

Dos números naturais aos números reais

Reinaldo Viana da Costa

Dissertação de Mestrado do Programa de Mestrado Profissional
em Matemática em Rede Nacional (PROFMAT)

SERVIÇO DE PÓS-GRADUAÇÃO DO ICMC-USP

Data de Depósito:

Assinatura: _____

Reinaldo Viana da Costa

Dos números naturais aos números reais

Dissertação apresentada ao Instituto de Ciências Matemáticas e de Computação - ICMC-USP, como parte dos requisitos para obtenção do título de Mestre em Ciências – Mestrado Profissional em Matemática em Rede Nacional. *VERSÃO REVISADA*

Area de Concentração : Mestrado Profissional em Matemática em Rede Nacional

Orientador : Prof. Dr. Hermano de Souza Ribeiro

**USP - São Carlos
Abril de 2019**

Ficha catalográfica elaborada pela Biblioteca Prof. Achille Bassi
e Seção Técnica de Informática, ICMC/USP,
com os dados inseridos pelo(a) autor(a)

C837n Costa, Reinaldo Viana
Dos números naturais aos números reais /
Reinaldo Viana Costa; orientador Hermano de Souza
Ribeiro. -- São Carlos, 2018.
113 p.

Dissertação (Mestrado - Programa de Pós-Graduação
em Mestrado Profissional em Matemática em Rede
Nacional) -- Instituto de Ciências Matemáticas e de
Computação, Universidade de São Paulo, 2018.

1. Conjuntos numéricos. 2. Números naturais. 3.
Números reais. 4. Axiomas de Peano. 5. Cortes de
Dedekind. I. Ribeiro, Hermano de Souza, orient. II.
Título.

Reinaldo Viana da Costa

From natural numbers to real numbers

Master dissertation submitted to the Institute of Mathematics and Computer Sciences - ICMC-USP, in partial fulfillment of requirements for the degree of Mathematics Professional Master's Program.

Concentration Area: Professional Master Degree Program in Mathematics in National Network

Advisor: Prof. Dr. Hermano de Souza Ribeiro

**USP - São Carlos
April 2019**

*À minha esposa Inaura, presente
em todos os momentos dessa
caminhada.*

Agradecimentos

Aos meus pais, Salvador e Benedicta, por me ensinarem os primeiros passos dessa jornada.

Ao meu professor e orientador Prof. Dr. Hermano de Souza Ribeiro, pela dedicação na orientação desse trabalho e por todas as aulas que ministrou durante o curso.

À Coordenadora do PROFMAT do ICMC-USP Profa. Dra. Ires Dias, pelo apoio em todos os momentos do curso.

A todos os professores e colegas do PROFMAT que, com seus ensinamentos e suas experiências, acrescentaram muito à minha formação.

RESUMO

COSTA R. V. Dos números naturais aos números reais. 2018. 113 p. Dissertação (Mestrado em Ciências – Mestrado Profissional em Matemática em Rede Nacional) – Instituto de Ciências Matemáticas e de Computação, Universidade de São Paulo, São Carlos – SP, 2018.

Este trabalho apresenta a construção dos conjuntos dos números naturais, inteiros, racionais e reais, buscando contemplar uma mediação entre alunos e professores do ensino médio que possa contribuir em uma abordagem facilitadora para o processo de ensino e aprendizagem. A construção dos conjuntos numéricos é feita de modo progressivo, apresentando leis e propriedades que definem cada um deles. Os capítulos apresentam teoremas que são provados de modo que o leitor possa conseguir, efetivamente, estabelecer um elo entre a teoria matemática e suas abstrações iniciais inerentes aos estudantes em formação.

Palavras-chave: Conjuntos numéricos, Números naturais, Axiomas de Peano, Números inteiros, Números racionais, Números reais, Cortes de Dedekind.

ABSTRACT

COSTA R. V. From natural numbers to real numbers. 2018. 113 p. Dissertação (Mestrado em Ciências – Mestrado Profissional em Matemática em Rede Nacional) – Instituto de Ciências Matemáticas e de Computação, Universidade de São Paulo, São Carlos – SP, 2018.

This work presents the construction of the sets of natural, integer, rational and real numbers, aiming to contemplate a mediation between high school students and teachers that can contribute to an easy approach to the teaching and learning processes. The construction of the numerical sets is done progressively presenting laws and properties that define each one of them. The chapters present theorems that are proven so that the reader can effectively establish a link between mathematical theory and its initial abstractions inherent in the students in formation.

Keywords: Numerical sets, Natural numbers, Peano axioms, Integer numbers, Rational numbers, Real numbers, Dedekind cuts.

Sumário

Introdução	17
1. O conjunto \mathbb{N} dos números naturais	21
1.1 Introdução ao conjunto dos números naturais	21
1.2 Relação de ordem em \mathbb{N}	23
1.3 Os Postulados de Peano	26
1.4 Adição no conjunto \mathbb{N} dos números naturais	27
1.5 Multiplicação no conjunto \mathbb{N} dos números naturais	30
1.6 Relação de ordem em \mathbb{N}	34
1.7 Lei da tricotomia para conjunto \mathbb{N} dos números naturais	35
1.8 Construção do conjunto \mathbb{N} pelo axioma do infinito	37
1.9 Adição no conjunto \mathbb{N} via teorema da recursão	46
1.10 Multiplicação no conjunto \mathbb{N} via teorema da recursão	48
1.11 Relação natural de ordem no conjunto $\mathbb{N} = \{ 0, 1, 2, \dots \}$	51
1.12 Relação de divisibilidade no conjunto \mathbb{N} dos números naturais	55
2 O conjunto \mathbb{Z} dos números inteiros	59
2.1 Adição no conjunto \mathbb{Z} dos números inteiros	61
2.2 Multiplicação no conjunto \mathbb{Z} dos números inteiros	63
2.3 Subtração no conjunto \mathbb{Z} dos números inteiros	66
2.4 Relação de divisibilidade no conjunto \mathbb{Z} dos números inteiros	67
2.5 Relação de ordem no conjunto \mathbb{Z} dos números inteiros	67
2.6 Inclusão do conjunto \mathbb{N} ao conjunto \mathbb{Z}	71
2.7 Três princípios de indução matemática no conjunto \mathbb{Z}	73
3. O conjunto \mathbb{Q} dos números racionais	75
3.1 Adição no conjunto \mathbb{Q} dos números racionais	76
3.2 Multiplicação no conjunto \mathbb{Q} dos números racionais	78
3.3 Subtração no conjunto \mathbb{Q} dos números racionais	82
3.4 Divisão no conjunto \mathbb{Q} dos números racionais	83
3.5 Relação de ordem no conjunto \mathbb{Q} dos números racionais	84
3.6 Inclusão do conjunto dos inteiros ao conjunto dos números racionais	85
4. O conjunto \mathbb{R} dos números reais	91
4.1 Adição no conjunto \mathbb{R} dos números reais	92

4.2	Relações de ordem em \mathbb{R}	96
4.3	Multiplicação no conjunto \mathbb{R} dos números reais	97
4.4	Equação polinomial incompleta	108
4.5	Representação decimal dos números reais	109
	Referencias	113

INTRODUÇÃO

O trabalho apresenta três construções do conjunto dos números naturais. A primeira e a mais elementar das construções pressupõe a existência do conjunto dos números naturais $\{1, 2, 3, \dots\}$ e pressupõe a existência das quatro operações aritméticas no conjunto dos números naturais, observando que a subtração e a divisão nem sempre são bem definidas no conjunto dos números naturais. Além das hipóteses de que a operação de adição e a operação de multiplicação para os números naturais possuem as propriedades associativa e comutativa, bem como a propriedade distributiva da multiplicação em relação à adição; esta construção elementar, adequada para alunos do ensino fundamental, também coloca como axiomas, o princípio da indução matemática e o axioma da tricotomia.

O axioma da tricotomia permite esclarecer a seguinte questão para o conjunto dos números naturais: Se a, b e c fossem números naturais e $a + c = b + c$, como justificar que $a = b$? O axioma da tricotomia permite esclarecer também outra questão: Se a, b e c fossem números naturais com ac igual a bc , como justificar que $a = b$? O axioma da tricotomia permite ao leitor interessado a justificativa dessas duas questões que são chamadas a lei do cancelamento para a operação de adição e lei do cancelamento para operação de multiplicação de números naturais.

A segunda construção, mais sofisticada e talvez adequada para alunos de graduação em matemática, é feita a partir dos cinco postulados de Peano, e em um dos quais é introduzido o conceito de número natural sucessor imediato assim como as suas propriedades. O quinto axioma de Peano é o princípio da indução matemática, que é o mesmo princípio que aparece na introdução mais elementar. Através dos axiomas de Peano, a adição de números naturais é agora definida e também a operação de multiplicação de números naturais. Pela utilização do princípio da indução matemática, são demonstradas as propriedades associativa e comutativa das operações de adição e multiplicação de números naturais bem como a propriedade distributiva da operação de multiplicação em relação à operação de adição. Além disso, é demonstrada a lei da tricotomia cujas consequências são as leis do cancelamento da adição da multiplicação para o conjunto dos números naturais.

A terceira construção do conjunto dos números naturais é feita a partir do axioma do infinito. Nos postulados de Peano a existência dos números naturais era feita por hipótese. Agora não, os números naturais são construídos e são conjuntos. A partir do teorema da recursão são definidas, mais uma vez, as operações de adição e multiplicação de números

naturais. O conjunto dos números naturais admite uma infinidade de relações de ordem total, mas apenas uma delas é compatível com as operações de adição e multiplicação.

O capítulo da construção dos números naturais contempla, ainda, o princípio da boa ordenação, o teorema fundamental da aritmética e a propriedade arquimediana do conjunto dos números naturais.

Os números inteiros são construídos a partir do conjunto dos números naturais $\mathbb{N} = \{ 0, 1, 2, \dots \}$. Alguns autores não consideram o zero como número natural, dado que o número zero foi definido quase um milênio após a construção dos números naturais $\{ 1, 2, 3, \dots \}$. A construção do conjunto dos números inteiros a partir do conjunto dos números naturais $\{ 1, 2, 3, \dots \}$ é análoga à construção feita a partir de \mathbb{N} . Os números inteiros são definidos como classes de equivalências de uma relação binária de equivalência definida no conjunto produto cartesiano $\mathbb{N} \times \mathbb{N}$, não importando se o conjunto dos números naturais inicia com 0 ou inicia com 1. As operações de adição, de multiplicação e mesmo a relação de ordem são definidas através dos representantes das classes de equivalências, independentemente dos representantes escolhidos. A lei da tricotomia justifica a lei do cancelamento da multiplicação no conjunto dos números inteiros.

O capítulo da construção dos números inteiros apresenta, também, três princípios de indução matemática. A introdução à construção do conjunto dos números inteiros é uma prévia mais elementar da construção do conjunto dos números racionais objeto do capítulo seguinte.

O conjunto dos números racionais é construído a partir do conjunto dos números inteiros. Os números racionais são classes de equivalência de uma relação de equivalência definida no conjunto dos números inteiros. As operações de adição, de multiplicação e a relação de ordem são definidas através dos representantes dos números racionais que são classes de equivalência, independentemente dos representantes escolhidos. A relação de ordem natural no conjunto dos números racionais é compatível com as operações de adição e de multiplicação, e qualquer outra relação de ordem total no conjunto dos números racionais compatível com as operações de adição e multiplicação coincide com a relação de ordem natural.

O capítulo da construção dos números racionais mostra que nem sempre subconjuntos dos números racionais limitados superiormente admitem supremo, isto é, o conjunto dos números racionais não é um conjunto completo, diferentemente do conjunto dos números reais construídos no capítulo seguinte.

Os números reais são construídos a partir do conjunto dos números racionais com a definição dos cortes de Dedekind. Um número real é um conjunto de números racionais diferente do vazio e do próprio conjunto dos números racionais com duas propriedades adicionais: dado um elemento deste conjunto, todo número racional menor do que ele pertence ao conjunto, e dado um elemento do conjunto, existe sempre um outro elemento do mesmo conjunto que é o maior do que o elemento dado. São definidas as operações de adição, multiplicação e subtração, assim como a relação de ordem total. O teorema do completamento do conjunto dos números reais e uma breve digressão sobre a representação decimal infinita de um número real finalizam o capítulo.

1. O CONJUNTO \mathbb{N} DOS NÚMEROS NATURAIS

Este capítulo apresenta três construções para os números naturais.

1.1 O CONJUNTO $\mathbb{N} = \{ 1, 2, 3, \dots \}$ DOS NÚMEROS NATURAIS : UMA INTRODUÇÃO ELEMENTAR.

Uma introdução elementar do conjunto $\mathbb{N} = \{ 1, 2, 3, \dots \}$ dos números naturais consiste em axiomatizar a sua existência assim como a existência das operações binárias internas de adição e de multiplicação definidas para todos os elementos de \mathbb{N} e elencar as propriedades da adição e da multiplicação como segue.

O conjunto $\mathbb{N} = \{ 1, 2, 3, \dots \}$ dos números naturais é um conjunto fechado em relação às operações binárias internas de adição e de multiplicação no sentido de que dados dois números naturais a e b , a soma $a + b$ de a e b nesta ordem e o produto ab de a e b nesta ordem são números naturais e são válidos os seguintes postulados.

Dados os números naturais a , b e c , valem as propriedades:

$$N1) (a + b) + c = a + (b + c) \quad \text{propriedade associativa da adição}$$

$$N2) (ab)c = a(bc) \quad \text{propriedade associativa da multiplicação}$$

$$N3) a + b = b + a \quad \text{propriedade comutativa da adição}$$

$$N4) ab = ba \quad \text{propriedade comutativa da multiplicação}$$

N5) $a(b + c) = ab + ac$ propriedade distributiva da operação de multiplicação em relação a operação de adição.

N6) Existência do elemento neutro para a operação de multiplicação: o número natural 1 tem a propriedade de que para cada número natural a

$$1a = a.$$

N7) Axioma da tricotomia: dados números naturais a e b , uma e exatamente uma das afirmações é verdadeira:

$$(1) \quad a + x = b \text{ para algum número natural } x$$

$$(2) \quad a = b$$

$$(3) \quad a = b + y \text{ para algum número natural } y$$

N8) Princípio da indução matemática

Seja um subconjunto A de \mathbb{N} com as propriedades

$$(1) \quad 1 \in A$$

(2) Se $n \in A$ então $n + 1 \in A$

Então $A = \mathbb{N}$.

O axioma da tricotomia é uma ferramenta adequada na demonstração da lei do cancelamento da operação de adição.

TEOREMA 1.1.1 LEI DO CANCELAMENTO DA OPERAÇÃO DE ADIÇÃO

(a) Dados os números naturais a , b e c ,

se $a + c = b + c$ então $a = b$

(b) Dados os números naturais a , b e c ,

se $c + a = c + b$ então $a = b$

(c) Dados os números naturais a , b e c ,

se $a + c = c + b$ então $a = b$.

Prova (a)

Pelo axioma da tricotomia, apenas uma e somente uma afirmação abaixo é verdadeira:

(1) Existe um número natural d tal que $a = b + d$

(2) Existe um número natural e tal que $d = a + e$

(3) $a = b$

No caso (1), $a = b + d$ para algum número natural d . Da hipótese,

$$a + c = b + c$$

por substituição

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

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

pela associatividade e pela comutatividade da adição de números naturais

$$\text{Então, } b + c = b + c$$

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

o que contraria o axioma da tricotomia.

Como o caso (2) é análogo ao caso (1), resta $a = b$.

Os casos (b) e (c) são provados a partir do caso (a) utilizando a comutatividade da adição de números naturais.

O axioma da tricotomia também é utilizado na demonstração da lei do cancelamento da operação de multiplicação.

TEOREMA 1.1.2 LEI DO CANCELAMENTO DA OPERAÇÃO DE MULTIPLICAÇÃO.

(a) Dados os números naturais a , b e c ,

se $ac = bc$, então $a = b$.

(b) Dados os números naturais a , b e c ,

se $ca = cb$, então $a = b$.

Prova (a)

Caso exista um número natural d tal que $a = b + d$, e pela hipótese de que $ac = bc$, por substituição, segue que:

$$(b + d)c = bc$$

e pela distributividade da multiplicação em relação a adição

$$bc + dc = bc$$

$$\text{Então } bc = bc$$

$$bc + dc = bc$$

o que contraria o axioma da tricotomia.

Como o caso em que $b = a + d$ para algum número natural d é análogo, resta apenas o caso $a = b$.

A prova de (b) é consequência lógica da prova de (a) pela comutatividade da multiplicação de números naturais,

Consequência: O número natural 1 é o único número natural com a propriedade de que: $a1 = a$ para cada número natural a .

Caso existam um número natural x e um número natural a de modo que

$$ax = a = a1,$$

pela lei do cancelamento da multiplicação, $x = 1$.

1.2 A RELAÇÃO DE ORDEM EM $\mathbb{N} = \{1, 2, 3, \dots\}$.

Dados os números naturais m, n diz-se que m é menor do que n , e escreve-se $m < n$, para significar que existe $p \in \mathbb{N}$ tal que $n = m + p$. Neste caso, diz-se, também, que n é maior do que m e escreve-se $n > m$ para exprimir que se tem $m < n$. A notação $m \leq n$ significa que $m < n$ ou $m = n$. Por definição, tem-se, portanto, $m < m + p$, para

quaisquer $m, p \in \mathbb{N}$. Em particular, $m < m + 1$. Segue-se que $1 < n$ para todo número natural $n \neq 1$. Esta afirmação pode ser provada pelo princípio da indução matemática, definindo $A = \{ n \in \mathbb{N} : n = 1 \text{ ou } n > 1 \}$.

O número natural a é menor ou igual ao número natural b ou o número natural b é maior ou igual ao número natural a (em símbolos, $a \leq b$ ou $b \geq a$) tem o significado de que ou $a = b$ ou $a < b$.

A relação de ordem natural \leq no conjunto dos números naturais goza das seguintes propriedades (de verificação imediata)

- (a) reflexiva: para cada número natural a , $a \leq a$
- (b) antissimétrica: dados os números naturais a e b , se $a \leq b$ e se $b \leq a$ então $a = b$
- (c) transitiva: dados os números naturais a , b , c , se $a \leq b$ e se $b \leq c$ então $a \leq c$.

TEOREMA 1.2.1 LEI DA TRICOTOMIA

Dados os números naturais a e b , uma e uma só das seguintes afirmações é verdadeira:

- (1) $a < b$ (2) $a = b$ (3) $a > b$

Prova: Imediata a partir do axioma da tricotomia.

Os resultados seguintes são de demonstração imediata.

TEOREMA 1.2.2 COMPATIBILIDADE DA RELAÇÃO DE ORDEM COM A OPERAÇÃO DE ADIÇÃO E COM A OPERAÇÃO DE MULTIPLICAÇÃO.

Dados os números naturais a , b , c e d .

- (a) Se $a < b$, então $a + c < b + c$ e $c + a < c + b$.
- (b) Se $a < b$ e se $c < d$, então $a + c < b + d$.
- (c) Se $a + c < b + c$ ou se $c + a < c + b$, então $a < b$.
- (d) Se $a + b < c + d$ e se $c \leq a$, então $b < d$.
- (e) Se $a < b$, então $ac < bc$ e $ca < cb$.
- (f) Se $a < b$ e se $c < d$, então $ac < bd$.
- (g) Se $ac < bc$ ou se $ca < cb$, então $a < b$.
- (h) Se $ab < cd$ e se $c \leq a$, então $b < d$.

Prova (c)

Da hipótese $c + a < c + b$, existe um número natural d tal que

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

ou

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

pela associatividade da adição de números naturais e, então,

$$a + d = b$$

pela lei do cancelamento da operação de adição e que é a definição de $a < b$.

Prova (g)

Da hipótese $ca < cb$, segue a existência de um número natural d tal que

$$ca + d = cb$$

caso $a = b$,

$$ca = ca$$

$$ca + d = ca \text{ ou } ca < ca$$

o que contraria o axioma da tricotomia

caso $a > b$, existe um número e tal que

$$a = b + e$$

e da igualdade $ca + d = cb$ por substituição

$$c(b + e) + d = cb$$

ou

$$cb + (ce + d) = cb$$

o que resulta que

$$cb = cb$$

$$cb < cb$$

o que é contrária o axioma da tricotomia.

Resta apenas então $a < b$.

TEOREMA 1.2.3 Se a é um número natural, então não existe um número natural b tal que $a < b < a + 1$.

Prova

Caso exista um número natural b tal que $a < b < a + 1$, como $a < b$, existe um número natural x tal que $b = a + x$ e, como $b < a + 1$, existe um número y tal que $a + 1 = b + y$. Assim $a + x + y = a + 1$. Pela lei do cancelamento da adição, $x + y = 1$ o que significa que $x < 1$. Isto é uma contradição. Portanto, não existe um número natural b tal que $a < b < a + 1$.

1.3 O CONJUNTO \mathbb{N} DOS NÚMEROS NATURAIS: UMA CONSTRUÇÃO ATRAVÉS DOS POSTULADOS DE PEANO.

O conjunto de postulados mais conhecido para a construção de números naturais foi publicado pelo matemático italiano Giuseppe Peano em 1889.

Uma redação dos cinco postulados de Peano é a seguinte:

Existe o conjunto \mathbb{N} dos números naturais com as seguintes propriedades:

P1) $1 \in \mathbb{N}$, isto é, 1 é um número natural.

P2) Para cada número natural n , existe e é único o número natural n^+ sucessor do número natural n .

P3) Dados os números naturais m e n com a propriedade de que os sucessores de m e de n são iguais, isto é, se

$$m^+ = n^+$$

então

$$m = n$$

P4) O número natural 1 não é sucessor de nenhum número natural.

P5) Princípio da indução matemática.

Seja A um subconjunto de \mathbb{N} com as propriedades

$$(1) \quad 1 \in A;$$

$$(2) \quad \text{Se } n \in A, \text{ então } n^+ \in A.$$

Então $A = \mathbb{N}$.

Definição 1.3.1

O número natural 2 é definido como o sucessor do número natural 1.

O número natural 3 é definido como o sucessor do número natural 2.

O número natural 4 é definido como o sucessor do número natural 3.

E assim por diante para os demais números naturais.

1.4 A OPERAÇÃO DE ADIÇÃO NO CONJUNTO \mathbb{N} DOS NÚMEROS NATURAIS:

A partir dos postulados de Peano, a adição de números naturais é, agora, definida e não é mais um axioma.

A operação de adição no conjunto dos números naturais é uma operação binária que associa a cada par ordenado de números naturais o número natural soma dos números naturais do par ordenado dado (pelo teorema abaixo, a soma de dois números naturais é um número natural).

Para cada número natural n , o número natural soma $n + 1$ das parcelas n e 1 nesta ordem é definido como o número natural sucessor do número natural n , isto é,

$$n + 1 = n^+$$

Dados números naturais m e n , definido o número natural soma $m + n$ das parcelas m e n nesta ordem, o número natural soma $m + n^+$ das parcelas m e n^+ nesta ordem é definido como o número natural sucessor do número natural soma das parcelas m e n nesta ordem, isto é,

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

TEOREMA 1.4.1 A operação binária interna fechada de adição de números naturais é bem definida: dados números naturais m e n , existe o número natural soma $m + n$ das parcelas m e n nesta ordem.

Prova

Fixado um número natural m , seja $A = \{ n \in \mathbb{N} : m + n \in \mathbb{N} \}$. Então,

(1) $1 \in A$ porque $m + 1 = m^+$, o sucessor natural do número natural m cuja existência é assegurada pelos postulados de Peano.

(2) Hipótese de indução: se $n \in A$ então, por hipótese, existe o número natural soma $m + n$ das parcelas m e n . O objetivo é mostrar que $n^+ \in A$, ou seja, é provar a existência do número natural soma $m + (n^+)$ das parcelas m e n^+ . Para tanto, por definição

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

que é o número natural $(m + n)^+$ sucessor do número natural soma $m + n$ cuja existência é garantida pela hipótese de indução.

TEOREMA 1.4.2 PROPRIEDADE ASSOCIATIVA RESTRITA PARA A OPERAÇÃO DE ADIÇÃO

Dados dois números naturais a e b , vale a igualdade:

$$(a + b) + 1 = a + (b + 1)$$

Prova

Para números naturais a e b , $a + b^+ = a + (b + 1) = (a + b)^+ = (a + b) + 1$.

TEOREMA 1.4.3 PROPRIEDADE ASSOCIATIVA DA OPERAÇÃO DE ADIÇÃO.

Dados números naturais a , b e c .

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

Prova

Fixados os números naturais dados a e b , seja

$$A = \{ n \in \mathbb{N} : (a + b) + n = a + (b + n) \}.$$

Então:

i) $1 \in A$, porque pelo teorema da associatividade restrita à operação de adição

$$(a + b) + 1 = a + (b + 1)$$

ii) Se $n \in A$ por hipótese $(a + b) + n = a + (b + n)$ e o objetivo é mostrar que $n^+ \in A$

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

Em conclusão, se $n \in A$ então $n^+ \in A$ e, pelo princípio da indução matemática, $A = \mathbb{N}$ e a propriedade associativa da adição é válida para os números naturais.

TEOREMA 1.4.4 PROPRIEDADE COMUTATIVA DA OPERAÇÃO DE ADIÇÃO.

Dados dois números naturais a e b ,

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

A prova necessita do seguinte lema.

LEMA 1.4.1

Dado um número natural a ,

$$a + 1 = 1 + a.$$

Prova

Seja $A = \{ n \in \mathbb{N} : n + 1 = 1 + n \}$,

Então:

- i) $1 \in A$ porque $1 + 1 = 1 + 1$
- ii) se $n \in A$ por hipótese $n + 1 = 1 + n$ e o objetivo é mostrar que $n^+ \in A$.

$$\begin{aligned} n^+ + 1 &= \\ &= (n + 1) + 1 = \\ &= (1 + n) + 1 = \text{(porque } n \in A) \\ &= 1 + (n + 1) = \\ &= 1 + n^+ . \end{aligned}$$

pela propriedade associativa da operação de adição pelos números naturais.

Em conclusão, se $n \in A$ então $n^+ \in A$ e, pelo princípio da indução matemática, $A = \mathbb{N}$ e o lema está demonstrado.

