UNIVERSIDADE FEDERAL DO CEARÁ

CENTRO DE CIÊNCIAS

DEPARTAMENTO DE MATEMÁTICA

PROGRAMA DE PÓS – GRADUAÇÃO EM MATEMÁTICA EM REDE NACIONAL

MARCELO BRISENO FROTA

RELAÇÃO DE EQUIVALÊNCIA, CONJUNTO QUOCIENTE E APLICAÇÕES

FORTALEZA

2017

MARCELO BRISENO FROTA

RELAÇÃO DE EQUIVALÊNCIA, CONJUNTO QUOCIENTE E APLICAÇÕES

Dissertação submetida à Coordenação do Mestrado Profissional em Matemática em Rede Nacional (PROFMAT), da Universidade Federal do Ceará, como requisito parcial para a obtenção em grau de Mestre em Matemática.

Área de concentração: Ensino de Matemática

Orientador: Prof. Dr. Marcelo Ferreira de Melo.

FORTALEZA

2017

Dados Internacionais de Catalogação na Publicação
Universidade Federal do Ceará
Biblioteca Universitária
Gerada automaticamente pelo módulo Catalog, mediante os dados fornecidos pelo(a) autor(a)

F961r Frota, Marcelo Briseno.

Relação de equivalência, conjunto quociente e aplicações / Marcelo Briseno Frota. – 2017.

89 f. : il.

Dissertação (mestrado) – Universidade Federal do Ceará, Centro de Ciências, Departamento de Matemática, Programa de Pós-Graduação em Matemática em Rede Nacional, Fortaleza, 2017.

Orientação: Prof. Dr. Marcelo Ferreira de Melo.

1. Construção dos números. 2. Espaço quociente. 3. Superfície quociente. I. Título.

CDD 510

MARCELO BRISENO FROTA

RELAÇÃO DE EQUIVALÊNCIA, CONJUNTO QUOCIENTE E APLICAÇÕES

Dissertação de Mestrado apresentada ao Programa de Pós-Graduação em Matemática em Rede Nacional, do Departamento de Matemática da Universidade Federal do Ceará, como requisito parcial para a obtenção do Título de Mestre em Matemática. Área de concentração: Ensino de Matemática.

Aprovada em: 07 / 07 / 2017.

BANCA EXAMINADORA

_____

Prof. Dr. Marcelo Ferreira de Melo (Orientador)
Universidade Federal do Ceará (UFC)

_____

Prof. Dr. Marcos Ferreira de Melo
Universidade Federal do Ceará (UFC)

_____

Prof. Dr. Carlos Augusto David Ribeiro
Universidade Federal do Piauí (UFPI)

AGRADECIMENTOS

Agradeço primeiramente a Deus, por nunca me desamparar em todos os momentos, difíceis ou não. Sabedoria e inteligência, dons estes, dados pelo Senhor, que permitem a expressão deste trabalho.

À minha esposa, companheira fiel, minha ajuda mais que adequada, pessoa que esteve sempre ao meu lado, dando-me forças em todos os instantes. Sem dúvidas, não teria conseguido sem sua presença.

Ao meu filho, por ser esta bênção de Deus, a sinceridade que cativa a todos, o sorriso que me encanta e renova minhas forças para correr atrás do que quero todos os dias.

Aos meus pais, pessoas que sempre se dedicaram a mim, este título é mérito deles também, por terem sempre a consciência que a educação é prioridade sempre.

Aos meus irmãos Priscila e Raphael, por acompanharem comigo todos os momentos, torcendo para que consiga a vitória em todos os caminhos que faça.

À minha sogra, que sempre esteve a me apoiar, com bastante felicidade ao me ver alcançando os objetivos por mim traçados.

Ao meu amigo Wilkson, pessoa esta que me ajudou e incentivou em todo processo neste mestrado.

À Universidade Federal do Ceará por proporcionar este momento, em que um grande desejo de me tornar mestre fosse realizado.

Ao meu orientador, o professor Dr. Marcelo Ferreira de Melo, pessoa de grande conhecimento e sabedoria, utilizando sempre estas virtudes para o proveito de seus alunos.

Aos meus amigos de trabalho, por sempre estarem dispostos a colaborar com meus estudos.

Àqueles que me ajudaram de alguma forma neste caminho para alcançar o título.

"Felizes aqueles que se divertem com problemas que educam a alma e elevam o espírito." (Fenelon)

RESUMO

Este trabalho visa inicialmente apresentar a construção dos números inteiros, racionais e reais, bem como suas relações de equivalência. Serão também analisadas as classes de equivalências em um espaço quociente, o teorema do núcleo e da imagem, forma de Jordan e finalizando com o estudo das superfícies quocientes: plano projetivo, toro e garrafa de Klein.

Palavras-chave: Construção dos números. Espaço quociente. Superfície quociente.

ABSTRACT

This work initially aims at presenting the construction of integers, rational and real, as well as their equivalence relations. We will also analyze the equivalence classes in a quotient space, the theorem of the nucleus and the image, form of Jordan and finalizing with the study of surfaces quotients: projective plane, torus and bottle of Klein.

Keywords: Construction of numbers. Space quotient. Quotient surface.

LISTA DE FIGURAS

SUMÁRIO

1 INTRODUÇÃO

As construções dos conjuntos numéricos, onde iniciaremos o nosso trabalho com os números inteiros, racionais e reais, são bastante férteis sobre vários aspectos, principalmente no que tange uma pretensão à fundamentação teórica de questões que já lhe são conhecidas. Assim, a partir de análises das teorias, definições e relações de equivalência, será permitida uma maior dedicação a tópicos mais específicos dessa disciplina.

Analisaremos algumas situações para esclarecer a respeito dos espaços vetoriais quociente, analisando as duas vezes em que o mesmo é utilizado, são elas: a demonstração do Teorema do Núcleo e da Imagem e também a demonstração na Forma Canônica de Jordan, sendo nesta última necessária a ideia do que seria uma base do espaço quociente e não deste espaço propriamente dito.

Por fim, mas não menos importante, será introduzida a noção de superfície abstrata (ou seja, sem referência a $\mathbb{R}^3$) e mencionaremos algumas generalizações como variedades diferenciáveis e Riemannianas.

2 NÚMEROS INTEIROS

2.1 Construção do conjunto dos números inteiros

Observando o rigor da matemática, vemos que não é adequado o estudo do ensino escolar, pois o mesmo admitia a existência de números inteiros negativos e que devíamos incorporá-los ao conjunto N (conjunto dos números naturais que surgiu da necessidade de construção, satisfazendo, através de axiomas de Piano, a sua existência) devido isto, trabalharemos as demonstrações destes conjuntos de números, utilizando noções básicas de relações de equivalências.

Iniciaremos com o número inteiro como uma relação de equivalência dada pelo conjunto N x N. O conjunto dos inteiros Z será o conjunto dessas classes de equivalência. Logo em seguida, definiremos duas operações em Z e também que Z possui uma cópia algébrica de N. Finalizando com a operação de subtração em Z que, restrita a elementos da cópia de N em Z, trará sentido às operações.

Teorema 1 Sejam (a; b); (c; d) ∈ N x N. Dizemos que (a; b) está relacionado com (c; d) quando a + d = b + c. Denotaremos por (a; b) ~ (c; d). A relação descrita é de equivalência.

Demonstração:

(i) Reflexiva: Se (a; b) ∈ N x N, então a + b = b + a, por herança da comutativa em N, logo, (a; b) ~ (a; b).

(ii) Simétrica: Se (a; b); (c; d) ∈ N x N e (a; b) ~ (c; d), então, a+d = b+c, e disso, c+b = d+a, que significa, (c; d) ~ (a; b).

(iii) Transitiva: Se (a; b); (c; d); (e; f) ∈ N x N, (a; b) ~ (c; d) e (c; d) ~ (e; f), temos que, a+d = b+c e c+f = d+e. Assim temos a+d+e = b+c+e e a+c+f = =a+d+e, daí, b + c + e = a + c + f⇒b + e = a + f⇒a + f = b + e:

Logo, (a; b) ~ (e; f).

Denotaremos por $\overline{(a,b)}$ a classe de equivalência do par ordenado (a; b) pela relação ~, isto é,

$$(a; b) = \{(x; y) \in N \times N \mid (x; y) \sim (a; b)\}.$$

a) $\overline{(4,2)}$ = {(4; 2); (5; 3); (6; 4); (7; 5); ...};

b) $\overline{(2,5)}$ = {(2; 5); (3; 6); (4; 7); (5; 8); ...};

c) $\overline{(7,5)}$ = {(4; 2); (5; 3); (6; 4); (7; 5); ...}.

Percebemos que $\overline{(4,2)}$ = $\overline{(7,5)}$.

Definição 1 O conjunto quociente N x N/ ~ constituído pelas classes de equivalência $\overline{(a,b)}$, denotado por Z e chamado de conjunto dos números inteiros. Assim, Z = (N x N/~) = {$\overline{(a,b)}$ | (a, b) ∈ N x N}.

2.2 Operações nos números inteiros

Serão construídos números negativos, a partir da estrutura aritmética dos número naturais, utilizando relações de equivalência.

2.2.1 Adição de números inteiros

Trabalharemos agora com a definição de (+) como operação de adição em Z. Sabendo que $\overline{(a,b)}$ representa (a – b) e $\overline{(c,d)}$ expressa (c – d), vemos pela matemática elementar que (a - b) + (c - d) = (a + c) - (b + d). Obtendo, assim, a classe $\overline{(a+c,b+d)}$.

Definição 2 Sejam $\overline{(a,b)}$; $\overline{(c,d)}$ em Z. A soma $\overline{(a,b)}$ + $\overline{(c,d)}$ é dada por $\overline{(a+c,b+d)}$.

Teorema 2 Se $\overline{(a,b)}$ = $\overline{(a',b')}$ e $\overline{(c,d)}$= $\overline{(c',d')}$, então, $\overline{(a,b)}$ + $\overline{(c,d)}$ = $\overline{(a',b')}$ + $\overline{(c',d')}$ isto é, a adição de números inteiros está bem definida.

Demonstração. Tendo $\overline{(a,b)}$ = $\overline{(a',b')}$, temos que, $\overline{(a,b)}$ ~ $\overline{(a',b')}$ ou seja,

$$a + b' = b + a' \quad (*)$$

Analogamente,

$$c + d' = d + c' \quad (**)$$

Já sabemos que $\overline{(a,b)}$ + $\overline{(c,d)}$ = $\overline{(a+c,b+d)}$ e $\overline{(a',b')}$ + $\overline{(c',d')}$ = $\overline{(a'+c',\ b'+d')}$. Devemos mostrar que (a + c; b' + d') = (b + d; a' + c'). De fato, somando os primeiros e segundos membros de (*) e (**), na ordem dada, obtemos, (a + c) + (b' + d') = (b + d) + (a'+ c') = (b + a') + (d + c') = (b + d) + (a'+ c'):

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

Teorema 3 A adição em Z é comutativa, associativa e tem $\overline{(0,0)}$ como elemento neutro.

Demonstração.

1. Comutativa: Devemos mostrar que, dados $\overline{(a,b)}$ e $\overline{(c,d)}$ em Z, temos $\overline{(a,b)}$ + $\overline{(c,d)}$ = $\overline{(c,d)} + \overline{(a,b)}$. De fato, $\overline{(a,b)}$ + $\overline{(c,d)}$ = $\overline{(a\ +\ c, b\ +\ d)}$ = $\overline{(c\ +\ a, d\ +\ b)}$ = $\overline{(c,d)} + \overline{(a,b)}$.

2. Associativa: Queremos mostrar que, dados $\overline{(a,b)}$, $\overline{(c,d)}$ e $\overline{(e,f)}$ em Z, temos $\overline{(a,b)}$ + ($\overline{(c,d)}$ + $\overline{(e,f)}$) = ($\overline{(a,b)}$ + $\overline{(c,d)}$) + $\overline{(e,f)}$

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

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

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

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

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

3. Elemento Neutro: Dado $\overline{(a,b)}$ e $\overline{(0,0)}$ em Z.

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

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

<u>Teorema 4</u> Cancelamento para a Adição). Dados *α, β,* γ ∈ Z e *α* + *β* = γ + *β*, então *α* = γ.

Demonstração. Seja *α* = (*a, b*), *β* = (*c, d*) e γ = (*e, f*). Logo,

$\overline{(a,b)}$ + $\overline{(c,d)}$ = $\overline{(e,f)}$ + $\overline{(c,d)}$ ⇒ $\overline{(a\ +\ c, b\ +\ d)}$ = $\overline{(e\ +\ c, f\ +\ d)}$

⇒ (a + c) + (f + d) = (b + d) + (e + c)

⇒ a + f = b + e

⇒ $\overline{(a,b)}$ = $\overline{(e,f)}$

<u>Teorema 5</u> (Propriedade do elemento oposto). Dado $\overline{(a,b)}$ ∈ Z, existe um único $\overline{(c,d)}$ ∈ Z tal que $\overline{(a,b)}$ + $\overline{(c,d)}$ = $\overline{(0,0)}$. Este $\overline{(c,d)}$ é o elemento $\overline{(b,a)}$.

Demonstração. Provaremos inicialmente a existência deste elemento oposto e, em seguida, a sua unicidade. Seja (*a, b*) ∈ Z. Tomemos (*c, d*) = (*b, a*) ∈ Z e assim,

$\overline{(a,b)}$ + $\overline{(c,d)}$ = $\overline{(e,f)}$ ⇒ $\overline{(a,b)}$ + $\overline{(b,a)}$ = $\overline{(e,f)}$

⇒ $\overline{(a+b, b+a)}$ = $\overline{(e,f)}$

⇒ a + b + f = b + a + e

⇒ f + 0 = e + 0

$$\Rightarrow \overline{(f,e)} = \overline{(0,0)}$$

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

Deste maneira, existe um elemento $\overline{(c,d)} = \overline{(b,a)} \in Z$, tal que, $\overline{(a,b)} + \overline{(c,d)} = \overline{(0,0)}$. Suponhamos que existam dois elementos distintos desta forma, $\overline{(c,d)}$, $\overline{(c',d')} \in Z$, ou seja, $\overline{(c,d)} \neq \overline{(c',d')} \Rightarrow \left.\begin{matrix} c + d' \neq d + c' \end{matrix}\right\}$ $(*)$. Como os dois são opostos a $\overline{(a,b)}$, vemos que:

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

$$\Rightarrow a + c = b + d \Big\} \text{ (**)}$$

e

$$\overline{(a,b)} + \overline{(c',d')} = \overline{(0,0)} \Rightarrow \overline{(a+c', b+d')} = \overline{(0,0)}$$

$$\Rightarrow a + c' = b + d' \Big\} \text{ (***)}$$

Somando o primeiro membro de (**) ao segundo de (***) e o primeiro de (***) com o segundo de (**) obtemos:

$a + c + b + d' = a + c' + b + d \Rightarrow c + d' = c' + d$, o que contradiz (*). Portanto, $\overline{(c,d)} = \overline{(c',d')}$.

Definição 3 Dado $\alpha \in Z$, o único $\beta \in Z$, tal que, $\alpha + \beta = \overline{(0,0)}$ chama-se simétrico de α (ou oposto de α, ou inverso aditivo de α). Sua unicidade permite que o utilizemos como símbolo o $-\alpha$.

Dessa maneira, $\alpha + (-\alpha) = \overline{(0,0)}$ e, como visto pelo teorema, $-\alpha = \overline{(b,a)}$. A existência e unicidade de oposto de um número inteiro permite que definamos uma outra operação em Z, denominada subtração.

Definição 4 A subtração em Z, denotada por $(-)$, é a operação definida da seguinte forma: Se $\alpha, \beta \in Z$, então: $\alpha - \beta = \alpha + (-\beta)$.

Assim, a subtração $\alpha - \beta$ representa a soma de α com o oposto ou simétrico de β.

Proposição 1 Para $\alpha, \beta, \gamma \in Z$, vale:

I. $-(-\alpha) = \alpha$;

II. $-\alpha + \beta = \beta - \alpha$;

III. $\alpha - (-\beta) = \alpha + \beta$;

IV. $-\alpha - \beta = -(\alpha + \beta)$;

V. $\alpha - (\beta + \gamma) = \alpha - \beta - \gamma$;

Demonstração.

I. Seja $\alpha = \overline{(a,b)}$, então, $-\alpha = \overline{(b,a)}$, e assim, $-(-\alpha) = -\overline{(b,a)} = \overline{(a,b)} = \alpha$.

II. Seja $\alpha = \overline{(a,b)}$ e $\beta = \overline{(c,d)}$. Claramente, $-\alpha = \overline{(b,a)}$. Temos:

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

III. Seja $\alpha = \overline{(a,b)}$ e $\beta = \overline{(c,d)}$, e assim, $-\alpha = \overline{(b,a)}$ e $-\beta = \overline{(d,c)}$.

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

IV. Se $\alpha = \overline{(a,b)}$ e $\beta = \overline{(c,d)}$, teremos, $-\alpha = \overline{(b,a)}$ e $-\beta = \overline{(d,c)}$, e assim:

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

V. Se $\alpha = \overline{(a,b)}$, $\beta = \overline{(c,d)}$ e $\gamma = \overline{(e,f)}$, então, $-\alpha = \overline{(b,a)}$, $-\beta = \overline{(d,c)}$ e $-\gamma = \overline{(f,e)}$ e assim:

$$\alpha - (\beta + \gamma) = \overline{(a,b)} - (\overline{(c,d)} + \overline{(e,f)}) = \overline{(a,b)} - \overline{(c+e,d+f)}$$
$$= \overline{(a,b)} + \overline{(d+f,c+e)} = \overline{(a,b)} + \overline{(d,c)} + \overline{(f,e)}$$
$$= \alpha - \beta - \gamma.$$

2.2.2 Multiplicação de números inteiros

Definiremos a seguir outra operação em Z, a qual chamaremos de multiplicação ou produto. Pensando que tendo $\overline{(a,b)}$ expresso por $(a - b)$, $\overline{(c,d)}$ expresso em $(c - d)$ e $(a - b) \cdot (c - d) = a \cdot c + b \cdot d - (a \cdot d + b \cdot c)$, vemos assim a definição seguinte.

Definição 5 Dados $\overline{(a,b)}$ e $\overline{(c,d)}$ em Z, definimos o produto $(a,b) \cdot (c,d)$ como sendo $\overline{(a \cdot c + b \cdot d, a \cdot d + b \cdot c)}$

Teorema 6 A multiplicação em Z está bem definida, isto é, se $\overline{(a,b)} = \overline{(a',b')}$ e $\overline{(c,d)} = \overline{(c',d')}$, então, $\overline{(a,b)} \cdot \overline{(c,d)} = \overline{(a',b')} \cdot \overline{(c',d')}$.

Demonstração: Seja $(a,b) = \overline{(a',b')}$, isto é, $a + b' = b + a'$, que nos fornece:

$$ca + cb' = cb + ca' \quad (*)$$

e

$$da + b'd = bd + a'd \quad (**)$$

Somando as equações (*) e (**) obtemos:

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

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

$$\overline{(a,b)} \,.\, \overline{(c,d)} = \overline{(a',b')} \,.\, \overline{(c,d)} \quad (***)$$

Do mesmo modo, $\overline{(c,d)} = \overline{(c',d')} \Rightarrow c + d' = d + c'$, de onde obtemos:

$$a'c + a'd' = a'd + a'c' \quad (\#) \quad \text{e} \quad b'c + b'd' = b'd + b'c' \quad (\#\#)$$

Novamente somando as equações (#) e (##) obtemos:

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

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

$$\overline{(a',b')} \,.\, \overline{(c,d)} = \overline{(a',b')} \,.\, \overline{(c',d')} \quad (****)$$

Dessa maneira, observando (***) e (****), obtemos que:

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

Teorema 7 A multiplicação em Z é comutativa, associativa, tem $\overline{(1,0)}$ como neutro multiplicativo e é distributiva em relação à adição. Além disso, vale a propriedade do cancelamento multiplicativo, ou seja, se $\alpha, \beta, \gamma \in Z$, com $\gamma \neq (0,0)$ e $\alpha\gamma = \beta\gamma$, então $\alpha = \beta$.

Demonstração. Tendo $\alpha = \overline{(a,b)}$, $\beta = \overline{(c,d)}$ e $\gamma = \overline{(e,f)} \neq \overline{(0,0)}$ tais que $\alpha\gamma = \beta\gamma$, ou seja, $\overline{(ae + bf, af + be)} = \overline{(ce + df, cf + de)}$, que equivale a $ae + bf + cf + de = af + be + ce + df$. Encontrando assim, $e(a + d) + f(b + c) = e(b + c) + f(a + d)$.

Como $\overline{(e,f)} \neq \overline{(0,0)}$, temos que $e + 0 \neq f + 0 \Rightarrow e \neq f$. Suponhamos $e > f$, ou seja, $e = f + q$, com $q \in N^*$. Obtendo assim:

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

Com o cancelamento aditivo, temos que q(a + d) = q(b + c), sendo q pertencente aos naturais não nulos, seguimos com cancelamento multiplicativo onde a + d = b + c, tendo $\overline{(a,b)} = \overline{(c,d)}$, ou melhor, $\alpha = \beta$.

Proposição 2 Dados $\alpha, \beta, \gamma \in Z$, é válida a propriedade distributiva da multiplicação em relação a subtração, isto é, $\alpha(\beta - \gamma) = \alpha\beta - \alpha\gamma$.

Demonstração.

$\alpha(\beta - \gamma) = \alpha(\beta + (-\gamma))$

$= \alpha\beta + \alpha(-\gamma)$

Assim, como $\alpha(-\gamma) = -\alpha\gamma$, *vemos que* $\alpha(\beta - \gamma) = \alpha\beta - \alpha\gamma$.

2.3 Relação de Ordem em Z

Façamos, uma comparação dos elementos de Z através de uma relação de ordem.

Definição 6 Dados os inteiros $\overline{(a,b)}$ e $\overline{(c,d)}$, escrevemos $\overline{(a,b)} \leq \overline{(c,d)}$ quando $a + d \leq b + c$.

Proposição 3 A relação definida anteriormente está bem representada, isto é, se $\overline{(a,b)} = \overline{(a',b')}$, $\overline{(c,d)} = \overline{(c',d')}$ e $\overline{(a,b)} \leq \overline{(c,d)}$, então, $\overline{(a',b')} \leq \overline{(c',d')}$.

Demonstração.

$\overline{(a,b)} = \overline{(a',b')} \Rightarrow a + b' = b + a'$. (F1)

$\overline{(c,d)} = \overline{(c',d')} \Rightarrow c + d' = d + c'$. (F2)

$\overline{(a,b)} \leq \overline{(c,d)} \Rightarrow a + d \leq b + c$

$\Rightarrow a + b' + d \leq b + b' + c$

$\Rightarrow a + b' + d + d' \leq b + b' + c + d'$ (F3)

Subtituindo (F1) e (F2) em (F3), obtemos:

$b + a' + d + d' \leq b + b' + d + c' \Rightarrow a' + d' \leq b' + c'$

$\Rightarrow \overline{(a',b')} \leq \overline{(c',d')}$

Teorema 8 A relação ≤ definida acima é uma relação de ordem em Z, ou seja, é reflexiva, antissimétrica e transitiva.

Demonstração.

1. Reflexiva: Seja $\alpha = \overline{(a,b)} \in Z$. Obviamente, $\overline{(a,b)} \leq \overline{(a,b)}$, pois, $\overline{(a,b)} = \overline{(a,b)}$.

2. Antissimétrica: Sejam $\alpha, \beta \in Z$, $\alpha \leq \beta$ e $\beta \leq \alpha$. Consideremos $\alpha = \overline{(a,b)}$ e $\beta = \overline{(c,d)}$ e assim,

$$\alpha \leq \beta$$
$$\overline{(a,b)} \leq \overline{(c,d)}$$
$$a + d \leq b + c$$
e
$$\beta \leq \alpha$$
$$\overline{(c,d)} \leq \overline{(a,b)}$$
$$c + b \leq d + a$$

Pela tricotomia dos naturais, obtemos que, $a + d = b + c$, isto é, $\overline{(a,b)} = \overline{(c,d)}$.

