que $Z(p) = Z(q)$. Agora, como Z é injetiva, obtemos que $p = q$, o que contradiz $q < p$. Portanto, $p \leq q$.
2. Seja $r \in Z(p+q)$, então $r < p+q$. Daí, $r-p-q < 0$. Assim, temos que

$$m = p + \frac{r-p-q}{2} < p \quad \text{e} \quad n = q + \frac{r-p-q}{2} < q$$

daí, $m \in Z(p)$ e $n \in Z(q)$. Além disso, tem-se que

$$r = \left(p + \frac{r-p-q}{2} \right) + \left(q + \frac{r-p-q}{2} \right) = m + n \in Z(p) \oplus Z(q).$$

Portanto,

$$Z(p+q) \subset Z(p) \oplus Z(q). \quad (6.36)$$

Reciprocamente, seja $r \in Z(p) \oplus Z(q)$ logo existem $m \in Z(p)$ e $n \in Z(q)$ tais que $r = m+n$. Como $m < p$ e $n < q$, pela monotonicidade da adição em \mathbb{Q} , tem-se $r = m+n < p+q$, logo $r \in Z(p+q)$. Portanto,

$$Z(p) \oplus Z(q) \subset Z(p+q). \quad (6.37)$$

De (6.36) e (6.37), obtemos $Z(p) \oplus Z(q) = Z(p+q)$.

3. Suponhamos inicialmente que $p \geq 0$ e $q \geq 0$. Daí, $Z(0) \subset Z(p) \cap Z(q)$. Seja $r \in Z(p \cdot q)$ logo $r < p \cdot q$. Se $r < 0$ então $r \in Z(0)$, assim pela Observação 6.3,

$Z(0) \subset Z(p) * Z(q)$. Logo, $r \in Z(p) * Z(q)$. Se $r \geq 0$, como $r \in Z(p \cdot q)$, temos que $0 \leq r < p \cdot q$, logo $p \cdot q > 0$, daí $p > 0$ e $q > 0$. Consideremos $s = \frac{r + p \cdot q}{2}$, logo tem-se $r < s < p \cdot q$. Observe agora que podemos escrever r da seguinte maneira

$$r = \left(p \cdot \frac{r}{s}\right) \cdot \left(q \cdot \frac{s}{p \cdot q}\right),$$

como $\frac{r}{s} < 1$ e $\frac{s}{p \cdot q} < 1$, temos $0 \leq p \cdot \frac{r}{s} < p$, logo $p \cdot \frac{r}{s} \in Z(p)$, e também temos $0 \leq q \cdot \frac{s}{p \cdot q} < q$, logo $q \cdot \frac{s}{p \cdot q} \in Z(q)$. Daí, $r \in Z(p) * Z(q)$. Portanto, em qualquer caso,

$$Z(p \cdot q) \subset Z(p) * Z(q) \quad (6.38)$$

Reciprocamente, seja $r \in Z(p) * Z(q)$. Se $r < 0$, daí $r < 0 \leq p \cdot q$ então $r < p \cdot q$. Logo $r \in Z(p \cdot q)$. Se $r \geq 0$, como $r \in Z(p) * Z(q)$, existem $m \in Z(p)$, $n \in Z(q)$, $m \geq 0$ e $n \geq 0$ tais que $r = m \cdot n$. Como $0 \leq m < p$ e $0 \leq n < q$, pela monotonicidade da multiplicação em \mathbb{Q} , $r = m \cdot n < p \cdot q$, assim $r \in Z(p \cdot q)$. Concluimos, em qualquer caso,

$$Z(p) * Z(q) \subset Z(p \cdot q) \quad (6.39)$$

De (6.37) e (6.38) temos a igualdade.

Vamos mostrar os outros casos. Se $p < 0$ e $q < 0$. Daí, tem-se que $-p > 0$ e $-q > 0$, assim temos que $Z(0) \subset Z(-p)$ e $Z(0) \subset Z(-q)$, logo $Z(0) \subset Z(-p) \cap Z(-q)$, e usando o caso anterior, temos que

$$Z(-p) * Z(-q) = Z((-p) \cdot (-q)) = Z(p \cdot q). \quad (6.40)$$

Por outro lado, note que $\ominus Z(a) = Z(-a)$ para qualquer $a \in \mathbb{Q}$. De fato, pelo item 2 temos que

$$Z(0) = Z(a + (-a)) = Z(a) \oplus Z(-a)$$

e, pela unicidade o elemento inverso aditivo, temos que $Z(-a) = \ominus Z(a)$.