Prova do teorema

Fixado o número natural a , seja $A = \{ n \in \mathbb{N} : a + n = n + a \}$

Então:

- i) $1 \in A$ porque pelo lema $1 + a = a + 1$.
- ii) se $n \in A$ por hipótese $a + n = n + a$ e o objetivo é mostrar que $n^+ \in A$.

$$\begin{aligned} a + n^+ &= a + (n + 1) = \\ &= (a + n) + 1 = && \text{(associatividade da adição)} \\ &= (n + a) + 1 = && \text{(hipótese de indução)} \\ &= n + (a + 1) = && \text{(associatividade da adição)} \\ &= n + (1 + a) = && \text{(lema)} \\ &= (n + 1) + a = && \text{(associatividade da adição)} \\ &= n^+ + a \end{aligned}$$

Em conclusão, se $n \in A$ então $n^+ \in A$ e, pelo princípio da indução matemática, $A = \mathbb{N}$ e a propriedade comutativa da adição é válida para os números naturais.

1.5 A OPERAÇÃO DE MULTIPLICAÇÃO NO CONJUNTO \mathbb{N} DOS NÚMEROS NATURAIS:

A partir dos postulados de Peano, a multiplicação de dois números naturais m e n nesta ordem é agora definida e não é mais um axioma.

A operação de multiplicação no conjunto dos números naturais é uma operação binária que associa a cada par ordenado de números naturais o número natural produto dos números naturais do par ordenado dado (pelo teorema abaixo, o produto de dois números naturais é um número natural).

Para cada número natural n , o produto $n \cdot 1$ dos fatores n e 1 nesta ordem é definido igual a n , isto é,

$$n \cdot 1 = n .$$

Dados dois números naturais m e n , definido o número natural produto dos fatores m e n nesta ordem, o produto $m \cdot n^+$ dos fatores m e n^+ é definido como o número natural soma das parcelas: a primeira parcela é o produto dos fatores m e n nesta ordem e a segunda parcela é o número natural m , isto é,

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

TEOREMA 1.5.1 A operação binária interna fechada de multiplicação de números naturais é bem definida: dados dois números naturais m e n , existe o número natural produto $m \cdot n$ dos fatores m e n nesta ordem.

Prova

Fixado um número natural m seja $A = \{ n \in \mathbb{N} : m \cdot n \in \mathbb{N} \}$. Então

(1) $1 \in A$ porque por definição $m \cdot 1 = m$.

(2) Hipótese de indução: Se $n \in A$, por hipótese o produto $m \cdot n$ dos fatores m e n nessa ordem é um número natural.

O objetivo é demonstrar que $n^+ \in A$, ou seja, que o produto $m \cdot (n^+)$ é um número natural. Para tanto, por definição,

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

TEOREMA 1.5.2 PROPRIEDADE DISTRIBUTIVA RESTRITA DA OPERAÇÃO DE MULTIPLICAÇÃO EM RELAÇÃO A OPERAÇÃO DE ADIÇÃO.

Dados dois números naturais a e b

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

Prova

Para números naturais a e b , $ab^+ = a(b + 1) = ab + a$.

TEOREMA 1.5.3 EXISTÊNCIA DO ELEMENTO NEUTRO PARA A OPERAÇÃO DE MULTIPLICAÇÃO.

Para cada número natural a , $1 \cdot a = a$.

Prova

Seja $A = \{ n \in \mathbb{N} : 1 \cdot n = n \}$,

Então:

- (i) $1 \in A$ porque $1 \cdot 1 = 1$.
- (ii) se $n \in A$, então por hipótese $1 \cdot n = n$.

O objetivo é mostrar que $n^+ \in A$.

$$\begin{aligned} 1n^+ &= 1(n + 1) = \\ &= 1 \cdot n + 1 \cdot 1 = && \text{(distributividade restrita)} \\ &= n + 1 = && \text{(hipótese de indução)} \\ &= n^+ . \end{aligned}$$

Em conclusão, se $n \in A$ então $n^+ \in A$ e, pelo princípio da indução matemática, $A = \mathbb{N}$ e o teorema está provado.

TEOREMA 1.5.4 PROPRIEDADE DISTRIBUTIVA DA OPERAÇÃO DE MULTIPLICAÇÃO EM RELAÇÃO A OPERAÇÃO DE ADIÇÃO.

Dados números naturais a , b e c

$$(1) \quad a(b + c) = a \cdot b + ac$$

$$(2) \quad (b + c)a = b \cdot a + ca$$

Prova (1)

Fixados os números naturais a e b , seja

$$A = \{ n \in \mathbb{N} : a(b + n) = a \cdot b + na \}.$$

Então:

$$(i) \quad 1 \in A \text{ porque } a(b + 1) = a \cdot b + a \cdot 1$$

pela propriedade distributiva restrita da operação de multiplicação em relação a operação de adição para números naturais.

$$(ii) \quad \text{Se } n \in A \text{ então, por hipótese,}$$

$$a(b + n) = ab + na.$$

O objetivo é mostrar que $n^+ \in A$.

$$\begin{aligned} a(b + n^+) &= a[b + (n + 1)] \\ &= a[(b + n) + 1] && \text{(associatividade da adição)} \\ &= a(b + n) + a && \text{(distributividade restrita)} \\ &= (ab + an) + a && \text{(hipótese de indução)} \\ &= ab + (na + a) && \text{(associatividade da adição)} \\ &= ab + a(n + 1) && \text{(distributividade restrita)} \\ &= ab + an^+. \end{aligned}$$

Em conclusão, se $n \in A$, então $n^+ \in A$ e, pelo princípio da indução matemática, $A = \mathbb{N}$ e a prova de (1) está completa.

Prova (2)

Fixados os números naturais b e c , seja

$$B = \{ (b + c)n = bn + cn \}$$

Então

$$(i) \quad 1 \in B \text{ porque } (b + c)1 = b + c$$

$$(ii) \quad \text{Se } n \in B \text{ então, por hipótese,}$$

$$(b + c)n = bn + cn$$

O objetivo é mostrar que $n^+ \in B$.

$$\begin{aligned}
 (b + c)(n^+) &= (b + c)(n + 1) \\
 &= (b + c)n + (b + c) = \\
 &= (bn + c \cdot n) + (b + c) = \\
 &= [(b \cdot n + cn) + b] + c = \\
 &= [bn + (cn + b)] + c = \\
 &= [bn + (b + cn)] + c = \\
 &= [(bn + b) + cn] + c = \\
 &= (bn + b) + (cn + c) = \\
 &= b(n + 1) + c(n + 1) = \\
 &= bn^+ + cn^+.
 \end{aligned}$$

Em conclusão, se $n \in B$ então $n^+ \in B$ e, pelo princípio da indução matemática, $B = \mathbb{N}$ e a prova de (2) está completa.

TEOREMA 1.5.5 PROPRIEDADE ASSOCIATIVA DA OPERAÇÃO DE MULTIPLICAÇÃO.

Dados números naturais a , b e c

$$(ab)c = a(bc).$$

Prova

Fixados os números naturais a e b , seja

$$A = \{n \in \mathbb{N} : (ab)n = a(bn)\}.$$

Então

$$\begin{aligned}
 (ab)(n + 1) &= (ab)n + (ab)1 && \text{propriedade distributiva} \\
 &= a(bn) + ab = && \text{hipótese de indução} \\
 &= a[bn + n] = && \text{propriedade distributiva} \\
 &= a[b(n + 1)].
 \end{aligned}$$

Em conclusão, se $n \in A$, então $n + 1 \in A$ e, pelo princípio de indução matemática, $A = \mathbb{N}$ e a prova do teorema está completa.

TEOREMA 1.5.6 PROPRIEDADE COMUTATIVA DA OPERAÇÃO DE MULTIPLICAÇÃO PARA NÚMEROS NATURAIS

Dados números naturais a e b

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

Prova

Fixado um número natural a , seja

$$A = \{ n \in \mathbb{N} : an = na \} .$$

Então

- i) $1 \in A$ porque $a \cdot 1 = 1 \cdot a = a$.
- ii) se $n \in A$ então, por hipótese $an = na$.

O objetivo é mostrar que $n^+ \in A$.

$$\begin{aligned} &= an^+ = \\ &= a(n+1) = && \text{propriedade distributiva} \\ &= an + a \cdot 1 = && \text{hipótese de indução} \\ &= an + a = && \text{propriedade distributiva} \\ &= na + a = \\ &= (n+1)a = && \text{propriedade distributiva} \\ &= n^+ \cdot a \end{aligned}$$

Em conclusão, se $n \in A$ então $n^+ \in A$ e, pelo princípio da indução matemática,

$A = \mathbb{N}$. O teorema está provado.

1.6 A RELAÇÃO DE ORDEM EM $\mathbb{N} = \{ 1, 2, 3, \dots \}$.

Dados os números naturais m, n diz-se que m é menor do que n , e escreve-se $m < n$, para significar que existe $p \in \mathbb{N}$ tal que $n = m + p$. Neste caso, diz-se também que n é maior do que m e escreve-se $n > m$ para exprimir que se tem $m < n$. A notação $m \leq n$ significa que $m < n$ ou $m = n$. Por definição, tem-se, portanto, $m < m + p$ para quaisquer $m, p \in \mathbb{N}$. Em particular, $m < m + 1$. Segue-se também da definição que $1 < n$ para todo número natural $n \neq 1$.

O número natural a é menor ou igual ao número natural b ou o número natural b é menor ou igual ao número natural a (em símbolos, $a \leq b$ ou $b \geq a$) tem o significado de que ou $a = b$ ou $a < b$.

A relação de ordem natural \leq no conjunto dos números naturais goza das seguintes propriedades (de verificação imediata)

- (a) reflexiva: para cada número natural a , $a \leq a$
- (b) antissimétrica: dados os números naturais a e b , se $a \leq b$ e se $b \leq a$ então $a = b$
- (c) transitiva: dados os números naturais a, b, c , se $a \leq b$ e se $b \leq c$ então $a \leq c$.

1.7 A LEI DA TRICOTOMIA PARA O CONJUNTO DOS NÚMEROS NATURAIS $\mathbb{N} = \{1, 2, 3, \dots\}$.

A lei da tricotomia para o conjunto dos números naturais é demonstrada a partir dos postulados de Peano através dos seguintes resultados.

TEOREMA 1.7.1 Para cada número natural $n \in \mathbb{N} = \{1, 2, 3, \dots\}$, $n^+ \neq n$.

Prova

Seja $A = \{n \in \mathbb{N} : n^+ \neq n\}$

Então

i) $1 \in A$, porque $1^+ \neq 1$ (pelos postulados de Peano, 1 não é sucessor imediato de número natural algum).

ii) Se $n \in A$ então, pela definição do conjunto A , $n^+ \neq n$.

O objetivo é mostrar que $n^+ \in A$. Caso $n^+ + 1 = (n + 1)^+ = n + 1 = n^+$ então, pelos postulados de Peano, $n + 1 = n^+ = n$, o que contradiz a hipótese de $n \in A$. Portanto, se $n \in A$ então $n^+ \in A$ e, pelo princípio da indução matemática, $A = \mathbb{N}$ e o teorema está provado.

TEOREMA 1.7.2 Se m e n são números naturais, então $m + n \neq n$.

Prova

Fixado um número natural m , seja

$$A = \{n \in \mathbb{N} : m + n \neq n\}.$$

Então

i) $1 \in A$, porque $m^+ = m + 1 \neq m$ (pelos postulados de Peano, 1 não é sucessor imediato de número natural algum).

ii) Se $n \in A$ então, pela definição do conjunto A , $m + n \neq n$.

O objetivo é mostrar que $n^+ \in A$. Caso $m + n^+ = (m + n)^+ = n^+$ então, pelos postulados de Peano, $m + n = n$, o que contradiz a hipótese de $n \in A$. Portanto, se $n \in A$ então $n^+ \in A$ e, pelo princípio da indução matemática, $A = \mathbb{N}$ e o teorema está provado.

TEOREMA 1.7.3 Se m e n são números naturais então $m + n \neq 1$.

Prova

Caso existam dois números naturais m e n cuja soma $m + n = 1$, então $1 < n$, pela definição de desigualdade, o que contradiz o resultado de que $1 \leq n$ para cada número natural n . O teorema está provado.

TEOREMA 1.7.4 Para cada número natural $n \in \mathbb{N} = \{ 1, 2, 3, \dots \}$, ou $n = 1$ ou existe $d \in \mathbb{N} = \{ 1, 2, 3, \dots \}$ tal que $n = 1 + d$.

Prova

Caso $n = 1$, $n \neq d + 1$ para cada número natural d . Caso exista um número natural d tal que $n = 1 + d = d + 1$, então $n \neq 1$ pelos postulados de Peano. O teorema está provado.

TEOREMA 1.7.5 A LEI DA TRICOTOMIA PARA O CONJUNTO DOS NÚMEROS NATURAIS $\mathbb{N} = \{ 1, 2, 3, \dots \}$.

Dados os números naturais m e n , uma e uma só das seguintes afirmações é verdadeira:

$$(1) m < n \quad (2) m = n \quad (3) m > n$$

Prova

Se a afirmação (1) é verdadeira, as afirmações (2) e (3) são falsas: de fato, caso exista um número natural d tal que $n = m + d \neq m$, o que mostra que a afirmação (2) é falsa; caso a afirmação (3) é verdadeira, existe um número natural c tal que $m = n + c$, e por substituição, $n = n + (c + d)$, o que contradiz um dos teoremas anteriores. E assim a afirmação (3) é falsa.

Se a afirmação (3) é verdadeira, as afirmações (1) e (2) são falsas por analogia.

Se a afirmação (2) é verdadeira, as afirmações (1) e (3) são falsas: de fato, caso a afirmação (1) é verdadeira existe um número natural d tal que $n = m + d = m$, o que contradiz um dos teoremas anteriores e assim a afirmação (1) é falsa assim como a afirmação (3) por analogia é falsa.

1.8 O CONJUNTO DOS NÚMEROS NATURAIS $\mathbb{N} = \{0, 1, 2, \dots\}$: UMA CONSTRUÇÃO A PARTIR DO AXIOMA DO INFINITO.

O que é um número natural ?

Números naturais são conjuntos.

O número natural zero indicado pelo símbolo $\mathbf{0}$ é definido como o conjunto vazio \emptyset (o qual não possui elemento algum)

$$\mathbf{0} = \emptyset$$

O número natural um, indicado pelo símbolo $\mathbf{1}$, é definido como o conjunto

$$\mathbf{1} = \emptyset \cup \{\emptyset\} = \{\emptyset\}$$

(que é um conjunto unitário cujo único elemento é o conjunto vazio)

Então

$$\mathbf{1} = \{\mathbf{0}\}$$

O número natural dois, indicado pelo símbolo $\mathbf{2}$, é definido como o conjunto

$$\mathbf{2} = \{\emptyset\} \cup \{\{\emptyset\}\} = \{\emptyset, \{\emptyset\}\}$$

Então

$$\mathbf{2} = \{\mathbf{0}, \mathbf{1}\}$$

O número natural três, indicado pelo símbolo $\mathbf{3}$, é definido como o conjunto

$$\begin{aligned} \mathbf{3} &= \{\emptyset, \{\emptyset\}\} \cup \{\{\emptyset, \{\emptyset\}\}\} \\ &= \{\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}\} \end{aligned}$$

Então

$$\mathbf{3} = \{\mathbf{0}, \mathbf{1}, \mathbf{2}\}$$

E assim por diante.

A existência do conjunto infinito dos naturais $\mathbb{N} = \{0, 1, 2, 3, \dots\}$ ainda não está assegurado apesar das definições dos números naturais zero, um, dois, três, ...

Para garantir a existência do conjunto $\mathbb{N} = \{0, 1, 2, \dots\}$ dos números naturais é preciso o seguinte axioma do infinito.

Axioma do infinito

Existe um conjunto X com as propriedades

- (1) $\emptyset \in X$
- (2) se $x \in X$, então $x \cup \{x\} \in X$.

A listagem de alguns elementos do conjunto X é dada na sequência

$$\emptyset \in X$$

$$\emptyset \cup \{\emptyset\} = \{\emptyset\} \in X$$

$$\{\emptyset\} \cup \{\{\emptyset\}\} \in X$$

Um conjunto X com as propriedades

$$(1) \emptyset \in X$$

é denominado um conjunto sucessor.

Por definição, o conjunto $\mathbb{N} = \{0, 1, 2, \dots\}$ dos números naturais é definido como a interseção (não vazia pelo axioma de infinito) de todos os conjuntos sucessores. Como interseção de todos os conjuntos sucessores, o conjunto dos números naturais também é um conjunto sucessor.

Por definição, o número natural \mathbf{n}^+ denominado sucessor imediato do número natural \mathbf{n} , é igual a

$$\mathbf{n}^+ = \mathbf{n} \cup \{\mathbf{n}\}$$

Em particular, pela definição,

$$1 = 0^+$$

$$2 = 1^+$$

$$3 = 2^+$$

e assim por diante.

TEOREMA 1.8.1 Para cada número natural \mathbf{n} , $\mathbf{n}^+ \neq 0$

Prova

Se \mathbf{n} é um número natural $\mathbf{n}^+ = \mathbf{n} \cup \{\mathbf{n}\}$ e então $\mathbf{n} \in \mathbf{n}^+$ enquanto que o número natural zero é o conjunto vazio (que não possui elemento algum).

TEOREMA 1.8.2 PRINCÍPIO ZERO DE INDUÇÃO MATEMÁTICA

Seja A um subconjunto do conjunto $\mathbb{N} = \{0, 1, 2, \dots\}$ dos números naturais com as propriedades:

$$(1) 0 \in A$$

$$(2) \text{ se } \mathbf{n} \in A, \text{ então } \mathbf{n}^+ \in A$$

Então $A = \mathbb{N} = \{0, 1, 2, \dots\}$.

Prova

Por hipótese, A é um conjunto sucessor contido em $\mathbb{N} = \{0, 1, 2, \dots\}$. Logo, \mathbb{N} por ser interseção de todos os conjuntos sucessores, $\mathbb{N} \subset A$.

Se $A \subset \mathbb{N}$ e $\mathbb{N} \subset A$ segue $A = \mathbb{N}$.

TEOREMA 1.8.3 Dados números naturais m e n , se os sucessores imediatos m^+ de m e n^+ de n são iguais, ou seja, se $m^+ = n^+$ então $m \in n$ ou $m = n$

Prova

Por definição e por hipótese

$$m^+ = m \cup \{m\} = n \cup \{n\} = n^+$$

Como $m \in m^+$, $m \in n^+$. Então ou

$$m = n$$

ou

$$m \in n$$

Números naturais são então conjuntos transitivos (Um conjunto X é um conjunto transitivo quando e somente quando para cada $x \in X$, $\{x\} \subset X$), pelo teorema a seguir.

TEOREMA 1.8.4 Todo número natural n é um conjunto transitivo.

Prova

Pelo princípio da indução matemática, seja A o subconjunto do conjunto dos números naturais $\mathbb{N} = \{0, 1, 2, \dots\}$ constituído pela totalidade dos números naturais que são conjuntos transitivos.

Então

- (i) $0 \in A$ por vacuidade.
- (ii) Hipótese de indução: Se $n \in A$ por hipótese, n é um conjunto transitivo.

O objetivo é mostrar que o sucessor imediato n^+ de número natural n é um conjunto transitivo.

$$m \in n^+$$

Então pelo teorema anterior ou

$$m \in n$$

ou

$$\mathbf{m = n}$$

Se $\mathbf{m = n}$, \mathbf{m} é um conjunto transitivo pela hipótese de indução, porque \mathbf{n} é um conjunto transitivo.

Se $\mathbf{m \in n}$ então $\mathbf{m \subset n}$ porque \mathbf{n} é um conjunto transitivo pela hipótese de indução e assim:

$$\mathbf{m \subset n \subset n^+}$$

Em conclusão, se $\mathbf{n \in A}$ então $\mathbf{n^+ \in A}$.

Pelo princípio de indução matemática

$$\mathbf{A = \mathbb{N} = \{ 0, 1, 2, \dots \}}$$

e, portanto, todo número natural é um conjunto transitivo.

TEOREMA 1.8.5 Dados números naturais \mathbf{m} e \mathbf{n} , se $\mathbf{m^+ = n^+}$ então $\mathbf{m = n}$

Prova

Por hipótese $\mathbf{m^+ = n^+}$.

Como

$$\mathbf{n \in n^+ = n \cup n}$$

$$\mathbf{n \in m^+ = m \cup m}$$

e assim ou

$$\mathbf{n \in m}$$

ou

$$\mathbf{n = m}$$

Analogamente

$$\mathbf{m \in n}$$

ou

$$\mathbf{m = n}$$

Na hipótese de que $\mathbf{n \in m}$ e $\mathbf{m \in n}$, como \mathbf{m} e \mathbf{n} são conjuntos transitivos,

$$\mathbf{n \subset m}$$

$$\mathbf{m \subset n}$$

O que prova a igualdade entre os números naturais \mathbf{m} e \mathbf{n} .

O conjunto $\mathbb{N} = \{ 0, 1, 2, \dots \}$ dos números naturais definido como interseção não vazia de todos os conjuntos sucessores satisfaz os cinco postulados de Peano P1 a P5 a seguir como ficou demonstrado nos teoremas anteriores.

P1) $0 \in \mathbb{N}$.

P2) Se $n \in \mathbb{N}$ então $n^+ \in \mathbb{N}$.

P3) Para cada $n \in \mathbb{N}$, $n^+ \neq 0$.

P4) Princípio da indução matemática.

Seja A um subconjunto de $\mathbb{N} = \{ 0, 1, 2, \dots \}$ com as propriedades

(1) $0 \in A$

(2) Se $n \in A$, então $n^+ \in A$.

Então $A = \mathbb{N}$.

P5) Se $n, m \in \mathbb{N}$ e se $n^+ = m^+$, então $n = m$.

TEOREMA 1.8.6 PRIMEIRO PRINCÍPIO DE INDUÇÃO MATEMÁTICA

Seja A um subconjunto de $\mathbb{N} = \{ 0, 1, 2, \dots \}$ com as propriedades:

(i) $1 \in A$.

(ii) Se $n \in A$ então $n + 1 \in A$,

então $A = \{ 1, 2, 3, 4, \dots \}$.

Prova

Seja $B = \{ n \in \mathbb{N} : n + 1 \in A \} \subset \mathbb{N} = \{ 0, 1, 2, \dots \}$,

Então B satisfaz as hipóteses do princípio de indução matemática.

(i) $0 \in B$ porque $0 + 1 = 1 \in A$.

(ii) Se $n \in B$ por definição de B , $n + 1 \in A$ e, pela hipótese (ii) sobre o conjunto A , $(n + 1) + 1 \in A$ o que prova que $n + 1 \in B$, pela definição de B .

Então $B = \{ 0, 1, 2, \dots \}$ e $A = \{ 1, 2, 3, \dots \}$.

TEOREMA 1.8.7 SEGUNDO PRINCÍPIO DE INDUÇÃO MATEMÁTICA

Seja A um subconjunto de $\mathbb{N} = \{ 0, 1, 2, \dots \}$ com as propriedades

(i) $2 \in A$.

(ii) Se $n \in A$, então $n + 1 \in A$.

Então $A = \{ 2, 3, 4, \dots \}$.

Prova

Seja $B = \{ n \in \mathbb{N} : n + 2 \in A \} \subset \mathbb{N} = \{ 0, 1, 2, \dots \}$

Então B satisfaz as hipóteses do princípio da indução matemática.

(i) $0 \in B$ porque $0 + 2 = 2 \in A$.

(ii) Se $n \in B$, então $n + 1 \in B$.

Então $B = \{ 0, 1, 2, \dots \}$ e $A = \{ 2, 3, 4, \dots \}$.

TEOREMA 1.8.8 PRINCÍPIO DE INDUÇÃO COMPLETA

Seja A um subconjunto de $\mathbb{N} = \{ 0, 1, 2, \dots \}$ com as propriedades

(i) $1 \in A$.

(ii) Se $1, 2, \dots, n \in A$, então $n + 1 \in A$.

Então $A = \{ 1, 2, 3, \dots \}$.

Prova

Seja $B = \{ n \in \mathbb{N} : 1, 2, 3, \dots, n \in A \}$.

Então B satisfaz as hipóteses do primeiro princípio da indução matemática.

(i) $1 \in B$ porque, por definição de B, $1 \in A$.

(ii) Se $n \in B$, por definição de B, $1, 2, 3, \dots, n \in A$ e, pela hipótese (ii) do conjunto

A, $n + 1 \in A$. Como $1, 2, 3, \dots, n + 1 \in A$, pela definição de B, $n + 1 \in B$.

Pelo primeiro princípio da indução matemática,

$$B = A = \{ 1, 2, 3, \dots \}.$$

TEOREMA 1.8.9 TEOREMA DA RECURSÃO

Sejam X um conjunto, $x_0 \in X$ e f uma função definida no conjunto X com valores em X. Então existe uma única função F definida no conjunto $\mathbb{N} = \{ 0, 1, 2, \dots \}$ dos números naturais com valores em X com as propriedades:

(1) $F(0) = x_0$.

(2) Para cada número natural n

$$F(n^+) = f[F(n)].$$

Prova

A função F a ser construída definida em $\mathbb{N} = \{ 0, 1, 2, \dots \}$ com valores em X é um subconjunto do produto cartesiano $\mathbb{N} \times X$ com as propriedades:

- (1) $(\mathbf{0}, x_0) \in F$.
- (2) Para cada número natural \mathbf{n} existe um elemento $x \in X$ tal que

$$(\mathbf{n}, x) \in F .$$
- (3) se $(\mathbf{n}, x_1) \in F$ e se $(\mathbf{n}, x_2) \in F$, em que \mathbf{n} é um número natural e x_1 e x_2 são elementos de X , então $x_1 = x_2$.
- (4) se $(\mathbf{n}, x) \in F$ então $(\mathbf{n}^+, f(x)) \in F$.

Prova da existência da função F.

Seja U o conjunto de todos os subconjuntos $Y \subset \mathbb{N} \times X$ tais que:

- (i) $(\mathbf{0}, x_0) \in Y$.
- (ii) se $(\mathbf{n}, x) \in Y$, então $(\mathbf{n}^+, f(x)) \in Y$.

O conjunto U é não vazio pois $\mathbb{N} \times X \in U$ e a interseção de elementos de U é um elemento de U .

A função F é definida como a interseção de todos os elementos de U e, portanto, F satisfaz as propriedades (i) e (ii) acima. Resta mostrar que:

- (iii) Para cada número natural \mathbf{n} existe um elemento $x \in X$ tal que

$$(\mathbf{n}, x) \in F .$$

(iv) Se $(\mathbf{n}, x_1) \in F$ e se $(\mathbf{n}, x_2) \in F$, em que \mathbf{n} é um número natural e x_1 e x_2 são elementos de X , então $x_1 = x_2$.