3. Transitiva: Sejam $\alpha, \beta, \gamma \in Z$, $\alpha \leq \beta$ e $\beta \leq \gamma$, com $\alpha = \overline{(a,b)}$, $\beta = \overline{(c,d)}$ e $\gamma = \overline{(e,f)}$. Destas desigualdades obtemos $a + d \leq b + c$ e $c + f \leq d + e$. Sendo assim, existem $p, q \in N$ tais que,

$$a + d + p = b + c$$
e
$$c + f + q = d + e.$$

Somando os primeiros e segundos membros das duas igualdades, na ordem dada, obtemos

$$a + d + p + c + f + q = b + c + d + e$$
$$a + f + p + q = b + e$$

Como $p + q \in N$, chegamos a conclusão que, $a + f \leq b + e$, ou seja, $\overline{(a,b)} \leq \overline{(e,f)}$.

Teorema 9 A relação ≤ é compatível com as operações em Z, isto é,

i. $\alpha \leq \beta \Rightarrow \alpha + \gamma \leq \beta + \gamma$;

ii. $\alpha \leq \beta$ e $\gamma \geq \overline{(0,0)} \Rightarrow \alpha\gamma \leq \beta\gamma$;

iii. (Lei da Tricotomia): Apenas uma das situações seguintes ocorre: $\alpha = \overline{(0,0)}$ ou $\alpha < \overline{(0,0)}$ ou $\alpha > \overline{(0,0)}$.

Demonstração.

i. Tendo $\alpha = \overline{(a,b)}$, $\beta = \overline{(c,d)}$ e $\gamma = \overline{(e,f)}$ em Z. Assim,

$\overline{(a,b)} \leq \overline{(c,d)} \Rightarrow a + d \leq b + c$

$\Rightarrow a + e + d + f \leq b + f + c + e$

$$\Rightarrow \overline{(a+e, b+f)} \leq \overline{(c+e, d+f)}$$

$$\Rightarrow \overline{(a,b)} + \overline{(e,f)} \leq \overline{(c,d)}\ \overline{(e,f)}$$

$$\Rightarrow \alpha + \gamma \leq \beta + \gamma$$

ii. Tomando $\alpha = \overline{(a,b)}$, $\beta = \overline{(c,d)}$ e $\gamma = \overline{(e,f)}$. Dessa forma obtemos, $a + d \leq b + c$ e $e \geq f$.

Sendo assim, existem $p, q \in \mathbb{N}$, tais que,

$$b + c = a + d + p$$

e

$$e = f + q.$$

Temos que,

$$b + c = a + d + p \Rightarrow be + ce = ae + de + pe \text{ (F.2.1)}$$

e

$$b + c = a + d + p \Rightarrow bf + cf = af + df + pf \text{ (F.2.2)}$$

Obtendo,

$$e = f + q \Rightarrow pe = pf + pq \text{ (F.2.3)}$$

Somando o segundo membro da igualdade (F.2.1) com o primeiro da igualdade (F.2.2) e o primeiro membro de (F.2.1) com o segundo de (F.2.2), obtemos,

$$ae + de + pe + bf + cf = be + ce + af + df + pf.$$

Substituindo (F.2.3) nesta última igualdade, obtemos:

$$ae + de + pf + pq + bf + cf = be + ce + af + df + pf$$

$$ae + de + bf + cf + pq = be + ce + af + df$$

$$ae + de + bf + cf \leq be + ce + af + df$$

$$\overline{(ae + bf, af + be)} \leq \overline{(ce + df, cf + de)}$$

$$\overline{(a,b)} \,.\, \overline{(e,f)} \leq \overline{(c,d)} \,.\, \overline{(e,f)}$$

$$\alpha\,\gamma \leq \beta\,\gamma$$

iii. Suponhamos $\alpha > (0,0)$ e $\alpha < (0,0)$ simultaneamente, com $\alpha = \overline{(a,b)}$.

$$\overline{(a,b)} > \overline{(0,0)} \Rightarrow a > b$$

e

$$\overline{(a,b)} < \overline{(0,0)} \Rightarrow a < b,$$

tendo aí um absurdo pela tricotomia dos naturais.

Suponhamos agora $\alpha = \overline{(0,0)}$ e $\alpha < \overline{(0,0)}$ (ou $\alpha > \overline{(0,0)}$) simultaneamente.

$$\overline{(a,b)} < \overline{(0,0)} \Rightarrow a < b$$

e

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

tendo aí novamente um absurdo, pela tricotomia dos naturais.

Teorema 10 (Tricotomia dos Inteiros). Para $\alpha, \beta, \gamma \in Z$, apenas uma das situações seguintes ocorre: $\alpha = \beta$ ou $\alpha < \beta$ ou $\alpha > \beta$.

Demonstração. Suponhamos $\alpha < \beta$ e $\beta < \alpha$ simultaneamente:

$$\alpha < \beta \Rightarrow \overline{(a,b)} < \overline{(c,d)} \Rightarrow a + d < b + c$$

$$\beta < \alpha \Rightarrow \overline{(c,d)} < \overline{(a,b)} \Rightarrow c + b < d + a,$$

absurdo pela tricotomia dos naturais. Da mesma forma, suponhamos $\alpha < \beta$ ou $\alpha > \beta$ e $\alpha = \beta$ simultaneamente:

$$\alpha < \beta \Rightarrow \overline{(a,b)} < \overline{(c,d)} \Rightarrow a + d < b + c$$

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

Absurdo pela tricotomia dos naturais. Além disto, novamente pela tricotomia dos naturais, necessariamente uma das seguintes ocorre:

$$a + d < b + c, b + c < a + d, a + d = b + c$$

Isto significa que uma das seguintes deve ocorrer:

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

Teorema 11 Para $\alpha, \beta \in Z$, $\alpha \leq \beta$ e $\gamma < \overline{(0,0)}$, temos que $\alpha\gamma \geq \beta\gamma$.

Demonstração. Sejam $\alpha = \overline{(a,b)}$, $\beta = \overline{(c,d)}$ e $\gamma = \overline{(e,f)}$. Temos que,

$\overline{(e,f)} < \overline{(0,0)} \Rightarrow e < f \Rightarrow \overline{(0,0)} < \overline{(f,e)}$.

Vendo que, como $\alpha \leq \beta$:

$$\overline{(a,b)} \cdot \overline{(f,e)} \leq \overline{(c,d)} \cdot \overline{(f,e)} \Rightarrow \overline{(af + be, ae + bf)} \leq \overline{(cf + de, ce + df)}$$

$$\Rightarrow af + be + ce + df \leq ae + bf + cf + de$$

$$\Rightarrow \overline{(ce + df, cf + de)} \leq \overline{(ae + bf, af + be)}$$

$$\Rightarrow \overline{(c,d)} \cdot \overline{(e,f)} \leq \overline{(a,b)} \cdot \overline{(c,d)}$$

$$\Rightarrow \alpha\gamma \geq \beta\gamma$$

Definição 7 Dado $\overline{(a,b)} \in Z$, dizemos que:

i. $\overline{(a,b)}$ é positivo quando $(a,b) > \overline{(0,0)}$;

ii. $\overline{(a,b)}$ é não negativo quando $(a,b) \geq \overline{(0,0)}$;

iii. $\overline{(a,b)}$ é negativo quando $(a,b) < \overline{(0,0)}$;

iv. $\overline{(a,b)}$ é não positivo quando $(a,b) \leq \overline{(0,0)}$;

Observemos que se $\overline{(a,b)} > \overline{(0,0)}$ então $a > b$, e assim, existe $m \in N^*$ tal que $b + m = a$, que equivale $\overline{(a,b)} = \overline{(m,0)}$. Analogamente, se $\overline{(a,b)} < \overline{(0,0)}$, existe $m \in N^*$, tal que $a + m = b$ e dessa forma, $\overline{(a,b)} = \overline{(0,m)}$. Dessa forma, temos que $Z = \{\overline{(0,m)} | m \in N^*\} \cup \{\overline{(0,0)}\} \cup \{\overline{(m,0)} | m \in N^*\}$, onde esta união é disjunta. Também vemos,

$Z_-^* = \{\overline{(0,m)} \mid m \in N^*\}$, $Z_- = \{\overline{(0,m)} \mid m \in N^*\} \cup \{\overline{(0,0)}\}$

$Z_+^* = \{\overline{(m,0)} \mid m \in N^*\}$, $Z_+ = \{\overline{(m,0)} \mid m \in N^*\} \cup \{\overline{(0,0)}\}$

Observemos que Z_+ encontra-se em bijeção com N, o que mostra que Z_+ é uma cópia algébrica de N, no sentido dado pelo teorema seguinte.

Teorema 12 Seja $f : N \to Z$ dada por $f(m) = \overline{(m,0)}$. Então f é injetora e valem as seguintes propriedades:

i. $f(m + n) = f(m) + f(n)$;

ii. $f(mn) = f(m) \cdot f(n)$;

iii. Se $m \leq n$, então $f(m) \leq f(n)$;

Demonstração. Provemos inicialmente que f é injetora. De fato,

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

Provemos agora os itens. Sejam $m, n \in N$.

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

ii. $f(mn,0) = (mn,0) = \overline{(m,0)} \cdot \overline{(n,0)} = f(m) \cdot f(n)$;

iii. Se $m \leq n$, temos que, $\overline{(m,0)} \leq \overline{(n,0)}$, ou seja, $f(m) \leq f(n)$.

O conjunto $f(N) = Z_+$ tem, pelo teorema acima, a mesma estrutura algébrica que N. Por exemplo, 5 + 7 = 12, corresponde, via f, a $\overline{(5,0)} + \overline{(7,0)} = \overline{(12,0)}$ em Z. Da mesma forma, 5 . 7 = 35, corresponde, via f, a $\overline{(5,0)} \cdot \overline{(7,0)} = \overline{(35,0)}$. Temos aí que a relação $5 \leq 7$ se preserva, via f, como $\overline{(5,0)} \leq \overline{(7,0)}$, confirmando a ideia de que a ordem em Z é uma extensão da ordem em N.

A função f descrita acima, chama-se imersão de N em Z.

Vejamos ainda que, se $m \in N$, o simétrico de $\overline{(m,0)}$ é $\overline{(0,m)}$, logo, se identificarmos $\overline{(m,0)}$ com m através de f, obtemos $-m = -\overline{(m,0)} = \overline{(0,m)}$. Dessa forma, identificando N com Z_+, via f, obtemos o que será definido a seguir.

Definição 8 Temos o conjunto dos inteiros como sendo:

$Z = \{-m \mid m \in N^*\} \cup \{0\} \cup N^* = \{..., -m, ..., -2, -1, 0, 1, 2, ..., m, ...\}$.

A partir de agora, esta identificação será a adotada e, então, consideraremos N como um subconjunto de Z. Assim podemos obter:

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

Teorema 13 Se $x, y \in Z$ temos:

1. Se $x > 0$ e $y > 0$, então $xy > 0$;
2. Se $x < 0$ e $y < 0$, então $xy > 0$;
3. Se $x < 0$ e $y > 0$, então $xy < 0$.

Demonstração.

1. Como x e y são elementos positivos de Z, podemos identificá-los por $x = \overline{(x,0)}$ e $y = \overline{(y,0)}$.

Dessa forma, $xy = \overline{(x,0)} \cdot \overline{(y,0)} = \overline{(xy,0)}$. Sabemos que $\overline{(xy,0)} > \overline{(0,0)}$, portanto, $xy > 0$.

2. Sabendo que, $x < 0 \Rightarrow -x > 0$ e $y < 0 \Rightarrow -y > 0$, sendo assim, $-x = \overline{(-x,0)} \Rightarrow x = -\overline{(-x,0)} = \overline{(0,-x)}$ e $-y = \overline{(-y,0)} \Rightarrow y = -\overline{(-y,0)} = \overline{(0,-y)}$

Vemos:

$xy = \overline{(0,-x)} \cdot \overline{(0,-y)}$

$= \overline{\left((-x)(-y),\ 0\right)}$

Sabemos que $((-x)(-y),0) > (0,0)$, portanto, $xy > 0$.

3. Tendo que, $x < 0 \Rightarrow -x > 0$, sendo assim, $-x = \overline{(-x,0)} \Rightarrow x = -\overline{(-x,0)} = \overline{(0,-x)}$.

Temos:

$xy = \overline{(0,-x)} \cdot \overline{(y,0)}$

$= \overline{(0,(-x)y)}$

Sabemos que, $(0,(-x)y) < (0,0)$, portanto, $xy < 0$.

Definição 9 Seja X um subconjunto não vazio de Z. Dizemos que X é limitado inferiormente se existe $\alpha \in Z$ tal que $\alpha \leq x$, para todo $x \in X$. Tal α chama-se cota inferior de X. Dizemos que X é limitado superiormente se existir $\beta \in Z$ tal que $x \leq \beta$ para todo $x \in X$. Tal β é chamado cota superior de X.

Exemplo: Claramente $0 \leq x$ para todo $x \in N \subset Z$, logo, 0 é cota inferior de N. Qualquer inteiro negativo também será.

Teorema 14 N não admite cota superior em Z.

Demonstração. Mostremos que, para todo $\beta \in Z$, existe $x \in N$, tal que $\beta < x$. Seja $\beta \in Z$:

- Se $\beta < 0$, basta tomar qualquer $x \in N$ que obtemos $\beta < x$;
- Se $\beta = 0$, basta tomar $x = 1 \in N$, logo, $\beta < x$;
- Se $\beta > 0$, então, $\beta \in N$, portanto, $s(\beta) \in N$. Sabemos que $\beta < s(\beta)$, ou seja, $\beta < \beta + 1$. Sendo assim, para todo $\beta > 0$ em Z, existe $x = \beta + 1 \in N$, tal que $\beta < x$.

Teorema 15 (Princípio da Boa Ordem para Z). Seja $X \subset Z$ não vazio e limitado inferiormente. Então X possui elemento mínimo.

Demonstração. Seja α uma cota inferior de X, ou seja, $\alpha \leq x$ para todo e qualquer $x \in X$. Consideremos $X' = \{x - \alpha \mid x \in X\}$. Claramente, $X' \subset N$ (identificado com Z_+) e, pelo Princípio da Boa Ordem em N, o conjunto X' possui elemento mínimo , digamos, m'. Assim, $m' \in X'$ e $m' \leq y$ para todo $y \in X'$. Como $m' \in X'$, $m' = m - \alpha$, para algum $m \in X$. Afirmamos que $m = m' + \alpha$ é elemento mínimo de X. Só falta verificar que $m \leq x$ para todo $x \in X$, mas isso equivale a $m - \alpha \leq x - \alpha$ para todo $x \in X$, ou ainda, $m' \leq x - \alpha$, que é verdade, pela definição de $m' \leq y$. Logo, m é o mínimo de X.

Corolário 1 Seja $x \in Z$ tal que $0 < x \leq 1$. Então $x = 1$.

Demonstração. Seja $A = \{y \in Z \mid 0 < y \leq 1\}$. Tem-se que $A \neq \emptyset$, dado que $1 \in A$, e A é limitado inferiormente por 0. Pelo Princípio da Boa Ordem, A possui elemento mínimo, digamos, m. Suponhamos $m < 1$. Sendo assim, $0 < m < 1$, logo, $0 < m^2 < m < 1$, o que significa que $m^2 \in A$, contradizendo a minimalidade de m. Assim, $m = 1$ e $A = \{1\}$.

Corolário 2 Sejam $n, x \in Z$ tais que $n < x \leq n + 1$. Então $x = n + 1$.

Demonstração. Seja $A = \{x \in Z \mid n < x \leq n+1, n \in Z\}$. Tem-se que $A \neq \emptyset$, (pois $n + 1 \in A$), e A é limitado inferiormente por n. Pelo Princípio da Boa Ordem, A possui elemento mínimo, digamos, m. Como $m \in A$, temos que $n < m \leq n+1$, de onde segue que $0 < m - n \leq 1$. Como $m, n \in Z$, $m - n \in Z$, assim, $m - n = 1$, ou seja, $m = n + 1$.

Definamos o conceito de módulo ou valor absoluto de um número inteiro.

Definição 10 Seja $x \in Z$. Definimos o valor absoluto de x (ou módulo de x), denotado por $|x|$, como sendo:

$$|x| = \begin{cases} x, se\ x \geq 0; \\ -x, se\ x < 0. \end{cases}$$

Exemplo: $|-5| = |5| = 5$; $|0| = 0$.

Proposição 4 Para todo $x \in Z$, temos que:

a) $|x| \geq 0$;

b) $|x| = 0 \Leftrightarrow x = 0$.

Demonstração.

a) Provemos que $|x| \geq 0$, para todo $x \in Z$.

- Se $x > 0$, por definição, $|x| = x$, logo, $|x| > 0$;
- Se $x < 0$, por definição, $|x| = -x$, e sabemos ainda que, $-x > 0$. Portanto, $|x| > 0$;
- Se $x = 0$, temos que $|x| = x = 0$.

Assim, para todo $x \in Z$, temos $|x| \geq 0$.

b) ($\Rightarrow$) Seja $|x| = 0$.

- Se $x > 0$, então $|x| = x = 0$. Contradição pela tricotomia;
- Se $x < 0$, então $|x| = -x = 0$, logo, $x = 0$. Novamente, contradição pela tricotomia.

Portanto, $x = 0$.

($\Leftarrow$) Seja $x = 0$. Logo, $|x| = x = 0$.

- Se $x > 0$, por definição, $|x| = x$, logo, $|x| > 0$;
- Se $x < 0$, por definição, $|x| = -x$, e ainda $-x > 0$. Portanto, $|x| > 0$;
- Se $x = 0$, temos que $|x| = x = 0$. Assim, para todo $x \in Z$, temos $|x| \geq 0$.

2. ($\Rightarrow$) Seja $|x| = 0$.

- Se $x > 0$, então $|x| = x = 0$. Contradição pela tricotomia;
- Se $x < 0$, então $|x| = -x = 0$, isto Ø, $x = 0$. Novamente, contradição pela tricotomia.

Portanto, $x = 0$.

($\Leftarrow$) Seja $x = 0$. Logo, $|x| = x = 0$.

Proposição 5 Para todo $x, y \in Z$, temos que $|xy| = |x|.|y|$.

Demonstração. Vejamos nos casos.

- Se $x > 0$ e $y > 0$, temos, $xy > 0$, e assim, por definição de módulo, $|xy| = xy$. Pela mesma definição, $|x| = x$ e $|y| = y$, logo, $|x|.|y| = x.y$. Portanto, $|x|.|y| = |xy|$.
- Se $x < 0$ e $y < 0$, temos, $xy > 0$, e assim, $|x.y| = x.y$. Temos que, $x < 0 \Rightarrow |x| = -x$ e $y < 0 \Rightarrow |y| = -y$, sendo assim, $|x||y| = (-x)(-y) = x.y$. Logo, $|x.y| = |x|.|y|$.

- Se $x < 0$ e $y > 0$ (ou $x > 0$ e $y < 0$), temos $xy < 0$, isto é, $|x.y| = -x.y$. Temos que, $x < 0 \Rightarrow |x| = -x$ e $y > 0 \Rightarrow |y| = y$, sendo assim, $|x|.|y| = (-x).(y) = -x.y$. Logo, $|x.y| = |x|.|y|$.

- Se $x = 0$ e y é qualquer (ou $y = 0$ e x qualquer), temos $x.y = 0$, logo, $|x.y| = 0$. Como $|x| = 0$, claramente, $|x|.|y| = 0 \cdot |y| = 0$. Portanto, $|x.y| = |x|.|y|$.

Dessa forma, chegamos a conclusão que $|x.y| = |x|.|y|$, para todos $x,y \in Z$.

Proposição 6 Para $n \in N^*$, tem-se: $|x| = n \Leftrightarrow x = n$ ou x = - n

Demonstração. ($\Rightarrow$) Seja $|x| = n$.

- Se $x > 0$, $|x| = x$. Sendo assim, x = n.

- Se $x < 0$, $|x| = -x$. Logo, $-x = n$, isto Ø, $x = -n$.

($\Leftarrow$) Seja $x = n$ ou $x = -n$.

- Se $x = n$, então, $|x| = |n|$. Como $n \in N^*$, obviamente, $n > 0$, logo, $|n| = n$, ou seja, $|x| = n$.

- Se $x = -n$, então $|x| = |- n|$. Como $n > 0$, pelo Teorema 3.4.6, $-n < 0$, sendo assim, por definição de módulo, $|- n| = -(-n) = n$. Logo, $|x| = n$.

Definição 11 Um elemento $x \in Z$ diz-se inversível se existe $y \in Z$ tal que $xy = 1$.

Proposição 7 Os únicos elementos inversíveis de Z são 1 e −1.

Demonstração. Seja $x \in Z$ inversível e $y \in Z$, tal que, $xy = 1$. Sendo assim, $|xy| = |x|.|y| = 1$. Como $|x| \geq 0$, $|y| \geq 0$ e $|x|.|y| = 1$, vemos que $|x| > 0$ e $|y| > 0$, logo, $|x| \geq 1$ e $|y| \geq 1$. Multiplicando esta última desigualdade por $|x|$, em ambos os membros, obtemos, $|x|.|y| \geq |x|$. Chegamos que, $1 = |x||y| \geq |x| \geq 1$, o que nos garante $|x| = 1$. Portanto, $x = 1$ ou $x = -1$.

3 NÚMEROS RACIONAIS

Aprendemos no ensino fundamental que um número racional é a razão entre dois inteiros, significando divisão. Utilizaremos o conceito de relação de equivalência a partir dos inteiros, do mesmo modo que o utilizamos para definir um número inteiro a partir do conceito de números naturais.

3.1 Construção dos números racionais

Sejam N o conjunto dos números naturais e Q o conjunto dos números racionais. Uma função s: N → Q é chamada uma sequência de números racionais. Como exemplo, seja s: N → Q tal que para todo número natural n, $s(n) = \frac{n}{1+n}$. Assim, $s(0) = 0$, $s(1) = 1/2$, $s(2) = 2/3$, etc.

Seja s: N → Q uma sequência de números racionais. Então quando n é um número natural, $s(n)$ é um certo número racional que também costuma ser indicado com esta notação s_n. Isto é, $s(n) = s_n$ e s_n é chamado o n-ésimo termo da sequência s.

É claro que sabendo quais são todos os s_n nós conhecemos completamente a nossa sequência s. Por essa razão uma sequência s: N → Q costuma ser indicada com a notação $\{s_n \mid n \in \mathrm{N}\}$, ou $\{s_n\}_{n\in\mathrm{N}}$, ou simplesmente s_n quando não há perigo de confusão.

Uma sequência de números racionais s_n é dita *limitada* quando existem dois números racionais p, q tais que para todo $n \in$ N:

$$p \leq s_n \leq q$$

Dizemos que duas sequências a_n e b_n de números racionais formam nessa ordem o par de Cauchy $\{a_n, b_n\}$ se as seguintes condições estão verificadas:

1) a_n é crescente, b_n é decrescente;

2) Para todo n ∈ N : $a_n \leq b_n$;

3) Dado qualquer número racional $\epsilon > 0$ existe um número natural n_0 tal que para todo n > n_0: $b_n - a_n < \epsilon$

Consideremos o conjunto Z × Z^* = {(a,b) | a ∈ Z e b ∈ Z^* }.

Definição 1 Sejam a ∈ Z e b ∈ Z^*. A relação dada por (a,b) ~ (c,d) quando $ad = bc$.

Teorema 1 A relação citada acima é de equivalência.

Demonstração.