Agora, como $Z(p), Z(q) \subset Z(0)$ e pela definição de produto, obtemos

$$Z(p) \odot Z(q) = |Z(p)| * |Z(q)| = (\ominus Z(p)) * (\ominus Z(q)) = Z(-p) * Z(-q) = Z(p \cdot q).$$

Agora vejamos o caso $p \geq 0$ e $q < 0$. Daí, $-q > 0$, assim temos que $Z(0) \subset Z(p)$ e $Z(0) \subset Z(-q)$. Logo, $Z(0) \subset Z(p) \cap Z(-q)$. Assim, como $Z(0) \subset Z(p)$ e $Z(q) \subset Z(0)$

e pela definição de produto, tem-se

$$\begin{aligned} Z(p) \odot Z(q) &= \ominus(Z(p) * |Z(q)|) = \ominus(Z(p) * (\ominus Z(q))) \\ &= \ominus(Z(p) * Z(-q)) = \ominus Z(p \cdot (-q)) \\ &= \ominus Z(-(p \cdot q)) = \ominus(\ominus Z(p \cdot q)) = Z(p \cdot q). \end{aligned}$$

Finalmente, se $p < 0$ e $q \geq 0$. Pelo item 1 do Teorema 6.4, o caso anterior e comutatividade em \mathbb{Q} , obtemos

$$Z(p) \cdot Z(q) = Z(q) \cdot Z(p) = Z(q \cdot p) = Z(p \cdot q).$$

Portanto, Z é homomorfismo de corpos ordenados. ■

Definição 6.9 Seja $\Gamma \subset \Omega$, não vazio. Se existir $S \in \Omega$ que seja a menor cota superior de Γ , isto é,

- (i) $A \subset S$ para todo $A \in \Gamma$;
- (ii) se R é cota superior de Γ , então $S \subset R$;

então dizemos que S é *supremo (finito)* de Γ , e escrevemos $\sup \Gamma = S$. Quando Γ é ilimitado superiormente (não existe cota superior para Γ), dizemos que o *supremo* de Γ é mais infinito e escrevemos $\sup \Gamma = +\infty$.

Exemplo 6.2 [Exemplo 3.2 em (MOREIRA; CABRAL, 2021)] Seja $\Gamma = \{A \in \Omega; A \subset Z(0)\}$. Então $Z(0)$ é o supremo de Γ .

De fato, seja $A \in \Gamma$, então $A \subset Z(0)$. Portanto, $A \subset Z(0)$, para todo $A \in \Gamma$. Assim, Γ é limitado superiormente por $Z(0) \in \Omega$. Por outro lado, se $M \in \Omega$ é cota superior de Γ , então

$$A \subset M, \text{ para todo } A \in \Gamma. \tag{6.41}$$

Note que $Z(0) \in \Omega$ e $Z(0) \subset Z(0)$, logo $Z(0) \in \Gamma$. Em particular, em (6.41), tem-se $Z(0) \subset M$. Portanto, pela Definição 6.9, $Z(0)$ é a menor cota superior de Γ . Assim, $Z(0)$ é o supremo de Γ .

Teorema 6.8 [Teorema 3.22 em (MOREIRA; CABRAL, 2021)] O corpo ordenado $\langle \Omega, \oplus, \odot, \subset \rangle$ é *completo*, isto é, todo subconjunto de Ω não vazio e limitado superiormente tem supremo finito.

Demonstração. Seja $\Gamma \subset \Omega$ não vazio e limitado superiormente. Consideremos, $S = \bigcup_{A \in \Gamma} A$. Claramente, $A \subset S$, para todo $A \in \Gamma$. Seja $M \in \Omega$ tal que M é cota superior de Γ , então $A \subset M$, para todo $A \in \Gamma$. Logo,

$$S = \bigcup_{A \in \Gamma} A \subset M.$$

Só nos resta provar que $S \in \Omega$. Primeiramente, vamos mostrar (i) da Definição 6.1: $S \neq \emptyset$ e $S^c \neq \emptyset$. De fato, como $\Gamma \neq \emptyset$, existe $A \in \Gamma \subset \Omega$ logo A é corte, então $A \neq \emptyset$ e, existe $p \in A$. Agora, como $A \in \Gamma$ temos que $A \subset S$ e, como $p \in A$, daí $p \in S$, assim temos $S \neq \emptyset$. Por outro lado, como $\Gamma \subset \Omega$ é limitado superiormente, então existe $M \in \Omega$ cota superior de Γ . Pelo visto anteriormente, $S \subset M$ logo $M^c \subset S^c$ e, como $M \in \Omega$ então $M^c \neq \emptyset$, daí $S^c \neq \emptyset$.

Vamos mostrar (ii) da Definição 6.1: Se $p \in S$, $q \in \mathbb{Q}$ e $q < p$, então $q \in S$. De fato, como $p \in S = \bigcup_{A \in \Gamma} A$, então existe $A \in \Gamma$ tal que $p \in A$. Como $A \in \Gamma \subset \Omega$ temos que A é corte e, como $q < p$ com $q \in \mathbb{Q}$, por (ii) da Definição 6.1, $p \in A$ então $q \in A$, logo $q \in S$. Finalmente, vamos mostrar (iii) da Definição 6.1: Se $p \in S$, então existe $q \in S$ tal que $p < q$. De fato, como $p \in S = \bigcup_{A \in \Gamma} A$, então existe $A \in \Gamma$ tal que $p \in A$ e, como A é corte, por (iii) da Definição 6.1, existe $q \in A$ tal que $p < q$, logo $q \in S$. Portanto S é corte. ■