Seja A o subconjunto do conjunto $\mathbb{N} = \{ \mathbf{0}, \mathbf{1}, \mathbf{2}, \dots \}$ dos números naturais constituído por todos os números naturais \mathbf{n} com a propriedade de que $(\mathbf{n}, x) \in F$ para um único elemento $x \in X$. Então,

o número natural $\mathbf{0} \in A$ porque $(\mathbf{0}, x_0) \in F$ e se $(\mathbf{0}, x_0) \in F$ e se $(\mathbf{0}, x_1) \in F$ com $x_0 \neq x_1$, seja $F \setminus \{(\mathbf{0}, x_1)\}$; assim

- (i) $(\mathbf{0}, x_0) \in F \setminus \{(\mathbf{0}, x_1)\}$
- (ii) Se $(\mathbf{n}, x) \in F \setminus \{(\mathbf{0}, x_1)\}$ então $(\mathbf{n}, x) \in F$, o que implica que

$$(\mathbf{n}^+, f(x)) \in F$$

e como $\mathbf{n}^+ \neq \mathbf{0}$

$$(\mathbf{n}^+, f(x)) \neq (\mathbf{0}, x_1)$$

e, em consequência,

$$(\mathbf{n}^+, f(x)) \in F \setminus \{(\mathbf{0}, x_1)\}.$$

Como F é a interseção de todos os subconjuntos Y de U ,

$$F \subset F \setminus \{(\mathbf{0}, x_1)\},$$

o que é uma contradição ao fato de que $(0, x_1) \in F$.

Admitindo que $\mathbf{n} \in A$ (hipótese de indução), o objetivo é mostrar que $\mathbf{n}^+ \in A$. Ao assumir a existência de $y \in X$ com $y \neq f(x)$, tal que $(\mathbf{n}^+, y) \in F$, segue que

$$(\mathbf{n}, x) \in F \text{ implica que } (\mathbf{n}^+, f(x)) \in F.$$

$$(\mathbf{n}^+, y) \in F \text{ com } y \neq f(x)$$

Então seja

$$F \{(\mathbf{n}^+, y)\}$$

e assim,

$$(0, x_0) \in F \{(\mathbf{n}^+, y)\} \text{ pois } \mathbf{n}^+ \neq 0.$$

Para um número natural \mathbf{m} e um elemento $z \in X$ com

$$(\mathbf{m}, z) \in F \{(\mathbf{n}^+, y)\}$$

implica que

$$(\mathbf{m}, z) \in F$$

o que implica

$$(\mathbf{m}^+, f(z)) \in F.$$

Dois casos a considerar:

$$(a) \quad \mathbf{m}^+ \neq \mathbf{n}^+$$

$$(b) \quad \mathbf{m}^+ = \mathbf{n}^+$$

Em (a) $\mathbf{m}^+ \neq \mathbf{n}^+$, $(\mathbf{m}^+, f(z)) \neq (\mathbf{n}^+, y)$

$$(\mathbf{m}^+, f(z)) \in F \setminus \{(\mathbf{n}^+, y)\}$$

Em (b) $\mathbf{m}^+ = \mathbf{n}^+$ implica $\mathbf{m} = \mathbf{n}$ e $(\mathbf{m}, z) = (\mathbf{n}, z)$ o que acarreta

$$(\mathbf{m}^+, f(z)) = (\mathbf{n}^+, f(z))$$

e, como $(\mathbf{n}^+, f(x)) \in F$,

$$f(x) = f(z)$$

e

$$(\mathbf{m}^+, f(z)) = (\mathbf{n}^+, f(x)) \in F \{(\mathbf{n}^+, y)\}.$$

Como F é a interseção de todos os subconjuntos Y de U ,

$$F \subset F \{(\mathbf{n}^+, y)\}$$

o que é uma contradição por admitir que

$$(\mathbf{n}^+, y) \in F \subset F \{(\mathbf{n}^+, y)\} \text{ com } y \neq f(x).$$

Pelo princípio da indução matemática, $A = \mathbb{N} = \{0, 1, 2, \dots\}$. A construção da função F , com as propriedades (1), (2), (3) e (4) está completa.

Prova da unicidade da função F.

Sejam F e G funções definidas para todos os números naturais com valores em X satisfazendo $(\mathbf{0}, x_0) \in F$, $(\mathbf{0}, x_0) \in G$ e para cada número natural \mathbf{n} .

$$F(\mathbf{n}^+) = f[F(\mathbf{n})]$$

$$G(\mathbf{n}^+) = f[G(\mathbf{n})]$$

Seja $B = \{ \mathbf{n} \in \mathbb{N} : F(\mathbf{n}) = G(\mathbf{n}) \}$.

Assim,

(i) $\mathbf{0} \in B$ pois $F(\mathbf{0}) = x_0 = G(\mathbf{0})$

(ii) Hipótese de indução: se $\mathbf{n} \in B$ por hipótese $F(\mathbf{n}) = G(\mathbf{n})$ o que implica

$$F(\mathbf{n}^+) = f[F(\mathbf{n})] = f[G(\mathbf{n})] = G(\mathbf{n}^+)$$

e que $\mathbf{n}^+ \in B$.

Pelo princípio da indução matemática, $B = \mathbb{N} = \{ \mathbf{0}, \mathbf{1}, \mathbf{2}, \dots \}$ e as funções F e G são idênticas.

Observação:

Seja f uma função injetora definida para todos os elementos de X com valores em X, de modo que x_0 não é um elemento do conjunto de valores de f. Então a função F do teorema da recursão também é injetora no sentido de que se \mathbf{m} e \mathbf{n} são números naturais com $F(\mathbf{m}) = F(\mathbf{n})$, então, $\mathbf{m} = \mathbf{n}$.

Caso $\mathbf{m} = \mathbf{0}$ e caso $\mathbf{n} = \mathbf{0}$ não há o que provar e se $\mathbf{n} \neq \mathbf{0}$ é tal que $F(\mathbf{n}) = F(\mathbf{0})$ então \mathbf{n} é o sucessor imediato de um número natural \mathbf{k} ou seja $\mathbf{n} = \mathbf{k}^+$ e

$$F(\mathbf{0}) = x_0 = F(\mathbf{n}) = f(\mathbf{k}) = f[F(\mathbf{k})]$$

o que é uma contradição pois x_0 não é elemento do conjunto de valores de F

Conclusão: se $F(\mathbf{n}) = F(\mathbf{0})$ então $\mathbf{n} = \mathbf{0}$.

Admitindo que para números naturais \mathbf{m} e \mathbf{n} $F(\mathbf{m}^+) = F(\mathbf{n})$, se $\mathbf{n} = \mathbf{0}$, $F(\mathbf{m}^+) = F(\mathbf{0})$ então $\mathbf{m}^+ = \mathbf{0}$, o que é uma contradição; se $\mathbf{n} \neq \mathbf{0}$, \mathbf{n} é sucessor imediato de um número natural \mathbf{k} , ou seja $\mathbf{n} = \mathbf{k}^+$ e $F(\mathbf{m}^+) = F(\mathbf{n}) = F(\mathbf{k}^+) = f[F(\mathbf{m})] = f[F(\mathbf{k})]$ e por f ser uma função injetora, $F(\mathbf{m}) = F(\mathbf{k})$. Pela hipótese de indução: $\mathbf{m} = \mathbf{k}$ e $\mathbf{m}^+ = \mathbf{k}^+ = \mathbf{n}$.

1.9 A OPERAÇÃO DE ADIÇÃO NO CONJUNTO DOS NÚMEROS NATURAIS VIA TEOREMA DA RECURSÃO

Seja \mathbf{m} um número natural e seja f a função sucessor imediato definida para todos os valores naturais, ou seja, para todo número natural \mathbf{n} , $f(\mathbf{n}) = \mathbf{n}^+$.

O teorema da recursão garante a existência e a unicidade de uma função F_m definida em $\mathbb{N} = \{ \mathbf{0}, \mathbf{1}, \mathbf{2}, \mathbf{3}, \dots \}$ com valores naturais de modo que $F_m(\mathbf{0}) = \mathbf{m}$ e

$F_m(\mathbf{n}^+) = [F_m(\mathbf{n})]^+$ para cada número natural \mathbf{n} .

A operação de adição de números naturais é definida como segue: dados números naturais \mathbf{m} e \mathbf{n} , a operação de adição associa ao par ordenado (\mathbf{m}, \mathbf{n}) a soma $\mathbf{m} + \mathbf{n}$ dos números naturais \mathbf{m} e \mathbf{n} nesta ordem que é definida como o número natural $F_m(\mathbf{n})$ ou seja, $\mathbf{m} + \mathbf{n} = F_m(\mathbf{n})$. Em outras palavras, para números naturais \mathbf{m} e \mathbf{n}

$$\mathbf{m} + \mathbf{0} = F_m(\mathbf{0}) = \mathbf{m}$$

$$\mathbf{m} + \mathbf{n}^+ = F_m(\mathbf{n}^+) = [F_m(\mathbf{n})]^+ = (\mathbf{m} + \mathbf{n})^+.$$

Em particular para cada número natural \mathbf{n} , o sucessor imediato \mathbf{n}^+ de \mathbf{n} é igual a $\mathbf{n}^+ = \mathbf{n} + \mathbf{1}$ lembrando que, por definição, $\mathbf{1} = \mathbf{0}^+$.

TEOREMA 1.9.1 PROPRIEDADES DA OPERAÇÃO DE ADIÇÃO

(a) Para cada número natural \mathbf{n} , $\mathbf{n}^+ = \mathbf{1} + \mathbf{n}$ em que o número natural $\mathbf{1}$ é definido como $\mathbf{0}^+$.

(b) Para cada número natural \mathbf{n} , $\mathbf{0} + \mathbf{n} = \mathbf{n}$.

(c) Lei associativa da operação de adição: dados os números naturais \mathbf{m} , \mathbf{n} e \mathbf{k}

$$(\mathbf{m} + \mathbf{n}) + \mathbf{k} = \mathbf{m} + (\mathbf{n} + \mathbf{k}).$$

(d) Lei comutativa da operação de adição: dados os números naturais \mathbf{m} e \mathbf{n} ,

$$\mathbf{m} + \mathbf{n} = \mathbf{n} + \mathbf{m}.$$

Prova de (a)

Seja $A = \{ n \in \mathbb{N} : n^+ = 1 + n \}$. Então $0 \in A$ porque $0^+ = 1 = 1 + 0$, lembrando que para cada número natural m , $m + 0 = m$. Se $n \in A$ então, pela definição de A ,

$$n^+ = 1 + n$$

e
$$1 + n^+ = (1 + n)^+ = (n^+)^+,$$

o que demonstra que $n^+ \in A$. Pelo princípio da indução matemática, $A = \mathbb{N}$ e a prova de (a) está completa.

Prova de (b)

Seja $A = \{ n \in \mathbb{N} : 0 + n = n \}$. Então $0 \in A$ porque $0 + 0 = 0$, lembrando que para cada número natural m , $m + 0 = m$. Se $n \in A$ então, pela definição de A ,

$$0 + n = n$$

e
$$0 + n^+ = (0 + n)^+ = n^+,$$

o que demonstra que $n^+ \in A$. Pelo princípio da indução matemática, $A = \mathbb{N}$ e a prova de (b) está completa.

Prova de (c)

Fixados os números naturais m e n nesta ordem, seja

$$A_{mn} = \{ k \in \mathbb{N} : (m + n) + k = m + (n + k) \}.$$

Então $0 \in A_{mn}$ porque $(m + n) + 0 = m + n = m + (n + 0)$, lembrando que para cada número natural m , $m + 0 = m$. Se $k \in A_{mn}$ então, pela definição de A_{mn} ,

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

$$(m + n) + k^+ = [(m + n) + k]^+ = [m + (n + k)]^+ = m + (n + k)^+ = m + (n + k^+),$$

o que demonstra que $\mathbf{k}^+ \in A_{mn}$. Pelo princípio da indução matemática, $A_{mn} = \mathbb{N}$ e a prova de (c) está completa.

Prova de (d)

Fixado o número natural m , seja $A_m = \{ \mathbf{n} \in \mathbb{N} : \mathbf{m} + \mathbf{n} = \mathbf{n} + \mathbf{m} \}$. Então $\mathbf{0} \in A_m$ porque $\mathbf{m} + \mathbf{0} = \mathbf{m} = \mathbf{0} + \mathbf{m}$, lembrando que para cada número natural \mathbf{m} , $\mathbf{m} + \mathbf{0} = \mathbf{m}$ e pelo item (b) $\mathbf{0} + \mathbf{m} = \mathbf{m}$. Se $\mathbf{n} \in A_m$ então, pela definição de A_m .

$$\mathbf{m} + \mathbf{n} = \mathbf{n} + \mathbf{m}$$

$$\begin{aligned} \mathbf{m} + \mathbf{n}^+ &= (\mathbf{m} + \mathbf{n})^+ && \text{(definição de adição de números naturais)} \\ &= (\mathbf{n} + \mathbf{m})^+ && \text{(utilizando a igualdade anterior)} \\ &= \mathbf{1} + (\mathbf{n} + \mathbf{m}) && \text{(item (a))} \\ &= (\mathbf{1} + \mathbf{n}) + \mathbf{m} && \text{(associatividade da operação de adição)} \\ &= \mathbf{n}^+ + \mathbf{m} && \text{(item (a))} \end{aligned}$$

o que demonstra que $\mathbf{n}^+ \in A_m$. Pelo princípio da indução matemática, $A_m = \mathbb{N}$ e a prova de (d) está completa.

1.10 A OPERAÇÃO DE MULTIPLICAÇÃO NO CONJUNTO N DOS NÚMEROS NATURAIS VIA TEOREMA DA RECURSÃO.

Seja \mathbf{m} um número natural e seja a função g_m definida para todos os números naturais com valores naturais: para cada número natural \mathbf{n} , $g_m(\mathbf{n}) = \mathbf{n} + \mathbf{m}$.

O teorema da recursão garante a existência e a unicidade de uma função G_m definida para todos os números naturais com valores naturais com as propriedades $G_m(0) = 0$ e para cada número natural n , $G_m(n^+) = g_m(G_m(n))$

A operação de multiplicação para números naturais é definida como segue: dados números naturais m e n , a operação de multiplicação associa ao par ordenado (m, n) o produto mn dos fatores naturais m e n nesta ordem definido como o número natural $G_m(n)$. Em outros termos, $m0 = G_m(0) = 0$ e para cada número natural n

$$G_m(n^+) = g_m[G_m(n)] = mn + m$$

ou seja, por definição

$$mn^+ = G_m(n) + m = mn + m$$

TEOREMA 1.10.1 PROPRIEDADES DA OPERAÇÃO DE MULTIPLICAÇÃO.

(a) Para cada número natural n , $0n = 0$.

(b) Para cada número natural n , $1n = n$.

(c) Leis distributivas da operação de multiplicação em relação a operação de adição: dados os números naturais m , n e k ,

$$c1) m(n + k) = (mn + mk)$$

$$c2) (n + k)m = nm + km$$

(d) Lei associativa da operação de multiplicação: dados os números naturais m , n e k ,

$$(mn)k = m(nk)$$

(e) Lei comutativa da operação de multiplicação: dados os números naturais m e n ,

$$mn = nm$$

Prova de (a)

Seja $A = \{ n \in \mathbb{N} : 0n = 0 \}$. Então $0 \in A$ porque $0 \cdot 0 = 0$ lembrando que para cada número natural n , $n0 = 0$. Se $n \in A$ então pela definição de A , $0n = 0$ e por definição

$$\mathbf{0n^+ = 0n + 0 = 0n = 0}$$

o que mostra que $\mathbf{n^+ \in A}$. Pelo princípio da indução matemática, $\mathbf{A = \mathbb{N}}$ e a prova está completa.

Prova de (b)

Seja $\mathbf{A = \{ n \in \mathbb{N} : 1n = n \}}$. Então $\mathbf{0 \in A}$ porque $\mathbf{1 \cdot 0 = 0}$ lembrando que para cada número natural \mathbf{n} , $\mathbf{n0 = 0}$. Se $\mathbf{n \in A}$ então pela definição de \mathbf{A} , $\mathbf{1n = n}$ e por definição

$$\mathbf{1n^+ = 1n + 1 = n + 1 = n^+},$$

o que mostra que $\mathbf{n^+ \in A}$. Pelo princípio da indução matemática, $\mathbf{A = \mathbb{N}}$ e a prova de (b) está completa.

Prova de (c1)

Fixados os números naturais \mathbf{m} e \mathbf{n} nesta ordem, seja

$$\mathbf{A_{mn} = \{ k \in \mathbb{N} : m(n + k) = mn + mk \}}$$

Então $\mathbf{0 \in A_{mn}}$ porque $\mathbf{m(n + 0) = mn = mn + m0}$ lembrando que para cada número natural \mathbf{m} , $\mathbf{m + 0 = m}$ e $\mathbf{m0 = 0}$. Se $\mathbf{k \in A_{mn}}$ então, pela definição de $\mathbf{A_{mn}}$,

$$\mathbf{m(n + k) = mn + mk}$$

$$\begin{aligned} \mathbf{m(n + k^+) &= m(n + k)^+} && \text{definição de adição} \\ &= \mathbf{m(n + k) + m} && \text{definição de multiplicação} \\ &= \mathbf{(mn + mk) + m} && \text{definição de A} \\ &= \mathbf{mn + (mk + m)} && \text{associatividade da adição} \\ &= \mathbf{mn + mk^+} && \text{definição de multiplicação} \end{aligned}$$

o que demonstra que $\mathbf{k^+ \in A_{mn}}$. Pelo princípio da indução matemática, $\mathbf{A_{mn} = \mathbb{N}}$ e a prova de (c1) está completa.

A prova de c2 é análoga.

Prova de (d)

Fixados os números naturais m e n nesta ordem, seja

$$A_{mn} = \{ k \in \mathbb{N} : (mn)k = m(nk) \}$$

Então $0 \in A_{mn}$ porque $(mn)0 = 0 = m(n0)$, lembrando que para cada número natural m , $m0 = 0$. Se $k \in A_{mn}$ então, pela definição de A_{mn} ,

$$(mn)k = m(nk)$$

$$\begin{aligned} (mn)k^+ &= (mn)k + mn && \text{definição de multiplicação} \\ &= m(nk) + mn && \text{definição de } A \\ &= m(nk + n) && \text{distributividade da multiplicação} \\ &= m(nk^+) && \text{definição de multiplicação} \end{aligned}$$

Prova de (e)

Fixado o número natural m , seja $A_m = \{ n \in \mathbb{N} : mn = nm \}$, então $0 \in A_m$ porque $m0 = 0 = 0m$, lembrando que para cada número natural m , $m0 = 0$ e $0m = 0$. Se $n \in A_m$ então, pela definição de A_m ,

$$mn = nm$$

$$mn^+ = m(n + 1) = mn + m = nm + m = (n + 1)m = n^+m$$

o que mostra que $n^+ \in A_m$. Pelo princípio da indução matemática, $A_m = \mathbb{N}$ e a prova de (e) está completa.

1.11 A RELAÇÃO NATURAL DE ORDEM NO CONJUNTO

$\mathbb{N} = \{ 0, 1, 2, \dots \}$ DOS NÚMEROS NATURAIS

Dados números naturais m e n o significado de $m \leq n$ (leia m é menor ou igual a n ou n é maior ou igual a m) é que:

$$\mathbf{m} = \mathbf{n} \text{ ou } \mathbf{m} \in \mathbf{n}.$$

A relação binária R_{\leq} em $\mathbb{N} = \{ 0, 1, 2, \dots \}$ definida por

$$\mathbf{R}_{\leq} = \{(\mathbf{m}, \mathbf{n}): \mathbf{m} \leq \mathbf{n}\}$$

é uma relação de ordem total em \mathbb{N} ou seja R_{\leq} tem as propriedades:

Reflexiva: para cada número natural n , $n \leq n$ (verificação imediata)

Antissimétrica: dados os números naturais m e n , se $\mathbf{m} \leq \mathbf{n}$ e se $\mathbf{n} \leq \mathbf{m}$ então $\mathbf{m} = \mathbf{n}$ (se $\mathbf{m} \leq \mathbf{n}$ e se $\mathbf{n} \leq \mathbf{m}$ então $\mathbf{m} = \mathbf{n}$ ou $\mathbf{m} \in \mathbf{n}$ e $\mathbf{n} \in \mathbf{m}$ e neste caso $\mathbf{m} \subset \mathbf{n}$ e $\mathbf{n} \subset \mathbf{m}$ o que implica novamente que $\mathbf{m} = \mathbf{n}$)

Transitiva: dados os números naturais m , n e p , se $\mathbf{m} \leq \mathbf{n}$ e se $\mathbf{n} \leq \mathbf{p}$ então $\mathbf{m} \leq \mathbf{p}$

Prova da propriedade transitiva

Com as hipóteses de que $\mathbf{m} \leq \mathbf{n}$ e $\mathbf{n} \leq \mathbf{p}$, há quatro possibilidades a considerar:

- (i) $\mathbf{m} \in \mathbf{n}$ e $\mathbf{n} \in \mathbf{p}$ o que resulta $\mathbf{m} \in \mathbf{n}$ e $\mathbf{n} \subset \mathbf{p}$ e que $\mathbf{m} \in \mathbf{p}$
- (ii) $\mathbf{m} \in \mathbf{n}$ e $\mathbf{n} = \mathbf{p}$ o que resulta $\mathbf{m} \in \mathbf{p}$
- (iii) $\mathbf{m} = \mathbf{n}$ e $\mathbf{n} \in \mathbf{p}$ o que resulta $\mathbf{m} \in \mathbf{p}$
- (iv) $\mathbf{m} = \mathbf{n}$ e $\mathbf{n} = \mathbf{p}$ o que resulta $\mathbf{m} = \mathbf{p}$

Em todos os casos, $\mathbf{m} \leq \mathbf{p}$.

TEOREMA 1.11.1 Dados os números naturais \mathbf{m} e \mathbf{n} , se $\mathbf{m} \leq \mathbf{n}$ então existe um único número natural \mathbf{d} tal que $\mathbf{n} = \mathbf{m} + \mathbf{d}$.

Prova

Se $\mathbf{m} \leq \mathbf{n}$ então ou $\mathbf{m} = \mathbf{n}$ e neste caso $\mathbf{d} = \mathbf{0}$ ou $\mathbf{m} \in \mathbf{n}$ e $\mathbf{m} < \mathbf{n}$ o que implica que $\mathbf{m}^+ \leq \mathbf{n}$. Se $\mathbf{m}^+ \leq \mathbf{n}$ então ou $\mathbf{m}^+ = \mathbf{m} + \mathbf{1} = \mathbf{n}$ e neste caso $\mathbf{d} = \mathbf{1}$ ou $\mathbf{m}^+ \in \mathbf{n}$ o que implica que $\mathbf{m}^+ < \mathbf{n}$. Se $\mathbf{m}^+ < \mathbf{n}$ então $(\mathbf{m} + \mathbf{1})^+ \leq \mathbf{n}$. Se $(\mathbf{m} + \mathbf{1})^+ \leq \mathbf{n}$ então ou $(\mathbf{m} + \mathbf{1})^+ = \mathbf{m} + \mathbf{1}^+ = \mathbf{m} + \mathbf{2} = \mathbf{n}$ e neste caso $\mathbf{d} = \mathbf{2}$ ou $(\mathbf{m} + \mathbf{1})^+ = \mathbf{m} + \mathbf{2} < \mathbf{n}$. Continuando o processo um número finito de

vezes porque n é um conjunto finito, está provado que se $m \leq n$ então existe um único número natural d tal que $n = m + d$.

TEOREMA 1.11.2 A LEI DA TRICOTOMIA

Dados os números naturais m e n , uma e somente uma das afirmações é verdadeira

$$(1) m < n \quad (2) m = n \quad (3) m > n$$

Prova

Idêntica à demonstração da lei da tricotomia (teorema 1.6.5).

As propriedades contidas no teorema seguinte são de verificação imediata.

TEOREMA 1.11.3 Dados os números naturais m , n e p então

$$(a) \text{ Se } m = n \text{ então } m + p = n + p \text{ e } mp = np$$

$$(b) \text{ Se } m < p \text{ então } m + n < p + n$$

$$(c) \text{ Se } m < p \text{ e se } n \neq 0 \text{ então } mn < pn$$

$$(d) \text{ Se } m + p < n + p \text{ ou se } mp < np \text{ então } m < n$$

$$(e) \text{ Lei do cancelamento da operação de adição: Se } m + n = m + p \text{ então } n = p$$

(f) Lei do cancelamento da operação de multiplicação: Se $mn = pn$ e se $n \neq 0$ então $m = p$.

TEOREMA 1.11.4 A LEI DA INTEGRIDADE DO CONJUNTO DOS NÚMEROS NATURAIS.

Dados os números naturais m e n , se $mn = 0$ então ou $m = 0$ ou $n = 0$.

Prova

Se m é um número natural diferente de zero então como $mn = m0$ pela lei do cancelamento da operação de multiplicação $n = 0$.

TEOREMA 1.11.5 Para cada número natural n , $0 \leq n$

Prova

Seja $A = \{ n \in \mathbb{N} : 0 \leq n \}$. Então $0 \in A$ porque $0 \leq 0$ pela propriedade reflexiva da relação de ordem. Se $n \in A$ então pela definição de A , $0 \leq n$ e de $n \in n+$ segue que $n \leq n+$; pela propriedade transitiva da relação de ordem, $0 \leq n+$. Pelo princípio da indução matemática, $A = \mathbb{N}$ e o teorema está provado.

TEOREMA 1.11.6 Dados os números naturais m e n , se $n < m$ (o que significa que n é menor ou igual a m e n é diferente de m) então $n+ \leq m$.

Prova

Fixado o número natural m , seja $A_m = \{ n \in \mathbb{N} : m < n \Rightarrow m+ \leq n \}$. Então $0 \in A_m$ porque $0 \notin A_m$ é equivalente a dizer que $m < 0$ e que $m+$ não é menor ou igual a 0 , o que é uma contradição: $m < 0$ significa que $m \in 0$ mas 0 é o conjunto vazio. Se $n \in A_m$ então, pela definição de A_m , $m < n$ implica $m+ \leq n$. Se $m < n+$ então $m \in n+$, ou seja $m \in n$ ou $m = n$; caso ocorra a igualdade $m+ = n+$ e no caso $m \in n$ segue que $m < n$, e então $m+ \leq n < n+$. Pelo princípio da indução matemática $A_m = \mathbb{N}$ e o teorema está provado.

Para cada enumeração do conjunto dos números naturais existe uma relação de ordem total no conjunto dos números naturais associada à enumeração dada, no sentido que $m < n$ tem o significado de que m precede n na enumeração considerada. Por exemplo na enumeração $2, 4, 6, 8, \dots, 0, \dots, 11, 9, 7, 5, 3, 1$, o número natural 8 é menor do que o número natural 3 .