1. Reflexiva: Temos que, se $a \in Z$ e $b \in Z^*$, $ab = ba$, portanto $(a, b) \sim (a,b)$.
2. Simétrica: Se $a, c \in Z$, $b, d \in Z^*$e $(a, b) \sim (c, d)$, então, $ad = bc$, ou ainda, $cb = da$, isto é, $(c, d) \sim (a, b)$.
3. Se $a, c, e \in Z$, $b, d, f \in Z^*$, $(a, b) \sim (c, d)$ e $(c, d) \sim (e, f)$, temos:

$$ad = bc \Rightarrow adf = bcf$$

$$cf = de \Rightarrow bcf = bde$$

Dessa forma, $adf = bde$, como $d \neq 0$, $af = be$, que significa, $(a,b) \sim (e,f)$.

Consideremos, por um momento, nossas noções intuitivas de números racionais. Temos que, ad = bc $\Leftrightarrow \frac{a}{b} = \frac{c}{d}$, digamos então que, se as divisões de *a* por *b* e *c* por *d* coincidem, podemos dizer que $(a,b) \sim (c,d)$,

Exemplo 1

1. $(1, 2) \sim (2, 4) \sim (5, 10)$;
2. $(7, 14) \sim (3, 6)$

Definição 2 Dado $(a,b) \in Z \times Z^*$, denotamos por $\frac{a}{b}$ (lemos a sobre *b*) a classe de equivalência do par (a,b) pela relação $\sim$ acima. Assim,

$\frac{a}{b} = \{(x, y) \in Z \times Z^* / (x, y) \sim (a, b)\}$

Exemplo 2

$\frac{1}{2} = \{(x, y) \in Z \times Z^* / (x, y) \sim (1, 2)\} = \{(x, y) \in Z \times Z^* / 2x = 1y\}$. Com isso, $(1, 2) \in \frac{1}{2}$; $(2, 4) \in \frac{1}{2}$; $(3, 7) \notin \frac{1}{2}$.

Teorema 2 (Propriedade Fundamental das Frações). Se (a,b) e (c,d) são elementos de $Z \times Z^*$, então $\frac{a}{b} = \frac{c}{d}$ se, e somente se, $ad = bc$.

Demonstração. Sabemos que: $\frac{a}{b} = \frac{c}{d} \Leftrightarrow (a,b) \sim (c,d) \Leftrightarrow ad = bc.$

Definição 3 Denotamos por Q, e denominamos por conjunto dos números racionais, o conjunto quociente de $Z \times Z^*$ pela relação de equivalência $\sim$, isto é, $Q = (Z \times Z^*)/\sim = \{\frac{a}{b} \mid a \in Z \text{ e } b \in Z^*\}$

3.2 Operações em Q

Definição 3 Sejam $\frac{a}{b}$ e $\frac{c}{d}$ números racionais, isto é, elementos de Q, onde a, b, c, d são inteiros. Definimos operações chamadas de adição e de multiplicação, respectivamente, por:

$\frac{a}{b} + \frac{c}{d} = \frac{ad+bc}{bd}$ e $\frac{a}{b} . \frac{c}{d} = \frac{ac}{bd}$.

Denotaremos $\frac{a}{b} . \frac{c}{d}$ também por $\frac{a}{b} \ \frac{c}{d}$.

Exemplo 3

1. $\frac{2}{3} + \frac{1}{4} = \frac{2.4+3.1}{3.4} = \frac{11}{12}$;
2. $\frac{2}{3} . \frac{1}{4} = \frac{2.1}{3.4} = \frac{2}{12}$.

Teorema 3 As operações em Q estão bem definidas, ou seja, se $\frac{a}{b} = \frac{a'}{b'}$ e $\frac{c}{d} = \frac{c'}{d'}$, então, $\frac{a}{b} + \frac{c}{d} = \frac{a'}{b'} + \frac{c'}{d'}$ e $\frac{a}{b} . \frac{c}{d} = \frac{a'}{b'} . \frac{c'}{d'}$

Demonstração. Vejamos, por hipótese, $ab' = ba'$ e $cd' = dc'$. Temos:

$$\frac{a}{b} + \frac{c}{d} = \frac{ad+bc}{bd} \qquad \text{e} \qquad \frac{a'}{b'} + \frac{c'}{d'} = \frac{a'd'+b'c'}{b'd'} .$$

Queremos provar que as duas somas são iguais, ou seja, que $(ad + bc)\, b'd' = (a'd' + b'c')bd$, isto é, $adb'd' + bcb'd' = a'd'bd + b'c'bd$, ou, $(ab')(dd') + (cd')(bb') = (a'b)(dd') + (bb')(c'd)$, o que é fato, pois, $ab' = ba'$ e $cd' = dc'$. Temos também:

$$\frac{a}{b} . \frac{c}{d} = \frac{ac}{bd} \qquad \text{e} \qquad \frac{a'}{b'} . \frac{c'}{d'} = \frac{a'c'}{b'd'} .$$

De forma análoga, provemos que $\frac{ac}{bd} = \frac{a'c'}{b'd'}$, isto é, $acb'd' = bda'c'$, ou, $(ab')(cd') = (dc')(a'b)$, que é verdadeiro, pela hipótese acima.

Teorema 4 O conjunto Q, munido das operações, adição e multiplicação, tem as propriedades algébricas de Z, onde o elemento neutro aditivo é $\frac{0}{1}$ e o neutro multiplicativo é $\frac{1}{1}$. Além disso, dado um racional $\frac{a}{b} \neq \frac{0}{1}$, existe $\frac{c}{d}$ em Q, tal que $\frac{a}{b} . \frac{c}{d} = \frac{1}{1}$, isto é, todo elemento não nulo de Q possui inverso multiplicativo.

Demonstração. Sejam $r, s, t \in$ Q com r = $\frac{a}{b}$, s = $\frac{c}{d}$ e t = $\frac{e}{f}$:

1. Comutativa:

r + s = $\frac{a}{b} + \frac{c}{d} = \frac{ad+bc}{bd}$

$= \frac{bc+da}{db} = \frac{c}{d} + \frac{a}{b}$

= s + r

2. Associativa:

(r + s) + t = $(\frac{a}{b} + \frac{c}{d}) + \frac{e}{f} = \frac{ad+bc}{bd} + \frac{e}{f}$

$= \frac{(adf+bcf)+bde}{bdf} = \frac{adf+(bcf+bde)}{bdf}$

$= \frac{a}{b} + \frac{cf+de}{df} = \frac{a}{b} + (\frac{c}{d} + \frac{e}{f})$

= r + (s + t)

3. Elemento Neutro:

r + $\frac{0}{1} = \frac{a}{b} + \frac{0}{1} = \frac{a.1+0.b}{b.1} = \frac{a}{b}$ = r.

4. Elemento simétrico ou oposto:

Existe r' tal que r + $r' = \frac{0}{1}$. Seja $r' = \frac{-a}{b}$,

r + $r' = \frac{a}{b} + \frac{-a}{b} = \frac{ab+(-ab)}{bb} = \frac{0}{bb} = \frac{0}{1}$

5. Comutativa da Multiplicação:

r . s= $\frac{a}{b} . \frac{c}{d} = \frac{ac}{bd} = \frac{ca}{bd} = \frac{c}{d} . \frac{a}{b}$ = sr

6. Associativa da Multiplicação:

(r.s).t = $(\frac{a}{b} . \frac{c}{d}). \frac{e}{f} = (\frac{ac}{bd}). \frac{e}{f} = \frac{ace}{bdf}$

$= \frac{a}{b}.(\frac{ce}{df}).= \frac{a}{b}.(\frac{c}{d}\frac{e}{f}) = r.(s.t)$

7. Elemento Neutro da Multiplicação:

r . $\frac{1}{1} = \frac{a}{b}. \frac{1}{1} = \frac{a.1}{a.1} = \frac{a}{b}$ = r

8. Elemento Inverso:

Se r ≠ $\frac{0}{1}$, existe r'' tal que r. $r'' = \frac{1}{1}$. Seja $r'' = \frac{b}{a}$:

r. $r'' = \frac{a}{b}. \frac{b}{a} = \frac{a.b}{b.a} = \frac{a.b}{a.b} = \frac{a}{b}. \frac{a}{b}$

$= \frac{1}{1}. \frac{1}{1} = \frac{1}{1}$

9. Distributiva da Multiplicação em relação a Adição:

r(s + t) = $\frac{a}{b}$. ($\frac{c}{d} + \frac{e}{f}$) = $\frac{a}{b}$. ($\frac{cf+de}{df}$) = $\frac{a(cf+de)}{b(df)}$)

= $\frac{acf+ade}{bdf}$ = $\frac{b}{b}$. $\frac{acf+ade}{bdf}$ = $\frac{b(acf+ade)}{b(bdf)}$

= $\frac{bacf+bade}{bbdf}$ = $\frac{ac}{bd}$. $\frac{ae}{bf}$ = rs + rt

Proposição 1 Os elementos r' e r'' são únicos e denotam-se por $-r$ e r^{-1}, chamados de simétrico e inverso de *r*, nesta ordem.

Demonstração. Suponhamos que u' seja também um simétrico de *r*. Assim, $u' + r = \frac{0}{1}$ e $r' + r = \frac{0}{1}$, dessa forma, $u' + r = r' + r$, daí , chegamos que, $u' = r'$.

Suponhamos agora que u'' seja também um inverso de *r*. Assim, $u''.r = \frac{1}{1}$e $r''.r = \frac{1}{1}$, dessa forma, $u''.r = r''.r$, daí , chegamos que, $u'' = r''$. ($r \neq \frac{0}{1}$para possuir inverso).

Proposição 2 Para $(a,b) \in Z \times Z^*$, temos que: $\frac{-a}{b} = \frac{a}{-b} = -\frac{a}{b} = -\frac{-a}{-b}$.

Demonstração. Para $(a,b) \in Z \times Z^*$, vemos:

$(-a)(-b) = ab = -(a)(-b) = -(-a)(b)$, chegando em:

$\frac{-a}{b} = \frac{a}{-b} = -\frac{a}{b} = -\frac{-a}{-b}$.

Observando esta proposição, se $\frac{a}{b} \in Q$, logo *b* pode ser tomado positivo. Utilizaremos esta informação para definir a relação de ordem em Q.

3.3 Relação de Ordem em Q

Definição 4 Sejam $\frac{a}{b}$ *e* $\frac{c}{d}$ números racionais com *b, d* > 0. Escrevemos $\frac{a}{b} \leq \frac{c}{d}$ quando $ad \leq bc$ e dizemos que $\frac{a}{b}$ é menor ou igual a $\frac{c}{d}$.

Teorema 5 A relação ≤ está bem definida e é uma relação de ordem em Q.

Demonstração. Vamos mostrar inicialmente que a relação está bem definida.

Seja $\frac{a}{b} = \frac{a'}{b'}$, isto é, $ab' = a'b$. Temos que $\frac{a}{b} \leq \frac{c}{d} \Rightarrow ad \leq bc$, e, como $b' > 0$, obtemos $ab'd \leq bcb'$,logo , pela igualdade acima, $a'bd \leq bcb'$, concluímos que $a'd \leq cb'$, ou seja, $\frac{a'}{b'} \leq \frac{c}{d}$.

Do mesmo modo, como $\frac{c}{d} = \frac{c'}{d} \Rightarrow cd' = dc'$,

$\frac{a'}{b'} \leq \frac{c}{d} \Rightarrow a'd \leq cb' \Rightarrow a'dd' \leq cb'd' \Rightarrow a'dd' \leq c'db' \Rightarrow a'd' \leq c'b' \Rightarrow \frac{a'}{b'} \leq \frac{c'}{d'}$

Logo, como $\frac{a}{b} \leq \frac{c}{d} \Rightarrow \frac{a'}{b'} \leq \frac{c}{d}$ e $\frac{a'}{b'} \leq \frac{c}{d} \Rightarrow \frac{a'}{b'} \leq \frac{c'}{d'}$, concluímos que $\frac{a}{b} \leq \frac{c}{d} \Rightarrow \frac{a'}{b'} \leq \frac{c'}{d'}$.

Provemos, agora, que esta é uma relação de ordem:

1. Reflexiva: se $\frac{a}{b} \in Q$, claramente, $\frac{a}{b} = \frac{a}{b}$, isto é, $\frac{a}{b} \leq \frac{a}{b}$;
2. Simétrica: se $\frac{a}{b}, \frac{c}{d} \in Q, \frac{a}{b} \leq \frac{c}{d}$ *e* $\frac{c}{d} \leq \frac{a}{b}$, temos que *ad* ≤ *bc* e *cb* ≤ *ad*, daí , pela tricotomia dos inteiros, obtemos, *ad* = *bc*, isto é, $\frac{a}{b} = \frac{c}{d}$;
3. Transitiva: se $\frac{a}{b}, \frac{c}{d}, \frac{e}{f} \in Q, \frac{a}{b} \leq \frac{c}{d}$ *e* $\frac{c}{d} \leq \frac{e}{f}$, temos *ad* ≤ *bc* e *cf* ≤ *ed*. Multiplicando *f* na primeira e *b* na segunda desigualdade (podemos fazer isto, pois, *b, d* > 0), obtemos *adf* ≤ *bcf* e *bcf* ≤ *bed*, daí , pela transitividade dos inteiros, obtemos, *adf* ≤ *bed*, ou ainda, *af* ≤ *be* (*d* > 0), que significa, $\frac{a}{b} \leq \frac{e}{f}$.

<u>Proposição 3</u> Se *r, s, t* ∈ Q, são válidos os itens seguintes:

1. *r* ≤ *s* ⇔ *r* + *t* ≤ *s* + *t*;
2. Se *r* ≤ *s* *e* *t* $\geq \frac{0}{1}$, então *rt* ≤ *st*;
3. Se *r* ≤ *s* *e* *t* $\leq \frac{0}{1}$, então *rt* ≥ *st*.

Demonstração. Sejam $r = \frac{a}{b}$ *e* $s = \frac{c}{d}$ *e* $t = \frac{e}{f}$:

1. $\frac{a}{b} \leq \frac{c}{d} \Leftrightarrow \text{da} \leq \text{bc} \Leftrightarrow \text{daf} \leq \text{bcf}$, pois f > 0

$\Leftrightarrow$ *daf* + *dbe* ≤ *bcf* + *dbe* por propriedade dos inteiros

$\Leftrightarrow \text{d(af} + \text{be)} \leq \text{b(cf} + \text{de)} \Leftrightarrow \text{df(af} + \text{be)} \leq \text{bf(cf} + \text{de)}$

$\Leftrightarrow \frac{af+be}{bf} \leq \frac{cf+de}{df} \Leftrightarrow \frac{a}{b} + \frac{e}{f} \leq \frac{c}{d} + \frac{e}{f}$.

2. Como t = $\frac{e}{f}$ e t ≥ $\frac{0}{1}$, temos $\frac{e}{f} \geq \frac{0}{1}$ que implica em e ≥ 0. Assim:

$\frac{a}{b} \leq \frac{c}{d} \Rightarrow \text{ad} \leq \text{cb}$

$\Rightarrow \text{aedf} \leq \text{cebf}$, pois e ≥ 0 e f > 0.

$\Rightarrow \frac{ae}{bf} \leq \frac{ce}{df} \Rightarrow \frac{a}{b}\frac{e}{f} \leq \frac{c}{d}\frac{e}{f}$.

3. Como t = $\frac{e}{f}$ e t ≤ $\frac{0}{1}$, temos $\frac{e}{f} \leq \frac{0}{1} \Rightarrow$ e ≤ 0. Assim:

$\frac{a}{b} \leq \frac{c}{d} \Rightarrow \text{ad} \leq \text{cb} \Rightarrow \text{adf} \leq \text{cbf}$, pois f > 0

$\Rightarrow aedf \geq cebf$ pois $e \leq 0$

$\Rightarrow \frac{ae}{bf} \geq \frac{ce}{df} \Rightarrow \frac{a}{b}\frac{e}{f} \geq \frac{c}{d}\frac{e}{f}$.

Como em Z, temos aqui:

$Q^* = \left\{\frac{a}{b}\middle|(a,b) \in Z^* \, x \, Z_+^*\right\}$, $Q_+^* = \left\{\frac{a}{b}\middle|(a,b) \in Z_+^* \, x \, Z_+^*\right\}$,

$Q_-^* = \left\{\frac{a}{b}\middle|(a,b) \in Z_-^* \, x \, Z_+^*\right\}$, $Q_- = \left\{\frac{a}{b}\middle|(a,b) \in Z_-^* \, x \, Z_+^*\right\} \cup \left\{\frac{0}{1}\right\}$,

$Q_{\mp} = \left\{\frac{a}{b}\middle|(a,b) \in Z_+^* \, x \, Z_+^*\right\} \cup \left\{\frac{0}{1}\right\}$ e $Q = Q_-^* \cup \left\{\frac{0}{1}\right\} \cup Q_+^*$

Teorema 6 (Lei da Tricotomia em Q). Dados *r, s* ∈ Q, uma, e apenas uma, das situações seguintes ocorre: ou *r* = *s*, ou *r* < *s*, ou *s* < *r*.

Demonstração. Tendo que r = $\frac{a}{b}$ e s = $\frac{c}{d}$ com *b, d* > 0. Pela tricotomia em Z, ou *ad* = *bc*, caso este que ocorre *r* = *s*, ou *ad* < *bc*, caso em que ocorre *r* < *s*, ou *bc* < *ad*, caso em que ocorre *s* < *r*. Além disso, somente uma delas pode ocorrer.

Vamos ver agora a função que imerge de Z em Q, a mesma que falamos, de N em Z, na contrução dos inteiros.

Teorema 7 A função *i* : Z → Q, definida por i(n) = $\frac{n}{1}$ é injetora. Além disso, ela preserva as operações e a relação de ordem de Z em Q no seguinte sentido:

1. *i*(*m* + *n*) = *i*(*m*) + *i*(*n*);
2. *i*(*mn*) = *i*(*m*).*i*(*n*);
3. Se *m* ≤ *n*, então *i*(*m*) ≤ *i*(*n*).

Demonstração. Provemos inicialmente que i é injetora. Se *i*(*m*) = *i*(*n*), temos que $\frac{m}{1} = \frac{n}{1}$, isto é, *m* · 1 = *n* · 1, equivalente a *m* = *n*, logo, *i*(*m*) = *i*(*n*) ⇒ *m* = *n*, portanto, *i* é injetora.

1. $i(m+n) = \frac{m+n}{1} = \frac{1.m+n.1}{1.1} = \frac{m}{1} + \frac{n}{1} = i(m) + i(n)$;
2. $i(mn) = \frac{m.n}{1} = \frac{m.n}{1.1} = \frac{m}{1} \cdot \frac{n}{1} = i(m).i(n)$;
3. $m \leq n \Rightarrow m.1 \leq n.1 \Rightarrow \frac{m}{1} \leq \frac{n}{1} \Rightarrow i(m) \leq i(n)$.

Faremos agora uma série de demonstrações para conseguirmos chegar ao teorema que garante que Q é enumerável. Antes de enunciar a próxima proposição, devemos lembrar que:

$$X \setminus (\cup_{n\in\mathbb{N}} A_n) = \cap_{n\in\mathbb{N}}(X \setminus A_n) \qquad (*)$$

e

$$X \setminus (\cap_{n\in\mathbb{N}} A_n) = \cup_{n\in\mathbb{N}}(X \setminus A_n). \qquad (**)$$

Lema 1 Todo subconjunto infinito de N é enumerável.

Demonstração. Seja X um subconjunto infinito de N. Pelo Princ pio da Boa Ordem, X possui menor elemento, chamando-o de x_0. Como X é infinito, o conjunto $Y_0 = X \setminus \{x_0\}$ é não vazio. Seja agora x_1 o menor elemento de Y_0. Obtidos $x_0, x_1, x_2, \ldots, x_n$ ($n \in \mathbb{N}$) dessa forma acima, obtemos x_{n+1} como sendo o menor elemento de $Y_n = X \setminus \{x_0, x_1, x_2, \ldots, x_n\}$, que existe, pois Y_n é não vazio, para todo n natural, caso contrário, X seria finito.

Temos que $X \setminus (\cup_{n\in\mathbb{N}} A_n) = \cap_{n\in\mathbb{N}}(X \setminus A_n) = \cap_{n\in\mathbb{N}} Y_n$, onde, neste caso, $A_n = \{x_0, x_1, x_2, \ldots, x_n\}$.

Se existisse $x \in X \setminus (\cup_{n\in\mathbb{N}} A_n)$, esse x também seria elemento de $\cap_{n\in\mathbb{N}} Y_n$ e, como tal, deveria ser maior do que x_0, por estar em Y_0, deveria ser maior do que x_1 por estar em Y_1 e, assim sucessivamente, x deveria ser maior do que x_n, para todo $n \in \mathbb{N}$. Dessa forma, o conjunto infinito $\cup_{n\in\mathbb{N}} A_n = \{x_0, x_1, x_2, \ldots, x_n, \ldots\}$ estaria contido no conjunto finito $\{1, 2, 3, \ldots, x\}$, o que é um absurdo. Portanto, não existe $x \in X \setminus (\cup_{n\in\mathbb{N}} A_n)$, isto é, $X \setminus (\cup_{n\in\mathbb{N}} A_n) = \emptyset$, ou ainda, $X = \cup_{n\in\mathbb{N}} A_n = \{x_0\} \cup \{x_0, x_1\} \cup \{x_0, x_1, x_2\} \cup \ldots = \{x_0, x_1, x_2, \ldots, x_n, \ldots\}$, o que significa que X é enumerável.

Lema 2 Todo número racional positivo $\frac{a}{b}$, (a, b > 0), pode ser escrito, de modo único, como uma fração irredutível, isto é, na forma $\frac{m}{n}$, onde m e n são primos entre si, ou seja, não possuem fatores primos em comum.

Demonstração. Pelo Teorema Fundamental da Aritmética, consideremos as decomposições em fatores primos de a e de b. Seja k o produto de todos os fatores primos comuns a a e a b, de modo que $\frac{a}{b} = \frac{ka'}{kb'}$. Obtemos $\frac{a}{b} = \frac{a'}{b'}$, onde a' e b' são relativamente primos. Existindo uma fração irredutível $\frac{c}{d}$ igual a $\frac{a'}{b'}$, a propriedade fundamental das frações nos daria $a'.d = b'.c$, o que, pela unicidade da decomposição em fatores primos, obrigaria d a conter os fatores primos de b' e vice-versa, o mesmo ocorrendo para a' e c, ou seja, $a' = c$ e $b' = d$.

Proposição 4 Q_+^* é enumerável.

Demonstração. Consideremos os números racionais escritos na forma irredutível, como no lema anterior. Seja f: $Q_+^* \to \mathbb{N}$ dada por $f(\frac{m}{n}) = 2^m.3^n$. Se $f(\frac{m}{n}) = f(\frac{m'}{n'})$, então, $2^m \cdot 3^n = 2^{m'}.3^{n'}$, vemos então que, pelo Teorema Fundamental da Aritmética e pela unicidade da representação de frações na forma irredutível, dada

pela proposição acima, $2^m = 2^{m'}$ e $3^n = 3^{n'}$, ou seja, $m = m'$ e $n = n'$, que nos garante que, $\frac{m}{n} = \frac{m'}{n'}$. Chegamos que, *f* é injetora e tem como imagem um subconjunto infinito de N, que é, pelo lema, enumerável.

Proposição 5 A união de dois conjuntos enumeráveis é enumerável. Além disso, a união de uma família finita de conjuntos enumeráveis é enumerável.

Demonstração. Sejam *A* e *B* dois conjuntos enumeráveis.Claramente, ou $A \cap B = \emptyset$ ou $A \cap B \neq \emptyset$.