Desta maneira concluímos nosso trabalho de mostrar que $\langle \Omega, \oplus, \odot, \subset \rangle$ é um corpo ordenado completo. Agora, vamos mudar as notações e nomenclaturas. Mudando para notações familiares, um corte será chamado de *número real*, o conjunto Ω passa a ser denotado por \mathbb{R} e será chamado de *conjunto dos números reais*. Os símbolos \oplus e \odot serão substituídos por $+$ e \cdot , respectivamente. Em relação ao ordem nos cortes, passamos a escrever $x \leq y$ ao invés de $x \subset y$. Observamos que, rigorosamente falando, um número racional não é número real. De fato, um número racional é um elemento do conjunto \mathbb{Q} , enquanto que um número real é um subconjunto de \mathbb{Q} . No entanto, através da função Z (Definição 6.2) passamos de um número racional r ao número real $Z(r)$. Sendo Z injetiva (Proposição 6.5) temos que o conjunto $Z(\mathbb{Q})$ é um subconjunto de \mathbb{R} que é uma espécie de “cópia” ou “clone” de \mathbb{Q} . Esta noção é estabelecida matematicamente pelo fato de Z ser um homomorfismo injetivo (ver proposição 6.5). Por esta razão, podemos, e faremos, os seguintes abusos de notação e de linguagem: “ $\mathbb{Q} \subset \mathbb{R}$ ” ou “todo número racional é número real”. E ainda, $Z(0)$ passa a ser denotado como 0 e $Z(1)$ passa a ser denotado como 1 , e assim por diante.

7 CONSIDERAÇÕES FINAIS

Neste trabalho, apresentamos os conjuntos dos números inteiros e dos números racionais, a partir da axiomatização do conjunto dos números naturais. Também, apresentamos os números reais através dos cortes de Dedekind, partindo da axiomatização do conjunto dos números racionais. A construção dos números naturais por meio do axioma de Dedekind trouxe a existência deste conjunto, assegurando que sempre existe um sucessor para cada número natural. Garantindo que a adição, subtração e multiplicação entre dois números naturais resultam em outro número natural, assim o conjunto dos números naturais é fechado em relação a essas operações. Um resultado essencial da construção dos números naturais é o princípio de indução, permitindo fazer afirmações válidas para todos os números naturais e ordenação total entre os números naturais, o que significa que é possível comparar e ordenar qualquer par de números naturais.

A construção dos números inteiros por meio de classes de equivalência ofereceu uma abordagem precisa e rigorosa para ampliar o conjunto dos números naturais. Essa construção estabelece a estrutura algébrica dos números inteiros, permitindo a realização de operações. Além disso, os números inteiros formam um anel, o que significa que as operações de adição e multiplicação são fechadas e obedecem a várias propriedades fundamentais, como associatividade, comutatividade e existência de elemento neutro.

A construção dos números racionais por meio de classes de equivalência é um processo que permite a inclusão de frações no sistema numérico, nota-se que a estrutura algébrica do conjunto dos racionais obedecem a várias propriedades algébricas, como associatividade, comutatividade, existência de elemento neutro e inverso.

A construção dos números reais feita por Richard Dedekind de forma rigorosa baseia-se no conceito de divisão do conjunto dos números racionais em duas partes e na identificação de um número real como um “corte” entre essas partes. Uma das principais conclusões da construção dos números reais via cortes de Dedekind é a obtenção de um conjunto numérico que é completo e ordenado. Isso significa que as operações estão definidas e obedecem a todas as propriedades algébricas e

ordenadas esperadas. A completude dos números reais significa que não há lacunas no conjunto, ou seja, qualquer sequência de números reais que esteja “aproximando-se” de um valor limite tem esse limite pertencente ao conjunto dos números reais.

E por fim, após toda essa construção numérica, no final de cada capítulo, observa-se a imersão dos conjuntos dos números naturais no conjunto dos números inteiro, a imersão do conjunto dos números inteiros para o conjunto dos números racionais e finalmente a imersão do conjunto dos números racionais para o conjunto dos números reais.

REFERÊNCIAS

BOYER, C. B. ***História da Matemática***. 3. ed. São Paulo: Editora Edgar Blucher Ltda., 2012.

COHEN, L. W.; EHRLICH, G. ***The Structure of the Real Number System***. 1. ed. New York: Van Nostrand Reinhold Company, 1963.

GUNDLACH, B. H. ***Tópicos de História da Matemática para uso em sala de aula: números e numerais***. 1. ed. São Paulo: Atual Editora, 1992.

IFRAH, G. ***OS NÚMEROS, a história de uma grande invenção***. 4. ed. Rio de Janeiro: Editora Globo, 1989.

LIMA, E. L. ***Análise Real***. 12. ed. Rio de Janeiro: Coleção Matemática Universitária - IMPA, 2014.

MOREIRA, C. N.; CABRAL, M. A. P. ***Curso de Análise Real***. 2. ed. Rio de Janeiro: Editora Instituto de Matemática, 2021.