TEOREMA 1.11.7 PRINCÍPIO DA BOA ORDENAÇÃO

Seja A um subconjunto não vazio do conjunto $\mathbb{N} = \{ 0, 1, 2, \dots \}$ dos números naturais. Então existe em A o elemento mínimo no sentido de que existe um elemento $m \in A$ tal que para todo elemento $a \in A$, $m \leq a$.

Prova

Admitindo-se a existência de um subconjunto não vazio A do conjunto dos números naturais que não admite a existência do elemento mínimo, seja

$$B = \{ n \in \mathbb{N} = \{ 0, 1, 2, \dots \} : n \leq a \forall a \in A \}$$

Então A e B são subconjuntos disjuntos do conjunto dos números naturais e $0 \in B$ porque $0 \leq n$ para todo número natural n ; se $n \in B$, por definição de B , $n \leq a \forall a \in A$ e $n \notin A$ por hipótese ($n \in A$ significa que n é o elemento mínimo de A). Portanto, $n < a \forall a \in A$ e em consequência $n^+ \leq a \forall a \in A$ mas $n^+ \notin A$ ($n^+ \in A$ significa que n^+ é o elemento mínimo de A). Assim, se $n \in B$ então $n^+ \in B$. Pelo princípio da indução matemática, $B = \mathbb{N}$ e $B \cap A = \emptyset$. Assim $A = \emptyset$ o que é uma contradição pois A é não vazio por hipótese. O princípio da boa ordenação para o conjunto \mathbb{N} dos números naturais está provado.

1.12 RELAÇÃO DE DIVISIBILIDADE NO CONJUNTO \mathbb{N} DOS NÚMEROS NATURAIS:

O número natural n é um múltiplo do número natural m , indicado pelo símbolo $m \mid n$, quando e somente quando o número natural n for o número natural produto do número natural m por algum outro número natural ou, equivalentemente, o número natural m é um divisor natural do número n quando e somente quando existir um número natural p de modo que n é o número natural produto dos fatores m e p , isto é, $n = mp$

A relação de divisibilidade R_d no conjunto dos números naturais é definida por:

$$R_d = \{ (n, m) : \exists p \in \mathbb{N} : n = mp \}$$

A relação de divisibilidade R_d definida em $\mathbb{N} \times \mathbb{N}$ é uma relação binária de ordem parcial no conjunto dos números naturais por possuir as propriedades reflexiva, antissimétrica e transitiva e de modo algum é compatível com as operações de adição e de multiplicação no conjunto \mathbb{N} dos números naturais.

A relação de divisibilidade R_d é uma relação binária reflexiva porque para cada número natural n $n \mid n$ em vista de que $1n = n$.

A relação de divisibilidade R_d é uma relação binária antissimétrica porque dados os números naturais m e n , se $m \mid n$ e se $n \mid m$ então $m = n$.

A relação de divisibilidade R_d é uma relação binária transitiva porque dados os números naturais m , n e p , se $m \mid n$ e se $n \mid p$, então $m \mid p$.

Os números naturais primos são os números naturais p cujos únicos divisores são 1 e p . Os números naturais primos são os átomos na relação de divisibilidade devido ao teorema fundamental da aritmética abaixo.

TEOREMA 1.12.1 TEOREMA FUNDAMENTAL DA ARITMÉTICA

Todo número natural n maior ou igual a 2 é produto de números primos não necessariamente distintos entre n , ou seja, existe um número natural r e números primos p_1, p_2, \dots, p_r e números primos e_1, e_2, \dots, e_r , tais que

$$p_1 < p_2 < \dots < p_r$$

$$n = p_1^{e_1} p_2^{e_2} \dots p_r^{e_r}$$

Prova

A demonstração do teorema fundamental da aritmética é baseada no princípio da indução matemática completa.

Seja A o subconjunto dos números naturais n de modo que $n + 1$ é produto de números naturais primos não necessariamente distintos.

Então

(i) $1 \in A$ porque $1 + 1 = 2$ é um número natural primo.

(ii) se $1, 2, \dots, n \in A$ então $n + 1 \in A$ porque ou $n + 1$ é um número primo e a demonstração está completa ou $n + 1$ é um número composto no sentido de que existem números naturais a e b com

$$n + 1 = ab$$

e com

$$a, b \in \{2, 3, \dots, n + 1\}$$

Pela hipótese de indução, a e b são produtos de números naturais primos não necessariamente distintos e $n + 1 = ab$, então também é produto de números naturais primos não necessariamente distintos.

TEOREMA 1.12.2 PROPRIEDADE ARQUIMEDIANA DO CONJUNTO DOS NÚMEROS NATURAIS.

Dados os números naturais m e n , existe um número natural k tal que $km \geq n$ e $(k + 1)m > n$.

Prova

Admitindo-se que, para cada número natural $l \in \{ 1, 2, 3, \dots \}$ $lm < n$, o subconjunto A do conjunto dos números naturais constituído pela totalidade dos números naturais k tal que $k > lm$ é não vazio pois $n \in A$ e, pelo princípio da boa ordenação, admite um mínimo $n_0 \in A$ e de $n_0 > lm$ para cada número natural e segue que $n_0 > m$ e que $n_0 - m \notin A$.

O que significa que existe um número natural l_0 tal que $n_0 - m < l_0 m$ ou $n_0 < (l_0 + 1)m$, o que é uma contradição ($n_0 > lm$ para cada número natural l). Portanto, existe um número natural k tal que $km \geq n$ e existe um número natural $k + 1$ tal que $(k + 1)m > km \geq n$.

2. O CONJUNTO \mathbb{Z} DOS NÚMEROS INTEIROS .

O conjunto \mathbb{Z} dos números inteiros é construído a partir do conjunto $\mathbb{N} = \{ 0, 1, 2, 3, 4, 5, 6, 7, 8, \dots \}$ dos números naturais.

O que é um número inteiro? Números inteiros são subconjuntos não vazios do produto cartesiano $\mathbb{N} \times \mathbb{N}$, isto é, números inteiros são conjuntos cujos elementos são pares ordenados de números naturais. Para ser mais preciso, números inteiros são classes de equivalência de uma relação binária de equivalência específica definida no conjunto $\mathbb{N} \times \mathbb{N}$ (uma relação binária no produto cartesiano $\mathbb{N} \times \mathbb{N}$ é um subconjunto $(\mathbb{N} \times \mathbb{N}) \times (\mathbb{N} \times \mathbb{N})$ e uma relação binária de equivalência é uma relação binária reflexiva, simétrica e transitiva).

A relação binária de equivalência (**R**) sobre o conjunto $\mathbb{N} \times \mathbb{N}$, cujas classes de equivalência são números inteiros, é definida por:

$$\mathbf{R} = \{ ((a, b), (c, d)) : a, b, c, d \in \mathbb{N} : a + d = b + c \} \subset (\mathbb{N} \times \mathbb{N}) \times (\mathbb{N} \times \mathbb{N}).$$

em que a operação de adição na definição de relação binária é a operação de adição números naturais.

A relação binária **R** no conjunto $\mathbb{N} \times \mathbb{N}$ é de fato uma relação de equivalência, por ser uma relação binária reflexiva, simétrica e transitiva no conjunto $\mathbb{N} \times \mathbb{N}$.

Os números inteiros são então definidos a seguir.

O número inteiro **0** é a classe de equivalência segundo **R** do elemento

$$(0, 0) \in \mathbb{N} \times \mathbb{N}, \text{ ou seja:}$$

$$\begin{aligned} \mathbf{0} &= \{ (n, m) \in \mathbb{N} \times \mathbb{N} : ((n, m), (0, 0)) \in \mathbf{R} \} \\ &= \{ (n, m) \in \mathbb{N} \times \mathbb{N} : n + 0 = m + 0 \} \\ &= \{ (n, n) : n \in \mathbb{N} \} \\ &= \{ (0, 0), (1, 1), (2, 2), (3, 3), \dots \}. \end{aligned}$$

O número inteiro **1** é a classe de equivalência segundo **R** do elemento

$$(1, 0) \in \mathbb{N} \times \mathbb{N}, \text{ ou seja:}$$

$$\mathbf{1} = \{ (n, m) \in \mathbb{N} \times \mathbb{N} : ((n, m), (1, 0)) \in \mathbf{R} \}$$

$$\begin{aligned}
&= \{ (n, m) \in \mathbb{N} \times \mathbb{N} : n + 0 = m + 1 \} \\
&= \{ (n + 1, n) : n \in \mathbb{N} \} \\
&= \{ (1, 0); (2, 1); (3, 2); (4, 3), \dots \}
\end{aligned}$$

O número inteiro -1 é a classe de equivalência segundo \mathbf{R} do elemento

$$(0, 1) \in \mathbb{N} \times \mathbb{N}, \text{ ou seja:}$$

$$\begin{aligned}
-1 &= \{ (n, m) \in \mathbb{N} \times \mathbb{N} : ((n, m), (0, 1)) \in \mathbf{R} \} \\
&= \{ (n, m) \in \mathbb{N} \times \mathbb{N} : n + 1 = m + 0 \} \\
&= \{ (n, n + 1) : n \in \mathbb{N} \} \\
&= \{ (0, 1); (1, 2); (2, 3); (3, 4), \dots \}
\end{aligned}$$

O número inteiro 2 é a classe de equivalência segundo \mathbf{R} do elemento

$$(2, 0) \in \mathbb{N} \times \mathbb{N}, \text{ ou seja:}$$

$$\begin{aligned}
2 &= \{ (n, m) \in \mathbb{N} \times \mathbb{N} : ((n, m), (2, 0)) \in \mathbf{R} \} \\
&= \{ (n, m) \in \mathbb{N} \times \mathbb{N} : n + 0 = m + 2 \} \\
&= \{ (n + 2, n) : n \in \mathbb{N} \} \\
&= \{ (2, 0); (3, 1); (4, 2); (5, 3), \dots \}.
\end{aligned}$$

Desse modo, o número inteiro -2 é a classe de equivalência segundo \mathbf{R} do elemento $(0, 2) \in \mathbb{N} \times \mathbb{N}$, ou seja:

$$\begin{aligned}
-2 &= \{ (n, m) \in \mathbb{N} \times \mathbb{N} : ((n, m), (0, 2)) \in \mathbf{R} \} \\
&= \{ (n, m) \in \mathbb{N} \times \mathbb{N} : n + 2 = m + 0 \} \\
&= \{ (n, n + 2) : n \in \mathbb{N} \} \\
&= \{ (0, 2); (1, 3); (2, 4); (3, 5), \dots \}.
\end{aligned}$$

Generalizando, para cada número inteiro m em que um dos representantes segundo \mathbf{R} é o par ordenado de números naturais (a, b) , o número inteiro $-m$ é definido como a classe de equivalência segundo \mathbf{R} do par ordenado de números naturais (b, a) . A definição é independente do representante segundo \mathbf{R} escolhido para o número inteiro.

2.1 A OPERAÇÃO DE ADIÇÃO NO CONJUNTO \mathbb{Z} DOS NÚMEROS INTEIROS.

Dados dois números inteiros \mathbf{m}_1 e \mathbf{m}_2 , cujos representantes são: (a_1, b_1) e (a_2, b_2) em que $a_1, b_1, a_2, b_2 \in \mathbb{N}$, respectivamente, o número inteiro $\mathbf{m}_1 + \mathbf{m}_2$, soma das parcelas \mathbf{m}_1 e \mathbf{m}_2 , é o número inteiro, que é uma classe de equivalência segundo R , cujo representante é o par ordenado $(a_1 + a_2, b_1 + b_2)$ pertencente a $\mathbb{N} \times \mathbb{N}$. Em que a operação de adição em cada elemento do par ordenado é a operação de adição de números naturais.

A definição da soma $\mathbf{m}_1 + \mathbf{m}_2$ de dois números inteiros \mathbf{m}_1 e \mathbf{m}_2 é independente da escolha dos representantes dos números inteiros \mathbf{m}_1 e \mathbf{m}_2 .

De fato, se (a_1, b_1) e (c_1, d_1) são representantes do número inteiro \mathbf{m}_1 e se (a_2, b_2) e (c_2, d_2) são representantes do número inteiro \mathbf{m}_2 .

$$(a_1 + a_2, b_1 + b_2), (c_1 + c_2, d_1 + d_2) \in R$$

tendo em vista que:

$$(a_1 + a_2) + (d_1 + d_2) = (b_1 + b_2, c_1 + c_2)$$

pois, por hipótese:

$$((a_1, b_1), (c_1, d_1)) \in R, \text{ ou equivalentemente } a_1 + d_1 = b_1 + c_1$$

ou

$$((a_2, b_2), (c_2, d_2)) \in R, \text{ ou equivalentemente } a_2 + d_2 = b_2 + c_2.$$

Em conclusão, o número inteiro $\mathbf{m}_1 + \mathbf{m}_2$ soma de dois números inteiros \mathbf{m}_1 e \mathbf{m}_2 está bem definido.

TEOREMA 2.1.1 PROPRIEDADE ASSOCIATIVA DA OPERAÇÃO DE ADIÇÃO.

Dados os números inteiros \mathbf{m}_1 , \mathbf{m}_2 e \mathbf{m}_3 , então $(\mathbf{m}_1 + \mathbf{m}_2) + \mathbf{m}_3 = \mathbf{m}_1 + (\mathbf{m}_2 + \mathbf{m}_3)$

Prova

Sejam os pares ordenados de números naturais (a_1, b_1) , (a_2, b_2) e (a_3, b_3) representantes dos números inteiros \mathbf{m}_1 , \mathbf{m}_2 e \mathbf{m}_3 respectivamente. Então um dos

representantes dos números inteiros $\mathbf{m}_1 + \mathbf{m}_2$ e $\mathbf{m}_2 + \mathbf{m}_3$ são respectivamente os pares ordenados dos números naturais $(a_1 + a_2, b_1 + b_2)$ e $(a_2 + a_3, b_2 + b_3)$; e um dos representantes dos números inteiros $(\mathbf{m}_1 + \mathbf{m}_2) + \mathbf{m}_3$ e $\mathbf{m}_1 + (\mathbf{m}_2 + \mathbf{m}_3)$ são respectivamente os pares ordenados dos números naturais

$$((a_1 + a_2) + a_3, (b_1 + b_2) + b_3) \text{ e } (a_1 + (a_2 + a_3), b_1 + (b_2 + b_3))$$

e estes pares ordenados de números naturais são iguais pela associatividade da operação de adição de números naturais.

A prova da associatividade da operação de adição de números inteiros está completa.

TEOREMA 2.1.2 PROPRIEDADE COMUTATIVA DA OPERAÇÃO DE ADIÇÃO.

Dados os números inteiros $\mathbf{m}_1, \mathbf{m}_2$ então $\mathbf{m}_1 + \mathbf{m}_2 = \mathbf{m}_2 + \mathbf{m}_1$

Prova

Sejam os pares ordenados de números naturais (a_1, b_1) e (a_2, b_2) representantes dos números inteiros \mathbf{m}_1 e \mathbf{m}_2 respectivamente. Então um dos representantes dos números inteiros $\mathbf{m}_1 + \mathbf{m}_2$ e $\mathbf{m}_2 + \mathbf{m}_1$ são respectivamente os pares ordenados dos números naturais $(a_1 + a_2, b_1 + b_2)$ e $(a_2 + a_1, b_2 + b_1)$; e estes pares ordenados de números naturais são iguais pela comutatividade da operação de adição de números naturais.

A prova da comutatividade da operação de adição de números inteiros está completa.

TEOREMA 2.1.3 EXISTÊNCIA DO ELEMENTO NEUTRO DA OPERAÇÃO DE ADIÇÃO.

Para cada número inteiro \mathbf{m} , $\mathbf{m} + \mathbf{0} = \mathbf{m}$.

Prova

Seja o par ordenado de números naturais (a, b) um dos representantes segundo R do número inteiro \mathbf{m} e seja $(0, 0)$ um dos representantes segundo R do número inteiro zero. Então

$$(a + 0, b + 0) = (a, b)$$

O par ordenado de números naturais $(a + 0, b + 0)$ é um dos representantes do número inteiro $\mathbf{m} + \mathbf{0}$ e o par ordenado de números naturais (a, b) é um dos representantes do número inteiro \mathbf{m} . Portanto, $\mathbf{m} + \mathbf{0} = \mathbf{m}$.

TEOREMA 2.1.4 EXISTÊNCIA DO ELEMENTO INVERSO ADITIVO OU ELEMENTO SIMÉTRICO DA OPERAÇÃO DE ADIÇÃO.

Para cada número inteiro \mathbf{m} , o número inteiro soma das parcelas inteiras \mathbf{m} e $-\mathbf{m}$ é igual ao número inteiro $\mathbf{0}$.

Prova

Seja o par ordenado (a, b) de números naturais um representante segundo \mathbf{R} do número inteiro \mathbf{m} . Então o par ordenado (b, a) de números naturais é um dos representantes segundo \mathbf{R} do número inteiro $-\mathbf{m}$ porque o par ordenado de números naturais $(a + b, a + b) = (a, b) + (b, a)$ é um dos representantes segundo \mathbf{R} do número inteiro soma das parcelas inteiras $\mathbf{m} + (-\mathbf{m})$ e é também um dos representantes segundo \mathbf{R} do número inteiro $\mathbf{0}$. Portanto $\mathbf{m} + (-\mathbf{m}) = -\mathbf{m} + \mathbf{m} = \mathbf{0}$.

2.2 A OPERAÇÃO DE MULTIPLICAÇÃO NO CONJUNTO \mathbb{Z} DOS NÚMEROS INTEIROS.

Dados dois números inteiros \mathbf{m}_1 e \mathbf{m}_2 que são classes de equivalência segundo \mathbf{R} , cujos representantes são os pares ordenados de números naturais (a_1, b_1) e (a_2, b_2) respectivamente, o número inteiro $\mathbf{m}_1 \cdot \mathbf{m}_2$ produto dos fatores inteiros \mathbf{m}_1 e \mathbf{m}_2 é a classe de equivalência segundo \mathbf{R} cujo representante é o par ordenado de números naturais:

$$(a_1a_2 + b_1b_2, a_1b_2 + b_1a_2)$$

em que as operações de adição e multiplicação são relativas a números naturais.

A definição do número inteiro produto $\mathbf{m}_1 \cdot \mathbf{m}_2$ dos números inteiros \mathbf{m}_1 e \mathbf{m}_2 é independente da escolha dos representantes dos números inteiros \mathbf{m}_1 e \mathbf{m}_2 que são classes de equivalência segundo \mathbf{R} .

De fato, sejam os pares ordenados (a_1, b_1) e (c_1, d_1) de números naturais representantes do número inteiro \mathbf{m}_1 e sejam os pares ordenados (a_2, b_2) e (c_2, d_2) de números naturais representantes do número inteiro \mathbf{m}_2 ; como

$$\{(a_1, b_1); (c_1, d_1)\} \in \mathbf{R}, \text{ isto é, } a_1 + d_1 = b_1 + c_1$$

e como

$$\{(a_2, b_2); (c_2, d_2)\} \in \mathbf{R}, \text{ isto é, } a_2 + d_2 = b_2 + c_2$$

logo

$$\{(a_1a_2 + b_1b_2, a_1b_2 + b_1a_2); (c_1c_2 + d_1d_2, c_1d_2 + d_1c_2)\}$$

são elementos de \mathbf{R} , pois

$$a_1a_2 + b_1b_2 + c_1d_2 + d_1c_2 = a_1b_2 + b_1a_2 + c_1c_2 + d_1d_2$$

em vista de que:

$$(a_1 + d_1)(a_2 + d_2) = (b_1 + c_1)(b_2 + c_2)$$

$$(a_1 + d_1)(b_2 + c_2) = a_1b_2 + a_1c_2 + d_1b_2 + d_1c_2$$

TEOREMA 2.2.1 PROPRIEDADE ASSOCIATIVA DA OPERAÇÃO DE MULTIPLICAÇÃO.

Dados os números inteiros m_1 , m_2 e m_3 , então $(m_1m_2)m_3 = m_1(m_2m_3)$

Prova

Sejam os pares ordenados de números naturais (a_1, b_1) , (a_2, b_2) e (a_3, b_3) representantes dos números inteiros m_1 , m_2 e m_3 respectivamente. Então um dos representantes dos números inteiros m_1m_2 e m_2m_3 são respectivamente os pares ordenados dos números naturais $(a_1a_2 + b_1b_2, a_1b_2 + a_2b_1)$ e $(a_2a_3 + b_2b_3, a_2b_3 + a_3b_2)$; e um dos representantes dos números inteiros $(m_1m_2)m_3$ e $m_1(m_2m_3)$ são respectivamente os pares ordenados dos números naturais

$$((a_1a_2 + b_1b_2)a_3 + (a_1b_2 + a_2b_1)b_3, (a_1a_2 + b_1b_2)b_3 + a_3(a_1b_2 + a_2b_1))$$

$$\text{e } (a_1(a_2a_3 + b_2b_3) + b_1(a_2b_3 + a_3b_2), a_1(a_2b_3 + a_3b_2) + (a_2b_3 + a_3b_2)b_1)$$

e estes pares ordenados de números naturais são iguais pelas propriedades das operações de adição e de multiplicação de números naturais.

A prova da associatividade da operação de multiplicação de números inteiros está completa.

TEOREMA 2.2.2 PROPRIEDADE COMUTATIVA DA OPERAÇÃO DE MULTIPLICAÇÃO.

Dados os números inteiros m_1 , m_2 então $m_1m_2 = m_2m_1$

Prova

Sejam os pares ordenados de números naturais (a_1, b_1) e (a_2, b_2) representantes dos números inteiros m_1 e m_2 respectivamente. Então um dos representantes dos números inteiros m_1m_2 e m_2m_1 são respectivamente os pares ordenados dos números naturais $(a_1a_2 + b_1b_2, a_1b_2 + a_2b_1)$ e $(a_2a_1 + b_2b_1, a_2b_1 + a_1b_2)$; e estes pares ordenados de números naturais são iguais pela comutatividade das operações de adição e de multiplicação de números naturais.

A prova da comutatividade da operação de multiplicação de números inteiros está completa.

TEOREMA 2.2.3 EXISTÊNCIA DO ELEMENTO NEUTRO DA OPERAÇÃO DE MULTIPLICAÇÃO.

Para cada número inteiro m , $1m = m$.

Prova

Seja (a, b) um dos representantes segundo \mathbf{R} do número inteiro m e seja o par ordenado de números naturais $(1, 0)$ um dos representantes segundo \mathbf{R} do número inteiro um. Então o par ordenado de números naturais (a, b) é um dos representantes segundo \mathbf{R} do número inteiro produto dos fatores inteiros 1 e m e é também um dos representantes segundo \mathbf{R} do número inteiro m . Portanto $1m = m$.

TEOREMA 2.2.4 PROPRIEDADE DISTRIBUTIVA DA OPERAÇÃO DE MULTIPLICAÇÃO EM RELAÇÃO À OPERAÇÃO DE ADIÇÃO.

Dados os números inteiros m_1 , m_2 e m_3 , então $(m_1 + m_2)m_3 = m_1m_3 + m_2m_3$

Prova

Sejam os pares ordenados de números naturais (a_1, b_1) , (a_2, b_2) e (a_3, b_3) representantes dos números inteiros m_1 , m_2 e m_3 respectivamente. Então um dos representantes dos números inteiros $(m_1 + m_2)$, $(m_1 + m_2)m_3$, m_1m_3 , m_2m_3 e $(m_1m_3 + m_2m_3)$ são respectivamente os pares ordenados dos números naturais :

$$(a_1 + a_2, b_1 + b_2)$$

$$((a_1 + a_2)a_3 + (b_1 + b_2)b_3, (a_1 + a_2)b_3 + (b_1 + b_2)a_3)$$

$$(a_1a_3 + b_1b_3, a_1b_3 + a_3b_1)$$

$$(a_2a_3 + b_2b_3, a_2b_3 + a_3b_2)$$

$$((a_1a_3 + b_1b_3) + (a_2a_3 + b_2b_3), (a_1b_3 + a_3b_1) + (a_2b_3 + a_3b_2))$$

Um dos representantes do número inteiro $(m_1 + m_2)m_3$ é igual a um dos representantes do número inteiro $(m_1m_3 + m_2m_3)$ e assim $(m_1 + m_2)m_3 = m_1m_3 + m_2m_3$.

A prova da distributividade da operação de multiplicação em relação à operação de adição de números inteiros está completa.

2.3 A OPERAÇÃO DE SUBTRAÇÃO NO CONJUNTO \mathbb{Z} DOS NÚMEROS INTEIROS.

Dados dois números \mathbf{m}_1 e \mathbf{m}_2 que são classes de equivalência segundo \mathbf{R} , cujos representantes são os pares ordenados de números naturais (a_1, b_1) e (a_2, b_2) respectivamente, o número inteiro $\mathbf{m}_1 - \mathbf{m}_2$ diferença dos números inteiros \mathbf{m}_1 e \mathbf{m}_2 é o número inteiro, que é uma classe de equivalência segundo \mathbf{R} cujo representante é o par ordenado de números naturais

$$(a_1 + b_2, a_2 + b_1)$$

em que a operação de adição é referente a números naturais.

A definição do número inteiro diferença $\mathbf{m}_1 - \mathbf{m}_2$ do número inteiro subtraendo \mathbf{m}_1 e do número inteiro minuendo \mathbf{m}_2 é independente da escolha dos representantes dos números inteiros \mathbf{m}_1 e \mathbf{m}_2 .

De fato, sejam os pares ordenados (a_1, b_1) e (c_1, d_1) de números naturais representantes do número inteiro \mathbf{m}_1 e sejam os pares ordenados (a_2, b_2) e (c_2, d_2) de números naturais representantes do número inteiro \mathbf{m}_2 ; como:

$$\{(a_1, b_1); (c_1, d_1)\} \in \mathbf{R}, \text{ isto é, } a_1 + d_1 = b_1 + c_1$$

e como

$$\{(a_2, b_2); (c_2, d_2)\} \in \mathbf{R}, \text{ isto é, } a_2 + d_2 = b_2 + c_2$$

logo

$$\{(a_1 + b_2, a_2 + b_1); (c_1 + d_2, c_2 + d_1)\} \in \mathbf{R}$$

visto que

$$(a_1 + b_2) + (c_2 + d_1) = (a_2 + b_1) + (c_1 + d_2)$$

PROPRIEDADE: Dados os números inteiros \mathbf{m}_1 e \mathbf{m}_2 , $\mathbf{m}_1 - \mathbf{m}_2 = \mathbf{m}_1 + (-\mathbf{m}_2)$.