Tentemos primeiro com $A \cap B = \emptyset$:

Como *A* é enumerável, existe $f_1 : A \rightarrow \mathbb{N}$ bijetora. Temos que existe também uma função $g_1 : \mathbb{N} \rightarrow \mathbb{N}p$ (onde N*p* representa os números naturais pares), dada por $g_1(n) = 2n$ para todo $n \in \mathbb{N}$. Como para todo $2n$ existe n, tal que $g(n) = 2n$ e $2n = 2m \Leftrightarrow n = m$, esta função é bijetora, desta forma, podemos ter $h_1 = g_1 \circ f_1 : A \rightarrow \mathbb{N}p$, dada por $h_1(x) = 2f(x)$, bijetora. Do mesmo modo, como *B* é enumerável, existe $f_2 : B \rightarrow \mathbb{N}$ bijetora e também $g_2 : \mathbb{N} \rightarrow \mathbb{N}_i$ (onde $\mathbb{N}_i$ são os números naturais ímpares), dada por $g_2(n) = 2n + 1$ para todo $n \in \mathbb{N}$, que Ø claramente bijetora. Desta forma, obtemos $h_2 = g_2 \circ f_2 : B \rightarrow \mathbb{N}_i$, dada por $h_2(x) = 2f_2(x) + 1$, bijetora. Sendo assim, $f : (A \cup B) \rightarrow (\mathbb{N}p \cup \mathbb{N}_i)$, dada por

$$f(x) = \begin{cases} h_1(x) se\ x\ \in A \\ h_2(x) se\ x\ \in B \end{cases}$$

é bijetora. Como $A \cap B = \emptyset$, *f* está bem definida e, como $\mathbb{N}p \cup \mathbb{N}_i = \mathbb{N}$, $A \cup B$ é enumerável.

Seja agora, $A \cap B \neq \emptyset$:

Seja $C = A \setminus B$, um conjunto tal que $A \cup B = C \cup B$. Temos $B \cap C = \emptyset$ por construção, portanto, pelo que já foi demonstrado acima, $C \cup B$ é enumerável, logo, $A \cup B$ também será.

Sejam agora $A_1, A_2, \ldots, A_n$ conjuntos enumeráveis. Precisamos provar que $\bigcup_{k \in \{1,2,\ldots,n\}} A_k$ é enumerável. Provemos por indução finita. Já sabemos que se $n = 2$ isto é verdade, então suponhamos que $\bigcup_{k \in \{1,2,\ldots,n-1\}} A_k$ é enumerável e provemos que $\bigcup_{k \in \{1,2,\ldots,n\}} Ak$ também será. De fato, como $\bigcup_{k \in \{1,2,\ldots,n-1\}} A_k$ é enumerável e A_n também, obviamente, $\bigcup_{k \in \{1,2,\ldots,n-1\}} A_k \cup A_n$ é enumerável.

Proposição 6 A união de um conjunto finito com um conjunto enumerável é enumerável.

Demonstração. Seja X um conjunto enumerável, isto é, existe $g : \mathbb{N} \to X$, bijetora. Seja também $Y = \{y_1, y_2, ..., y_n\}$ com $n \in \mathbb{N}$ um conjunto finito qualquer. Temos que, ou $X \cap Y = \emptyset$ ou $X \cap Y \neq \emptyset$.

Suponhamos primeiro que $X \cap Y = \emptyset$:

Assim, podemos ter $f : \mathbb{N} \to X \cup Y$ dada como segue:

$$f(x) = \begin{cases} y_k, \text{se} 1 \leq k \leq n, \\ f(k) = g(k - n), \text{se } (n + 1) \leq k \end{cases}$$

Esta função está bem definida, pois $X \cap Y = \emptyset$ e é bijetora, portanto, $X \cup Y$ é enumerável.

Seja agora, $X \cap Y \neq \emptyset$:

Seja $C = X \setminus Y$, um conjunto tal que $X \cup Y = C \cup Y$. Temos $Y \cap C = \emptyset$ por construção, portanto, chegamos agora que, $C \cup Y$ é enumerável, logo, $X \cup Y$ também será.

Teorema 8 Q é enumerável.

Demonstração. Se escrevermos Q como Q^*_- U {0} U Q^*_+ $\mathbb{Q}^*_- \cup \{0\} \cup \mathbb{Q}^*_+$, pelas proposições chegamos que Q é enumerável.

3.4 Q como corpo ordenado

O conjunto dos números racionais está representado pelas duas operações, adição e multiplicação, como também pelas subtração e divisão, que são definidas a partir das duas primeira e simbolizadas por (−) e (:), respectivamente. Sendo a subtração definida como: se $r, s \in \mathbb{Q}$, $r - s = r + (-s)$. Tem-se a divisão como sendo:

Definição 5 Sejam $r, s \in \mathbb{Q}$ com $s \neq 0$. Dizemos que r dividido por s é dado por $r : s = r \cdot s^{-1}$.

Observando a operação, podemos ver que, a divisão não se realiza em Q, dado que o seu domínio é $Q \times Q^*$e não Q × Q.

Proposição 7 Se $a, b \in \mathbb{Z}$, com $b \neq 0$, então $\frac{a}{1} : \frac{b}{1} = \frac{a}{b}$.

Demonstração. Pela Definição 2.3.12, $\frac{a}{1} : \frac{b}{1} = \frac{a}{1} . \frac{1}{b} = \frac{a.1}{1.b} = \frac{a}{b}$.

Identicando Z com sua cópia algébrica $i(\mathbb{Z})$ em Q, a igualdade da proposição é escrita a : b = $\frac{a}{b}$.

Proposição 8 Se $\frac{a}{b}, \frac{c}{d} \in Q$, com $\frac{c}{d} \neq \frac{0}{1}$, então $\frac{a}{b} : \frac{c}{d} = \frac{ad}{bc}$.

Demonstração. $\frac{a}{b} : \frac{c}{d} = \frac{a}{b} . \frac{d}{c} = \frac{ad}{bc}$.

Normalmente, nos textos elementares de matemática, apresenta-se a notação $\frac{\frac{a}{b}}{\frac{c}{d}}$ para $\frac{a}{b} : \frac{c}{d}$.

Proposição 9 Admitindo a identificação de Z com *i*(Z), para *r, s* racionais arbitrários, valem:

1. se $r.s = 0$, então $s = 0$ ou $r = 0$;
2. se $r > 0$ e $s > 0$, então $r.s > 0$;
3. se $r > 0$ e $s < 0$, então $r.s < 0$;
4. se $r < 0$ e $s < 0$, então $r.s > 0$;
5. se $r > 0$, então $r^{-1} > 0$;
6. se $r < s$, então $r < (r + s) \cdot 2^{-1} < s$;

Demonstração. Sejam r = $\frac{a}{b}$ e s = $\frac{c}{d}$.

1. Suponhamos $\frac{c}{d} \neq 0$, ou seja, $c \neq 0$:

$\frac{a}{b} . \frac{c}{d} = \frac{a.c}{b.d} = 0 \Rightarrow ac = 0 \Rightarrow a = 0$, portanto, $\frac{a}{b} = 0$. De forma análoga, supondo $\frac{a}{b} \neq 0$, percebemos que $\frac{c}{d} = 0$.

2. $\frac{a}{b} > 0 \Rightarrow a > 0$ *e* $\frac{c}{d} > 0 \Rightarrow c > 0$, desta forma, $ac > 0$, logo $\frac{ac}{bd} > 0$;
3. $\frac{a}{b} > 0 \Rightarrow a > 0$ *e* $\frac{c}{d} < 0 \Rightarrow c < 0$, desta forma, $ac < 0$, logo $\frac{ac}{bd} < 0$;
4. $\frac{a}{b} < 0 \Rightarrow a < 0$ *e* $\frac{c}{d} < 0 \Rightarrow c < 0$, desta forma, $ac > 0$, logo $\frac{ac}{bd} > 0$;
5. $\frac{a}{b} > 0 \Rightarrow a > 0$, desta forma, $b > 0$, logo $\frac{b}{a} > 0$, ou seja, $r^{-1} > 0$;
6. Se $r < s$, temos que, $2r < r + s$ e $r + s < 2s$, da , $2r < r + s < 2s$ e assim,

$2 . \frac{a}{b} < \frac{a}{b} + \frac{c}{d} < 2.\frac{c}{d} \Rightarrow \frac{a}{b} < 2^{-1}\left(\frac{a}{b} + \frac{c}{d}\right) < \frac{c}{d}$, ou seja, $r < 2^{-1}(r + s) < s$.

Teorema 9 Q não é bem ordenado.

Demonstração. Provemos que existem subconjuntos de Q não vazios, limitados inferiormente, mas que não possuem elemento mínimo. De fato, seja

$X = \left\{\frac{a}{b} \in Q \middle| 2^{-1} < \frac{a}{b}\right\}$. Temos que *X* é limitado inferiormente por 2^{-1} e $X \neq \emptyset$, dado que $1 \in X$. Suponhamos que *X* possua um elemento mínimo, digamos $\frac{c}{d}$. Sendo assim $\frac{c}{d} \leq \frac{a}{b}$ para todo $\frac{a}{b} \in X$. Como 2^{-1} é limitante inferior de X, $2^{-1} < \frac{c}{d}$, vemos então que:

$2^{-1} < \frac{c}{d} \Rightarrow 2^{-1} < \left(2^{-1} + \frac{c}{d}\right)2^{-1} < \frac{c}{d}$, assim,

$\left(2^{-1} + \frac{c}{d}\right)2^{-1} \in X$ e $\left(2^{-1} + \frac{c}{d}\right)2^{-1} < \frac{c}{d}$, o que é uma contradição com a minimalidade de $\frac{c}{d}$. Logo, X não possui elemento mínimo.

Acabamos de ver que Q não é um conjunto bem ordenado como Z, porém, ele possui, além de todas as propriedades aritméticas de Z, a propriedade de que todo elemento não nulo possui inverso.

Teorema 10 Sejam (*K, +, ·*) um conjunto munido de duas operações. Dizemos que *K* é um corpo, se:

1. + e · são associativas;
2. + e · possuem elementos neutros distintos;
3. + possui elemento simétrico e · elemento inverso, para todo elemento distinto do neutro da adição;
4. + e · são comutativas;
5. · é distributiva em relação a +.

E ainda, se este corpo estiver uma relação de ordem compatível com suas operações, ele é chamado de corpo ordenado.

Um exemplo de tal corpo ordenado é Q. Vejamos a seguir uma propriedade de corpos ordenados em geral.

Proposição 10 Seja *K* um corpo ordenado, cujo elemento neutro de + é representado por 0 e a relação de ordem é denotada por ≤. Então $0 \leq x^2$ para todo $x \in K$.

Demonstração. Se $x < 0$, temos que $x^2 > 0$, se $x = 0$, então $x^2 = 0$ e, se $x > 0$, temos que $x^2 > 0$, logo, para todo $x \in K$, $x^2 \geq 0$.

Teorema 11 Q não possui elemento máximo e nem mínimo.

Demonstração. Suponhamos que exista um elemento máximo em Q, digamos, $m_x = \frac{m}{n}$, isto é, $\frac{a}{b} \leq \frac{m}{n}$, para todo $\frac{a}{b} \in Q$. Claramente, $\frac{m}{n} + 1 = \frac{m+n}{n} \in Q$, além disso, $\frac{m}{n} < \frac{m+n}{n}$, o que contradiz a maximalidade de m_x, logo Q não possui um elemento máximo. De forma análoga, obtemos que Q não possui um elemento mínimo.

Vimos que um conjunto $X \subset$ Q diz-se limitado superiormente quando existe algum $b \in$ Q tal que $x \leq b$ para todo $x \in X$. Neste caso, diz-se que *b* é uma cota superior de *X*. Vejamos, partir disso o seguinte:

Definição 6 Seja $X \subset \mathbb{Q}$ limitado superiormente e não vazio. Um número $b \in \mathbb{Q}$, chama-se o supremo do conjunto X quando é a menor das cotas superiores de X, isto é, quando é a cota superior mínima de X. Em outras palavras, b é o supremo de X quando cumpre as seguintes condições:

1. Para todo $x \in X$, tem-se $x \leq b$;
2. Se $c \in \mathbb{Q}$ é tal que $x \leq c$ para todo $x \in X$ então $b \leq c$;

Escrevemos $b = \sup X$ para indicar que b é o supremo do conjunto X. O ínfimo de um conjunto é dado analogamente, sendo a maior das cotas inferiores (cota inferior máxima de X) e, escreve-se $a = \inf X$, quando a é o ínfimo do conjunto X.

Temos que, se existe o supremo b de X, então este supremo é único. De fato, suponhamos que existam dois supremos b_1 e b_2. Dessa forma, $x \leq b_1$ para todo $x \in X$ e, se $c \in \mathbb{Q}$ tal que $x \leq c$ para todo $x \in X$, então $b_1 \leq c$. Analogamente $x \leq b_2$ para todo $x \in X$ e, se $c \in \mathbb{Q}$ tal que $x \leq c$ para todo $x \in X$, então $b_2 \leq c$. Logo, como $b_1, b_2 \in \mathbb{Q}$, então $b_1 \leq b_2$ e $b_2 \leq b_1$, então $b_1 = b_2$.

Definição 7 Seja K um corpo ordenado. Dizemos que K é arquimediano se, dados $a, b \in K$, existe $n \in \mathbb{N}$ tal que $n \cdot a > b$;

Teorema 12 O conjunto $\mathbb{N} \subset \mathbb{Q}$ não é limitado superiormente;

1. O ínfimo do conjunto $\left\{\frac{1}{n} \middle| n \in N^*\right\}$, igual a 0;
2. Q é um corpo arquimediano.

Demonstração.

1. Suponhamos que exista $\frac{a}{b} \in Q$, tal que $\frac{a}{b} \geq n$, para todo $n \in \mathbb{N}$. Temos que a. b $\in Z_+^*$, isto é, $a, b \in N^*$. Dessa forma, $b \geq 1$ e, assim, $a \geq \frac{a}{b}$.

Se $a > \frac{a}{b}$, como $a \in N^*$, encontramos uma contradição com o fato de que $\frac{a}{b}$ é um limitante superior de N em Q.

Se $a = \frac{a}{b}$, então $a + 1 > a = \frac{a}{b}$, e, como $a \in N^* \Rightarrow a + 1 \in \mathbb{N}$, encontramos uma contradição com o fato de que $\frac{a}{b}$ é um limitante superior de N em Q. Logo, N não é limitado superiormente em Q;

2. Claramente, 0 é uma cota inferior de X. Basta então provar que nenhum $c > 0$ é cota inferior de X. Dado $c > 0$, existe, pelo item 1, um número natural $n > \frac{1}{c}$, da , $\frac{1}{n} < c$.

3. Dados *a, b* ∈ Q, usamos 1 para obter *n* ∈ N tal que $n > \frac{b}{a}$. Então, *n* · *a* > *b*.

As três propriedades acima são equivalentes.

Propriedades válidas desta mesma forma, não somente para Q, mas para todo corpo ordenado.

4 NÚMEROS REAIS

Temos nos conceitos de números reais um dos mais profundos da matemática, remonta aos gregos da escola pitagórica, com a descoberta da incomensurabilidade entre o lado e a diagonal de um quadrado. A construção desse conceito passou por Eudoxo, com sua teoria das proporções, registrada nos Elementos de Euclides, e só foi concretizada em XIX. Os matemáticos alemães, Cantor e Dedekind, construíram os números reais a partir dos racionais por métodos diferentes, respectivamente conhecidos por Classes de equivalência de sequências de Cauchy (Suponha que os números racionais e suas propriedades são conhecidos, neste método de Cantor, cada número real é definido como uma classe de equivalência de sequências de Cauchy de números racionais) e por Cortes de dedekind, onde ambos geram o mesmo ambiente, ou seja, dois corpos ordenados complexos são isomorfos. O último, que apresentaremos aqui, inspirou-se na Teoria das Proporções de Eudoxo.

No Ensino Fundamental, o que diz sobre os números reais é o seguinte: admite-se que a cada ponto de uma reta está associado um número real. Há pontos que não correspondem a números racionais. A esses pontos sem abscissa racional correspondem os números com nome irracionais. Outra forma de introduzi-los é a seguinte: admite-se ou, em alguns casos, demonstra-se que a representação decimal dos números racionais é periódica e, reciprocamente, toda representação decimal periódica corresponde à de um número racional. Conclui-se por definir número irracional como sendo aqueles que possuem representação decimal não periódica. Ao conjunto constituído pelos racionais e irracionais dá-se o nome de conjunto dos números reais.

Em linhas gerais, o que faremos é construir rigorosamente os números reais, tendo como ponto de partida o conjunto dos números racionais. Definiremos a noção de corte, devida a Dedekind. Consideraremos o conjunto constituído de todos os cortes e nele definiremos duas operações, adição e multiplicação, e uma relação de ordem.

A este conjunto de cortes chamaremos de conjunto dos números reais, que será denotado por R.

4.1 Cortes de Dedekind

Definição 1 Um conjunto α de números racionais diz-se um corte se satisfizer as seguintes condições:

1. $\alpha \neq \emptyset$ e $\alpha \neq \mathbb{Q}$;
2. Se $r \in \alpha$ e $s < r$ (s racional) então $s \in \alpha$;
3. Em α não existe elemento máximo.

Exemplo 1 O conjunto A = $\left\{x \in Q \middle| x < \frac{3}{5}\right\}$ é um corte:

1. $A \neq \emptyset$, pois $0 \in A$ e $A \neq \mathbb{Q}$, pois $1 \in \mathbb{Q}$ e $1 \notin A$;
2. Seja $r \in A$ e $s < r$, assim, $s < r < \frac{3}{5}$, logo $s < \frac{3}{5}$, isto é, $s \in A$;
3. Suponhamos que exista uma máximo em A, digamos m. Sendo assim, $r \leq m$ para todo $r \in A$. Sabemos que $m < \frac{3}{5}$, portanto, $m < \left(m + \frac{3}{5}\right)2^{-1} < \frac{3}{5}$, o que contradiz a maximalidade de m. Então, A não possui máximo.

Chegando a conclusão que A é um corte.

Exemplo 2 O conjunto B = $\left\{x \in Q \middle| x > \frac{3}{5}\right\}$ não é um corte:

1. $B \neq \emptyset$, pois $1 \in B$ e $B \neq \mathbb{Q}$, pois $0 \in \mathbb{Q}$ e $0 \notin B$;
2. Seja $r \in B$ e $s < r$. Tomemos $r = 1$ e $s = 0$, assim, $s < r$, entretanto, $s \notin B$.

Logo, B não é um corte.

Exemplo 3 O conjunto C = $\left\{x \in Q \middle| x \leq \frac{3}{5}\right\}$ não é um corte:

1. $C \neq \emptyset$, pois, $0 \in C$ e $C \neq \mathbb{Q}$ pois $1 \in \mathbb{Q}$ e $1 \notin C$;
2. Seja $r \in C$ e $s < r$, assim, $s < r \leq \frac{3}{5}$, logo $s < \frac{3}{5}$, isto é, $s \in C$;
3. Temos que $x \leq \frac{3}{5}$ para todo $x \in C$. Sendo assim, podemos ver que $m = \frac{3}{5}$, é o máximo deste conjunto, por definição de máximo.

Portanto, C não é um corte.

Exemplo 4 O conjunto C = $\left\{x \in Q \middle| -3 < x < \frac{8}{5}\right\}$ não é um corte:

1. $D \neq \emptyset$, pois, $0 \in D$ e $D \neq \mathbb{Q}$ pois $2 \in \mathbb{Q}$ e $2 \notin D$;
2. Seja $-3 < r < \frac{8}{5}$ *e* $s < r$. Tomemos $s = -4$ e $r = 0$. Assim, $s < r$, entretanto, $s \notin D$.

Logo, D não é um corte.

Exemplo 5 $E = \mathbb{Q} \setminus \{0\}$ não é um corte.

1. $E \neq \emptyset$, pois, $1 \in E$ e $E \neq \mathbb{Q}$ pois $0 \in \mathbb{Q}$ e $0 \notin E$;
2. Seja $r \in E$ e $s < r$. Tomemos $s = 0$ e $r = 1$. Assim, $s < r$, entretanto, $s \notin E$. Sendo assim, E não é um corte.

Exemplo 6 $F = \left\{1, 4, \frac{3}{5}\right\}$ não é corte.

1. $F \neq \emptyset$, pois, $1 \in F$ e $F \neq \mathbb{Q}$ pois $0 \in \mathbb{Q}$ e $0 \notin F$;
2. Seja $r \in F$ e $s < r$. Tomemos $s = 0$ e $r = 1$. Assim, $s < r$, entretanto, $s \notin F$. Portanto, F não é um corte.

Proposição 1 Sejam α um corte e $r \in \mathbb{Q}$. Então, r é cota superior de α se, e somente se, $r \in \mathbb{Q} \setminus \alpha$.

Demonstração. ($\Rightarrow$) Se r é uma cota superior de α, então $x \leq r$, para todo $x \in \alpha$, entretanto, pelo item 3 da definição de corte, α não possui elemento máximo, portanto r não pode pertencer a α, isto é, $r \in \mathbb{Q} \setminus \alpha$.

($\Leftarrow$) Seja $r \in \mathbb{Q} \setminus \alpha$ e $s \in \alpha$. Temos que, ou $r \geq s$, ou $r < s$. Se o segundo caso ocorre, pelo item 2 da definição de corte, $r \in \alpha$, o que é uma contradiz a hipótese, logo, $r \geq s$, isto é, r é uma cota superior de α.

Proposição 2 Se $r \in \mathbb{Q}$ e $\alpha = \{x \in \mathbb{Q} \mid x < r\}$ então α é um corte e r é a menor cota superior de α.

Demonstração.

1. $\alpha \neq \emptyset$, pois $x = r - 1 \in \alpha$ e $\alpha \neq \mathbb{Q}$ pois $r \in \mathbb{Q}$ e $r \notin \alpha$;
2. Sejam $s \in \alpha$ e $t < s$. Assim, $t < s < r$, logo $t < r$, ou seja, $t \in \alpha$;
3. Suponhamos que exista $s \in \alpha$ tal que $x \leq s$ para todo $x \in \alpha$. Como $s \in \alpha$, então $s < r$, daí, $s < (s + r)2^{-1} < r$. Como $(s + r)2^{-1} \in \mathbb{Q}$ e $(s + r)2^{-1} < r$, então $(s + r)2^{-1} \in \alpha$, o que contradiz a maximalidade de s, portanto, α não possui um elemento máximo.

Seja $s \in \mathbb{Q}$ uma cota superior de α. Suponhamos que $s < r$, o que implica que $s \in \alpha$, assim s é um elemento máximo de α, contradizendo o fato de α ser corte. Tendo então, $r \leq s$ para toda cota superior s de α, ou melhor dizendo, r é a menor cota superior de α.

Definição 2 Os cortes do tipo da proposição anterior são chamados cortes racionais e se representam por r^*

Proposição 3 Todo corte que possui cota superior mínima é racional.

Demonstração. Seja α um corte com cota superior mínima r, isto é, $x \leq r$ para todo $x \in \alpha$. Temos que $r \notin \alpha$ pois, caso contrário, r seria máximo de α, o que não pode acontecer, por definição de corte, sendo assim $x < r$ para todo $x \in \alpha$. Como r é a mínima das cotas superiores de α, temos que, qualquer $s \in Q$, tal que $s < r$, não é cota superior de α, isto é, pertence a α.

Logo, se $r \in Q$ é cota superior mínima de α, então $\alpha = \{x \in Q \mid x < r\}$, ou seja, α é racional.

Teorema 1 Seja $\alpha = Q_-^* \cup \{x \in Q_+ \mid x^2 < 2\}$. Então α é um corte que não é racional.

Demonstração.

1. $\alpha \neq \emptyset$ pois $0 \in \alpha$ e $\alpha \neq Q$ pois $2 \in Q$ e $2 \notin \alpha$.
2. Sejam $r \in \alpha$ e $s \in Q$, $s < r$.