2.4 RELAÇÃO DE DIVISIBILIDADE NO CONJUNTO \mathbb{Z} DOS NÚMEROS INTEIROS.

O número inteiro n é um múltiplo do número inteiro m , indicado pelo símbolo $m \mid n$, quando e somente quando o número natural n é o número inteiro produto do número inteiro m por algum outro número inteiro ou equivalentemente, o número inteiro m é um divisor inteiro do número n quando e somente quando existir um número inteiro p de modo que n é o número inteiro produto dos fatores m e p , isto é:

$$n = mp$$

A relação de divisibilidade R_d definida em $\mathbb{Z} \times \mathbb{Z}$ não é uma relação de ordem parcial entre números inteiros por possuir apenas as propriedades reflexiva e transitiva; a propriedade antissimétrica não é válida em R_d pois se $m \mid n$ e $n \mid m$ então $n = \pm m$.

A relação de divisibilidade R_d entre números inteiros não é compatível com as operações de adição e de multiplicação no conjunto \mathbb{Z} dos números inteiros.

Por exemplo:

$$2 \mid 10$$

$$4 \mid 12$$

não implica nem que $(2 + 4)$ é um divisor de $(10 + 12)$ e nem que $(2 \cdot 4)$ é um divisor de $(10 \cdot 12)$.

2.5 A RELAÇÃO NATURAL DE ORDEM NO CONJUNTO \mathbb{Z} DOS NÚMEROS INTEIROS.

Seja \mathbb{P} o subconjunto dos números inteiros que são classes de equivalência segundo R dos pares ordenados de números naturais em que o primeiro elemento do par ordenado é um número natural diferente de zero e o segundo elemento do par ordenado é o número natural zero.

O subconjunto \mathbb{P} dos números inteiros é um subconjunto fechado em relação as operações de adição e de multiplicação de números inteiros no sentido de que: se $m \in \mathbb{P}$ e se $n \in \mathbb{P}$ então $(m + n) \in \mathbb{P}$ e $mn \in \mathbb{P}$.

O número inteiro \mathbf{m} é menor do que o número inteiro \mathbf{n} indicado pela notação $\mathbf{m} < \mathbf{n}$ ou o número inteiro \mathbf{n} é maior do que o número inteiro \mathbf{m} indicado pela notação $\mathbf{n} > \mathbf{m}$ quando e somente quando existe um número inteiro \mathbf{p} pertencente ao subconjunto \mathbb{P} tal que:

$$\mathbf{n} = \mathbf{m} + \mathbf{p}$$

Em particular, o número inteiro zero é menor do que qualquer número inteiro pertencente ao subconjunto \mathbb{P} de números inteiros.

A sentença $\mathbf{m} \leq \mathbf{n}$ ou $\mathbf{n} \geq \mathbf{m}$ em que \mathbf{m} e \mathbf{n} são números inteiros significa que ou \mathbf{m} é igual a \mathbf{n} (indicado pelo símbolo $\mathbf{m} = \mathbf{n}$) ou que o número inteiro \mathbf{m} é menor do que o número inteiro \mathbf{n} .

A relação canônica de desigualdade entre números inteiros é a relação binária de ordem total $\mathbf{R}_{\leq} \subset \mathbb{Z} \times \mathbb{Z}$ definida em $\mathbb{Z} \times \mathbb{Z}$ por :

$$\mathbf{R}_{\leq} = \{ (m, n) \in \mathbb{Z} \times \mathbb{Z} : m \leq n \}$$

De fato, \mathbf{R}_{\leq} é uma relação binária de ordem total no conjunto \mathbb{Z} dos números inteiros pois satisfaz as propriedades reflexiva, antissimétrica e transitiva.

O conjunto \mathbb{Z} dos números inteiros é união disjunta do conjunto \mathbb{P} , do conjunto unitário cujo único elemento é o número inteiro zero e do conjunto $-\mathbb{P}$ em que

$$-\mathbb{P} = \{ n \in \mathbb{Z} : -n \in \mathbb{P} \}$$

TEOREMA 2.5.1 LEI DA TRICOTOMIA PARA O CONJUNTO DOS NÚMEROS INTEIROS.

Dados dois números inteiros \mathbf{m} e \mathbf{n} , uma e somente uma das afirmações é verdadeira:

$$(1) \mathbf{m} = \mathbf{n} \quad (2) \mathbf{m} < \mathbf{n} \quad (3) \mathbf{m} > \mathbf{n}.$$

Prova

Dados os números inteiros \mathbf{m} e \mathbf{n} , ou $\mathbf{m} - \mathbf{n} = \mathbf{0}$ ou $\mathbf{m} - \mathbf{n} \in -\mathbb{P}$ ou $\mathbf{m} - \mathbf{n} \in \mathbb{P}$.

Se $\mathbf{m} - \mathbf{n} = \mathbf{0}$ então $\mathbf{m} = \mathbf{n}$.

Se $\mathbf{m} - \mathbf{n} \in -\mathbb{P}$ então por definição $\mathbf{m} < \mathbf{n}$.

Se $\mathbf{m} - \mathbf{n} \in \mathbb{P}$ então por definição $\mathbf{m} > \mathbf{n}$.

A relação de ordem total \mathbf{R}_{\leq} sobre o conjunto dos números inteiros é uma relação binária \mathbf{R}_{\leq} sobre \mathbb{Z} com as propriedades: reflexiva, antissimétrica e transitiva, e é definida também da seguinte maneira:

Sejam $\mathbf{m}, \mathbf{n} \in \mathbb{Z}$ e (a, b) e $(c, d) \in \mathbb{N} \times \mathbb{N}$, representantes de \mathbf{m} e \mathbf{n} respectivamente, tomados em suas respectivas classes de equivalência. Por definição,

$$(\mathbf{m}, \mathbf{n}) \in \mathbf{R}_{\leq} \text{ ou } \mathbf{m} \mathbf{R}_{\leq} \mathbf{n} \text{ quando e somente quando } a + d \leq b + c.$$

A definição da relação de ordem em \mathbb{Z} é independente dos representantes da classe de equivalência de \mathbf{m} e dos representantes da classe de equivalência de \mathbf{n} .

TEOREMA 2.5.2 COMPATIBILIDADE DA RELAÇÃO DE ORDEM COM A OPERAÇÃO DE ADIÇÃO.

Dados os números inteiros $\mathbf{m}, \mathbf{n}, \mathbf{p}$ e \mathbf{q} .

- (i) Se $\mathbf{m} < \mathbf{n}$ então $\mathbf{m} + \mathbf{p} < \mathbf{n} + \mathbf{p}$
- (ii) Se $\mathbf{m} < \mathbf{n}$ e se $\mathbf{n} < \mathbf{p}$ então $\mathbf{m} < \mathbf{p}$.
- (iii) Se $\mathbf{m} < \mathbf{n}$ e se $\mathbf{p} < \mathbf{q}$ então $\mathbf{m} + \mathbf{p} < \mathbf{n} + \mathbf{q}$.
- (iv) Se $\mathbf{m} < \mathbf{n}$ e se $\mathbf{p} > \mathbf{0}$ então $\mathbf{mp} < \mathbf{np}$.
- (v) Se $\mathbf{m} < \mathbf{n}$ e se $\mathbf{p} < \mathbf{0}$ então $\mathbf{mp} > \mathbf{np}$.
- (vi) Se $\mathbf{m} + \mathbf{p} < \mathbf{n} + \mathbf{p}$ então $\mathbf{m} < \mathbf{n}$.
- (vii) Se $\mathbf{mp} < \mathbf{np}$ e se $\mathbf{p} > \mathbf{0}$ então $\mathbf{m} < \mathbf{n}$.
- (viii) Se $\mathbf{mp} < \mathbf{np}$ e se $\mathbf{p} < \mathbf{0}$ então $\mathbf{m} > \mathbf{n}$.

Faremos as provas de (vi) e (vii).

Prova de (vi)

$\mathbf{m} = \mathbf{m} + \mathbf{0} = \mathbf{m} + (\mathbf{p} + (-\mathbf{p})) = (\mathbf{m} + \mathbf{p}) + (-\mathbf{p}) < (\mathbf{n} + \mathbf{p}) + (-\mathbf{p}) = \mathbf{n}$ (pela hipótese e pelo item (i)).

Prova de (vii)

Admitindo $\mathbf{n} < \mathbf{m}$ e como $\mathbf{p} > \mathbf{0}$, $\mathbf{np} < \mathbf{mp}$ pelo item (iv) o que contradiz a hipótese $\mathbf{mp} < \mathbf{np}$. Admitindo $\mathbf{m} = \mathbf{n}$ segue que $\mathbf{mp} = \mathbf{np}$ o que contradiz a hipótese $\mathbf{mp} < \mathbf{np}$. Pela lei da tricotomia para o conjunto dos números inteiros resta a alternativa $\mathbf{m} < \mathbf{n}$.

TEOREMA 2.5.3 LEIS DO CANCELAMENTO PARA AS OPERAÇÕES BINÁRIAS DE ADIÇÃO E DE MULTIPLICAÇÃO NO CONJUNTO \mathbb{Z} DOS NÚMEROS INTEIROS.

Dados os números inteiros m , n e p .

- (i) Se $m + p = n + p$ então $m = n$.
- (ii) Se $mp = np$ e se $p \neq 0$ então $m = n$.

Prova de (i)

A prova de (i) é obtida adicionando $-p$ a ambos os membros da equação

$$m + p = n + p$$

Prova de (ii)

Sem perda de generalidade, admitindo que $m < n$, duas situações ocorrem: ou $p > 0$ ou $p < 0$. Caso $p > 0$ e $m < n$ segue que $mp < np$. Caso $p < 0$ e $m < n$ segue que $mp > np$. Por hipótese $mp = np$ e pela lei da tricotomia para o conjunto dos números inteiros $m = n$.

TEOREMA 2.5.4 A LEI DA INTEGRIDADE DO CONJUNTO DOS NÚMEROS INTEIROS.

Dados os números inteiros m e n , se $mn = 0$ então ou $m = 0$ ou $n = 0$.

Prova

Se m é um número inteiro diferente de zero então como $mn = m0$ pela lei do cancelamento da operação de multiplicação $n = 0$.

TEOREMA 2.5.5 A REGRA DOS SINAIS NO CONJUNTO \mathbb{Z} DOS NÚMEROS INTEIROS:

Dados os números inteiros m e n ,

- (i) $(-m)n = m(-n) = -(mn)$
- (ii) $(-m)(-n) = mn$.

Prova de (i)

$m(-n) + mn = m(-n + n) = m0 = 0 = -(mn) + mn$ e, pela lei do cancelamento no conjunto dos números inteiros para a operação de adição, $m(-n) = -(mn)$.

$(-m)n + mn = (-m + m)n = 0n = 0 = -(mn) + mn$ e, pela lei do cancelamento no conjunto dos números inteiros para a operação de adição, $(-m)n = -(mn)$.

Prova de (ii)

$(-m)(-n) + m(-n) = (-m + m)(-n) = 0(-n) = 0 = mn + m(-n)$ e, pela lei do cancelamento no conjunto dos números inteiros para a operação de adição,

$$(-m)(-n) = mn.$$

2.6 A INCLUSÃO DO CONJUNTO \mathbb{N} DOS NÚMEROS NATURAIS AO CONJUNTO \mathbb{Z} DOS NÚMEROS INTEIROS.

Para cada número natural $n \in \mathbb{N} = \{0, 1, 2, 3, \dots\}$ é definido o valor $j(n)$ da função inclusão natural j no número natural n sendo igual ao número inteiro classe de equivalência segundo \mathbf{R} do par ordenado de números naturais :

$(n + 1, 1)$ ou do par ordenado $(n, 0)$ com zero sendo considerado um número natural.

A função inclusão natural ou canônica j é uma função cujo domínio é o conjunto \mathbb{N} dos números naturais e cujo conjunto de valores é a união do subconjunto \mathbb{P} com o subconjunto unitário $\{0\}$ de números inteiros contido no conjunto dos números inteiros \mathbb{Z} .

A função inclusão natural j de \mathbb{N} em \mathbb{Z} é uma função injetora e tem as seguintes propriedades: dados dois números naturais m e n ,

$$(1) j(m + n) = j(m) + j(n),$$

$$(2) j(mn) = j(m)j(n)$$

A identificação entre o número natural n e o número inteiro $j(n)$ e o fato de que a soma de dois números naturais m e n é identificado como a soma dos números inteiros $j(m)$ e $j(n)$ pela propriedade (1) da função j e além disso o fato de que o produto de dois números naturais m e n é identificado como o produto dos números inteiros $j(m)$ e $j(n)$ pela propriedade (2) da função j faz com que o conjunto \mathbb{N} dos números naturais seja considerado um subconjunto do conjunto \mathbb{Z} dos números inteiros o que não é verdadeiro, já que $\{j(n): n \in \mathbb{N}\} \subset \mathbb{Z}$.

TEOREMA 2.6.1 A UNICIDADE DA ORDENAÇÃO DO CONJUNTO DOS NÚMEROS INTEIROS.

Seja \mathbf{R} uma relação binária de ordem total no conjunto \mathbb{Z} dos números inteiros com as seguintes propriedades:

(1) Lei da compatibilidade da relação binária de ordem total \mathbf{R} com a operação de adição: Dados os números inteiros \mathbf{m} , \mathbf{n} e \mathbf{p} ,

$$\text{se } (\mathbf{m}, \mathbf{n}) \in \mathbf{R} \text{ então } (\mathbf{m} + \mathbf{p}, \mathbf{n} + \mathbf{p}) \in \mathbf{R}$$

(2) Lei da compatibilidade da relação binária de ordem total \mathbf{R} com a operação de multiplicação: Dados os números inteiros \mathbf{m} , \mathbf{n} e \mathbf{p} ,

$$\text{se } (\mathbf{m}, \mathbf{n}) \in \mathbf{R} \text{ e se } (\mathbf{0}, \mathbf{p}) \in \mathbf{R} \text{ então } (\mathbf{mp}, \mathbf{np}) \in \mathbf{R}.$$

$$(3) (\mathbf{0}, \mathbf{1}) \in \mathbf{R}.$$

Então \mathbf{R} é a relação binária de ordem total canônica do conjunto \mathbb{Z} dos números inteiros. Além disso, a relação binária de ordem total canônica do conjunto \mathbb{Z} dos números inteiros induz de ordem total canônica do conjunto \mathbb{N} dos números naturais.

Prova

Das propriedades (1) e (3), para cada número natural n ,

$$(n, n + 1) = (n + 0, n + 1)$$

é um elemento da relação binária de ordem \mathbf{R} . Portanto a relação de ordem total \mathbf{R} no conjunto dos números inteiros induz a relação de ordem natural no conjunto dos números naturais: Para cada número natural n , $(0, n) \in \mathbf{R}$. Reciprocamente, se \mathbf{m} é um número inteiro pertencente a

$$-\mathbb{P} = \{ n \in \mathbb{Z} : -n \in \mathbb{P} \}$$

Então $\mathbf{m} = -n$ para algum número natural n diferente de zero: se $(\mathbf{0}, \mathbf{m}) = (\mathbf{0}, -n)$ é um elemento de \mathbf{R} , como $(\mathbf{0}, n) \in \mathbf{R}$, $(-n, \mathbf{0}) = (-n + \mathbf{0}, -n + n) \in \mathbf{R}$. De

$$(\mathbf{0}, -n) \in \mathbf{R} \text{ e } (-n, \mathbf{0}) \in \mathbf{R}$$

vem a contradição de que $n = \mathbf{0}$. Está demonstrado que para cada número inteiro \mathbf{m}

$$(\mathbf{0}, \mathbf{m}) \in \mathbf{R} \text{ se e somente se } \mathbf{m} \in \{ \mathbf{0}, \mathbf{1}, \mathbf{2}, \dots \}$$

A unicidade da relação de ordem total \mathbf{R} no conjunto dos números inteiros compatível com as operações de adição e multiplicação é demonstrada quando: para números inteiros \mathbf{m} e \mathbf{n} , se $(\mathbf{m}, \mathbf{n}) \in \mathbf{R}$ então $(\mathbf{n} - \mathbf{m}) \in \{ \mathbf{0}, \mathbf{1}, \mathbf{2}, \dots \}$. De fato, se $(\mathbf{m}, \mathbf{n}) \in \mathbf{R}$ então $(\mathbf{0}, \mathbf{n} - \mathbf{m}) = (\mathbf{m} + (-\mathbf{m}), \mathbf{n} + (-\mathbf{m})) \in \mathbf{R}$, o que é equivalente a afirmar que

$$(\mathbf{n} - \mathbf{m}) \in \{ \mathbf{0}, \mathbf{1}, \mathbf{2}, \dots \}.$$

2.7 TRÊS PRINCÍPIOS DA INDUÇÃO MATEMÁTICA NO CONJUNTO DOS NÚMEROS INTEIROS.

TEOREMA 2.7.1 PRIMEIRO PRINCÍPIO

Seja A um subconjunto do conjunto \mathbb{Z} dos números inteiros com as seguintes propriedades:

- (i) $0 \in A$.
- (ii) se $n \in A$, então $n + 1 \in A$.
- (iii) se $n \in A$, então $n - 1 \in A$.

Então $A = \mathbb{Z}$.

TEOREMA 2.7.2 SEGUNDO PRINCÍPIO

Seja A um subconjunto do conjunto \mathbb{Z} dos números inteiros com as seguintes propriedades:

- (i) $0 \in A$.
- (ii) se $n \in A$, então $n + 1 \in A$.
- (iii) se $n \in A$, então $-n \in A$.

Então $A = \mathbb{Z}$.

TEOREMA 2.7.3 TERCEIRO PRINCÍPIO

Seja A um subconjunto não vazio do conjunto \mathbb{Z} dos números inteiros com as seguintes propriedades:

- (i) se $n \in A$, então $n + 1 \in A$.
- (ii) se $n + 1 \in A$, então $n \in A$.

Então $A = \mathbb{Z}$.

Prova do primeiro princípio

Como $0 \in A$, $1 = 0 + 1 \in A$ (propriedade (ii))

Seja $A_1 = \{ n \in \mathbb{N} : n \in A \}$. Então $1 \in A_1$ e se $n \in A_1$ então $n \in A$ o que acarreta que $n + 1 \in A$ pela definição de A , $n + 1 \in A$.

Seja $B = \{ n \in \mathbb{N} : 1 - n \in A \} \subset \mathbb{N}$

Como $0 \in A$, $-1 = 0 - 1 \in A$ (propriedade (iii)) e então, pela definição do conjunto B , $1 \in B$, se $n \in B$ então pela definição de B , $-n \in A$ e pela propriedade (iii)

$$-(n + 1) = -n - 1 \in A$$

O que implica que $n + 1 - n \in B$.

Pelo princípio da indução matemática no conjunto dos números naturais, com B tem as propriedades

(i) $1 \in B$

(ii) se $n \in B$ então $n + 1 \in B$

segue que $B = \{ 1, 2, 3, \dots \}$ e em consequência A contém todos os inversos aditivos de todos os números naturais.

Pela lei da tricotomia no conjunto \mathbb{Z} dos números inteiros, ou um número inteiro é um número natural ou é o número inteiro zero ou é o negativo de um número natural.

Em resumo, $A = \mathbb{Z}$

Então $A_1 = \{ 1, 2, 3, \dots \}$ e, em consequência, está contido em A .

3. O CONJUNTO \mathbb{Q} DOS NÚMEROS RACIONAIS .

A construção do conjunto \mathbb{Q} dos números racionais é obtida a partir da construção do conjunto \mathbb{Z} dos números inteiros.

O que é um número racional?

Números racionais são subconjuntos não vazios do produto cartesiano $\mathbb{Z} \times \mathbb{Z}^*$ em que \mathbb{Z}^* é o conjunto dos números inteiros diferentes de zero. Mais precisamente, os números racionais são classes de equivalência de uma relação binária de equivalência específica \mathbf{R} no conjunto $\mathbb{Z} \times \mathbb{Z}^*$.

A relação binária de equivalência \mathbf{R} no conjunto $\mathbb{Z} \times \mathbb{Z}^*$ é definida por

$$\mathbf{R} = \{ ((a, b), (c, d)) \in \mathbb{Z} \times \mathbb{Z}^* : ad = bc \} \subset (\mathbb{Z} \times \mathbb{Z}^*) \times (\mathbb{Z} \times \mathbb{Z}^*)$$

em que a operação de multiplicação envolvida é referente a números inteiros.

O número racional zero indicado pelo símbolo $\mathbf{0}$ é a classe de equivalência segundo \mathbf{R} do elemento

$$(0, 1) \in \mathbb{Z} \times \mathbb{Z}^*,$$

ou seja:

$$\mathbf{0} = \{ (0, 1), (0, -1), (0, 2), (0, -2), (0, 3), (0, -3), \dots \}$$

O número racional um indicado pelo símbolo $\mathbf{1}$ é a classe de equivalência segundo \mathbf{R} do elemento

$$(1, 1) \in \mathbb{Z} \times \mathbb{Z}^*,$$

ou seja:

$$\mathbf{1} = \{ (1, 1), (-1, -1), (2, 2), (-2, -2), (3, 3), (-3, -3), \dots \}$$

Dados os números inteiros p e q com $q \neq 0$, o número racional $\frac{p}{q}$ é definido como a classe de equivalência segundo \mathbf{R} do par ordenado de números inteiros (p, q) e os outros representantes do número racional $\frac{p}{q}$ são os pares ordenados de números inteiros (a, b) com $b \neq 0$ e com a propriedade de que $aq = bp$. Sem perda de generalidade, um dos representantes segundo \mathbf{R} do número racional $\frac{p}{q}$ é o par ordenado de números inteiros (p, q) com $q > 0$.

Sem perda de generalidade, o número racional $\frac{p}{q}$ é definido como a classe de equivalência

segundo \mathbf{R} do par ordenado de números inteiros (p, q) com $q \neq 0$ e p e q sem fatores primos comuns.

Dado um número racional \mathbf{m} , que é classe de equivalência segundo \mathbf{R} do par ordenado de números inteiros (a, b) com $b \neq 0$, o número racional $-\mathbf{m}$ é definido como a classe de equivalência segundo \mathbf{R} do par ordenado de números inteiros $(-a, b)$.

Dado um número racional \mathbf{m} diferente do número racional zero, que é classe de equivalência segundo \mathbf{R} do par ordenado de números inteiros (a, b) com $a \neq 0$ e $b \neq 0$, o número racional \mathbf{m}^{-1} é definido como a classe de equivalência segundo \mathbf{R} do par ordenado de números inteiros (b, a) .

3.1 A OPERAÇÃO DE ADIÇÃO NO CONJUNTO \mathbb{Q} DOS NÚMEROS RACIONAIS:

Dados dois números racionais \mathbf{m}_1 e \mathbf{m}_2 , que são classes de equivalência segundo \mathbf{R} , cujos representantes são respectivamente os pares ordenados de números inteiros (a_1, b_1) e (a_2, b_2) com b_1 e b_2 diferentes do número inteiro 0, o número racional $\mathbf{m}_1 + \mathbf{m}_2$ soma das parcelas \mathbf{m}_1 e \mathbf{m}_2 é definido como a classe de equivalência segundo \mathbf{R} do par ordenado de números inteiros:

$$(a_1b_2 + a_2b_1, b_1b_2)$$

A definição da soma $\mathbf{m}_1 + \mathbf{m}_2$ de dois números racionais \mathbf{m}_1 e \mathbf{m}_2 é independente da escolha dos representantes dos números racionais \mathbf{m}_1 e \mathbf{m}_2 . De fato, sejam (a_1, b_1) e (c_1, d_1) pares ordenados de números inteiros com b_1 e d_1 diferentes do número inteiro 0 representantes segundo \mathbf{R} do número racional \mathbf{m}_1 e sejam (a_2, b_2) e (c_2, d_2) pares ordenados de números inteiros com b_2 e d_2 diferentes do número inteiro 0 representantes segundo \mathbf{R} do número racional \mathbf{m}_2 ; como:

$$\{(a_1, b_1), (c_1, d_1)\} \in \mathbf{R}$$

$$a_1d_1 = b_1c_1$$

e como:

$$\{(a_2, b_2), (c_2, d_2)\} \in \mathbf{R}$$

$$a_2d_2 = b_2c_2$$

segue que:

$$(a_1b_2 + a_2b_1) d_1d_2 = b_1b_2 (c_1d_2 + c_2d_1)$$

ou equivalentemente:

$$\{ (a_1b_2 + a_2b_1, b_1b_2), (c_1d_2 + c_2d_1, d_1d_2) \} \in \mathbf{R}$$

e que os pares ordenados de números inteiros

$$(a_1b_2 + a_2b_1, b_1b_2) \text{ e } (c_1d_2 + c_2d_1, d_1d_2)$$

são representantes segundo \mathbf{R} do mesmo número racional.

TEOREMA 3.1.1 PROPRIEDADE ASSOCIATIVA DA OPERAÇÃO DE ADIÇÃO.

Dados os números racionais \mathbf{m}_1 , \mathbf{m}_2 e \mathbf{m}_3 , então

$$(\mathbf{m}_1 + \mathbf{m}_2) + \mathbf{m}_3 = \mathbf{m}_1 + (\mathbf{m}_2 + \mathbf{m}_3)$$

Prova

Sejam os pares ordenados de números inteiros (a_1, b_1) , (a_2, b_2) e (a_3, b_3) com b_1 , b_2 e b_3 números inteiros não nulos, representantes dos números racionais \mathbf{m}_1 , \mathbf{m}_2 e \mathbf{m}_3 respectivamente. Então um dos representantes dos números racionais $\mathbf{m}_1 + \mathbf{m}_2$ e $\mathbf{m}_2 + \mathbf{m}_3$ são respectivamente os pares ordenados dos números inteiros $(a_1b_2 + a_2b_1, b_1b_2)$ e $(a_2b_3 + a_3b_2, b_2b_3)$; e um dos representantes dos números inteiros $(\mathbf{m}_1 + \mathbf{m}_2) + \mathbf{m}_3$ e $\mathbf{m}_1 + (\mathbf{m}_2 + \mathbf{m}_3)$ são respectivamente os pares ordenados dos números inteiros

$$((a_1b_2 + a_2b_1)b_3 + a_3(b_1b_2), (b_1b_2)b_3)$$

$$\text{e } (a_1(b_2b_3) + (a_2b_3 + a_3b_2)b_1, b_1(b_2b_3))$$

e estes pares ordenados de números inteiros são iguais pelas propriedades das operações de adição e de multiplicação de números inteiros.

A prova da associatividade da operação de adição de números racionais está completa.

TEOREMA 3.1.2 PROPRIEDADE COMUTATIVA DA OPERAÇÃO DE ADIÇÃO.

Dados os números racionais \mathbf{m}_1 e \mathbf{m}_2 , então $\mathbf{m}_1 + \mathbf{m}_2 = \mathbf{m}_2 + \mathbf{m}_1$

Prova

Sejam os pares ordenados de números inteiros (a_1, b_1) e (a_2, b_2) com b_1 e b_2 números inteiros não nulos, representantes dos números racionais \mathbf{m}_1 e \mathbf{m}_2 respectivamente. Então um dos representantes dos números racionais $\mathbf{m}_1 + \mathbf{m}_2$ e $\mathbf{m}_2 + \mathbf{m}_1$ são respectivamente os pares ordenados dos números inteiros $(a_1b_2 + a_2b_1, b_1b_2)$ e $(a_2b_1 + a_1b_2, b_2b_1)$; e estes pares

ordenados de números inteiros são iguais pelas propriedades das operações de adição e de multiplicação de números inteiros.

A prova da comutatividade da operação de adição de números racionais está completa.

TEOREMA 3.1.3 EXISTÊNCIA DO ELEMENTO NEUTRO DA OPERAÇÃO DE ADIÇÃO.

Para cada número racional \mathbf{m} , $\mathbf{m} + \mathbf{0} = \mathbf{m}$.

Prova

Seja o par ordenado (a, b) de números inteiros com b diferente do número inteiro zero um dos representantes segundo \mathbf{R} do número racional \mathbf{m} e seja o par ordenado de números inteiros $(0, 1)$ um dos representantes segundo \mathbf{R} do número racional $\mathbf{0}$. Então o par ordenado (a, b) de números inteiros com b diferente do número inteiro zero é um dos representantes segundo \mathbf{R} do número racional soma das parcelas racionais \mathbf{m} e $\mathbf{0}$ e é também um dos representantes segundo \mathbf{R} do número racional \mathbf{m} . Portanto $\mathbf{m} + \mathbf{0} = \mathbf{m}$.

TEOREMA 3.1.4 EXISTÊNCIA DO ELEMENTO INVERSO ADITIVO OU ELEMENTO SIMÉTRICO DA OPERAÇÃO DE ADIÇÃO.

Para cada número racional \mathbf{m} , o número racional soma das parcelas inteiras \mathbf{m} e $-\mathbf{m}$ é igual ao número racional $\mathbf{0}$.

Prova

Seja o par ordenado (a, b) de números inteiros, com b um número inteiro maior que zero, um representante segundo \mathbf{R} do número racional \mathbf{m} . Então o par ordenado de números inteiros $(-a, b)$ é um dos representantes segundo \mathbf{R} do número racional $-\mathbf{m}$ porque o par ordenado de números inteiros $(0, b)$ é um dos representantes segundo \mathbf{R} do número racional soma das parcelas racionais $\mathbf{m} + (-\mathbf{m})$ e é também um dos representantes segundo \mathbf{R} do número racional $\mathbf{0}$. Portanto $\mathbf{m} + (-\mathbf{m}) = -\mathbf{m} + \mathbf{m} = \mathbf{0}$.

3.2 A OPERAÇÃO DE MULTIPLICAÇÃO NO CONJUNTO \mathbb{Q} DOS NÚMEROS RACIONAIS

Dados dois números racionais \mathbf{m}_1 e \mathbf{m}_2 que são classes de equivalência segundo \mathbf{R} , cujos representantes são respectivamente os pares ordenados de números inteiros (a_1, b_1)

com $b_1 \neq 0$ e (a_2, b_2) com $b_2 \neq 0$, o número racional $\mathbf{m_1 m_2}$ produto dos fatores $\mathbf{m_1}$ e $\mathbf{m_2}$ é definido como a classe de equivalência segundo \mathbf{R} do par ordenado de números inteiros:

$$(a_1 a_2, b_1 b_2) \text{ com } b_1 b_2 \neq 0$$

O número racional produto $\mathbf{m_1 m_2}$ dos fatores racionais $\mathbf{m_1}$ e $\mathbf{m_2}$ é independente dos representantes segundo \mathbf{R} dos números racionais $\mathbf{m_1}$ e $\mathbf{m_2}$. De fato, sejam (a_1, b_1) e (c_1, d_1) pares ordenados de números inteiros com $b_1 d_1 \neq 0$ representantes segundo \mathbf{R} do número racional $\mathbf{m_1}$ e sejam (a_2, b_2) e (c_2, d_2) pares ordenados de números inteiros com $b_2 d_2 \neq 0$ representantes segundo \mathbf{R} do número racional $\mathbf{m_2}$; como:

$$\{(a_1, b_1), (c_1, d_1)\} \in \mathbf{R}$$

$$a_1 d_1 = b_1 c_1$$

e como:

$$\{(a_2, b_2), (c_2, d_2)\} \in \mathbf{R}$$

$$a_2 d_2 = b_2 c_2$$

o que implica que (pela multiplicação membro a membro)

$$a_1 a_2 d_1 d_2 = b_1 b_2 c_1 c_2$$

e que equivale colocar que:

$$\{(a_1 a_2, b_1 b_2), (c_1 c_2, d_1 d_2)\} \in \mathbf{R}$$

com:

$$b_1 b_2 \neq 0 \quad d_1 d_2 \neq 0$$

e que os pares ordenados de números inteiros:

$$(a_1 a_2, b_1 b_2) \text{ e } (c_1 c_2, d_1 d_2)$$

são representantes da mesma classe de equivalência segundo \mathbf{R} e conseqüentemente do mesmo número racional.

Por exemplo, o produto do número racional \mathbf{m} e do número racional zero é o número racional zero. Um dos representantes do número racional zero é o par ordenado $(0, 1)$ de números inteiros e um dos representantes do número racional \mathbf{m} é o par ordenado (a, b) de números inteiros, com $b \neq 0$.

O número racional $\mathbf{m \cdot 0}$ produto dos fatores racionais \mathbf{m} e $\mathbf{0}$ tem como um dos representantes segundo \mathbf{R} , o par ordenado de números inteiros $(a \cdot 0, b \cdot 1) = (0, b)$ e o par

ordenado de números inteiros $(0, b)$ é um dos representantes segundo \mathbf{R} do número racional zero.

$$\mathbf{m} \cdot \mathbf{0} = \mathbf{0}.$$

O número racional $\mathbf{m} \cdot \mathbf{1}$, produto dos número racional \mathbf{m} e do número racional $\mathbf{1}$ é o número racional \mathbf{m} . Um dos representantes segundo \mathbf{R} do número racional \mathbf{m} é o par ordenado de números inteiros (a, b) com $b \neq 0$ e um dos representantes segundo \mathbf{R} do número racional $\mathbf{1}$ é o par ordenado de números inteiros $(1, 1)$ e, por definição, $(a \cdot 1, b \cdot 1)$ é o par ordenado de números inteiros representante do número racional produto $\mathbf{m} \cdot \mathbf{1}$ e (a, b) é um dos representantes segundo \mathbf{R} do número racional \mathbf{m} .

$$\mathbf{m} \cdot \mathbf{1} = \mathbf{m}.$$

TEOREMA 3.2.1 PROPRIEDADE ASSOCIATIVA DA OPERAÇÃO DE MULTIPLICAÇÃO.

Dados os números racionais \mathbf{m}_1 , \mathbf{m}_2 e \mathbf{m}_3 , então

$$(\mathbf{m}_1\mathbf{m}_2)\mathbf{m}_3 = \mathbf{m}_1(\mathbf{m}_2\mathbf{m}_3).$$

Prova

Sejam os pares ordenados de números inteiros (a_1, b_1) , (a_2, b_2) e (a_3, b_3) com b_1, b_2 e b_3 números inteiros não nulos, representantes dos números racionais \mathbf{m}_1 , \mathbf{m}_2 e \mathbf{m}_3 respectivamente. Então um dos representantes dos números racionais $\mathbf{m}_1\mathbf{m}_2$ e $\mathbf{m}_2\mathbf{m}_3$ são respectivamente os pares ordenados dos números inteiros (a_1a_2, b_1b_2) e (a_2a_3, b_2b_3) e um dos representantes dos números racionais $(\mathbf{m}_1\mathbf{m}_2)\mathbf{m}_3$ e $\mathbf{m}_1(\mathbf{m}_2\mathbf{m}_3)$ são respectivamente os pares ordenados dos números inteiros

$$((a_1a_2)a_3, (b_1b_2)b_3) \text{ e } (a_1(a_2a_3), b_1(b_2b_3))$$

e estes pares ordenados de números inteiros são iguais pela associatividade da operação de multiplicação de números inteiros.

A prova da associatividade da operação de multiplicação de números racionais está completa.

TEOREMA 3.2.2 PROPRIEDADE COMUTATIVA DA OPERAÇÃO DE MULTIPLICAÇÃO.

Dados os números racionais m_1 e m_2 , então $m_1m_2 = m_2m_1$

Prova

Sejam os pares ordenados de números inteiros (a_1, b_1) e (a_2, b_2) com b_1 e b_2 números inteiros não nulos, representantes dos números racionais m_1 e m_2 respectivamente. Então um dos representantes dos números racionais m_1m_2 e m_2m_1 são respectivamente os pares ordenados dos números inteiros (a_1a_2, b_1b_2) e (a_2a_1, b_2b_1) e estes pares ordenados de números inteiros são iguais pela comutatividade da operação de multiplicação de números inteiros.

A prova da comutatividade da operação de multiplicação de números racionais está completa.

TEOREMA 3.2.3 EXISTÊNCIA DO ELEMENTO NEUTRO DA OPERAÇÃO DE MULTIPLICAÇÃO.

Para cada número racional m , $1m = m$.

Prova

Seja o par ordenado de números inteiros (a, b) , com b diferente do número inteiro zero, um dos representantes segundo \mathbf{R} do número racional m e seja o par ordenado de números inteiros $(1, 1)$ um dos representantes segundo \mathbf{R} do número racional um. Então o par ordenado de números inteiros (a, b) é um dos representantes segundo \mathbf{R} do número racional produto dos fatores racionais 1 e m e é também um dos representantes segundo \mathbf{R} do número racional m . Portanto $1m = m$.

TEOREMA 3.2.4 EXISTÊNCIA DO ELEMENTO INVERSO MULTIPLICATIVO OU ELEMENTO RECÍPROCO DE UM NÚMERO RACIONAL.

Para cada número racional m diferente do número racional zero, o número racional m^{-1} tem a propriedade de que $mm^{-1} = 1$.

Prova

Seja o par ordenado de números inteiros (a, b) , com b um número inteiro maior que zero e a diferente do número inteiro zero, um representante segundo \mathbf{R} do número racional m . Então, o par ordenado de números inteiros (b, a) é um dos representantes segundo \mathbf{R} do número racional m^{-1} , pois o par ordenado de números inteiros $(1, 1)$ é um dos representantes

segundo \mathbf{R} do número racional produto dos fatores racionais \mathbf{mm}^{-1} e é também um dos representantes segundo \mathbf{R} do número racional 1. Portanto, segue que $\mathbf{mm}^{-1} = \mathbf{1}$.

TEOREMA 3.2.5 PROPRIEDADE DISTRIBUTIVA DA OPERAÇÃO DE MULTIPLICAÇÃO EM RELAÇÃO À OPERAÇÃO DE ADIÇÃO.

Dados os números racionais \mathbf{m}_1 , \mathbf{m}_2 e \mathbf{m}_3 , então $(\mathbf{m}_1 + \mathbf{m}_2)\mathbf{m}_3 = \mathbf{m}_1\mathbf{m}_3 + \mathbf{m}_2\mathbf{m}_3$

Prova

Sejam os pares ordenados de números inteiros (a_1, b_1) , (a_2, b_2) e (a_3, b_3) representantes dos números racionais \mathbf{m}_1 , \mathbf{m}_2 e \mathbf{m}_3 respectivamente. Então um dos representantes dos números racionais $(\mathbf{m}_1 + \mathbf{m}_2)$, $(\mathbf{m}_1 + \mathbf{m}_2)\mathbf{m}_3$, $\mathbf{m}_1\mathbf{m}_3$, $\mathbf{m}_2\mathbf{m}_3$ e $(\mathbf{m}_1\mathbf{m}_3 + \mathbf{m}_2\mathbf{m}_3)$ são respectivamente os pares ordenados dos números inteiros com o produto $b_1b_2b_3$ diferente de zero:

$$\begin{aligned} & (a_1b_2 + a_2b_1, b_1b_2) \\ & ((a_1b_2 + a_2b_1)a_3, (b_1b_2)b_3) \\ & (a_1a_3, b_1b_3) \\ & (a_2a_3, b_2b_3) \\ & ((a_1a_3)b_2 + (a_2a_3)b_1, (b_1b_2)b_3) \end{aligned}$$

Um dos representantes do número racional $(\mathbf{m}_1 + \mathbf{m}_2)\mathbf{m}_3$ é igual a um dos representantes do número racional $(\mathbf{m}_1\mathbf{m}_3 + \mathbf{m}_2\mathbf{m}_3)$ e assim $(\mathbf{m}_1 + \mathbf{m}_2)\mathbf{m}_3 = \mathbf{m}_1\mathbf{m}_3 + \mathbf{m}_2\mathbf{m}_3$.

A prova da distributividade da operação de multiplicação em relação à operação de adição de números racionais está completa.

3.3 A OPERAÇÃO DE SUBTRAÇÃO NO CONJUNTO \mathbb{Q} DOS NÚMEROS RACIONAIS.

Dados dois números racionais \mathbf{m}_1 e \mathbf{m}_2 , os quais são classes de equivalência segundo \mathbf{R} cujos representantes são definidos pelas classes de equivalência segundo \mathbf{R} dos pares ordenados de números inteiros (a_1, b_1) e (a_2, b_2) com b_1 e b_2 diferentes do número inteiro 0, o número racional $\mathbf{m}_1 - \mathbf{m}_2$ diferença dos números racionais \mathbf{m}_1 e \mathbf{m}_2 é a classe de equivalência segundo \mathbf{R} do par ordenado de números inteiros:

$$(a_1b_2 - a_2b_1, b_1b_2)$$

O número racional $\mathbf{m}_1 - \mathbf{m}_2$ diferença dos números racionais \mathbf{m}_1 e \mathbf{m}_2 é independente da escolha dos representantes dos números racionais a_1 e a_2 . De fato, sejam os pares ordenados de números inteiros (a_1, b_1) e (a_1', b_1') com $b_1 \neq 0$ e $b_1' \neq 0$, representantes do número racional \mathbf{m}_1 , e sejam os pares ordenados de números inteiros (a_2, b_2) e (a_2', b_2') com $b_2 \neq 0$ e $b_2' \neq 0$, representantes do número racional \mathbf{m}_2 ; como

$$\{(a_1, b_1), (a_1', b_1')\} \in \mathbf{R}$$

$$a_1b_1' = a_1'b_1 \quad (\text{produto de números inteiros})$$

e como:

$$\{(a_2, b_2), (a_2', b_2')\} \in \mathbf{R}$$

$$a_2b_2' = a_2'b_2 \quad (\text{produto de números inteiros})$$

então o produto de números inteiros:

$$a_1a_2b_1'b_2' = a_1'a_2'b_1b_2$$

o que significa que:

$$\{(a_1a_2, b_1b_2), (a_1'a_2', b_1'b_2')\} \in \mathbf{R}$$

PROPRIEDADE: Dados os números racionais \mathbf{m}_1 e \mathbf{m}_2 , $\mathbf{m}_1 - \mathbf{m}_2 = \mathbf{m}_1 + (-\mathbf{m}_2)$

3.4 A OPERAÇÃO DE DIVISÃO NO CONJUNTO \mathbb{Q} DOS NÚMEROS RACIONAIS.

Dados dois números racionais \mathbf{m}_1 e \mathbf{m}_2 , em que \mathbf{m}_2 é um número racional não nulo, os quais são classes de equivalência segundo \mathbf{R} com representantes definidos pelos pares ordenados de números inteiros (a_1, b_1) e (a_2, b_2) com $b_1 \neq 0$, com $b_2 \neq 0$, $a_2 \neq 0$, o número racional quociente resultado da divisão do número racional \mathbf{m}_1 pelo número racional $\mathbf{m}_2 \neq 0$, indicado pelo símbolo $\frac{\mathbf{m}_1}{\mathbf{m}_2}$ com $\mathbf{m}_2 \neq 0$, é o número que é a classe de equivalência segundo \mathbf{R} definida pelo par ordenado de números inteiros:

$$(a_1b_2, a_2b_1) \text{ em que } a_2b_1 \neq 0.$$

O número racional quociente $\frac{\mathbf{m}_1}{\mathbf{m}_2}$ com $\mathbf{m}_2 \neq 0$ resultado da divisão do número racional \mathbf{m}_1 pelo número racional \mathbf{m}_2 é independente da escolha dos representantes dos números

racionais m_1 e m_2 . De fato, sejam os pares ordenados de números inteiros (a_1, b_1) e (a_1', b_1') com $b_1 \neq 0$ e $b_1' \neq 0$, representantes do número racional m_1 sejam os pares ordenados de números inteiros (a_2, b_2) e (a_2', b_2') com $b_2 \neq 0$ e $b_2' \neq 0$, representantes do número racional a_2 diferente do número racional zero; como

$$\{(a_1, b_1), (a_1', b_1')\} \in \mathbf{R}$$

$$a_1 b_1' = a_1' b_1 \quad (\text{produto de números inteiros})$$

e como:

$$\{(a_2, b_2), (a_2', b_2')\} \in \mathbf{R}$$

$$a_2 b_2' = a_2' b_2 \quad (\text{produto de números inteiros})$$

a igualdade entre o produto de números inteiros:

$$(a_1 b_2) (a_2' b_1') = (a_2 b_1) (a_1' b_2')$$

é logicamente é equivalente a:

$$\{(a_1 b_2, a_2 b_1), (a_1' b_2', a_2' b_1')\} \in \mathbf{R}$$

O inverso multiplicativo do número racional m diferente do número racional zero e indicado também m^{-1} ou $\frac{1}{m}$ é o número racional quociente resultado da divisão do número racional 1 pelo número racional $m \neq 0$.

A propriedade fundamental do inverso multiplicativo $\frac{1}{m}$ do número racional a diferente de zero é que o número racional produto $m \cdot \frac{1}{m}$ dos fatores m e $\frac{1}{m}$ é o número racional um.

$$m \cdot \frac{1}{m} = 1$$

PROPRIEDADE: Dados os números racionais m_1 e m_2 , $\frac{m_1}{m_2} = m_1 m_2^{-1}$

3.5 A INCLUSÃO DO CONJUNTO \mathbb{Z} DOS NÚMEROS INTEIROS NO CONJUNTO \mathbb{Q} DOS NÚMEROS RACIONAIS.

Para cada número inteiro $n \in \mathbb{Z} = \{ \dots, -3, -2, -1, 0, 1, 2, 3, \dots \}$, definimos o valor $J(n)$ da função inclusão canônica no número inteiro n como sendo igual ao número racional classe de equivalência segundo \mathbf{R} do par ordenado de números inteiros $(n, 1)$.

A função inclusão natural ou canônica J é uma função cujo domínio é o conjunto \mathbb{Z} dos números inteiros e cujo conjunto de valores é um subconjunto do conjunto \mathbb{Q} dos números racionais.

A função inclusão canônica J de \mathbb{Z} em \mathbb{Q} é uma função injetora e tem as seguintes propriedades dados dois números inteiros m e n .

$$(1) \quad J(m + n) = J(m) + J(n)$$

$$(2) \quad J(mn) = J(m)J(n)$$

A identificação entre o número inteiro n e o número racional $J(n)$ e o fato de que a soma de dois números inteiros m e n é identificado como a soma dos números racionais $J(m)$ e $J(n)$ além do que o produto de dois números inteiros m e n é identificado como o produto dos números racionais $J(m)$ e $J(n)$ pelas propriedades (1) e (2) da função J faz com que o conjunto \mathbb{Z} dos números inteiros seja considerado um subconjunto do conjunto \mathbb{Q} dos números racionais o que não é verdadeiro, já que $\{ J(n) : n \in \mathbb{Z} \} \subset \mathbb{Q}$.

3.6 A RELAÇÃO NATURAL DE ORDEM NO CONJUNTO \mathbb{Q} DOS NÚMEROS RACIONAIS.

Seja \mathbb{P} o subconjunto dos números racionais que são classes de equivalência segundo \mathbf{R} dos pares ordenados de números inteiros em que o primeiro elemento do par ordenado é um número natural diferente de zero e o segundo elemento do par ordenado é o número natural zero.

O subconjunto \mathbb{P} dos números racionais é um subconjunto fechado em relação as operações de adição e de multiplicação de números racionais no sentido de que: se $\mathbf{m} \in \mathbb{P}$ e se $\mathbf{n} \in \mathbb{P}$ então $(\mathbf{m} + \mathbf{n}) \in \mathbb{P}$ e $\mathbf{mn} \in \mathbb{P}$.

O número racional \mathbf{m} é menor que o número racional \mathbf{n} indicado pela notação $\mathbf{m} < \mathbf{n}$ ou o número racional \mathbf{n} é maior que o número racional \mathbf{m} indicado pela notação $\mathbf{n} > \mathbf{m}$ quando e somente quando existe um número racional \mathbf{p} pertencente ao subconjunto \mathbb{P} tal que:

$$\mathbf{n} = \mathbf{m} + \mathbf{p}$$

Em particular, o número racional zero é menor do que qualquer número racional pertencente ao subconjunto \mathbb{P} de números racionais.

A sentença $\mathbf{m} \leq \mathbf{n}$ ou $\mathbf{n} \geq \mathbf{m}$ em que \mathbf{m} e \mathbf{n} são números racionais significa que ou \mathbf{m} é igual a \mathbf{n} (indicado pelo símbolo $\mathbf{m} = \mathbf{n}$) ou que o número racional \mathbf{m} é menor do que o número racional \mathbf{n} .

A relação canônica de desigualdade entre números racionais é a relação binária de ordem total $\mathbf{R}_{\leq} \subset \mathbb{Q} \times \mathbb{Q}$ definida em $\mathbb{Q} \times \mathbb{Q}$ por :

$$\mathbf{R}_{\leq} = \{ (m, n) \in \mathbb{Q} \times \mathbb{Q} : m \leq n \}$$

De fato, \mathbf{R}_{\leq} é uma relação binária de ordem total no conjunto \mathbb{Q} dos números racionais pois satisfaz as propriedades reflexiva, antissimétrica e transitiva além de ser válida a lei da tricotomia para números racionais.

O conjunto \mathbb{Q} dos números racionais é união disjunta do conjunto \mathbb{P} , do conjunto unitário cujo único elemento é o número racional zero e do conjunto $-\mathbb{P}$ em que

$$-\mathbb{P} = \{ n \in \mathbb{Q} : -n \in \mathbb{P} \}$$

TEOREMA 3.6.1 Para cada número natural p primo não existe número racional m tal que $m^2 = pm$ e não existe número racional m tal que $m^3 = pm^2$, e assim por diante.

Prova: Seja o par ordenado de números naturais (a, b) um dos representantes do número racional $m > 0$. Da igualdade $m^2 = pm$ segue que $a^2 = pb^2$. Na decomposição em fatores primos do número natural a^2 ocorre um número par (possivelmente zero) de fatores primos iguais a p enquanto que o número de fatores primos iguais a p do número natural pb^2 é um número natural ímpar, o que é uma contradição.

TEOREMA 3.6.2 LEI DA TRICOTOMIA PARA O CONJUNTO DOS NÚMEROS RACIONAIS

Dados dois números racionais m e n , uma e somente uma das afirmações é verdadeira:

$$(1) m = n \quad (2) m < n \quad (3) m > n.$$

Prova

Dados os números racionais m e n , ou $m - n = 0$ ou $m - n \in -\mathbb{P}$ ou $m - n \in \mathbb{P}$.

Se $m - n = 0$ então $m = n$.

Se $m - n \in -\mathbb{P}$ então por definição $m < n$.

Se $m - n \in \mathbb{P}$ então por definição $m > n$.

TEOREMA 3.6.3 Dados os números racionais m, n, p e q .

- (i) Se $m < n$ então $m + p < n + p$
- (ii) Se $m < n$ e se $n < p$ então $m < p$.
- (iii) Se $m < n$ e se $p < q$ então $m + p < n + q$.
- (iv) Se $m < n$ e se $p > 0$ então $mp < np$.
- (v) Se $m < n$ e se $p < 0$ então $mp > np$.
- (vi) Se $m + p < n + p$ então $m < n$.
- (vii) Se $mp < np$ e se $p > 0$ então $m < n$.
- (viii) Se $mp < np$ e se $p < 0$ então $m > n$.

Prova de (vi)

$m = m + 0 = m + (p + (-p)) = (m + p) + (-p) < (n + p) + (-p) = n$ (pela hipótese e pelo item (i)).

Prova de (vii)

Admitindo $n < m$ e como $p > 0$, $np < mp$ pelo item (iv) o que contradiz a hipótese $mp < np$. Admitindo $m = n$ segue que $mp = np$ o que contradiz a hipótese $mp < np$. Pela lei da tricotomia para o conjunto dos números racionais resta a alternativa $m < n$.

TEOREMA 3.6.4 LEIS DO CANCELAMENTO PARA AS OPERAÇÕES BINÁRIAS DE ADIÇÃO E DE MULTIPLICAÇÃO NO CONJUNTO \mathbb{Q} DOS NÚMEROS RACIONAIS.

Dados os números racionais m, n e p .

- (i) Se $m + p = n + p$ então $m = n$
- (ii) Se $mp = np$ e se $p \neq 0$ então $m = n$

Prova

A prova de (i) é obtida adicionando $-p$ a ambos os membros da equação

$$m + p = n + p$$

e a prova de (ii) é resultado da multiplicação pelo elemento inverso de p em ambos os membros da igualdade (ii).

TEOREMA 3.6.5 A LEI DA INTEGRIDADE DO CONJUNTO \mathbb{Q} DOS NÚMEROS RACIONAIS.

Dados os números racionais m e n , se $mn = 0$ então ou $m = 0$ ou $n = 0$.

Prova

Se m é um número racional diferente de zero então como $mn = m0$ pela lei do cancelamento da operação de multiplicação $n = 0$, ou de outra maneira, se m é um número racional diferente de zero basta multiplicar ambos os membros da igualdade $mn = 0$ pelo elemento inverso de m .

TEOREMA 3.6.6 A UNICIDADE DA ORDENAÇÃO DO CONJUNTO DOS NÚMEROS RACIONAIS.