- Se $s \leq 0$ então $s \in \alpha$;
- Se $s > 0$ e $s < r$, então $s^2 < r^2 < 2$, isto é, $s \in \alpha$;

3. Devemos provar que se $x \in \alpha$, *logo existe* $y \in \alpha$, *com* $y > x$. *Será óbvio se* $x \leq 0$. *Suponhamos que* $x > 0$ *com* $x^2 < 2$. Para encontrar y nas condições que são apresentadas, basta ter $h \in Q_+^*$ tal que $(x + h)^2 < 2$ e colocar $y = x + h$. Temos então que $x^2 + 2xh + h^2 < 2$. Resolvendo esta inequação em h seria conduzida a expressão de forma indesejável, então para não perder a generalidade, façamos com $h < 1$. Obteremos: $x^2 + 2xh + h^2 < x^2 + 2xh + h$, que fica menor que 2, se tomarmos $h < \frac{2-x^2}{2x+1}$ e como esta expressão é positiva, tomando $h < \min\{1, \frac{2-x^2}{2x+1}\}$, $h \in Q_+$ e $y = x + h$, chegamos que $y^2 = (x + h)^2 < 2$, isto é, $y \in \alpha$ e $y > x$. Existindo h pelo fato de Q ser arquimediano.

Disto temos que α é um corte.

Verifiquemos agora que α não possui cota superior mínima. Os racionais que não pertencem a α são os positivos que têm quadrado maior ou igual a 2, e sabemos que não existe racional cujo quadrado é igual a 2. Sendo assim, q é uma cota superior de α se $q > 0$ e $q \in Q$ tal que $q^2 > 2$. Mostraremos que, para cada cota superior p, encontraremos outra cota superior q tal que $q < p$. De fato, seja p uma cota superior, isto é, $p \in Q$ e $p^2 > 2$.

Seja q = p - $\frac{p^2-2}{2p}$. Dessa forma, 0 < q < p e $q^2 = p^2 - 2p(\frac{p^2-2}{2p}) + (\frac{p^2-2}{2p})^2 = 2 + (\frac{p^2-2}{2p})^2 > 2$. Portanto, $q < p$ e $q^2 > 2$.

4.2 Relação de ordem em C

Denotaremos em C o conjunto de todos os cortes.

Definição 3 Sejam $\alpha, \beta \in C$. Dizemos que $\alpha < \beta$ quando $\beta \setminus \alpha \neq \emptyset$. Em outras palavras, $\alpha < \beta$ se existe um racional p tal que $p \in \beta$ e $p \notin \alpha$.

Exemplo 7

1. $5^* > \frac{4^*}{5}$, pois $1 \in 4^* \setminus \frac{4^*}{5}$;
2. $1^* > 0^*$ pois $\frac{1}{2} \in 1^* \setminus 0^*$;
3. $(-3)^* < 0^*$, pois -1 $\in 0^* \setminus (-3)^*$; ;
4. Se $\propto = \{x \in Q_+ \mid x^2 < 2\} \cup Q_-^*$, então $\alpha < 2^*$, pois $\frac{18}{10} \in 2^* \setminus \propto$.

Definição 4 Se $\alpha \in C$ e $\alpha > 0^*$, α chama-se corte positivo. Se $\alpha < 0^*$, é chamado de corte negativo. Se $\alpha \geq 0^*$, α é corte não negativo e se $\alpha \leq 0^*$, ele chama-se corte não positivo.

Proposição 4 Para $\alpha, \beta \in C$, valem as equivalências:

1. $\alpha < \beta \Leftrightarrow \alpha \subset \beta$ e $\alpha \neq \beta$;
2. $\alpha \leq \beta \Leftrightarrow \alpha \subset \beta$.

Demonstração.

1. ($\Rightarrow$) $\alpha < \beta \Rightarrow$ existe $p \in \beta$ tal que $p \notin \alpha$. Claramente $\alpha \neq \beta$. Suponhamos que $\alpha * \beta$, isto é, existe $p \in \alpha$ tal que $p \notin \beta$, o que é uma contradição, pois por definição, se isto ocorre, então $\beta < \alpha$. Logo $\alpha \subset \beta$.

($\Leftarrow$) Se $\alpha \subset \beta$ e $\alpha \neq \beta$, então existe p em β tal que p não está em α, ou seja, $\alpha < \beta$;

2. ($\Rightarrow$) $\alpha \leq \beta \Rightarrow \alpha < \beta$ ou $\alpha = \beta$. Se $\alpha < \beta$, pelo item anterior $\alpha \subset \beta$. Se $\alpha = \beta$, obviamente $\alpha \subset \beta$.

($\Leftarrow$) $\alpha \subset \beta$ implica, pelo item anterior, que $\alpha < \beta$, ou seja, $\alpha \leq \beta$.

Teorema 2 (Tricotomia). Sejam $\alpha, \beta \in C$, temos então uma e somente uma das possibilidades a seguir ocorre:

$$\alpha = \beta \quad \text{ou} \quad \alpha < \beta \quad \text{ou} \quad \beta < \alpha.$$

Demonstração. Pela definição da igualdade de conjuntos, se α = β, exclui as outras duas possibilidades. Também, α < β ou β < α, excluem α = β, Supomos que *α < β e β < α ocorrem simultaneamente, então existe* $r \in \beta \setminus \propto$ e $s \in \alpha \setminus \beta$. De r ∈ β e s ∉ *β resulta r < s e de* $s \in \alpha$ *e* r ∉ ∝ resulta s < r, o que contradiz a tricotomia em Q. Logo, não acontecem ao mesmo tempo. E para mostrar que uma delas deve ocorrer, temos que α = β ou α ≠ β. Se α = β, não há nada a provar. Sendo α ≠ β, então $\alpha \setminus \beta \neq \emptyset$ ou $\beta \setminus \propto \neq \emptyset$, vendo então que no caso primeiro β < α e no segundo α < β.

Teorema 3 A relação ≤ é uma relação de ordem em *C*.

Demonstração.

1. Reflexiva: Seja *α* ∈ *C*. Obviamente *α* = *α*, portanto, *α* ≤ *α*;

2. Antissimétrica: Sejam *α, β* ∈ *C*, *α* ≤ *β* e *β* ≤ *α*. Pela tricotomia, *α* = *β*;

3. Transitiva: Sejam *α, β,* γ ∈ *C*, *α* ≤ *β* e *β* ≤ γ. Onde *α* ≤ *β* ⇒ *α* ⊂ *β e β* ≤ γ ⇒ *β* ⊂ γ.

Temos que a inclusão de conjuntos é transitiva, portanto, *α* ⊂ *β* e *β* ⊂ γ implicam que *α* ⊂ γ, da *α* ≤ γ.

4.3 Operações com cortes

Teorema 4 Sejam *α, β* ∈ *C*. Se γ = {*r* + *s* | *r* ∈ *α* e *s* ∈ *β*}, então γ ∈ *C*.

Demonstração. Devemos mostrar que γ ∈ *C*, isto é, provar que satisfaz as três condições para ser um corte:

1. Como *α* ≠ ∅ e *β* ≠ ∅, claramente γ ≠ ∅. Sejam *t* ∈ Q \ *α* e *u* ∈ Q \ *β*. Sendo assim, *t* > *r* para todo *r* ∈ *α* e *u* > *s* para todo *s* ∈ *β*, logo, *t* + *u* > *r* + *s*, para todo *r* ∈ *α* e para todo *s* ∈ *β*. Sendo assim, *t* + *u* ∉ γ, logo γ ≠ Q.

2. Sejam *r* ∈ *γ* e *s* ∈ Q com *s* < *r*. Como *r* ∈ γ, temos que *r* = *p* + *q* com *p* ∈ *α* e *q* ∈ *β*, da , *s* < *p* + *q*. Sendo assim, podemos tomar $q' < q$, tal que *s* = $p + q'$, portanto, *s* ∈ γ.

3. Devemos mostrar que γ não possui elemento máximo, isto é, para todo *r* ∈ γ, existe *s* ∈ γ tal que *r* < *s*. De fato, temos que *r* = *p* + *q* com *p* ∈ *α* e *q* ∈ *β*. Como existe p' ∈ *α* tal que *p* < p', o racional *s* = $p' + q \in \gamma$ e é maior do que *r*.

Definição 5 Definimos por *α* + *β* como sendo o corte γ do teorema anterior, isto é,

$$\alpha + \beta = \{r + s \mid r \in \alpha \text{ e } s \in \beta\}.$$

Teorema 5 A adição em *C* é comutativa, associativa e tem 0^* como elemento neutro.

Demonstração.

1. Comutativa: Sejam $\alpha, \beta \in C$. Devemos mostrar que $\alpha + \beta = \beta + \alpha$. De fato, tomemos $r + s \in \alpha + \beta$ tal que $r \in \alpha$ e $s \in \beta$. Vimos que a comutativa é válida em Q, portanto, $r + s = s + r$. Sabemos que $s + r \in \beta + \alpha$ com $s \in \beta$ e $r \in \alpha$, sendo assim, $r + s \in \beta + \alpha$. Logo, $\alpha + \beta \subset \beta + \alpha$. Da mesma forma podemos concluir que $\beta + \alpha \subset \alpha + \beta$, logo, $\alpha + \beta = \beta + \alpha$.

2. Associativa: sejam $\alpha, \beta, \gamma \in C$. Devemos mostrar que $\alpha + (\beta + \gamma) = (\alpha + \beta) + \gamma$. De fato, tomemos $r + (s + t) \in \alpha + (\beta + \gamma)$ tal que $r \in \alpha, s \in \beta$ e $t \in \gamma$. Vimos que a associativa é válida em Q, portanto, $r + (s + t) = (r + s) + t$. Sabemos que $(r + s) + t \in (\alpha + \beta) + \gamma$ com $r \in \alpha, s \in \beta$ e $t \in \gamma$, sendo assim, $r + (s + t) \in (\alpha + \beta) + \gamma$. Logo, $\alpha + (\beta + \gamma) \subset (\alpha + \beta) + \gamma$. Da mesma forma, podemos concluir que, $(\alpha + \beta) + \gamma \subset \alpha + (\beta + \gamma)$, então, $\alpha + (\beta + \gamma) = (\alpha + \beta) + \gamma$.

3. Elemento Neutro da Adição: devemos mostrar que $\alpha + 0^* = \alpha$. Seja $r = p + q \in \alpha + 0^*$ com $p \in \alpha$ e $q \in 0^*$, isto é, $q < 0$. Assim, $r < p$, portanto, $r \in \alpha$. Logo, $\alpha + 0^* \subset \alpha$. Tomemos agora $r \in \alpha$ e $s \in \alpha$, tal que $r < s$. Podemos apresentar r como $r = s + (r - s)$, onde $r - s < 0$ e, portanto, $(r - s) \in 0^*$. Logo, $r \in \alpha + 0^*$ e assim, $\alpha \subset \alpha + 0^*$, de onde segue que, $\alpha = \alpha + 0^*$.

Lema 1 Sejam $\propto \in C \; e \; r \in Q_+^*$. Então existem números racionais *p* e *q* tais que $p \in \alpha$, $q \notin \alpha$, *q* não é cota superior mínima de α e $q - p = r$.

Demonstração. Tomemos *s* arbitrário em α e consideremos a sequência $s_n = s + nr$ para $n = 0,1,2,\ldots$. Seja $A = \{n \in \mathrm{N} \mid s_n \in \alpha\}$. Temos que:

- $A \subset \mathrm{N}$, por definição de *A*;
- $A \neq \emptyset$, pois $0 \in A$;
- *A* é finito, por consequência das condições 2 e 3 para α ser corte.

Portanto podemos afirmar que o conjunto *A* assume um máximo *m*. Isto acarreta que $s_m \in \alpha$ e $s_{m+1} \notin \alpha$.

Se $s + (m + 1)r$ não for cota superior mínima de α, devemos tomar $p = s + mr$ e $q = s + (m + 1)r$, logo , $q - p = r$. Se $s + (m + 1)r$ for cota superior mínima de α, devemos tomar: $p = s + mr + \frac{r}{2}$ e $q = s + (m + 1)r + \frac{r}{2}$, vemos então que q – p = r.

Teorema 6 Seja $\alpha \in \mathbb{C}$, existe um único corte β tal que $\alpha + \beta = 0^*$. Como nos casos dos inteiros e racionais, tal β denota-se por $-\alpha$ e se chama simétrico (ou oposto) de α.

Demonstração. Provemos inicialmente a unicidade. Suponhamos que $\alpha + \beta = \alpha + \beta' = 0^*$:

$\beta' = \beta' + 0^* = \beta' + (\alpha + \beta) = (\beta' + \alpha) + \beta = 0^* + \beta = \beta$.

Provemos agora a existência e um corte β que satisfaça $\alpha + \beta = 0^*$. Iniciemos tomando um β e mostrar que é corte. Seja $\beta = \{p \in Q \mid -p \notin \alpha$ e $-p$ não é cota superior mínima de $\alpha\}$.

1. (a) Para mostrar que $\beta \neq \emptyset$, consideremos dois casos:

- α não possui cota superior mínima:

Como α é um corte, então $\alpha \neq Q$ e portanto, existe $q \in Q$ tal que $q \neq \alpha$. Assim, basta tomar $p = -q \in Q$ e $-p = q \neq \alpha$. Logo $p \in \beta$ e portanto $\beta \neq \emptyset$.

- α possui cota superior mínima m:

Como m é cota superior mínima de α, $m \notin \alpha$ (se $m \in \alpha$, m seria máximo de α, o que contradiz a definição de corte) e com isso, $m + 1 \notin \alpha$. Seja $p = -m - 1 \in Q$ e $-p = m + 1 \notin \alpha$ e, além disso, $-p = m + 1$ 6= m. Portanto $p \in \beta$ e $\beta \neq \emptyset$.

(b) Para mostrar que $\beta \neq Q$, consideremos novamente dois casos:

- α não possui cota superior mínima:

Como α é corte, então $\alpha \neq \emptyset$ e portanto existe $r \in \alpha$ (da $r \in Q$). Tomemos $p = -r \in Q$ e, portanto, $-p = r \in \alpha$. Logo $p \notin \beta$ e $p \in Q$, isto é, $\beta \neq Q$.

- α possui cota superior mínima m:

Como m é cota superior mínima de α, então $m - 1 \in \alpha$. Seja $p = -m + 1 \in Q$ e $-p = m - 1 \in \alpha$. Portanto, $p \notin \beta$ e $p \in Q$, isto é, $\beta \neq Q$.

2. Seja $p \in \beta$ e $q \in Q$ tal que $q < p$. Queremos mostrar que $q \in \beta$. Como $p \in \beta$, temos que $-p \notin \alpha$ e $-p$ não é cota superior mínima de α. Como $q < p$, então $-p < -q$ (*) da , $-q \notin \alpha$ (visto que $-p \notin \alpha$). Temos também que $-q$ não é cota superior mínima de α. Como $q \in Q$, $-q \notin \alpha$ e $-q$ não é cota superior mínima de α, chegamos a conclusão que $q \in \beta$.

3. Seja $p \in \beta$, queremos mostrar que existe $q \in \beta$ tal que $p < q$. Dividiremos em dois casos.

- α não possui cota superior mínima:

Como $-p \notin \alpha$ e α não possui cota superior mínima, então existe uma cota superior q de α (isto é, $q \notin \alpha$), tal que $q < -p$. Assim, $-q \in \beta$ e $p < -q$, logo β não possui máximo.

- α possui cota superior mínima m:

Seja $r = \frac{-m+p}{2} \in$ Q. Como $p \in \beta$, temos que $-p \notin \alpha$, ou seja, é uma cota superior de α, mas não é cota superior mínima de α, portanto, $m < -p$, vemos que, $p < -m$. Sendo assim, $r = \frac{-m+p}{2} = \frac{-m}{2} + \frac{p}{2} > \frac{p}{2} + \frac{p}{2} = p$.

Por outro lado,

$-r = \frac{m-p}{2} = \frac{m}{2} - \frac{p}{2} > \frac{m}{2} + \frac{m}{2} = m$, portanto, $-r \neq m$. Como $-r > m$, então $-r \notin \alpha$. Finalmente, como $r \in$ Q, $-r \notin \alpha$ e $-r$ não é cota superior mínima de α, temos que $r \in \beta$ e $p < r$, logo, β não possui máximo.

Finalizando, basta mostra que $\alpha + \beta = 0^*$. Para isso, mostremos que $\alpha + \beta \subset 0^*$ e $0^* \subset \alpha + \beta$.

- Seja $q + r \in \alpha + \beta$ com $q \in \alpha$ e $r \in \beta$ ($r \in$ Q, $-r \notin \alpha$ e $-r$ não é cota superior mínima de α). Como $q \in \alpha$ e $-r \notin \alpha$, então, $q < -r$, da , $q + r < 0$, isto é, $q + r \in 0^*$.
- $p \in 0^* \Rightarrow p \in$ Q e $p < 0$ ($-p > 0$). Sejam $r \in \alpha$ e $r' \notin \alpha$ tais que $r' - r = -p$. Segue que $p = r + (-r')$, com $r \in \alpha$ e $-r' \in \beta$, ou seja, $p \in \alpha + \beta$.

Logo, $\alpha + \beta = 0^*$.

Definição 6 Definimos a subtração em C por $\alpha - \beta = \alpha + (-\beta)$, para todo $\alpha, \beta \in C$.

Proposição 5 Se $\alpha \in C$, então $\alpha = -(-\alpha)$.

Demonstração. Sabemos que oposto de α é $-\alpha$, portanto, $\alpha + (-\alpha) = \alpha - \alpha = -\alpha + \alpha = 0^*$.

Também vemos que, sabemos que o oposto de $(-\alpha)$ é $-(-\alpha)$, então $(-\alpha) + (-(-\alpha)) = -\alpha + (-(-\alpha)) = 0^*$.

Temos conhecimento que o oposto de um corte é único, sendo assim, $\alpha = -(-\alpha)$.

Teorema 7 (Compatibilidade da relação de ordem com a adição). Sejam $\alpha, \beta, \gamma \in C$ tais que $\alpha \leq \beta$. Então $\alpha + \gamma \leq \beta + \gamma$.

Demonstração. $\alpha \leq \beta \Leftrightarrow \alpha \subset \beta$. Seja $t \in \alpha + \gamma$, ou seja, $t = r + s$ com $r \in \alpha$ e $s \in \gamma$. Como $\alpha \subset \beta$, então $r \in \beta$, e $t = r + s \in \beta + \gamma$, ou seja, $\alpha + \gamma \subset \beta + \gamma$. Portanto, $\alpha + \gamma \leq \beta + \gamma$.

Teorema 8 Sejam α e β cortes tais que $\alpha \geq 0^*$, $\beta \geq 0^*$. Seja $\gamma = \{p \in Q \mid p < 0\} \cup \{q \in Q \mid q = r.s,$ onde $r \in \alpha, s \in \beta, r \geq 0, s \geq 0\}$. Então γ é um corte.

Demonstração.

1. $p = -1 \in \gamma$, portanto $\gamma \neq \emptyset$. Temos ainda que, $\alpha \neq Q \Rightarrow \exists p_0 \in Q$ tal que $p_0 \notin \alpha$, $\beta \neq Q \Rightarrow \exists q_0 \in Q$ tal que $q_0 \notin \beta$.

Chegamos que $p_0 q_0 \in Q$. Mostremos que $p_0 q_0 \notin \gamma$. Suponhamos que $p_0 q_0 \in \gamma$, isto é, existem $p \in \alpha$, $q \in \beta$, $p \geq 0$ e $q \geq 0$ tal que $p_0 q_0 = pq$. Não podemos ter $p_0 \leq p$, porque teríamos $p_0 \in \alpha$, nem $q_0 \leq q$, pois teríamos $q_0 \in \beta$. Assim, $p < p_0$ e $q < q_0$, logo, $pq < p_0 q_0$, o que é uma impossível com $p_0 q_0 = pq$. Portanto, $p_0 q_0 \notin \gamma$ e, assim, $\gamma \neq Q$.

2. Sejam $r \in \gamma$ e $s < r$. Devemos mostrar que $s \in \gamma$. De fato, se $s < 0$, $s \in \gamma$. Suponhamos $s \geq 0$ e, portanto $r > 0$. Como $r \in \gamma$, existem $p \in \alpha$ e $q \in \beta$, tais que $r = pq$, com $p \geq 0$ e $q \geq 0$.

Como $r > 0$, segue que $p > 0$ e $q > 0$. Seja $t = \frac{s}{p}$ ($s \geq 0$, $p > 0 \Rightarrow t \geq 0$). Se $q \leq t$, teríamos $pq \leq pt$, ou seja, $r \leq s$, o que é um absurdo, pois, $s < r$. Logo, devemos ter $t < q$ e, como $q \in \beta$, então $t \in \beta$. Assim, como $s = p.t$, $p \in \alpha$, $t \in \beta$, $p > 0$ e $t \geq 0$, então $s \in \gamma$.

3. Seja $r \in \gamma$ e mostremos que existe $s \in \gamma$ tal que $r < s$. De fato, se $r < 0$, basta tomar $s = \frac{r}{2} < 0$, da $s > r$. Suponhamos $r \geq 0$. Neste caso, $r \in \gamma$ significa que $r = p.q$, com $p \in \alpha$, $q \in \beta$, $p \geq 0$ e $q \geq 0$. Existem $t \in \alpha$ e $u \in \beta$ tais que $p < t$ e $q < u$ (pois α e β não possuem máximo). Logo, $r = p.q < t.u$. Tomando $s = t.u$, temos $s \in \gamma$ (pois $s = tu$ com $t \in \alpha$, $u \in \beta$, $t > 0$ e $u > 0$) e $s > r$. Portanto, γ não tem máximo.

Definição 7 Denotamos por $\alpha.\beta$ e chamamos produto de α e β o corte γ do teorema anterior, isto é, $\alpha.\beta = \{p \in Q \mid p < 0\} \cup \{q \in Q \mid q = r.s,$ onde $r \in \alpha, s \in \beta, r \geq 0, s \geq 0\}$.

Começamos com noção de valor absoluto de um corte para definir produto de cortes que contém fatores negativos.

Definição 8 A cada corte α associamos um corte $|\alpha|$ que chamamos valor absoluto de α, definido por

$$|\alpha| = \begin{cases} \alpha \ se \ \alpha \geq 0^* \\ -\alpha \ se \ \alpha < 0^* \end{cases}$$

Proposição 6 Se $\alpha < 0^*$, então $-\alpha > 0^*$.

Demonstração. Sabemos que $\alpha < 0^*$ se, e somente se, existe $q \in 0^*$ tal que $q \not\in \alpha$, e podemos admitir, sem perda de generalidade que q não é cota superior mínima de α. Como $q \in 0^*$, então $q < 0$. Tomemos $r = -q$, que nos fornece $r > 0$. Nestas condições, vemos que $r \in -\alpha$ (por definição de corte oposto, pois $-r = q$, $q \notin \alpha$ e q não é cota superior mínima de α) e $r > 0$, ou seja, $r \notin 0^*$, o que nos garante que $-\alpha > 0^*$.

Proposição 7 Para qualquer $\alpha \in C$, tem-se:

1. $|\alpha| \geq 0^*$;
2. $|\alpha| = 0^* \Leftrightarrow \alpha = 0^*$.

Demonstração.

1. Se $\alpha \geq 0^*$, então $|\alpha| = \alpha \geq 0^*$, da , $|\alpha| \geq 0^*$. Se $\alpha < 0^*$, então $|\alpha| = -\alpha$ e ainda, $-\alpha > 0^*$, assim, $|\alpha| > 0^*$.

2. ($\Rightarrow$) Seja $|\alpha| = 0^*$. Se $\alpha > 0^*$ então $|\alpha| = \alpha > 0^*$, que é absurdo, pois, por hipótese, $|\alpha| = 0^*$.

Se $\alpha < 0^*$, $-\alpha > 0^*$ e, por definição, $|\alpha| = -\alpha > 0^*$, absurdo também.

Logo, pela tricotomia, $\alpha = 0^*$.

($\Leftarrow$) Seja $\alpha = 0^*$. $\alpha = 0^* \Rightarrow |\alpha| = \alpha = 0^*$.

Definição 9 Sejam $\alpha, \beta \in C$, definimos:

$$\alpha.\beta = \begin{cases} -(|\alpha||\beta|), \text{se } \alpha \leq 0^*, \beta \geq 0^*; \\ -(|\alpha||\beta|), \text{se } \alpha \geq 0^*, \beta \leq 0^*; \\ |\alpha||\beta|, \text{se } \alpha < 0^*, \beta < 0^*; \end{cases}$$

Teorema 9 Para $\alpha, \beta \in C$, temos $(-\alpha)\beta = \alpha(-\beta) = -(\alpha\beta)$ e $(-\alpha)(-\beta) = \alpha\beta$.

Demonstração. De fato, temos,

$$(-\alpha).\beta + \alpha.\beta = (-\alpha + \alpha).\beta = 0^* \cdot \beta = 0^*. \qquad (*)$$

Significa que $(-\alpha).\beta = -(\alpha.\beta)$, pois o oposto de um corte é único.

Temos,

$$a.(-\beta) + \alpha.\beta = \alpha.(-\beta + \beta) = \alpha \cdot 0^* = 0^*. \qquad (**)$$

Do mesmo modo $\alpha(-\beta) = -(\alpha\beta)$

Temos,

$(-\alpha)(-\beta) = -(\alpha(-\beta))$ por (*)

$= -(-(\alpha\beta))$ por (**)

$= \alpha\beta$

Teorema 10 (Distributividade). Se $\alpha, \beta, \gamma \in C$, então $\alpha(\beta + \gamma) = \alpha\beta + \alpha\gamma$.

Demonstração. Demonstraremos apenas o caso em que $\alpha > 0^*$, $\beta > 0^*$ e $\gamma > 0^*$. Mostremos inicialmente que $\alpha(\beta + \gamma) \subset \alpha\beta + \alpha\gamma$. De fato, $\alpha(\beta + \gamma) = \{q \in Q \mid q < 0\} \cup \{p \in Q \mid p = r.s$ onde $r \in \alpha, s \in (\beta + \gamma), r \geq 0, s \geq 0\}$. Dessa forma, se $x \in \alpha.(\beta + \gamma)$, então, ou $x \in 0^*$ ou $x = r.s$ com $r \in \alpha, s \in (\beta + \gamma), r \geq 0$ e $s \geq 0$.

Sendo $x \in 0^*$, então $\frac{x}{2} \in 0^*$ *e* $\frac{x}{2} + \frac{x}{2} = x$, que significa que $x \in \alpha\beta + \alpha\gamma$.

Sendo $x = r.s$ com $r \in \alpha, s \in (\beta + \gamma), r \geq 0$ e $s \geq 0$, então $s = q + p$ onde $q \in \beta$, $p \in \gamma$, $q \geq 0$ e $p \geq 0$. Portanto, $x = r.s = r(q + p) = r.q + r.p$, logo $x \in \alpha\beta + \alpha\gamma$. Concluímos que $\alpha(\beta + \gamma) \subset \alpha\beta + \alpha\gamma$.

Provemos agora que $\alpha\beta + \alpha\gamma \subset \alpha(\beta + \gamma)$. Com efeito, $\alpha\beta + \alpha\gamma = \{t \in Q \mid t = ps + pq$ onde $ps \in \alpha\beta, pq \in \alpha\gamma\}$.

Seja $u \in \alpha\beta + \alpha\gamma$, ou seja, $u = ps + pq$, com $ps \in \alpha\beta, pq \in \alpha\gamma$.

- $ps \in \alpha\beta \Rightarrow ps < 0$ ou $p \in \alpha$ e $s \in \beta$ com $p \geq 0$ e $s \geq 0$;
- $pq \in \alpha\gamma \Rightarrow pq < 0$ ou $p \in \alpha$ e $q \in \gamma$ com $p \geq 0$ e $q \geq 0$.

Dessa maneira, temos quatro casos:

1. Fazendo $ps < 0$ e $pq < 0$. Claramente, $u \in \alpha(\beta + \gamma)$ pois $u = ps + pq < 0$;
2. Suponhamos $ps < 0$ e $p \in \alpha$ e $q \in \gamma$ com $p \geq 0$ e $q \geq 0$. Como $ps < 0$ e $p \geq 0$, então $s < 0$, logo , se $-s > q$, então $s + q < 0$ e, portanto, $u = ps + pq = p(s + q) < 0$. Se $-s \leq q$, então $s + q \geq 0$ e, como $p \geq 0$, temos $u = p(s + q) \in \alpha(\beta + \gamma)$, pois $p \in \alpha$ e $s + q \in \beta + \gamma$ com $p \geq 0$ e $s + q \geq 0$;
3. Supondo $p \in \alpha$ e $s \in \beta$ com $p \geq 0$ e $s \geq 0$ e $pq < 0$, podemos obter, analogamente ao caso anterior que $u = ps + pq \in \alpha(\beta + \gamma)$;
4. Vendo que $p \in \alpha$, $s \in \beta$ e $q \in \gamma$, com $p \geq 0$, $s \geq 0$ e $q \geq 0$. Dessa forma, $u = ps + pq = p(s + q)$, onde $p \in \alpha$ e $s + q \in \beta + \gamma$, com $p \geq 0$ e $s + q \geq 0$, logo $u \in \alpha(\beta + \gamma)$.

Acabamos de provar que existe a dupla inclusão entre $\alpha\beta + \alpha\gamma$ e $\alpha(\beta + \gamma)$, ou seja, $\alpha\beta + \alpha\gamma = \alpha(\beta + \gamma)$.

Definição 10 Seja α um corte tal que $\alpha \neq 0^*$. Se $\alpha > 0^*$, então o corte β denotado por α^{-1} é chamado de inverso de α. Se $\alpha < 0^*$, então definimos o inverso de α como $\alpha^{-1} = -|\alpha|^{-1}$.

Teorema 11 Seja α um corte tal que $\alpha \neq 0^*$. Então $\alpha\alpha^{-1} = 1^*$. Além disso, o inverso de α é único.

Demonstração. Consideremos dois casos, $\alpha > 0^*$ e $\alpha < 0^*$.

• $\alpha > 0^*$:

Vemos que $r \in \alpha\alpha^{-1}$. Se $r \leq 0$, então $r \in 1^*$. Suponhamos $r > 0$. Como $r \in \alpha\alpha^{-1}$ existem $s \in \alpha$, $p \in \alpha^{-1}$ tal que $r = sp$, $s \geq 0$, $p \geq 0$. Como $r > 0$, devemos ter $s > 0$ e $p > 0$. Como $p \in \alpha^{-1}$ e $p > 0$, existe $q \not\in \alpha$ tal que $q < p^{-1}$. Como $s \in \alpha$ e $q \notin \alpha$, então $s < q$. De $q < p^{-1}$, temos $p < q^{-1}$, logo $s.p < sq^{-1}$. Portanto, como $s < q$, temos que $sq^{-1} < 1$, e assim, $r = s.p < sq^{-1} < 1$, da $r \in 1^*$.

Reciprocamente, seja $r \in 1^*$, isto Ø, $r < 1$. Se $r < 0$, então $r \in \alpha\alpha^{-1}$. Se $r = 0$, temos $r = p \cdot 0$, ponde $p \in \alpha$, $0 \in \alpha^{-1}$ e $p > 0$, logo $r \in \alpha\alpha^{-1}$. Suponhamos agora, $0 < r < 1$. Seja $s \in \alpha$ com $s > 0$. Seja n o maior natural que satisfaz $s(r^{-1})^n \notin \alpha$ Tomemos $p_1 = s(r^{-1})^{n-1} \in \alpha$ e $t = s(r^{-1})^n \notin \alpha$. Seja $p \in \alpha$ tal que $p_1 < p$ (α não possui máximo). Tomemos $q = t^{-1}p^{-1}p_1$, ou seja, $q^{-1} = t.p.p_1^{-1}$. Assim, podemos ter

$$p_1 < p \Rightarrow p_1.p_1^{-1} < p.p_1^{-1} \Rightarrow 1 < p.p_1^{-1} \Rightarrow t < p.p_1^{-1} \Rightarrow t < q^{-1}..$$

Assim, como $t \notin \alpha$, $q^{-1} \notin \alpha$ e q^{-1} não é a menor cota superior de α. Temos ainda,

$$q = t^{-1}.p^{-1}.p_1 \Rightarrow pq = p.t^{-1}.p^{-1}.p_1 \Rightarrow pq = t^{-1}.p_1$$

$$\Rightarrow pq = (s(r^{-1})^n)^{-1}.s.(r^{-1})^{n-1}$$

$$\Rightarrow pq = s^{-1}.r^n.s.r^{-n+1} \Rightarrow pq = r.$$

Desta forma, $p \in \alpha$ e, como $q^{-1} \notin \alpha$ e existe $t \notin \alpha$ tal que $t < q^{-1}$, logo, $q \in \alpha^{-1}$.

Portanto $r \in \alpha\alpha^{-1}$.

Então, concluímos que, se $\alpha > 0^*$, chegando que $\alpha\alpha^{-1} = 1^*$.

• $\alpha < 0^*$:

Se $\alpha < 0^*$, por definição, $\alpha^{-1} = -|\alpha|^{-1}$. Sabemos que $|\alpha|^{-1} > 0^*$ e que $-|\alpha|^{-1} < 0^*$ isto é, $\alpha^{-1} < 0^*$. Então, por definição de produto, $\alpha\alpha^{-1} = |\alpha||\alpha^{-1}| = ||\alpha| - |\alpha|^{-1}| = |\alpha||\alpha|^{-1} = 1^*$.

Provemos agora a unicidade de α^{-1}. Suponhamos que existam α_1^{-1} *e* α_2^{-1}, tais que $\alpha.\alpha_1^{-1} = 1^*$ e $\alpha.\alpha_2^{-1} = 1^*$. Assim, $\alpha_1^{-1} = \alpha_1^{-1}.1^* = \alpha_1^{-1}.(\alpha.\alpha_2^{-1}) = (\alpha.\alpha_1^{-1})\,\alpha_2^{-1} = 1^*.\alpha_2^{-1} = \alpha_2^{-1}$.

<u>Proposição 8</u> Seja α um corte qualquer, então $\alpha \cdot 0^* = 0^*$.

Demonstração. Temos, $\alpha\cdot 0^* = \alpha(0^*+0^*) = \alpha\cdot 0^*+\alpha\cdot 0^*$, da , $\alpha\cdot 0^*-\alpha\cdot 0^* = \alpha\cdot 0^*+\alpha\cdot 0^*-\alpha\cdot 0^*$, portanto, $0^* = \alpha \cdot 0^*$.

<u>Proposição 9</u> Sejam α e β cortes. Nesta condição, $\alpha\beta = 0^*$ se e somente se $\alpha = 0^*$ ou $\beta = 0^*$.

Demonstração. Se $\alpha = 0^*$ ou $\beta = 0^*$, temos que $\alpha\beta = 0^*$. Seja, agora, $\alpha\beta = 0^*$. Suponhamos $\alpha \neq 0^*$, isto é, existe $\gamma \in C$, tal que $\alpha\gamma = 1^*$. Dessa forma, $\beta = \beta \cdot 1^* = \beta(\alpha\gamma) = (\alpha\beta)\gamma = 0^*\gamma = 0^*$. Reciprocamente, se supormos que $\beta \neq 0^*$, concluiremos que $\alpha = 0^*$.

Temos, C munido de duas operações e uma relação de ordem, de forma que C é um corpo ordenado. Em particular, define-se também a divisão em C e adota-se a notação de fração $\frac{\alpha}{\beta}$, como nos racionais.

Teorema 12 Se $\alpha \leq \beta$ e $\gamma \geq 0^*$, então, $\alpha\gamma \leq \beta\gamma$.

Demonstração. Vendo que $0^* = \alpha + (-\alpha) \leq \beta + (-\alpha)$, portanto, $\beta + (-\alpha) \geq 0^*$. Além disso, como $\gamma \geq 0^*$, temos $(\beta + (-\alpha))\gamma \geq 0^*$, por definição de produto de cortes. Logo, $\beta\gamma + (-\alpha)\gamma \geq 0^*$, $\beta\gamma \geq \alpha\gamma$, isto é, $\alpha\gamma \leq \beta\gamma$.

Teorema 13 A aplicação $j : Q \to C$, dada por $j(r) = r^*$ é injetora e preserva adição, multiplicação e ordem, isto é, os seguintes itens são válidos:

1. $j(p) + j(q) = j(p + q)$, ou seja, $p^* + q^* = (p + q)^*$;
2. $j(p)j(q) = j(pq)$, isto é, $p^*q^* = (pq)^*$;
3. $j(p) < j(q)$ se e somente se $p < q$, ou ainda, $p^* < q^*$ se, e somente se $p<q$;
4. $j(p) = j(q)$ se e somente se $p = q$, ou seja, $p^* = q^*$ se, e somente se, $p = q$.

Demonstração.

1. Seja $t \in p^* + q^*$, isto é, $t = r + s$ com $r \in p^*$ e $s \in q^*$, ou ainda, $r < p$ e $s < q$. Dessa forma, $t = r + s < p + q$, ou seja, $t = r + s \in (p + q)^*$. Seja, agora, $u \in (p + q)^*$, isto é, $u < p + q$. Sejam $h = p + q - u$, $s = p - \frac{h}{2}$ e $t = q - \frac{h}{2}$. Dessa forma, $s < p$ e $t < q$, ou seja, $s \in p^*$ e $t \in q^*$. Logo, $u = s + t \in p^* + q^*$

2. Provaremos apenas para o caso $p > 0$ e $q > 0$, os outros casos podem ser provados de forma análoga.

Se $r \in p^*q^*$, então, ou $r < 0$ ou $r = st$, com $p > s \geq 0$ e $q > t \geq 0$, de modo que, ou $r < 0$ ou $r = st < pq$ e assim, $r \in (pq)^*$.

Seja $r \in (pq)^*$, então podemos afirmar que ou $r < 0$ ou $0 \leq r < pq$. Se $r < 0$, claramente $r \in p^*q^*$, pela definição de corte positivos. Se $0 \leq r < pq$ então existem $p_1 \in Q$ e $q_1 \in Q$ tais que $0 < p_1 < p$, $0 < q_1 < q$ e, ainda, $r < p_1q_1 < pq$. Fica claro que $p_1 \in p^*$, $q_1 \in q^*$, $p_1q_1 \in p^*q^*$ e assim, $r \in p^*q^*$.

3. Se $p < q$, então $p \in q^*$. Como $p \notin p^*$, concluímos que $p^* < q^*$.

De forma análoga, se $p^* < q^*$, existe um racional r tal que $r \in q^*$ e $r \notin p^*$, ou seja, $r < q$ e $r \geq p$. Logo $p \leq r < q$, ou seja, $p < q$.

4. Se $p = q$, obviamente $p^* = q^*$.

Suponhamos $p^* = q^*$. Como $p \notin p^*$, segue que $p \notin q^*$, logo $p \geq q$. Por outro lado, como $q \notin q^*$, segue que $q \notin p^*$, então $p \leq q$. Com isso, pela tricotomia, $p = q$.

Uma cópia algébrica de um conjunto em outro, ou seja, um homomorfismo injetor. Desta vez, $j(\mathbb{Q})$ é uma cópia de Q em C, sendo $j(\mathbb{Q})$ precisamente o conjunto dos cortes racionais. Sabemos que existem cortes não racionais em C. Assim, $C \setminus j(\mathbb{Q}) \neq \emptyset$.

Vemos ainda que o corpo ordenado dos números racionais é isomorfo ao corpo ordenado de todos os cortes racionais (C^*) o que nos permite identificar o corte racional r^* como o número racional r. Naturalmente r^* não é, de modo algum, o mesmo número racional, mas as propriedades que interessam são as mesmas nos dois corpos ordenados.

Proposição 10 Se $\alpha \in C$, temos que $r \in \alpha$ se, e somente se, $r^* < \alpha$.

Demonstração. Se $r \in \alpha$, como $r \notin r^*$, então $r^* < \alpha$. Reciprocamente, se $r^* < \alpha$, existe $s \in \alpha$, tal que $s \notin r^*$. Temos então, $s \geq r$ e $s \in \alpha$, logo, $r \in \alpha$.

Teorema 14 Se $\alpha, \beta \in C$ e $\alpha < \beta$, então existe um corte racional r^* tal que $\alpha < r^* < \beta$.

Demonstração. Do fato que $\alpha < \beta$, podemos afirmar que existe um número racional $s \in \beta$, tal que $s \not\in \alpha$. Uma vez que $s \in \beta$, segue da definição de corte que existe um racional r tal que $s < r$ e ainda $r \in \beta$, o que implica $r^* < \beta$, pelo resultado anterior. Sabemos que, $s^* < r^*$, portanto, $\alpha \leq s^* < r^*$ (como $s \notin \alpha$) e assim, chegamos que, $\alpha < r^* < \beta$.

Definição 11 O conjunto C dos cortes será, a partir de agora, denominado de conjunto dos números reais e denotado por R. Os cortes racionais serão identificados, via injeção j, com os números racionais. Todo corte que não for racional será denominado número irracional. A identificação de $j(\mathbb{Q})$ com Q nos permite escrever $\mathbb{Q} \subset \mathbb{R}$. O conjunto $\mathbb{R} \setminus \mathbb{Q}$ representa o conjunto dos números irracionais.

Teorema de Dedekind é a principal propriedade que difere o conjunto dos números racionais do conjunto dos números reais, será vista a seguir.

Teorema 15 (Dedekind). Sejam A e B subconjuntos de R tais que:

1. $\mathbb{R} = A \cup B$;

2. $A \cap B = \emptyset$;

3. $A \neq \emptyset$ e $B \neq \emptyset$;

4. se $\alpha \in A$ e $\beta \in B$, então $\alpha < \beta$.

Nestas condições, existe um, e apenas um, número real γ tal que $\alpha \leq \gamma \leq \beta$, para todo $\alpha \in A$ e para todo $\beta \in B$.

Demonstração. Provemos inicialmente a unicidade:

Suponhamos que existam dois números distintos γ_1 e γ_2, com $\gamma_1 < \gamma_2$ (ou $\gamma_2 < \gamma_1$, sem perda de generalidade) nas condições do enunciado. Consideremos γ_3 tal que $\gamma_1 < \gamma_3 < \gamma_2$, que existe. Temos que $\gamma_2 \leq \beta$, para todo $\beta \in B$, dessa forma, se $\gamma_3 \in B$, teríamos $\gamma_2 \leq \gamma_3$, o que não pode acontecer, pois $\gamma_1 < \gamma_3 < \gamma_2$, portanto, como R = $A \cup B$, temos que $\gamma_3 \in A$. Da mesma forma, de $\gamma_1 < \gamma_3$, obtemos $\gamma_3 \in B$. Resulta então $\gamma_3 \in A \cap B$, uma contradição. Portanto não podemos ter γ_1 e γ_2 distintos nas condições do enunciado.

Provemos agora a existência: Seja $\gamma = \{r \in \mathrm{Q} \mid r \in \alpha,$ para algum $\alpha \in A\}$. Devemos mostrar que γ é um corte.

1. Como $A \neq \emptyset$, obviamente $\gamma \neq \emptyset$. Para mostra que $\gamma \neq$ Q, tomemos $\beta \in B$. Seja $s \in \beta$ um racional. Como $\alpha \subset \beta$, para todo $\alpha \in A$, então, $s \notin \alpha$, para todo $\alpha \in A$, de onde resulta $s \notin \gamma$;

2. Seja $r \in \gamma$ e $s < r$. Temos que $r \in \alpha$ para algum $\alpha \in A$ e, como $s < r$, então $s \in \alpha$, de onde segue que $s \in \gamma$;

3. Temos que $r \in \alpha$ para algum $\alpha \in A$ e, como $\alpha \emptyset$ um corte, existe $s > r$ em α, logo $s \in \gamma$;

Tendo então que γ é um número real e temos que $\alpha \leq \gamma$ para todo $\alpha \in A$, pois sabemos que $\alpha \subset \gamma$, para todo $\alpha \in A$.

Mostremos agora apenas que $\gamma \leq \beta$ para todo $\beta \in B$. Suponhamos que exista $\beta \in B$ com $\beta < \gamma$. Com isso, existe um racional $r \in \gamma$, tal que $r \notin \beta$. Como $r \in \gamma$, então r pertence a algum $\alpha \in A$ e, não sendo elemento de β, obtemos $\beta < \alpha$, contradizendo a última hipótese do teorema. Logo, $\gamma \leq \beta$ para todo $\beta \in B$.

Exemplo 8 Consideremos os seguintes subconjuntos de Q:

$A = \{x \in Q_+ \mid x^2 < 2\} \cup Q_-^*$ e $A = \{x \in Q_+ \mid x^2 > 2\}$.

Podemos ver que A e B satisfazem as hipóteses do teorema anterior, com Q em lugar de R, mas que não existe $r \in$ Q satisfazendo $s \leq r$ para todo $s \in A$ e $r \leq t$ para

todo $t \in B$. Notemos que, este exemplo nos diz, informalmente, que em R não há lacunas, mas em Q, há. Desta forma, dizemos que R possui a propriedade da completude ou que R é completo.

Corolário 1 Nas condições do teorema anterior, ou existe em A um número máximo, ou, em B, um número mínimo.

Demonstração. Seja γ como no teorema anterior. Então γ está em A ou γ está em B e, em apenas um desses conjuntos, pela segunda hipótese. Se $\gamma \in A$, então ele é elemento máximo de A. Se $\gamma \in B$, então, ele é elemento mínimo de B.

Observemos que, se o conjunto A do Teorema 3.3.28 não contiver γ, então ele é um corte em R, no sentido da definição de corte em Q apresentada. A diferença entre ambas a situações é que em Q não se tem necessariamente, como no Teorema 3.3.28 para os números reais, um elemento como γ. Essas lacunas é que geram os cortes irracionais. Como tais lacunas não ocorrem em R, então cortes em R não geram elementos novos.

Devemos aqui retomar o conceito de supremo. As definições de supremo e ínfimo, dadas para o conjunto dos racionais, são equivalentes no conjunto dos reais. Por exemplo, se A é um subconjunto de R, limitado superiormente, e existe uma cota superior de A, digamos s, que seja mínima, então, s diz-se supremo de A. O ínfimo é dado analogamente.

Teorema 16 Se $X \subset$ R Ø um conjunto não vazio e limitado superiormente, então existe sup$X$.

Demonstração. Sendo $A = \{\alpha \in \mathrm{R} \mid \alpha < x,$ para algum $x \in X\}$ e $B = \mathrm{R} \setminus A$, isto é, A é o conjunto constituído precisamente pelos números reais que não são cotas superiores de X e B é o conjunto constituído pelas cotas superiores de X.

Verificar que A e B satisfazem as condições do Teorema de Dedekind.

As duas primeiras condições são claramente válidas. Observemos a terceira. Temos que, sendo $X \neq \emptyset$, existe $x \in X$, e assim, qualquer $\alpha < x$ é elemento de A, logo $A \neq \emptyset$. Como X é limitado superiormente, $B \neq \emptyset$. Para verificar a última condição do teorema, sejam, $\alpha \in A$ e $\beta \in B$. Assim, existe $x \in X$ tal que $\alpha < x$. Como $x \leq \beta$, obtemos $\alpha < \beta$.

Verificamos que A e B satisfazem as condições do Teorema de Dedekind, logo, pelo Corolário 4.3.30, ou A possui máximo, ou B possui mínimo. Mostremos que A não possui máximo. De fato, tomemos α arbitrário em A. Existe $x \in X$ tal que $\alpha < x$.