Seja R uma relação binária de ordem total no conjunto \mathbb{Q} dos números racionais com as seguintes propriedades:

(1) Lei da compatibilidade da relação binária de ordem total R com a operação de adição: Dados os números racionais m, n e p ,

$$\text{se } (m, n) \in R \text{ então } (m + p, n + p) \in R$$

(2) Lei da compatibilidade da relação binária de ordem total R com a operação de multiplicação: Dados os números racionais m, n e p ,

$$\text{se } (m, n) \in R \text{ e se } (0, p) \in R \text{ então } (mp, np) \in R.$$

(3) $(0, 1) \in R$.

Então R é a relação binária de ordem total canônica do conjunto \mathbb{Q} dos números racionais. Além disso, a relação binária de ordem total canônica do conjunto \mathbb{Q} dos números racionais induz de ordem total canônica do conjunto \mathbb{Z} dos números inteiros.

Prova

Para cada número racional não nulo m com $(0, m) \in R$, $(0, m^{-1}) \in R$. De fato, se $(m^{-1}, 0) \in R$ então $(1, 0) = (mm^{-1}, m0) \in R$, o que é uma contradição à propriedade (3). Está demonstrado que: para cada número racional não nulo m ,

$$(0, m) \in R \text{ se e somente se } (0, m^{-1}) \in R.$$

Na sequencia é demonstrado que para cada número racional não nulo m

$$(0, m) \in R \text{ se e somente se } m \in \mathbb{P}$$

De fato, se $\mathbf{m} \in \mathbb{P}$ então um dos representantes do número racional não nulo \mathbf{m} é o par ordenado de números inteiros (a, b) com a e b pertencentes a $\{1, 2, 3, \dots\}$ e de

$$(\mathbf{0}, \mathbf{a}) = (\mathbf{0}, \mathbf{bm}) \in \mathbf{R}$$

segue que

$$(\mathbf{0}, \mathbf{m}) = (\mathbf{0b}^{-1}, \mathbf{bmb}^{-1}) \in \mathbf{R}$$

Reciprocamente, se \mathbf{m} é um número racional não nulo tal que $(\mathbf{0}, \mathbf{m}) \in \mathbf{R}$ então um dos representantes de \mathbf{m} é o par ordenado de números inteiros (a, b) com $a \in \mathbb{Z}$ e b pertencente a $\{1, 2, 3, \dots\}$. De $(\mathbf{0}, \mathbf{m}) \in \mathbf{R}$ vem $(\mathbf{0}, \mathbf{a}) = (\mathbf{0b}, \mathbf{mb}) \in \mathbf{R}$, o que é equivalente afirmar que $\mathbf{a} \in \mathbb{P}$ e que $\mathbf{m} \in \mathbb{P}$.

Resta provar que para números racionais \mathbf{m} e \mathbf{n} ,

$$(\mathbf{m}, \mathbf{n}) \in \mathbf{R} \text{ se e somente se } (\mathbf{n} - \mathbf{m}) \in \mathbb{P}.$$

De $(\mathbf{m}, \mathbf{n}) \in \mathbf{R}$, $(\mathbf{m} + (-\mathbf{m}), \mathbf{n} + (-\mathbf{m})) = (\mathbf{0}, \mathbf{n} - \mathbf{m}) \in \mathbf{R}$ o que é equivalente afirmar que $(\mathbf{n} - \mathbf{m}) \in \mathbb{P}$.

4. O CONJUNTO \mathbb{R} DOS NÚMEROS REAIS.

O que são números reais?

Números reais são subconjuntos não vazios do conjunto dos números racionais.

Um número real α é definido como um subconjunto α do conjunto \mathbb{Q} dos números racionais com as seguintes propriedades:

i) $\alpha \neq \emptyset$.

ii) $\alpha \neq \mathbb{Q}$.

iii) se $x \in \alpha$ e se $y \in \mathbb{Q}$ é tal que $y < x$, então $y \in \alpha$.

iv) se $x \in \alpha$ então existe $y \in \alpha$ tal que $x < y$.

em que o símbolo de desigualdade $<$ é relativo aos números racionais.

O número real zero, indicado pelo símbolo $\mathbf{0}$, é definido como o conjunto :

$$\mathbf{0} = \{ x \in \mathbb{Q} : x < 0 \} .$$

O número real um, indicado pelo símbolo $\mathbf{1}$, é definido como o conjunto :

$$\mathbf{1} = \{ x \in \mathbb{Q} : x < 1 \} .$$

O número real menos um, indicado pelo símbolo $-\mathbf{1}$, é definido como o conjunto :

$$-\mathbf{1} = \{ x \in \mathbb{Q} : x < -1 \} .$$

O número real cinco terços, indicado pelo símbolo $\frac{5}{3}$, é definido como o conjunto :

$$\frac{5}{3} = \{ x \in \mathbb{Q} : x < \frac{5}{3} \} .$$

O número real menos três sétimos, indicado pelo símbolo $-\frac{3}{7}$, é definido como o conjunto :

$$-\frac{3}{7} = \{ x \in \mathbb{Q} : x < -\frac{3}{7} \} .$$

De agora em diante os números reais serão indicados pelas letras do alfabeto grego: $\alpha, \beta, \dots, \omega$.

4.1 A OPERAÇÃO DE ADIÇÃO NO CONJUNTO \mathbb{R} DOS NÚMEROS REAIS.

A operação de adição no conjunto \mathbb{R} dos números reais associa a cada par ordenado (α, β) de números reais α e β , o número real soma $\alpha + \beta$ dos números reais α e β nesta ordem definido como:

$$\alpha + \beta = \{ x \in \mathbb{Q} : (\exists y \in \alpha) (\exists z \in \beta) : (x = y + z) \}$$

De fato, $\alpha + \beta$, assim definido, é um número real, pois satisfaz as seguintes propriedades:

i) $\alpha + \beta \neq \emptyset$.

Como $\alpha \neq \emptyset$ e $\beta \neq \emptyset$, $\alpha + \beta \neq \emptyset$

ii) $\alpha + \beta \neq \mathbb{Q}$.

Como $\alpha \neq \mathbb{Q}$ e $\beta \neq \mathbb{Q}$, existem números racionais a e b com $a \notin \alpha$, $b \notin \beta$; além disso, se $y \in \alpha$, então $y < a$ (se $a < y$ e $y \in \alpha$ então $a \in \alpha$) e se $z \in \beta$, então $z < b$ (se $b < z$ e $z \in \beta$, então $b \in \beta$) e, portanto, $(y + z) < (a + b)$. O que foi provado é que:

$$\forall y \in \alpha \quad \forall z \in \beta \quad (y + z) < (a + b)$$

Então $(a + b)$ não é um elemento de $\alpha + \beta$, (se $a + b$ é um elemento de $\alpha + \beta$ existem $y \in \alpha$ e $z \in \beta$ tais que $(a + b) = (y + z)$, o que contraria a última desigualdade).

iii) Se $x \in \alpha + \beta$, então existem números racionais $y \in \alpha$ e $z \in \beta$ com $x = y + z$.

Seja $w \in \mathbb{Q}$, com $w < x = y + z$. Então $w - y < z$ o que mostra $w - y \in \beta$. Assim

$$w = y + (w - y)$$

com $y \in \alpha$ e $(w - y) \in \beta$. Portanto $w \in \alpha + \beta$

iv) Se $x \in \alpha + \beta$, então existem números racionais $y \in \alpha$ e $z \in \beta$ com

$$x = y + z$$

e, como α e β são números reais, existem números racionais $u \in \alpha$, $v \in \beta$ com

$$y < u$$

$$z < v$$

e assim, se $w = u + v$, então $x < w$ e $w \in \alpha + \beta$.

TEOREMA 4.1.1 PROPRIEDADE ASSOCIATIVA DA OPERAÇÃO DE ADIÇÃO.

Dados números reais α , β e γ , vale

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

Prova

Basta verificar que, dados $x \in \alpha$, $y \in \beta$ e $z \in \gamma$, temos x , y , z números racionais e a propriedade $(x + y) + z = x + (y + z)$ é verdadeira. Então o primeiro membro da igualdade é um elemento de $(\alpha + \beta) + \gamma$ e o segundo membro da igualdade é um elemento de $\alpha + (\beta + \gamma)$. Portanto todo elemento de $(\alpha + \beta) + \gamma$ é elemento de $\alpha + (\beta + \gamma)$ e a recíproca é verdadeira.

TEOREMA 4.1.2 PROPRIEDADE COMUTATIVA DA OPERAÇÃO DE ADIÇÃO.

Dados os números reais α e β , vale

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

Prova

Um elemento x de $\alpha + \beta$ é tal que $x = y + z$, com $y \in \alpha$ e $z \in \beta$. Mas $x = z + y$, com $y \in \alpha$ e $z \in \beta$. Portanto $x \in \beta + \alpha$ e $\alpha + \beta \subset \beta + \alpha$.

A prova da inclusão $\beta + \alpha \subset \alpha + \beta$ é análoga.

TEOREMA 4.1.3 EXISTENCIA DO ELEMENTO NEUTRO DA OPERAÇÃO DE ADIÇÃO.

Para cada número real α , a soma de α com o número real zero é igual a α .

Prova $\alpha + 0 \subset \alpha$

Se $x \in \alpha$, então existe um número $x_1 \in \alpha$ com $x < x_1$ e como já afirmamos que

$$x = x_1 + (x - x_1)$$

no caso em que $x_1 \in \alpha$ e $(x - x_1) < 0$, equivale a dizer que

$$(x - x_1) \in 0$$

Assim temos

$$x \in \alpha + 0$$

portanto

$$x \subset \alpha + 0.$$

Logo

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

LEMA 4.1.1:

Seja α um número real e seja x um número racional positivo. Então existem números racionais y e z com $y \in \alpha$ e $z \notin \alpha$ em que z não é o menor elemento de $\mathbb{Q} - \alpha$ tal que $x = z - y$.

Prova do lema:

Caso $x \in \alpha$:

Se todos os números racionais $x, 2x, 3x, 4x, \dots$ são elementos de α então todo número racional w também é elemento de α pela propriedade arquimediana dos números racionais: $w < nx$ para algum número natural n . Pelo princípio da boa ordenação dos números naturais aplicado ao conjunto não vazio

$$A = \{ n \in \mathbb{N} : nx \notin \alpha \}$$

existe o número natural m , elemento mínimo de A , tal que $mx \notin \alpha$ e $(m-1)x \notin \alpha$, pois $m \geq 2$.

Por definição $z = mx \notin \alpha$ e $y = (m-1)x \in \alpha$, $z - y = x$. Na hipótese de z ser o menor elemento de $\mathbb{Q} - \alpha$, existe um número racional t de modo que $t > y$ e $t \in \alpha$; por definição $w = z + t - y$ e logo $w - t = z - y = x$, com $w \notin \alpha$ e $t \in \alpha$.

Caso $x \notin \alpha$:

O conjunto \mathbb{P} dos números reais estritamente maiores do que o número real zero.

$$\mathbb{P} = \{ \alpha \in \mathbb{R} : \alpha > 0 \}$$

é um subconjunto do conjunto dos números reais fechado em relação à adição:

Se $\alpha \in \mathbb{P}$ $\beta \in \mathbb{P}$ então $\alpha + \beta \in \mathbb{P}$. De fato, se $\alpha \in \mathbb{P}$, então $0 \subset \alpha$ e se $\beta \in \mathbb{P}$, então $0 \subset \beta$, o que implica que $0 \subset \alpha + \beta$.

TEOREMA 4.1.4 EXISTENCIA DO ELEMENTO SIMÉTRICO DA OPERAÇÃO DE ADIÇÃO

Para cada número real α , a soma de α com o número real $-\alpha$ abaixo definido é igual a zero, em que

$$-\alpha = \{ x \in \mathbb{Q} : -x \notin \alpha \text{ e } -x \text{ não é o menor elemento de } \mathbb{Q} - \alpha \}$$

Prova: se α é um número real, então $-\alpha$ é um número real.

i) $-\alpha \neq \emptyset$ porque como $\alpha \neq \mathbb{Q}$, existe um número real y tal que $y \notin \alpha$ e, sem perda de generalidade, y não é o menor elemento de $\mathbb{Q} - \alpha$ (caso y seja o menor elemento de $\mathbb{Q} - \alpha$, então $y + 1$ não é um elemento de α , pois se $y + 1 \in \alpha$ então $y \in \alpha$). Portanto $-y$ é um elemento de $-\alpha$, pois $-(-y) = y \notin \alpha$ e y não é o menor elemento de $\mathbb{Q} - \alpha$.

ii) $-\alpha \neq \mathbb{Q}$ porque, como $\alpha \neq \emptyset$, existe um número racional $x \in \alpha$ e então $-x \notin -\alpha$ (se $-x \in -\alpha$ então $-(-x) = x \notin \alpha$ o que é uma contradição)

iii) seja x um número racional pertencente a $-\alpha$ e seja y um número racional menor que x ; logo $-y > -x$ e $-y \notin \alpha$ (se $-y \in \alpha$ então $-x \in \alpha$ pois $x \in -\alpha$ implica em $-x \notin \alpha$) e com certeza $-y$ não é o menor elemento de $\mathbb{Q} - \alpha$, uma vez que $-y > -x$ e $-x \notin \alpha$ e, portanto, $y \in -\alpha$.

iv) seja x um número racional pertencente a $-\alpha$; então $-x \notin \alpha$ e existe um número racional y com $y < -x$ e $y \notin \alpha$; a média aritmética z entre os números racionais y e $-x$ satisfaz $y < z < -x$ e $z \notin \alpha$ e com certeza não é o menor elemento de $\mathbb{Q} - \alpha$; portanto o número racional $-z \in -\alpha$ com $-z > x$.

Prova: se α é um número real então $\alpha + (-\alpha) = 0$

i) $0 \subset \alpha + (-\alpha)$

Seja x um número racional pertencente ao número real 0 , então $x < 0$ e $-x > 0$.

De acordo com o lema abaixo, existe um número racional $y \in \alpha$ e um número racional $z \notin \alpha$, em que z não é o menor elemento de $\mathbb{Q} - \alpha$ tal que $z - y = -x$ ou $x = y + (-z)$ com $y \in \alpha$ e $-z \in -\alpha$. A prova da inclusão está completa.

ii) $\alpha + (-\alpha) \subset 0$

Um elemento pertencente a $\alpha + (-\alpha)$ é um número racional soma de um número racional $x \in \alpha$ e de um número racional $y \in -\alpha$. Logo $-y \notin \alpha$ e $-y > x$ (se $-y < x$ e $x \in \alpha$ então $-y \in \alpha$, o que é uma contradição). Assim $x + y < 0$. A prova da inclusão está completa.

A lei da tricotomia é válida para o conjunto dos números reais. A saber, se α é um número real, então uma única situação das três situações abaixo é verdadeira:

(i) $\alpha = 0$

(ii) $\alpha \in \mathbb{P}$

(iii) $-\alpha \in \mathbb{P}$

Prova:

A existência de um número racional estritamente positivo x tal que $x \in \alpha$ implica que todo número racional estritamente negativo é um elemento de α pela definição de um número real e neste caso $0 \subset \alpha$ e $\alpha \in \mathbb{P}$.

A negação da existência de um número racional estritamente positivo x tal que $x \in \alpha$ conduz a duas possibilidades mutuamente exclusivas. A primeira possibilidade é a de que todos os números racionais estritamente negativos são elementos de α e neste caso:

$\alpha = 0$. A segunda possibilidade é a de que existe um número racional estritamente negativo x , tal que $x \notin \alpha$ e, sem perda de generalidade, x não é elemento mínimo de $\mathbb{Q} - \alpha$ (caso contrário, considere $x/2 > x$); assim, $-x \in -\alpha$ e $-x > 0$ o que implica que $0 \subset -\alpha$ e $-\alpha \in \mathbb{P}$.

4.2 A RELAÇÃO DE ORDEM CANÔNICA NO CONJUNTO DOS NÚMEROS REAIS.

A relação de ordem canônica no conjunto dos números reais \mathbb{R} é definida do seguinte modo:

Para α e $\beta \in \mathbb{R}$ então $\alpha < \beta$ quando e somente quando $\alpha \neq \beta$ e $\alpha \subset \beta$.

Para α e $\beta \in \mathbb{R}$ então $\alpha \leq \beta$ quando e somente quando ou $\alpha = \beta$ ou $\alpha \subset \beta$

De fato, a relação de ordem canônica no conjunto dos números reais é uma relação de ordem por ser uma relação binária reflexiva, antissimétrica e transitiva no conjunto \mathbb{R} dos números reais.

4.3 A OPERAÇÃO DE MULTIPLICAÇÃO NO CONJUNTO \mathbb{R} DOS NÚMEROS REAIS.

A operação de multiplicação é definida primeiramente como uma operação binária interna no conjunto \mathbb{P} dos números reais estritamente positivos: para cada $\alpha \in \mathbb{P}$, $\beta \in \mathbb{P}$, o número real $\alpha\beta$, produto de α e β é definido como:

$$\alpha\beta = \{ x \in \mathbb{Q} : x \leq 0 \} \cup \{ x \in \mathbb{Q} : (\exists y \in \alpha : y > 0) (\exists z \in \beta : z > 0) x = yz \} \quad \alpha\beta \in \mathbb{P}$$

Se α e β são números reais com $\alpha > 0$ e $\beta > 0$ então $\alpha\beta$ é um número real com $\alpha\beta > 0$.

Prova:

i) $\alpha\beta \neq \emptyset$

$\alpha\beta \neq \emptyset$ pois contém $\{ x \in \mathbb{Q} : x \leq 0 \}$

ii) $\alpha\beta \neq \mathbb{Q}$

Se $x \notin \alpha$ e $y \notin \beta$, então $\forall u \in \alpha \quad x > u$ (caso $u \in \alpha$ e $x < u$, $x \in \alpha$)

$\forall v \in \beta \quad (y > v)$ (caso $v \in \beta$ e $y < v$, $y \in \beta$)

$\forall u \in \alpha$, com $u > 0$

$\forall v \in \beta$, com $v > 0 \quad xy > uv$.

Portanto, $xy \notin \alpha\beta$, ou seja, $\alpha\beta \neq \mathbb{Q}$

Caso exista u positivo pertencente a α e caso exista v positivo pertencente a β , tal que $xy = uv$, então $xy \in \alpha\beta$. Mas o que foi provado é que para qualquer u positivo pertencente a α e qualquer v positivo pertencente a β , temos $xy > uv$.

iii) $x \in \alpha\beta$ e seja um número racional $u > 0$ tal que $u < x$ (caso $u > 0$, $u \in \alpha\beta$). Logo

$$x > 0 \text{ com } x \in \alpha\beta$$

implica na existência de números racionais $y \in \alpha$, com $y > 0$ e $z \in \beta$, com $z > 0$ tais que:

$$x = yz$$

e uma vez que:

$$0 < u < x$$

$$0 < \frac{u}{x} < 1$$

$$\frac{u}{x} y < y.$$

Como $y \in \alpha$ implica que $\frac{u}{x}y \in \alpha$ e como $u = (\frac{u}{x}y)z$ e $z \in \beta$, $u \in \alpha\beta$

iv) Seja $x \in \alpha\beta$. Caso $x \leq 0$, existem números racionais $y \in \alpha$, com $y > 0$ e $z \in \beta$, com $z > 0$ e

$$z = xy \in \alpha\beta$$

$$z > x$$

Caso $x > 0$, existem números racionais $y \in \alpha$ com $y > 0$ e $z \in \beta$ com $z > 0$ tais que :

$$x = yz$$

e, além disso, existem números racionais $y_1 \in \alpha$ com $y_1 > y$ e $z_1 \in \beta$ com $z_1 > z$, tais que

$$x = yz < y_1z_1$$

e

$$y_1z_1 \in \alpha\beta$$

Finalmente, como $0 \in \alpha\beta$ então $\alpha\beta > 0$.

Com a definição de módulo de um número real α

$$|\alpha| = \begin{cases} \alpha & \text{se } \alpha \geq 0 \\ -\alpha & \text{se } \alpha < 0 \end{cases}$$

é possível definir a operação de multiplicação para a totalidade dos números reais:

$$\alpha\beta = \begin{cases} 0 & \text{se } \alpha = 0 \\ |\alpha||\beta| & \text{se } \alpha > 0 \text{ e } \beta > 0 \text{ ou se } \alpha < 0 \text{ e } \beta < 0 \\ -|\alpha||\beta| & \text{se } \alpha > 0 \text{ e } \beta < 0 \text{ ou se } \alpha < 0 \text{ e } \beta > 0 \end{cases}$$

A operação binária interna da multiplicação definida sobre o conjunto \mathbb{R} dos números reais é comutativa e associativa, ou seja:

$$\forall \alpha \in \mathbb{R} \quad \forall \beta \in \mathbb{R} \quad \forall \gamma \in \mathbb{R}$$

$$\alpha\beta = \beta\alpha$$

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

e admite a existência do elemento neutro para a operação de multiplicação de cada número real α , $\alpha \cdot 1 = \alpha$.

Prova: Para qualquer $\alpha \in \mathbb{R}$, $\alpha \cdot 1 = \alpha$

1º caso

Seja α um número real com $\alpha > 0$. Então $\alpha \cdot 1 \subset \alpha$. Para provar que $\alpha \subset \alpha \cdot 1$, seja $x \in \alpha$ com $x > 0$ (se $x \leq 0$, $x \in \alpha \cdot 1$ pela própria definição de $\alpha \cdot 1$) e existe um número racional $x_1 \in \alpha$ com $x < x_1$ e assim $x = x_1 \left(\frac{x}{x_1} \right)$ com $0 < \frac{x}{x_1} < 1$ $\frac{x}{x_1} \in \mathbb{Q}$

$$x_1 \in \alpha \quad \frac{x}{x_1} \in \mathbb{Q} \quad x \in \alpha \cdot 1$$

2º caso $\alpha < 0$

$$\alpha \cdot 1 = -(|\alpha| \cdot |1|) = -|\alpha| = \alpha$$

3º caso $\alpha = 0$ (trivial)

A definição do elemento inverso α^{-1} de um número real $\alpha > 0$ é a seguinte:

$$\alpha^{-1} = \{ x \in \mathbb{Q} : x \leq 0 \} \cup \{ x \in \mathbb{Q} : x > 0 : \frac{1}{x} \notin \alpha, \frac{1}{x} \text{ não é o elemento mínimo de } \mathbb{Q} - \alpha \}$$

A definição do elemento inverso α^{-1} de um número real $\alpha < 0$ é:

$$\alpha^{-1} = -|\alpha|^{-1}$$

Prova: Se α é um número real e se $\alpha > 0$, então α^{-1} é um número real e $\alpha^{-1} > 0$.

i) $\alpha^{-1} \neq \emptyset$, pois contém $\{ x \in \mathbb{Q} : x \leq 0 \}$

ii) $\alpha^{-1} \neq \mathbb{Q}$, pois como $\alpha > 0$ existe um número racional x com $x > 0$ e $x \in \alpha$; assim

$$\frac{1}{x} \notin \alpha^{-1} \quad \left(\text{se } \frac{1}{x} \in \alpha^{-1} \text{ então } \left(\frac{1}{x} \right)^{-1} = x \notin \alpha \right)$$

iii) Seja $x \in \alpha^{-1}$ e seja um número real y com $y < x$; caso $y \leq 0$, $y \in \alpha^{-1}$.

Caso $y > 0$, então $0 < y < x$ e por definição $\frac{1}{x} \notin \alpha$

$$\frac{1}{y} > \frac{1}{x} \text{ e } \frac{1}{y} \notin \alpha$$

(caso $\frac{1}{y} \in \alpha$, $\frac{1}{x} \in \alpha$ pois $0 < \frac{1}{x} < \frac{1}{y}$ e $\frac{1}{y}$ não é elemento mínimo de $\mathbb{Q} - \alpha$, pois $\frac{1}{x} < \frac{1}{y}$).

Portanto: $y \in \alpha^{-1}$

iv) Seja $x \in \alpha^{-1}$

Se $x > 0$ $\frac{1}{x} \notin \alpha$ e como $\frac{1}{x}$ não é elemento mínimo de $\mathbb{Q} - \alpha$, existe um número racional x_1 , $x_1 \in \alpha$, tal que

$$x_1 < \frac{1}{x}$$

Considerando y um número racional entre x_1 e $\frac{1}{x}$, ou seja,

$$x_1 < y < \frac{1}{x},$$

(a média aritmética $\frac{1}{2} \left(x_1 + \frac{1}{x} \right)$ é uma possível escolha de um número racional entre x_1 e $\frac{1}{x}$

e então: $\frac{1}{y} \in \alpha^{-1}$ $\frac{1}{y} > x$ pois $\left(\frac{1}{y} \right)^{-1} = y \notin \alpha$ (caso $y \in \alpha$, $x_1 \in \alpha$)

Se $x \leq 0$, existe um número racional $y \in \alpha^{-1}$ com $y > x$, já que α^{-1} contém pelo menos um número racional estritamente positivo.

TEOREMA 4.3.1 PROPRIEDADE ASSOCIATIVA DA OPERAÇÃO DE MULTIPLICAÇÃO.

Dados os números reais α , β e γ , $(\alpha \beta)\gamma = \alpha(\beta\gamma)$.

Prova: Caso $\alpha > 0$, $\beta > 0$ e $\gamma > 0$.

Seja x um número racional positivo pertencente a α e seja y um número racional positivo pertencente a β . Então xy é um número racional pertencente a $\alpha\beta$. Se z é um número racional positivo pertencente a γ , então $(xy)z$ é um número racional positivo pertencente a $(\alpha\beta)\gamma$ e $x(yz)$ é um número racional positivo pertencente a $\alpha(\beta\gamma)$. A prova da inclusão $(\alpha\beta)\gamma \subset \alpha(\beta\gamma)$ está concluída.

A inclusão reversa é análoga.

TEOREMA 4.3.2 PROPRIEDADE COMUTATIVA DA OPERAÇÃO DE MULTIPLICAÇÃO.

Dados os números reais α e β , $\alpha\beta = \beta\alpha$

Prova: Caso $\alpha > 0$ e $\beta > 0$

Seja x um número racional positivo pertencente a α e seja y um número racional positivo pertencente a β . Então xy é um número racional positivo pertencente a $\alpha\beta$ e $xy = yx$ é um número racional positivo pertencente a $\beta\alpha$. A prova da inclusão $\alpha\beta \subset \beta\alpha$ está demonstrada. A prova da inclusão reversa é análoga.

TEOREMA 4.3.3 EXISTÊNCIA DO ELEMENTO NEUTRO DA OPERAÇÃO DE MULTIPLICAÇÃO.