Consideremos α' tal que $\alpha < \alpha' < x$. Como $\alpha' < x$, então $\alpha' \in A$ e é maior do que α, ou seja, nenhum elemento de *A* é maior do que os demais, ou seja, *A* não possui máximo. Sendo assim, obrigatoriamente *B* possui mínimo, ou seja, *X* possui supremo. Essa propriedade válida para R não se verifica em Q, isto é, não é verdade que todo subconjunto de números racionais não vazio e limitado superiormente em Q sempre admita supremo em Q. Por exemplo, o conjunto $A = \{x \in Q_+ \mid x^2 < 2\}$ não possui supremo racional, mas tem supremo, se considerado como subconjunto de R.

O resultado seguinte mostra que R, assim como Q, é um corpo arquimediano.

Teorema 17 O conjunto N dos naturais é ilimitado em R.

Demonstração. Por suposição, temo N limitado superiormente em R e seja $\alpha = supN$. Assim, $\alpha \geq n$, para todo $n \in N$. Como n + 1 ∈ N, para todo $n \in N$, então $n + 1 \leq \alpha$, para todo $n \in N$, de onde obtemos $\alpha - 1 \geq n$, para todo $n \in N$, ou seja, $\alpha - 1$ é cota superior de N menor do que o sup N, uma contradição.

Definição 12 Seja a ∈ R e n ∈ N. Definimos a potência na recursivamente como sendo 1, se n = 0 e, para n > 1, como sendo $a.a^{n-1}$. Finalmente, se a ≠ 0, definimos a^{-n} como sendo $(a^{-1})^n$.

Teorema 18 Seja *a* um real positivo e *n* > 0 natural. Existe um único número real positivo que é solução da equação $x^n = a$.

Demonstração. A prova deste teorema depende fundamentalmente da completude de R.

Definição 13 Dado um número real positivo *a*, o único número real positivo que é solução da equação $x^n = a$, estabelecido pelo teorema anterior, chama-se raiz n-ésima de *a* e é denotado por $\sqrt[n]{a}$ ou por $a^{\frac{1}{n}}$. A raiz n-ésima de *a* permite que se defina expoente racional do seguinte modo: se *m* e *n* são inteiros positivos, $a^{\frac{m}{n}} = \left(a^{\frac{1}{n}}\right)^m$ e, como para expoentes inteiros, $a^{-\frac{m}{n}} = (a^{-1})^{\frac{m}{n}}$.

5 ESPAÇO VETORIAL QUOCIENTE

Definição 1 Sabendo que Y é subespaço de X. Se x_1 e $x_2 \in$ X, teremos que x_1 é congruente a x_2 módulo Y, representado por $x_1 \equiv x_2 \, mod \, Y$, x_1 - $x_2 \in$ Y.

Dividamos o espaço X em diferentes classes de equivalência módulo Y e denotaremos a classe contendo x por $[x]$.

Definição 2 Sendo $[x]$ e $[z]$ classes de equivalência módulo Y e $\lambda \in$ K, definimos

$[x] + [z] = [x + z]$, $\lambda[x] = \lambda[\lambda x]$.

Com estas operações, o conjunto de todas as classes de equivalência módulo Y torna-se um espaço vetorial, chamado

$$\frac{X}{Y} \; ou \; {}^{X}/_{Y}$$

e denominado de espaço quociente de X por Y.

A classe de equivalência $[x]$ muitas vezes é representada por x + Y. Precisamos mostrar que as operações em ${}^{X}/_{Y}$ estão bem definidas, isto é, não dependem dos representantes de cada classe de equivalência. Logo, suponhamos que $x_1 \in [x]$ e $z_1 \in [z]$. Então $x_1 = x + y_1$ e $z_1 = z + y_2$, com $y_1, y_2 \in Y$. Mas então $x_1 + z_1 = x + y_1 + z + y_2 = x + z + (y_1 + y_2)$ e assim, $x_1 + z_1 \equiv x + z \, mod \, Y$. Do mesmo modo, $\lambda \, . \, x_1 = \lambda \, . \, x + (\lambda \, . \, y_1)$ e $\lambda \, . \, x_1 \equiv \lambda \, . \, x \bmod Y$.

Exemplo 1 Seja x $\in K^n$ e considere Y o subespaço de todos os vetores cujas duas primeiras coordenadas são iguais. Isto é,

$$(x_1, x_2, \dots, x_n) \equiv (y_1, y_2, \dots, y_n) \, mod \, Y \Leftrightarrow x_1 = y_1 \; e \; x_2 = y_2.$$

Cada classe de equivalência pode ser vista como um vetor com duas componentes, quais sejam, as duas coordenadas que eles possuem em comum.

Teorema 1 Seja Y um subespaço do espaço vetorial de dimensão finita X. Então dim X = dim Y + dim $\frac{X}{Y}$.

Demonstração. Sendo $\{y_1, y_2, \dots, y_j\}$ uma base de Y. Podemos completa-la de forma que $\{y_1, y_2, \dots, y_j, \; x_{j+1}, \dots, x_n\}$ seja uma base de X. sabemos então que $\{x_{j+1}, \dots, x_n\}$ é uma base de ${}^{X}/_{Y}$. De fato, se v $\in {}^{X}/_{Y}$, então v = $\lambda_1 \, . \, y_1$+ ...+ $\lambda_j \, . \, y_j$ + $\lambda_{j+1} \, . \, x_{j+1}$ + ...+ $\lambda_n \, . \, x_n$. Mas então v = $\lambda_{j+1} \, . \, x_{j+1}$ + ...+ $\lambda_n \, . \, x_n + y$, em que y = $\lambda_1 \, . \, y_1$+ ...+ $\lambda_j \, . \, y_j \in Y$.

Chegamos ao seguinte:

Corolário 1 Se Y é um subespaço de X e dim Y = dim X, então Y = X.

5.1 Teorema do núcleo e da imagem

Definição 3 Sendo T : X → Y uma aplicação linear. Chamamos de imagem de T, denotada por ImT, por

$$\mathcal{I}m\ T := \{y \in Y;\ y = Tx\}$$

Chamamos de núcleo de T, denotado por KerT, por:

$$KerT := \{x \in YX;\ Tx = 0\}.$$

Sabendo que o núcleo e a imagem de T são subespaços vetoriais de X e Y, respectivamente. De fato, se x_1, x_2 ∈ KertT e λ ∈ K, então $T(x_1 + \lambda . x_2) = T(x_1) + \lambda . T(x_2)$ = 0 + λ . 0 = 0, provando que $x_1 + \lambda . x_2$ ∈ KertT. Se y_1, y ∈ ImT, então existem x_1, x_2 ∈ X, tais que $y_1 = T(x_1)$ e $y_2 = T(x_2)$. Logo, se λ ∈ K, $y_1 + \lambda . y_2 = T(x_1) + \lambda . T(x_2) = T(x_1 + \lambda . x_2)$, o que mostra que $y_1 + \lambda . y_2$ ∈ ImT.

Exemplo 2 Considere $\mathbb{C}^2$ e $\mathbb{R}^3$ como espaços vetoriais sobre $\mathbb{R}$ e seja T : $\mathbb{C}^2 \rightarrow \mathbb{R}^3$ a transformação linear dada por T(a + bi, c + di) = (a – c, b + 2d, a + b – c + 2d) onde a, b, c, d ∈ $\mathbb{R}$. Se considerarmos a base {(1, 0), (i, 0), (0, 1), (0, i)} de $\mathbb{C}^2$ (sobre $\mathbb{R}$), teremos, que os vetores T(1, 0) = (1, 0, 1), T(0, 1) = (-1, 0, -1) e T(0, i) = (0, 2, 2) geram $\mathcal{I}m\ T$. Como T(1, 0) = -T(0, 1) = (1, 0, 1), T(i, 0) = 2T(0, i) e T(1, 0) não é múltiplo de T(i, 0), segue que {T(1, 0), T(i, 0)} é uma base de $\mathcal{I}m\ T$. Observe também que $NucT = [(1, 1), (-2i, i)]$.

Teorema 2 Sejam X e Y espaços vetoriais de dimensão finita e T ∈ $\mathcal{L}$(X, Y). Então

$$\dim X = \dim \text{Ker } T + \dim \text{Im } T.$$

Serão apresentadas duas demonstrações diferentes deste teorema, sendo a primeira utilizando espaço quociente que é bastante sintética e a segunda muito construtiva.

Motivando a primeira demonstração, apresentamos:

Exemplo 3 Seja A uma matriz m x n e considere o sistema linear não homogêneo Ax = b. Suponhamos que x_p seja uma solução desse sistema. Vemos claramente que $x_p + z$ também é solução desse sistema para qualquer z ∈ Kert A.

Mas essas são as únicas soluções. De fato, se x é outra solução, temos que A$(x - x_p) = 0$, de modo que $x - x_p = z \in$ Kert A.

A igualdade $x = x - x_p$, com $z \in$ Kert A, significa que $x \equiv x_p \, mod \ker A$. Portanto, no espaço quociente R^n/ker A a equação Ax = b terá solução única $[x_p]$!

1ª demonstração: Essa prova pode ser sintetizada pelo diagrama a seguir:

$$\begin{array}{ccc} & & T \\ X & \longrightarrow & \mathcal{I}mT \subset Y \\ \downarrow & \nearrow & \\ \dfrac{X}{\ker T} & & T_q \end{array}$$

Definamos o isomorfismo $T_q : \frac{X}{\ker T} \to ImT$. Como espaços isomorfos de dimensão finita têm a mesma dimensão, deduzimos que

$$\dim\left(\frac{X}{\ker T}\right) = \dim ImT.$$

Mas, dim X/ker T = dim X – dim ker T, de onde segue o teorema.

Definimos, para $[x] \in$ X/ker T, $T_q([x]) = Tx$. Temos:

a) T está bem definida: $x \equiv y \bmod \ker T$ significa que T(x – y) = 0, ou seja, T(x)= T (y).

b) T_q é linear: $T_q([x] + \lambda.[y]) = T_q([x + \lambda.y]) = T_q(x + \lambda.y) = Tx + \lambda Ty = T_q[x]) + \lambda.T_q([y])$.

c) T_q é injetiva: se $T_q([x]) = \lambda.T_q([y])$, então Tx = Ty e T(x - y) = 0, onde x$\equiv y \, mod \ker T$

d) T_q é sobrejetiva por definição.

Chegamos que T_q é um isomorfo e seu resultado está provado.

A demonstração acima é a própria essência da utilidade do espaço quociente. Mesmo que T não tenha inversa, podemos construir, de forma natural, um isomorfo à partir de T, no caso, a aplicação de T_q.

2ª demonstração: Como Im ⊂ Y é um espaço vetorial de dimensão finita, existe uma base $\{y_1, y_2, \dots, y_j\}$ para Im T. Pata cada elemento y_i existe $x_i \in X$ tal que T$x_i = y_i$, com $1 \leq i \leq j$. Sendo assim, o conjunto $\{x_1, x_2, \dots, x_j\}$ obtido é linearmente independente. De foto, suponhamos que $\lambda_1 x_1 + \cdots + \lambda_j x_j = 0$. Então:

$$0 = T\left(\lambda_1 x_1 + \cdots + \lambda_j x_j\right) = \lambda_1 T(x_1) + \cdots + \lambda_j T\left(x_j\right) = \lambda_1 y_1 + \cdots + \lambda_j y_j.$$

Como $y_1, y_2, \dots, y_j$ são linearmente independentes, λ_i = 0 para $1 \leq i \leq j$.

Consideremos agora $\{w_1, w_2, \dots, w_k\}$ do núcleo de T. Afirmamos que

$$\{x_1, x_2, \dots, x_j, w_1, w_2, \dots, w_k\} \text{ é uma sabe de X.}$$

Dado x ∈ X, como Tx ∈ Im T, Tx = $\lambda_1 x_1 + \cdots + \lambda_j x_j$, ou seja, Tx = T($\lambda_1 x_1 + \cdots + \lambda_j x_j$) e portanto T($x - \lambda_1 x_1 - \cdots - \lambda_j x_j$) = 0. Assim, $x - \lambda_1 x_1 - \cdots - \lambda_j x_j \in \ker T$, onde

$$x - \lambda_1 x_1 - \cdots - \lambda_j x_j = \alpha_1 w_1 + \cdots + \alpha_k w_k$$

Isso mostra que x = $\lambda_1 x_1 + \cdots + \lambda_j x_j + \alpha_1 w_1 + \cdots + \alpha_k w_k$, e que $\{x_1, x_2, \dots, x_j, w_1, w_2, \dots, w_k\}$ gerando X.

Suponhamos agora que $\lambda_1 x_1 + \cdots + \lambda_j x_j + \alpha_1 w_1 + \cdots + \alpha_k w_k = 0$. Aplicando T nessa igualdade temos $\lambda_1 y_1 + \cdots + \lambda_j y_j = 0$, o que nos permite concluir que $\lambda_i = 0$ para $i = 1, \dots, k$, o que nos mostra que todos os escalares são nulos e completa a demonstração.

Comparando as demonstrações, perceberemos que a essência da segunda é o procedimento aplicado na primeira: mostrou-se que existe um isomorfismo entre ImT, espaço cuja base $\{y_1, \dots, y_j\} = \{Tx_1, \dots, Tx_j\}$, e o espaço gerado por $\{x_1, \dots, x_j\}$. Esse último espaço é justamente X/ ker T!

Apresentemos agora algumas consequências do Teorema do Núcleo e da Imagem. As demonstrações seguem imediatamente da fórmula

$$\dim X = \dim \mathcal{I}m\ T + \dim \ker T$$

Corolário 2 Suponhamos que dim Y < dim X. Então existe $x \neq 0$, tal que Tx = 0.

Demonstração. Temos que, em particular, dim $\mathcal{I}m$ T < dim X

Corolário 3 Seja T : $R^n \to R^m$ linear, com m < n. Então o sistema linear homogêneo Tx = 0 (onde T é a matriz que a representa) possui solução não trivial, isto é, existe $x \neq 0$, tal que Tx = 0.

Corolário 4 Se dim X = dim Y, então T é injetiva se, e somente se, T é sobrejetiva.

Demonstração. Se T é injetiva, T(x) = 0, implica x = 0. Logo, dim ker T = 0. Dessa forma, dim $\mathcal{I}m$ T = dim X = dim Y e, portanto, $\mathcal{I}m$ T = Y. De forma recíproca, se T é sobrejetiva, $\mathcal{I}m$ T = Y e portanto, dim ker T = 0.

Particularmente, este corolário garante que, quando dim X = dim Y, T é injetiva se, e somente se, ker T = {0}. Sendo válido, na verdade, para quaisquer espações vetoriais X e Y. Se T é injetiva, obviamente ker T= {0}; se existisse $x_1 \neq x_2$ tal que T(x_1) = T(x_2), logo T($x_1 - x_2$) = 0, com $x_1 - x_2 \neq 0$.

Corolário 5 Seja T : $R^n \to R^m$ linear. Então o sistema não homogêneo Tx = y tem solução única para todo y ∈ Y se, e somente e, o sistema homogêneo Tx = 0 = 0 tem solução única.

Proposição 1 Sendo y ∈ R^m um elemento da imagem de T : $R^n \to R^m$. Logo, existe um único elemento $x_p \in R^n$, tal que toda a solução de Tx = y é congruente a x_p mod ker T, ou seja, se Tx = y, então x = x_p + z, para algum z ∈ ker T.

5.2 A forma canônica de Jordan

Sabendo que V é um espaço vetorial de dimensão finita. Mostraremos como encontrar uma base de V na qual um operador linear T : V → V assume uma matriz especialmente simples.

Definição 4 Uma matriz complexa J, n x n, está na forma canônica de Jordan se

$$J = \begin{pmatrix} J_1 & 0 & \cdots & 0 \\ 0 & J_2 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & J_k \end{pmatrix}, \quad em\ que\ \ J_i = \begin{pmatrix} \lambda & 1 & 0 & \cdots & 0 \\ 0 & \lambda & 1 & \cdots & 0 \\ \vdots & \vdots & \ddots & \ddots & \vdots \\ 0 & 0 & \cdots & \lambda & 1 \\ 0 & 0 & \cdots & 0 & \lambda \end{pmatrix},$$

onde λ é um dos autovalores distintos λ_1, ..., λ_i da matriz J.

Mostraremos a seguir que toda matriz complexa é semelhante a uma matriz na forma canônica de Jordan. No caso de matrizes reais, sempre podemos vê-la como uma matriz complexa, sabendo que, neste sentido, o resultado abaixo é geral. Também vemos que a necessidade de considerarmos o corpo complexo é para garantir que os autovalores estão todos presentes no corpo.

Teorema 3 Sejam A, B ∈ M_{nxn}(C) duas matrizes semelhantes, isto é,

$$A = P^{-1}BP.$$

Logo,

I. A e B possuem os mesmos autovalores λ_i;

II. Os espaços $N_j(\lambda_i) = \ker(A - \lambda_i I)^j$ e $M_j(\lambda_i) = \ker(B - \lambda_i I)^j$ possuem a mesma dimensão para todo j ∈ N e todo autovalor λ_i.

De forma recíproca, caso aconteçam estas duas condições, então A e B são semelhantes.

Demonstração. Inicialmente percebemos que os núcleos de duas matrizes semelhantes têm dimensão igual. Certamente, se C = Q^{-1}DQ e $\{x_1,..., x_k\}$ é uma base do núcleo de C, então $\{Qx_1,..., Qx_k\}$ é uma base do núcleo de D.

Vemos também que se A e B são semelhantes, então também são as matrizes $A - aI$ e $B - aI$, bem como qualquer potência delas:

$$(A - aI)^m = P^{-1}(B - aI)^m P$$

Temos na segunda relação citada anteriormente que os núcleos dessas matrizes têm a mesma dimensão. Particularmente, como um elemento $v \in ker(A - \lambda_i I)^{d_i} \setminus ker(A - \lambda_i I)^{d_i - 1}$ é tal que $(A - \lambda_i I)^{d_i - 1} v$ representa um autovetor de A associado ao autovalor de λ_i.

Mostrando a recíproca, denotaremos $N_k = ker(A - \lambda_i I)^k$. Iniciaremos pelo:

Lema 1 A aplicação

$$A - \lambda_i I: \frac{N_{k+1}}{N_k} \to W_i \text{ tem imagem contida em } \frac{N_k}{N_{k-1}} \text{ e é injetiva.}$$

Demonstração: Sendo $x \in \frac{N_{k+1}}{N_k}$. Isso quer dizer que $(A - \lambda_i I)^{k+1} x = 0$ e $(A - \lambda_i I)^{k+1} x \neq 0$. Consideremos então $(A - \lambda_i I)x$. Como $(A - \lambda_i I)^k (A - \lambda_i I)x = (A - \lambda_i I)^{k+1} x$, vemos que $(A - \lambda_i I)x \in \mathrm{N_k}$. Por outro lado, $(A - \lambda_i I)^{k-1} (A - \lambda_i I)x = (A - \lambda_i I)^k x \neq 0$, mostrando assim que $(A - \lambda_i I)x \notin N_{k-1}$.

Sabemos agora que essa aplicação é injetiva. Sejam x, y ∈ $\frac{N_{k+1}}{N_k}$, com $(A - \lambda_i I)x = (A - \lambda_i I)y$. Então $(A - \lambda_i I)(x - y) = 0$ e que é impossível, pois então x – y estaria em N_k.

Iremos agora construir uma base especial para W_i. Já sabemos que uma base de $\frac{N_k}{N_{k-1}}$ é obtida ao se escolher uma base para N_{k-1} então completá-la para uma base de N_k; os elementos introduzidos formam a base procurada.

Seja x_1,..., x_l uma base de $\frac{N_{d_i}}{N_{d_i-1}}$. De acordo com o lema, os elementos

$$(A-\lambda_i I)x_1, \ldots, (A-\lambda_i I)x_l$$

são linearmente independentes e pertencem a $\frac{N_{d_{i-1}}}{N_{d_i-2}}$. Completamos esses elementos até obtermos uma base desse espaço. Utilizando o mesmo raciocínio, a imagem por $(A-\lambda_i I)$ dos elementos dessa base é linearmente independente e iremos completar esse conjunto até obter uma base, assim como feito anteriormente; procedemos desse modo até chegarmos ao espaço N_1. A base de W_i assim construída é a base de Jordan do subespaço W_i. Encontrando, desta forma, uma base do espaço inteiro ao obtermos as bases de Jordan de cada espaço W_i. Essa base é chamada base de Jordan.

Os subespaços $M_k = ker(B-\lambda_i)^k$ têm a mesma dimensão do espaço correspondente N_k. Ou seja, o procedimento aplicado a N_k, se repetido para a matriz B, produzirá o mesmo número de elementos para cada base de $\frac{M_k}{M_{k+1}}$. Existe uma aplicação P que faz correspondera cada elemento da base de Jordan $x_j \in \frac{N_k}{N_{k-1}}$ o elemento correspondente na base de $y_j \in \frac{M_k}{M_{k-1}}$, de modo que $(A-\lambda_i I)x_j$ seja levado em $(B-\lambda_i I)y_j$. Conhecida a imagem dos vetores da base, existe uma única aplicação linear que estende essa aplicação; seja P tal extensão. Como base está sendo levada em base, esta aplicação linear tem inversa. Utilizando o mesmo procedimento aplicado ao autoespaço associado a λ_i constrói a aplicação P.

Por fim, a definição de P afirma que $P(A-\lambda_i I)x_j$=$(B-\lambda_i I)y_j = (B-\lambda_i I)Px_j$. Logo, que $P(A-\lambda_i I)$=$(B-\lambda_i I)$P. Daí, PA = BP.

Exemplo 4 Seja T : $\mathbb{R}^4 \to \mathbb{R}^4$ definido por

$$T(x_1, x_2, x_3, x_4) = (2x_1 - x_2 + x_4, 3x_2 - x_3, x_2 + x_3, -x_2 + 3x_4).$$

Vamos obter a forma canônica de Jordan de T, bem como também a base em que T assume essa forma.

Tendo como polinômio característico de T de p(t) = (t – 3).(t – 2)^3. Assim, todos os autovalores de T estão no corpo $\mathbb{R}$ e podemos obter a forma de Jordan de T. Para autovalor 3, na forma escalonada reduzida de

$$(T-3I)=\begin{pmatrix}-1 & -1 & 0 & 1\\ 0 & 0 & -1 & 0\\ 0 & 1 & -2 & 0\\ 0 & -1 & 0 & 0\end{pmatrix} \text{ é } \begin{pmatrix}1 & 0 & 0 & 0\\ 0 & 1 & 0 & 0\\ 0 & 0 & 1 & 0\\ 0 & 0 & 0 & 1\end{pmatrix}.$$

Desta forma, o subespaço $W_i = ker(T-3I)$ é dado por:

$$\{(x_1, 0, 0, x_1);\ x_1 \in \mathbb{R}\}.$$

Da mesma forma, verifica-se que:

$$ker(T-2I) = \{(x_1, x_2, x_2, x_2);\ x_1, x_2 \in \mathbb{R}\}$$

$$ker(T-2I)^2 = \{(x_1, x_2+x_3, 2x_3, 2x_2);\ x_1, x_2, x_3 \in \mathbb{R}\}$$

Como a dimensão de $ker(T-2I)^3$ é igual a multiplicidade de 2 como raiz do polinômio característico p(t) de T, temos que o espaço W_2 é dado por $ker(T-2I)^2$.

O subespaço W_1 tem base (1, 0, 0, 1) = w_1. Esse é o primeiro elemento da base de Jordan.