Para cada número real α , $1\alpha = \alpha$

Prova:

i) $\alpha \subset 1\alpha$

Seja x um número racional tal que $x > 0$ e $x \in \alpha$. Então existe um número racional y tal que $y \in \alpha$ e $x < y$ ou $\frac{x}{y} < 1$. Portanto, $x = \frac{x}{y}y$ e $x \in 1\alpha$, porque $xy \in 1$ (número real) e $y \in \alpha$.

ii) $1\alpha \subset \alpha$

Seja z um número racional tal que $z > 0$ e $z \in 1\alpha$. Então existem um número racional $x > 0$ tal que $x \in 1$ e um número racional $y > 0$ tal que $y \in \alpha$ com $z = xy < y$. Portanto, $z \in \alpha$, pois $z < y$.

TEOREMA 4.3.4 EXISTÊNCIA DO ELEMENTO INVERSO DA OPERAÇÃO DE MULTIPLICAÇÃO.

Para cada número real α , $\alpha \cdot \alpha^{-1} = 1$

Prova: se $\alpha \in \mathbb{R}$ e $\alpha > 0$, então $\alpha \cdot \alpha^{-1} = 1$

i) $\alpha \cdot \alpha^{-1} \subset 1$

Seja $\alpha \in \mathbb{R}$ e considere um número racional x tal que: $x > 0$ e $x \in \alpha$.

Além disso, considere um número racional y tal que $y > 0$ e $y \in \alpha^{-1}$

o que implica que $\frac{1}{y} \notin \alpha$ e que $\frac{1}{y} > x$. (caso $\frac{1}{y} < x$, como $x \in \alpha$, $\frac{1}{y} \in \alpha$)

$xy < 1$ e $xy \in 1$, visto que $\{ x \in \mathbb{Q} : x \leq 0 \} \subset 1$,

$$\alpha \cdot \alpha^{-1} \subset 1$$

$$\text{ii) } 1 \subset \alpha \cdot \alpha^{-1}$$

Seja $x \in 1$. Como $x \leq 0$, $x \in \alpha \cdot \alpha^{-1}$

Como $0 < x < 1$ e, de acordo com o lema anterior, existem números racionais positivos:

$y > 0$ e $z > 0$, tais que $y \in \alpha$ e $z \notin \alpha$, tais que: $\frac{z}{y} = \frac{1}{x}$ e ainda podemos assumir que z não é o

elemento mínimo de $\mathbb{Q} - \alpha$, o que significa que :

$x = y \left(\frac{1}{x} \right)$ com: $y \in \alpha$ e $\frac{1}{x} \in \alpha^{-1}$ pois $\left(\frac{1}{z} \right)^{-1} = z \notin \alpha$, o que implica que:

TEOREMA 4.3.5 PROPRIEDADE DISTRIBUTIVA DA OPERAÇÃO DE MULTIPLICAÇÃO EM RELAÇÃO A OPERAÇÃO DE ADIÇÃO.

Para números reais α , β e γ

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

Prova

Caso 1: $\alpha > 0$, $\beta > 0$ e $\gamma > 0$

As inclusões $\{ x \in \mathbb{Q} : x \leq 0 \} \subset \alpha (\beta + \gamma)$ e $\{ x \in \mathbb{Q} : x \leq 0 \} \subset \alpha\beta + \alpha\gamma$ são válidas.

Se $x \in \mathbb{Q}$, $x > 0$ e $x \in \alpha (\beta + \gamma)$ então $x = y (z + w)$ para números racionais y , z e w com $y > 0$, $y \in \alpha$, $z > 0$, $z \in \beta$, $w > 0$, $w \in \gamma$. Mas $x = y (z + w) = yz + yw$ com $yz > 0$, $yz \in \alpha\beta$, $yw > 0$, $yw \in \alpha\gamma$ o que mostra que $x \in \alpha\beta + \alpha\gamma$ e que a inclusão

$$\alpha (\beta + \gamma) \subset \alpha\beta + \alpha\gamma$$

é verdadeira.

Para demonstrar a inclusão contrária, seja $x \in \mathbb{Q}$, $x > 0$ e se $x \in \alpha\beta + \alpha\gamma$ então existem números racionais u , v , z e w tais que $u > 0$, $v > 0$, $z > 0$, $w > 0$, $u \in \alpha$, $v \in \alpha$, $z \in \beta$ e $w \in \gamma$ com $x = uz + vw$. No caso em que $u \leq v$ (o caso $v \leq u$ é análogo).

$$\frac{u}{v} z \leq z$$

e pela definição de número real $\frac{u}{v} z \in \beta$.

Então

$$x = uz + vw = v \left[\frac{u}{v} z + w \right]$$

é um elemento de $\alpha (\beta + \gamma)$ e a inclusão

$$\alpha\beta + \alpha\gamma \subset \alpha (\beta + \gamma)$$

está demonstrada.

Caso 2: $\alpha > 0, \beta < 0$ e $\gamma > 0$

Caso 2a: $\beta + \gamma > 0$

$$\alpha\gamma = \alpha [\beta + \gamma + |\beta|] = \alpha [(\beta + \gamma) + |\beta|] = \alpha (\beta + \gamma) + \alpha |\beta|$$

porque $\alpha > 0$, $\beta + \gamma > 0$ e $|\beta| = -\beta > 0$ (caso 1).

$$\alpha (\beta + \gamma) = -\alpha |\beta| + \alpha\gamma = \alpha\beta + \alpha\gamma$$

Caso 2b: $\beta + \gamma \leq 0$

$$\alpha |\beta| = \alpha (-\beta) = \alpha [(-\beta - \gamma) + \gamma] = \alpha (|\beta + \gamma| + \gamma) = \alpha |\beta + \gamma| + \alpha\gamma$$

pelo caso 1 e de outra maneira

$$\alpha (\beta + \gamma) = -\alpha |\beta + \gamma| = -\alpha |\beta| + \alpha\gamma = \alpha\beta + \alpha\gamma$$

Os demais casos a considerar são análogos

TEOREMA 4.3.6 TEOREMA DO COMPLEMENTO DO CONJUNTO DOS NÚMEROS REAIS.

Seja A um subconjunto não vazio do conjunto dos números reais limitado superiormente no sentido de que existe um número real ω tal que para cada $\alpha \in A$, $\alpha \leq \omega$. Então existe o número real supremo de A .

Prova:

$$\text{Seja } \beta = \{ x \in \mathbb{Q} : (\exists \alpha \in A) (x \in \alpha) \}$$

A prova de que β é um número real é demonstrada em quatro passos.

i) $\beta \neq \emptyset$, porque, como $A \neq \emptyset$, existe um número real $x \in A$ e existe um número racional x tal que $x \in \alpha$ pois $\alpha \neq \emptyset$.

ii) $\beta \neq \mathbb{Q}$, porque, como o conjunto A é limitado superiormente, existe um número real γ tal que para cada $\alpha \in A$, $\alpha < \gamma$, isto é, $\alpha \subset \gamma$, como $\gamma \neq \mathbb{Q}$, existe um número racional x tal que $x \notin \gamma$ e como $\alpha \subset \gamma$, $x \notin \alpha$.

iii) Seja um número racional $x \in \beta$ e seja um número racional $y < x$; por definição de β , existe um número real $\alpha \in A$ com $x \in \alpha$ e a hipótese de que $y < x$ implica em $y \in \alpha$ e, portanto, $y \in \beta$.

iv) Seja um número racional $x \in \beta$. Por definição de β , existe um número real $\alpha \in A$, tal que $x \in \alpha$ e como α é um número real, existe um número racional y tal que $y \in \alpha$ e $x < y$. Portanto $y \in \beta$ pela definição de β .

A demonstração de que β é o supremo do conjunto A é feita em duas etapas: a primeira etapa é que para cada $\alpha \in A$, temos $\alpha \leq \beta$, isto é, β é um limitante superior do conjunto A e a segunda etapa é que se γ é um limitante superior do conjunto A , então $\beta \leq \gamma$, pois, para cada número real $\alpha \in A$, temos $\alpha \leq \gamma$, o que significa $\alpha = \gamma$ ou $\alpha \subset \gamma$ e, neste caso, $\beta \subset \gamma$.

COROLÁRIO: Seja A um subconjunto não vazio do conjunto dos números reais limitado inferiormente. Então existe o número real ínfimo do conjunto A .

Prova:

Como A é subconjunto do conjunto dos números reais limitado inferiormente, o subconjunto dos números reais:

$$-A = \{ -\alpha : \alpha \in A \}$$

é um subconjunto não vazio limitado superiormente e o supremo de $-A$ é o ínfimo do conjunto A .

TEOREMA 4.3.7 PROPRIEDADE ARQUIMEDIANA DO CONJUNTO DOS NÚMEROS REAIS.

Dados os números reais α e β com $\alpha > 0$, existe um número natural $n \in \{ 1, 2, 3, \dots \}$ tal que $n\alpha \geq \beta$ e $(n + 1)\alpha > \beta$.

Prova:

Admitindo que não exista número natural n tal que $n\alpha \geq \beta$, isto é, para cada número natural n , $n\alpha < \beta$, então

$$A = \{ n\alpha : n = 1, 2, 3, \dots \}$$

é um subconjunto não vazio do conjunto dos números reais limitado superiormente por β e que admite como supremo de A um número real β e, em particular, $0 < \alpha < \beta$. Além disso, $\beta - \alpha$ não é um limitante superior do subconjunto A , o que significa que existe um número natural m tal que $m\alpha > \beta - \alpha$ ou $\beta < (m + 1)\alpha$ com $(m + 1)\alpha \in A$, o que é uma contradição.

Portanto, existe um número natural n e existe um número natural $(n + 1)$, tais que

$$n\alpha \geq \beta \text{ e } (n + 1)\alpha > n\alpha \geq \beta.$$

TEOREMA 4.3.8 A DENSIDADE DO CONJUNTO \mathbb{Q} DOS NÚMEROS RACIONAIS NO CONJUNTO \mathbb{R} DOS NÚMEROS REAIS.

Dados os números reais α e β com $\alpha < \beta$, existe um número racional $\frac{m}{n}$ tal que $\alpha < \frac{m}{n} < \beta$ em que m e n são números naturais com $n \neq 0$.

Prova:

Sejam α e β dois números reais com $\alpha < \beta$ ou $\beta - \alpha > 0$. Existe um número natural n tal que $n(\beta - \alpha) > 1$ pela propriedade arquimediana dos números reais ou $1 + n\alpha < n\beta$ e novamente pela propriedade arquimediana dos números reais existe um número natural l tal que $l = l \cdot 1 > \alpha$ e existe um número natural k tal que $k = k \cdot 1 > -l\alpha$ ou $-k < l\alpha$.

Assim, l e n são números naturais tais que $-k < n\alpha < l$

Existe um número inteiro m tal que $m - 1 \leq \alpha < m$ ou $m \leq n\alpha + 1$ e assim $n\alpha < m \leq n\alpha + 1 < n\beta$, portanto,

$$\alpha < \frac{m}{n} < \beta$$

TEOREMA 4.3.9 A DENSIDADE DO CONJUNTO DOS NÚMEROS RACIONAIS E DO CONJUNTO DOS NÚMEROS IRRACIONAIS.

Dados os números reais α e β com $\alpha < \beta$, existe um número racional q tal que $\alpha < q < \beta$ e existe um número real não racional γ com $\alpha < \gamma < \beta$.

Prova:

Caso: $\beta > 0$

Sejam α e β dois números reais tais que $\gamma = \beta - \alpha > 0$. Pela propriedade arquimediana dos números reais, existe um número natural m_1 tal que $m_1 = m_1 \cdot 1 > \frac{1}{\gamma}$ e existe um número natural m_2 tal que $m_2 = m_2 \cdot 1 > \frac{2}{\beta}$.

O número natural $m = m_1 + m_2$ é tal que $m > \frac{1}{\gamma}$ e $m > \frac{2}{\beta} > \frac{1}{\beta}$

Pela propriedade arquimediana dos números reais, existe um número natural k tal que $k \frac{1}{m} \geq \beta$, pois, $\beta > 2 \frac{1}{m} > \frac{1}{m}$.

O conjunto $A = \{ l \in \{ 3, 4, \dots \} : l \frac{1}{m} \geq \beta \}$ é um subconjunto do conjunto dos números naturais não vazio ($k \in A$) e, pelo princípio da boa ordenação dos números naturais, A admite um mínimo $n \in A$ e assim $n \frac{1}{m} \geq \beta$ e como $n - 1$ é um número natural maior do que dois e menor do que o mínimo n do conjunto A , temos

$$(n - 1) \frac{1}{m} < \beta$$

Se $(n - 1) \frac{1}{m} \leq \alpha$ então $\frac{1}{m} < \gamma = \beta - \alpha < \beta - (n - 1) \frac{1}{m} = \beta - n \frac{1}{m} + \frac{1}{m} \leq \frac{1}{m}$

já que $\beta - n \frac{1}{m} < 0$, o que é uma contradição pois $m > \frac{1}{\gamma}$ ou $\gamma > \frac{1}{m}$.

Portanto, $(n - 1) \frac{1}{m} > \alpha$ e $(n - 1) \frac{1}{m} < \beta$ ou

$$\alpha < \frac{n - 1}{m} < \beta.$$

Caso $\beta > 0$

Sejam α e β dois números reais tais que $\beta > 0$ e $\gamma = \beta - \alpha > 0$. Pela propriedade arquimediana dos números reais, existe um número natural m_1 tal que $m_1\gamma > \frac{1}{\sqrt{2}}$ e existe um número natural m_2 tal que $m_2\sqrt{2} > \frac{2}{\beta}$.

O número natural $m = m_1 + m_2$ é tal que $m\sqrt{2} > \frac{2}{\beta}$ ou $\beta > \frac{2}{m\sqrt{2}} = \frac{\sqrt{2}}{m}$.

Pela propriedade arquimediana dos números reais existe um número natural k tal que $k \frac{\sqrt{2}}{m} \geq \beta$ e $k \geq 2$ o que garante que o subconjunto A do conjunto dos números naturais

$A = \{ l \in \{ 2, 3, \dots \} : l \frac{\sqrt{2}}{m} \geq \beta \}$ é não vazio e pelo princípio da boa ordenação dos números naturais, A tem um mínimo $n \in A$, ou seja, $n \in \{ 2, 3, 4, \dots \}$

$$n \frac{\sqrt{2}}{m} \geq \beta$$

e

$$(n-1) \frac{\sqrt{2}}{m} < \beta$$

Se $(n-1) \frac{\sqrt{2}}{m} \leq \alpha$ então

$$\gamma = \beta - \alpha \leq \beta - (n-1) \frac{\sqrt{2}}{m}$$

$$\beta - \frac{n\sqrt{2}}{m} + \frac{\sqrt{2}}{m} \leq \frac{\sqrt{2}}{m},$$

visto que $\beta - \frac{n\sqrt{2}}{m} \leq 0$, o que é uma contradição pois $\gamma > \frac{\sqrt{2}}{m}$

Então $q = (n-1) \frac{\sqrt{2}}{m}$ é tal que

$$\alpha < q < \beta.$$

Se q fosse um número irracional, isto é, não racional,

$$\sqrt{2} = \frac{mq}{n-1} = \left(\frac{m}{n-1} \right) q \text{ seria um número racional produto de fatores racionais.}$$

Caso $\beta < 0$

Basta aplicar o caso anterior aos números reais $-\alpha$ e $-\beta$, em que $-\alpha$ e $-\beta$ são números reais positivos.

O caso $\alpha = 0$ e $\beta > 0$ é interessante porque basta considerar o número natural n tal que $n\beta > 1$ ou $0 < \frac{1}{n} < \beta$ cuja existência é assegurada pela propriedade arquimediana dos números reais.

4.4 A EQUAÇÃO POLINOMIAL INCOMPLETA $x^n = \alpha$

Para cada número natural $n \in \{1, 2, 3, \dots\}$ e para cada número real α , a equação $x^n = \alpha$ tem solução real.

Para $n = 1$, a equação é $x = \alpha$.

Para $n = 2, 3, \dots$, seja $\alpha > 1$, isto é, existe $\beta > 0$ tal que $\alpha = 1 + \beta$ e seja $A = \{x \in \mathbb{R} : x > 0, x^n \leq \alpha = 1 + \beta\}$

Então $1 \in A$ e se $x > \alpha$ então $x^n > \alpha^n = (1 + \beta)^n > 1 + n\beta > 1 + \beta = \alpha$ e assim $x \notin A$; logo para cada $x \in A$, $x \leq \alpha$.

Pelo teorema do complemento do conjunto dos números reais, existe $\gamma \in \mathbb{R}$ tal que $\gamma = \sup A$.

Caso $\gamma^n < \alpha$, $\alpha - \gamma^n > 0$ e pela propriedade arquimediana do conjunto dos números reais, existe um número natural $m \in \{1, 2, 3, \dots\}$ tal que

$$m(\alpha - \gamma^n) \geq (1 + \gamma)^n - \gamma^n$$

ou equivalentemente

$$\alpha - \gamma^n \geq \frac{(1 + \gamma)^n - \gamma^n}{m}$$

e então

$$\begin{aligned} \left(\gamma + \frac{1}{m}\right)^n &= \gamma^n + \binom{n}{1} \gamma^{n-1} \frac{1}{m} + \dots + \binom{n}{n} \left(\frac{1}{m}\right)^n \\ &= \gamma^n + \frac{1}{m} \left[\binom{n}{1} \gamma^{n-1} + \dots + \binom{n}{n} \left(\frac{1}{m}\right)^{n-1} \right] \\ &= \gamma^n + \left(1 + \frac{\gamma}{m}\right)^n - \gamma^n \leq \gamma^n + \alpha - \gamma^n = \alpha \end{aligned}$$

o que mostra que $\gamma + \frac{1}{m} \in A$ e $\gamma < \gamma + \frac{1}{m}$, o que é uma contradição porque γ é o número real supremo do conjunto A .

Caso $\gamma^n > \alpha$, $\gamma^n - \alpha > 0$ e pela propriedade arquimediana do conjunto dos números reais, existe um número natural $m \in \{1, 2, 3, \dots\}$ tal que

$$m(\gamma^n - \alpha) \geq (1 + \gamma)^n - \gamma^n$$

ou

$$\gamma^n - \alpha \geq \frac{(1 + \gamma)^n - \gamma^n}{m}.$$

Existe um número real $\delta \in A$ tal que $\gamma - \frac{1}{m} < \delta \leq \gamma$, lembrando que $1 \in A$ e $\gamma \geq 1$ e, então,

$\delta^n =$

$$\begin{aligned} \delta^n &> \left(\delta - \frac{1}{m}\right)^n = \gamma^n - \binom{n}{1} \frac{1}{m} \gamma^{n-1} + \binom{n}{2} \frac{1}{m^2} \gamma^{n-2} + \dots + \binom{n}{n} \left(\frac{-1}{m}\right)^n \\ &> \gamma^n - \frac{1}{m} \left[\binom{n}{1} \gamma^{n-1} + \dots + \binom{n}{n} \left(\frac{1}{m}\right)^{n-1} \right] \\ &= \gamma^n - \frac{1}{m} [(1 + \gamma)^n - \gamma^n] \geq \gamma^n + \alpha - \gamma^n = \alpha \end{aligned}$$

Pela lei da tricotomia para o conjunto dos números reais resta apenas a possibilidade

$$\gamma^n = \alpha.$$

Caso $\alpha \in \mathbb{R}$ é tal que $0 < \alpha < 1$, a equação $x^n = \frac{1}{\alpha} > 1$ é considerada.

4.5 REPRESENTAÇÃO DECIMAL DOS NÚMEROS REAIS

O processo para representação decimal de números reais segue os seguintes passos.

Seja α um número real tal que $\alpha > 0$.

1º passo

Seja a_0 o maior número pertencente a $\{0, 1, 2, \dots\}$ tal que $a_0 < \alpha$.

Se $a_0 = \alpha$ o processo termina.

Se $a_0 < \alpha$ segue o 2º passo

2º passo

Seja a_1 o maior número pertencente a $\{0, 1, 2, \dots\}$ tal que

$$a_0 + \frac{a_1}{10} \leq \alpha$$

Então $a_1 \in \{0, 1, 2, \dots, 9\}$ porque se $a_1 \geq 10$, então

$$a_0 + \frac{a_1}{10} \geq a_0 + a_1 \geq a_0,$$

o que contraria o fato de a_1 ser o maior número inteiro com a propriedade de que

$$a_0 + \frac{a_1}{10} < \alpha.$$

Se $a_0 + \frac{a_1}{10} = \alpha$ o processo termina.

Se $a_0 + \frac{a_1}{10} < \alpha$ segue o 3º passo.

3º passo

Seja a_2 o maior número pertencente a $\{0, 1, 2, \dots\}$, tal que

$$a_0 + \frac{a_1}{10} + \frac{a_2}{10^2} \leq \alpha$$

Então $a_2 \in \{0, 1, 2, \dots, 9\}$ porque se $a_2 \geq 10$, então

$$a_0 + \frac{a_1}{10} + \frac{a_2}{10^2} \geq a_0 + \frac{a_1 + a_2}{10}$$

o que contraria o fato de a_2 ser o maior número inteiro com a propriedade de que

$$a_0 + \frac{a_1}{10} + \frac{a_2}{10^2} \leq \alpha.$$

Se $a_0 + \frac{a_1}{10} + \frac{a_2}{10^2} = \alpha$ o processo termina.

Se $a_0 + \frac{a_1}{10} + \frac{a_2}{10^2} < \alpha$ segue o próximo passo.

Caso o processo continue indefinidamente, seja o conjunto

$$A = \left\{ q_n = a_0 + \frac{a_1}{10} + \frac{a_2}{10^2} + \dots + \frac{a_n}{10^n} : n \in \{0, 1, 2, \dots\} \right\}$$

de números racionais que é um conjunto limitado superiormente pelo número real α . Pelo teorema do complemento dos números reais, o conjunto A admite como supremo o número real β . Abaixo segue a demonstração da igualdade entre α e β .

Caso $\beta < \alpha$, $\alpha - \beta > 0$ e existe um número natural m tal que

$$0 < \frac{1}{10^m} < \alpha - \beta$$

e

$$q_m + \frac{1}{10^m} = a_0 + \frac{a_1}{10} + \frac{a_2}{10^2} + \dots + \frac{a_m + 1}{10^m} \leq \beta + \frac{1}{10^m} < \alpha,$$

o que contraria a propriedade maximal de a_m . Então $\beta \geq \alpha$ mas β não pode ser maior do que α (que é um limitante superior de A)

Conclusão $\beta = \alpha$.

Na construção da sequência dos dígitos a_1, a_2, \dots pertencentes a $\{0, 1, \dots, 9\}$ não ocorre que, a partir de um certo número natural N,

$$a_n = 9 \quad n = N+1, N+2, \dots$$

Porque caso $a_n = 9$ para cada número natural $n > N$,

$\alpha = \beta$ é a soma do número racional q_N com o supremo do conjunto

$$S = \left\{ \frac{9}{10^{n+1}} + \dots + \frac{9}{10^n} : n = N+1, N+2, \dots \right\}$$

que é igual a $\frac{1}{10^N}$ porque $\frac{9}{10^{n+1}} + \dots + \frac{9}{10^n} = \frac{1}{10^N} - \frac{1}{10^n}$

$$\frac{9}{10^{n+1}} \left[1 + \dots + \frac{1}{10^{n-N}} \right]$$

$$\frac{9}{10^{n+1}} \frac{1 - \frac{1}{10^{n-N}}}{1 - \frac{1}{10}} = \frac{10^N}{10^{n+1} - 10^2} \frac{9}{10},$$

ou seja

$$\alpha = \beta = q_N + \frac{1}{10^N} = a_0 + \frac{a_1}{10} + \frac{a_2}{10^2} + \dots + \frac{a_N + 1}{10^N} \leq \alpha,$$

o que contraria a propriedade maximal de a_N .

Lema 4.4.4 O subconjunto não vazio E dos números racionais

$$E = \{ x \in \mathbb{Q} : x > 0 \text{ e } x^2 < 2 \}$$

é tal que se $x \in E$, então existe $y \in E$ com $x < y$, isto é, o subconjunto E dos números racionais não tem supremo no conjunto Q dos números racionais.

Prova

Se $x \in E$ e $x < 1$, então como $1 \in E$, o lema está provado neste caso.

Se $x \in E$ e $x > 1$, então de $x^2 < 2 \rightarrow 2 - x^2 > 0$ e

$$r = \frac{2 - x^2}{2x + 1} > 0 \quad 2 - x^2 < 2x + 1 \rightarrow 2 < (x + 1)^2$$

e existe um número racional q tal que $0 < q < 1$ e $q < \frac{2-x^2}{2x+1}$. Assim,

$$q < \frac{2-x^2}{2x+q}$$

$$2xq + q^2 < 2 - x^2$$

$$(x+q)^2 < 2$$

o que mostra que $x < x+q$

$$x+q \in \mathbb{Q} \text{ e } (x+q)^2 < 2.$$

Como consequência, está demonstrado que

$$\sqrt{2} = \{ x \in \mathbb{Q} : x \leq 0 \} \cup \{ x \in \mathbb{Q} : x > 0 \text{ e } x^2 < 2 \}$$

Analogamente $\sqrt{3} = \{ x \in \mathbb{Q} : x \leq 0 \} \cup \{ x \in \mathbb{Q} : x > 0 \text{ e } x^2 < 3 \}$

$$\sqrt{5} = \{ x \in \mathbb{Q} : x \leq 0 \} \cup \{ x \in \mathbb{Q} : x > 0 \text{ e } x^2 < 5 \}$$

$$\sqrt{7} = \{ x \in \mathbb{Q} : x \leq 0 \} \cup \{ x \in \mathbb{Q} : x > 0 \text{ e } x^2 < 7 \}.$$

Referências

GUIDORIZZI, H.: *Um Curso de Cálculo* (V.1): Rio de Janeiro, LTC, 1995.

LIMA, E. L.: *Análise Real* (V.1) : Rio de Janeiro, IMPA, 1993.

MILIES, C.P.; COELHO, S.P. *Números : Uma introdução à Matemática.*: São Paulo, Edusp, 2003

MONTEIRO, L.H.J. : *Elementos de Álgebra* : Rio de Janeiro, Ao Livro Técnico S.A., 1969

SPIVAK, M.: *Calculus*. 3ª edição. : Houston, Publish or Perish, 1994.

EISENBERG, M.: *Axiomatic theory of sets and classes* : New York, Holt, Rinehart and Winston, 1971.

PINTER, C.C.; *Set theory*: Reading, Addison-Wesley Pub. Co., 1971.

DODGE, C. W.: *Sets, Logic & Numbers* : Boston, Prindle, Weber & Schmidt, Inc, 1969.