Obtendo agora a base de Jordan de W_2, começaremos por conhecer o vetor em $W_2 = N_2 = ker(T-2I)^2$, vetor este que não se encontra em $N_1 = ker(T-2I)$, onde é possível obter apenas um vetor, pois a diferença de dimensão entre estes espaço é 1. Ele fornecerá a base de $\frac{N_2}{N_1}$ da demonstração do teorema de Jordan. De forma clara, temos que o vetor $w_4 = (0,1,0,2) \in N_2\ e\ w_4 \neq N_1$. Temos também que $w_3 = (T-2I)w_4 = (1,1,1,1)$. Pelo teorema de Jordan, temos que $w_3 \in N_1$ e que w_3 e w_4 são linearmente independentes. Escolhemos o vetor $w_2 = (1,0,0,0)$ para obter uma base de N_1, que é claramente linearmente independente com w_3.

Temos assim a base B = $\{w_1, w_2, w_3, w_4\}$, que é a base de Jordan de T. Os vetores w_2 e w_3 são autovetores de T, associado ao autovalor 2, porque eles pertencem a N_1. Por fim, $(T-2I)w_4 = w_3$, de modo que $Tw_4 = 2w_4 + w_3$. Representando T na base B, vemos:

$$T_B = J = \begin{pmatrix}3 & 0 & 0 & 0\\ 0 & 2 & 0 & 0\\ 0 & 0 & 2 & 1\\ 0 & 0 & 0 & 2\end{pmatrix}, \text{ que é a forma canônica de Jordan de T.}$$

Observação Comparando o exemplo acima, caso tivéssemos encontrado dois vetores distintos $\frac{N_2}{N_1}$, consideraríamos o ciclo formado pelo primeiro e então o ciclo formado pelo segundo e ordenaríamos a base nessa ordem.

Exemplo 5 Obtenha uma base $\mathcal{B}$ onde a matriz A esteja na forma canônica:

$$A = \begin{pmatrix} 2 & 0 & 0 & 0 & 0 & 0 \\ 1 & 2 & 0 & 0 & 0 & 0 \\ -1 & 0 & 2 & 0 & 0 & 0 \\ 0 & 1 & 0 & 2 & 0 & 0 \\ 1 & 1 & 1 & 1 & 2 & 0 \\ 0 & 0 & 0 & 0 & 1 & -1 \end{pmatrix}$$

Tendo como polinômio característico de A $p(t) = (t - 2)^5(t + 1)$, pois a matriz A é triangular superior.

Caso chamemos de W_1 o subespaço relacionado ao autovalor – 1, saberemos que dim $W_1 = 1$ e que uma base para esse subespaço é dado pelo vetor e_6. Denotaremos $v_1 = e_6$ o primeiro vetor da base procurada.

Vemos agora o espaço W_2 associado ao autovalor 2. Temos que dim $W_2 = 5$ e que

$$A - 2I = \begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 \\ -1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & -3 \end{pmatrix}$$

Caso chamemos de $N_1 = \ker(A - 2I)$, vemos que dim $N_1 = 2$. Logo teremos:

$$N_1 = \ker(A - 2I) = \left\{\left(0, 0, x_3, -x_3, x_4, \frac{x_4}{3}\right);\ x_3, x_4 \in \mathbb{R}\right\}$$

$$N_2 = \ker(A - 2I)^2 = \{(0, 0, x_3, x_4, x_5, (3x_5 - x_4 - x_3)/9)\}$$

$$N_3 = \ker(A - 2I)^3 = \left\{\left(0, x_2, x_3, x_4, x_5, \frac{(-2x_2 - 3x_3 - 3x_4 + 9x_5}{27}\right)\right\}$$

$$N_4 = \ker(A - 2I)^4 = \left\{\left(x_1, x_2, x_3, x_4, x_5, \frac{(-10x_1 - 6x_2 - 9x_3 - 9x_4 + 27x_5}{81}\right)\right\}$$

Tendo como dim $\ker(A - 2I)^5 = 5$, observamos que o coeficiente que estabiliza o espaço $A - 2I$ é 4. Se W_2 é o autoespaço generalizado associado ao autovalor 2,

temos W2 = N_4. Logo, o vetor $v_6 = (1,0,0,0,0,-\frac{10}{81}) \in N_4 \setminus N_3$. Tendo aqui a aplicação $A-2I : \frac{N_4}{N_3} \to \frac{N_3}{N_2}$ é injetiva e dim $\frac{N_3}{N_2}$ = 1, vemos então que:

$v_5 = (A-2I)v_6 = \left(0,1,-1,0,1,\frac{10}{27}\right)$, é o quinto vetor da base procurada.

Pelo mesmo motivo, $v_2 = (A-2I)^2 v_6 = (A-2I)v_4 = \left(0,0,0,0,1,\frac{1}{3}\right)$ é um autovetor de A, pois ele pertence a N_1. Como N_1 tem dimensão 2, existe um outro vetor nesse espaço, linearmente independente com v_3. Esse é o vetor $v_2 = (0,0,1,-1,0,0)$. Obtendo os vetores $\{v_1, \dots, v_6\}$, a representação de A nessa base é dada por:

$Av_1 = -v_1\ (pois\ (A+I)v_1 = 0)$

$Av_2 = 2v_2\ (pois\ (A-2I)v_2 = 0)$

$Av_3 = 2v_3\ (pois\ (A-2I)v_3 = 0)$

$Av_4 = v_3 + 2v_4\ (pois\ (A-2I)v_4 = 0)$

$Av_5 = v_4 + 2v_5\ (pois\ (A-2I)v_5 = 0)$

$$Av_6 = v_5 + 2v_6\ (pois\ (A-2I)v_6 = 0)$$

A representação de A nessa base é:

$$J = \begin{pmatrix} -1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 2 & 0 & 0 & 0 & 0 \\ 0 & 0 & 2 & 1 & 0 & 0 \\ 0 & 0 & 0 & 2 & 1 & 0 \\ 0 & 0 & 0 & 0 & 2 & 1 \\ 0 & 0 & 0 & 0 & 0 & 2 \end{pmatrix}$$

A matriz J tem um bloco 1 x 1 associado ao autovalor – 1. Associado ao autovalor 2 ela tem dois blocos de Jordan: o bloco 1 x 1 associado ao autovetor v_2 e o bloco 4 x 4 associado aos elementos $\{v_3, v_4, v_5, v_6\}$, $\{(A-2I)^3 v_6, (A-2I)^2 v_6, (A-2I)v_{6,}\ v_{6,}\}$.

Teorema 4 Toda matriz $\in M_{n\,x\,n}$(C) é semelhante a sua transposta.

Demonstração. Uma vez que $\det A = detA^T$, obtemos que o polinômio característico dessas duas matrizes é igual. Vemos então que eles têm os mesmos autovalores.

Percebemos que se q é um polinômio e B uma matriz n x n, então $[q(B)]^T=q(B^T)$. Se λ_i é um autovalor de A, aplicando esse resultado para os polinômios $(t-\lambda_i)^k$ e então considerando a dimensão de seus núcleos, decorre que a condição II do teorema de Jordan também é cumprida.

Teorema 5 Um operador linear T : V → V é diagonalizável se, e somente se, o seu polinômio mínimo é produto de fatores lineares distintos.

Demonstração: Tomando como suposição T diagonalizável e $\lambda_1, \dots, \lambda_k$ os autovalores distintos de T. Logo V possui uma base formada por autovetores de T.

Considere o polinômio

$$h(z) = (t - \lambda_1) \dots (t - \lambda_k).$$

Se v é um autovetor de T associado ao autovalor λ_i então $(T-\lambda_i)\, v = 0$. Implicando em h(T) $v = 0$ para qualquer autovetor de T. Sabendo que o polinômio mínimo e característico possuem os mesmos fatores irredutíveis, mostramos que h é o polinômio mínimo de T.

De maneira recíproca, se $p(t) = (t - \lambda_1) \dots (t - \lambda_k)$ é o polinômio mínimo de T, então $W_i = (\ker(T-\lambda_i)$. De forma bastante clara, todo elemento de W_i é autovetor de T. Tomando bases $\mathcal{B}_i$ de cada espaço W_i, temos que $\mathcal{B} = \{\mathcal{B}_1, \dots, \mathcal{B}_k\}$ é uma base de V formada por autovetores de T.

5.3 A forma real de Jordan

Definição 5 Sejam A ∈ $M_{n\,x\,n}$ e $z \in \mathbb{K}^n$ um vetor qualquer. Definamos por $\bar{A} \in M_{n\,x\,n}$ como a matriz obtida ao se tomar o conjugado em cada uma das entradas de A e $\bar{z} \in \mathbb{K}^n$ como vetor obtido ao se tomar o conjugado em cada uma das coordenadas de z.

Para quaisquer matrizes A, B ∈ $M_{n\,x\,n}$ e $\lambda \in \mathbb{K}$, verifica-se que $\overline{A + \lambda B} = \bar{A} + \overline{\lambda B}, \overline{AB} = \bar{A}.\bar{B}$. Também vale que $\overline{Az} = \bar{A}.\bar{z}$ em qualquer $z \in \mathbb{K}^n$.

Definição 6 Seja V um espaço vetorial real. A complexidade de V será

$$V_{\mathbb{C}} = \{u + iv; u, v \in V\}$$

Em $V_{\mathbb{C}}$ soma-se e multiplica-se por complexo de forma "natural". Verificamos que $V_{\mathbb{C}}$ torna-se, assim, um espaço vetorial sobre os complexos.

Sendo T : V → V uma aplicação linear, realizamos a definição da complexidade de T desta forma: $T_{\mathbb{C}} : V_{\mathbb{C}} \to V_{\mathbb{C}}$ definida por $T_{\mathbb{C}}(u + iv) = Tu + iTv$.

Caso identifiquemos o vetor $v \in$ V com o vetor $v + i0 \in V_{\mathbb{C}}$, V será um subespaço de $V_{\mathbb{C}}$. Identidade esta a ser utilizada no resultado seguinte:

Lema 2 Sejam V um espaço vetorial de dimensão finita e T : V → V uma aplicação linear. Temos a seguir, situações válidas:

i. Toda base de V é base de $V_{\mathbb{C}}$;

ii. Os polinômios característicos de T e $T_{\mathbb{C}}$ são iguais;

iii. Sendo λ um autovalor de $T_{\mathbb{C}}$, então $\bar{\lambda}$ é também um autovalor de $T_{\mathbb{C}}$; são iguais as multiplicidades algébricas dos autovalores λ e $\bar{\lambda}$.

iv. Seja $\widetilde{W}$ um subespaço tal que $w = u + iv \in \widetilde{W}$ implica que $\overline{w} = u - iv \in \widetilde{W}$. Logo $\widetilde{W}$ possui uma base formada por vetores reais.

Demonstração:

i. Notemos apenas que as partes real u e imaginária v de qualquer vetor $u + v$ podemos escrever como combinação linear dos elementos da base de V.

ii. Apresentamos como uma decorrência do quesito anterior, com a identificação V ∋ $v = v + i0 \in V_{\mathbb{C}}$, pois então as representações de T e $T_{\mathbb{C}}$ numa base de V são iguais.

iii. Sejam λ um autovalor de $T_{\mathbb{C}}$ e p(z) o polinômio caraterístico de $T_{\mathbb{C}}$. Os coeficientes de p(z) são reais, pois este é também polinômio característico de T. Vemos na equação p(λ) = 0 que seu conjugado também resulta em zero, o que mostra que $\bar{\lambda}$ também é uma raiz do polinômio característico de $T_{\mathbb{C}}$. Sendo $p'(\lambda)$ = ... = $p^{(d-1)}(\lambda)$ = 0 e $p^{(d)}(\lambda) \neq 0$, mostrando que $\bar{\lambda}$ também tem multiplicidade d.

iv. Seja $\{w_1, \dots, w_k\}$ uma base de W, com $w_j = u_j + iv_j, j = 1, \dots, k$. Somando e subtraindo os vetores w_j e $\overline{w_j}$, obtemos que $u_j = u_j + i0$ *e* $v_j = v_j + i0$ estão em $\widetilde{W}$. Assim, S = $\{u_1, v_1, \dots, u_k, v_k\}$ é um conjunto de vetores reais que gera $\widetilde{W}$. Uma base formada de vetores reais é obtida ao se adquirir um subconjunto de S com k elementos linearmente independentes em $V_{\mathbb{C}}$.

Lema 3 Sejam T : V → V um operador linear e $T_{\mathbb{C}}$ sua complexidade. Se o subespaço $\widetilde{W} \subset V_{\mathbb{C}}$ possui uma base formada por vetores reais, então ele é a complexidade de um subespaço W ⊂ V.

Demonstração. Sabendo que todo vetor $\widetilde{W}$ é da forma $w = u + iv$, sendo u e v vetores reais. Tomando u e v em termos dos vetores da base real, teremos que $\widetilde{W}$ é a complexidade real W gerado pelos vetores dessa base.

Teorema 6 (Forma de Jordan real)

Sejam T : V → V um operador linear real. Logo existe uma base C de V onde T é representado por uma matriz J, diagonal em blocos, cujos blocos diagonais, podem ter a forma:

$$J_{\alpha,\beta} = \begin{pmatrix} D_{\alpha,\beta} & I_2 & 0 & \cdots & 0 \\ 0 & D_{\alpha,\beta} & I_2 & \cdots & 0 \\ \vdots & \vdots & \ddots & \cdots & \vdots \\ 0 & 0 & 0 & D_{\alpha,\beta} & I_2 \\ 0 & 0 & 0 & 0 & D_{\alpha,\beta} \end{pmatrix} \quad em\ que\ \ D_{\alpha,\beta} = \begin{pmatrix} \alpha & \beta \\ -\beta & \alpha \end{pmatrix},$$

tendo aí $\alpha + i\beta$ um autovalor complexo de $T_{\mathbb{C}}$ e I_2 a matriz identidade 2 x 2.

Demonstração. Sabemos que o espaço vetorial V pode ser decomposto como soma direta de espaços invariantes pela aplicação T. Caso $\lambda \in \mathbb{R}$ seja um autovalor de T, obtemos o espaço invariante W_λ. A base do espaço W_λ na qual T assume sua forma de Jordan nesse espaço existe como na demonstração do teorema de Jordan.

Desta forma, podemos observar apenas o caso de autovalores $\lambda \in \mathbb{C} \setminus \mathbb{R}$ da complexidade $T_{\mathbb{C}}$ de T. Suponhamos que $T_{\mathbb{C}}$ possua um autovalor $\lambda \notin \mathbb{R}$. Sabemos também que $\bar{\lambda}$ é autovalor de $T_{\mathbb{C}}$, o que nos garante que existem os espaços W_λ e $W_{\bar{\lambda}}$. Se os vetores $w_j = u_j + iv_j, j = 1, \dots, k$, formam uma base de W_λ, temos que os vetores $u_j + iv_j$formam uma base de $W_{\bar{\lambda}}$.

Temos então que

$$S = \{u_1, v_1, \dots, u_k, v_k\}$$

é uma base de $W_\lambda \oplus W_{\bar{\lambda}}$. De fato, como dim $W_\lambda = W_{\bar{\lambda}} = k$, o conjunto S tem dimensão do espaço $W_\lambda \oplus W_{\bar{\lambda}}$. Qualquer vetor desse espaço é combinação linear dos elementos de S. Isso prova o afirmado.

Por fim, se $w_1 = u_1 + iv_1$ satisfaz $T_{\mathbb{C}} w_1 = \lambda w_1$ para $\lambda = \alpha + i\beta \in \mathbb{C} \setminus \mathbb{R}$, logo:

$$T(u_1) + iT(v_1) = (\alpha u_1 - \beta v_1) + i(\beta u_1 + \alpha v_1).$$

Se, para $j \in \{2, \dots, r\}$, temos $T_{\mathbb{C}} w_j = \lambda w_j + w_{j-1}$, vemos que:

$$Tu_j + iTv_j = (\alpha u_j - \beta v_j + u_{j-1}) + i(\beta u_j + \alpha v_j + v_{j-1}),$$

seguindo que, na base = $\{u_1, v_1, \ldots, u_k, v_k\}$ de $W_\lambda \oplus W_{\bar{\lambda}}$, $T_{\mathbb{C}}$ é representado por bloco(s) da forma descrita pelo início do teorema. Sabendo que $T_{\mathbb{C}} = T$ para qualquer vetor dessa base, a demonstração está válida.

6 SUPERFÍCIE QUOCIENTE OU ABSTRATA

6.1 Definição

Uma superfície abstrata é um conjunto S composto de uma família de aplicações bijetivas $x_\alpha : U_\alpha \to S$ de conjuntos abertos $U_\alpha \subset \mathbb{R}^2$ em S tal que

1. $U_\alpha x_\alpha(U_\alpha) = S$,

2. Para cada par α, β com $x_\alpha(U_\alpha) = W \neq \emptyset$, temos que x_α^{-1}(W), x_β^{-1}(W) são conjuntos abertos em $\mathbb{R}^2$ e $x_\beta^{-1} \circ x_\alpha, x_\alpha^{-1} \circ x_\beta$ são aplicações diferenciáveis (ver figura seguinte).

O par (U_α, x_α) com p $\in x_\alpha(U_\alpha)$ é chamado parametrização (ou sistema de coordenadas) de S em torno de p. Temos que $x_\alpha(U_\alpha)$ é uma vizinha coordenada, e se q = $x_\alpha(u_\alpha, v_\alpha) \in S$, que (u_α, v_α) são coordenadas de q neste sistema de coordenadas. A família $\{U_\alpha, x_\alpha\}$ é chamada uma estrutura diferenciável em S. Diremos que um subconjunto V ⊂ S é aberto em S se x_α^{-1}(V) é aberto em $\mathbb{R}^2$ para todo α.

Observando a opção 2, vemos que a *mudança de parâmetros*

$$x_\beta^{-1} \circ x_\alpha : x_\alpha^{-1}(W) \to x_\beta^{-1}(W)$$

é um difeomorfismo.

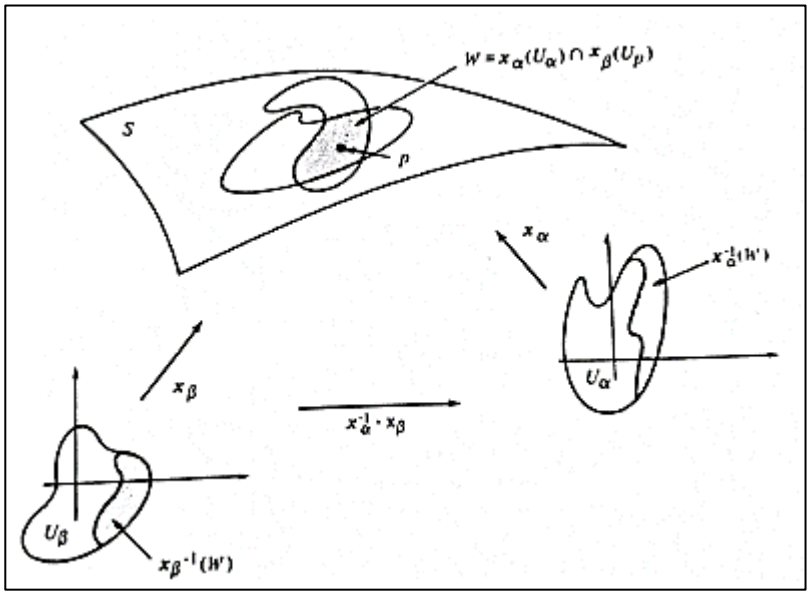

Figura 1: Aplicações diferenciais

Observação 1. Ás vezes é útil acrescentar um axioma á definição 1 e dizer que a estrutura diferenciável deve ser máxima em relação às condições 1 e 2. Temos então que $\{U_\alpha, x_\alpha\}$ não está contida propriamente em nenhuma outra família de vizinhanças coordenadas, satisfazendo assim as condições 1 e 2 da definição 1.

Sejam S_1 e S_2 superfícies abstratas. Uma aplicação $\varphi : S_1 \to S_2$ é diferenciável em p ∈ S_1 se dada uma parametrização y : V ⊂ $\mathbb{R}^2 \to S_2$ em torno de φ(x(U)) ⊂ y(U) e a aplicação

$$y^{-1} \circ \varphi \circ x : U \subset \mathbb{R}^2 \to \mathbb{R}^2 \ (*)$$

é diferenciável em x^{-1}(p). φ é diferenciável em S_1 se é diferenciável em todo p ∈ S_1 $(ver\ figura\ seguinte)$.

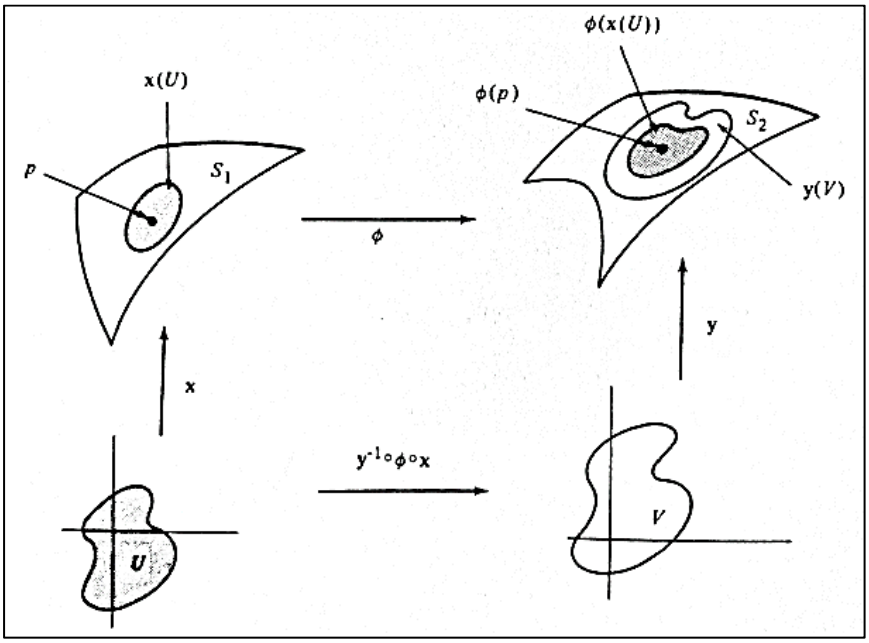

Figura 2: φ é diferenciável em S_1 se é diferenciável em todo p ∈ S_1

Essa definição, observando a condição 2, não depende das escolhas de parametrização. A aplicação 1 recebe o nome de expressão de φ nas parametrizações x, y.

Desta forma, faz sentido falar de aplicações diferenciáveis em superfícies abstratas, e já demos o primeiro passo para uma generalização da geometria intrínseca.

Exemplo 1 Seja $S^2 = \{(x, y, z) \in \mathbb{R}^3; x^2 + y^2 + z^2 = 1\}$ a esfera unitária e seja A : $S^2 \to S^2$ a aplicação antípoda; A(x, y, z) = (- x, - y, - z). Seja P^2 o conjunto obtido de S^2 identificando p com A(p) e denotemos por $\pi : S^2 \to P^2$ a aplicação natural de $\pi = \{p, A(p)\}$. Cubramos S^2 com parametrizações $x_\alpha : U_\alpha \to S^2$, tais que $x_\alpha(U_\alpha) \cap (A \circ x_\alpha)(U_\alpha) = \emptyset$. Como S^2 é uma superfície regular e A é um difeomorfismo, segue-se que P^2 munido da família $\{U_\alpha, x_\alpha \circ \pi\}$ é uma superfície abstrata, que denotaremos também por P^2 . P^2 é chamada de plano projetivo real.

O plano projetivo é geralmente definido como sendo a esfera com os pontos antípodas relacionados. Com a construção de espaços quocientes onde a esfera $S^2 = \{x \in \mathbb{R}^3;\ |x| = 1\}$ munido da topologia do subespaço $S^2 \subset \mathbb{R}^3$, introduziremos em S^2 a relação que identifica pontos antípodas e assim temos definidas classes $[x] = \{x, -x\} \in S^2/\sim$ elementos de $S^2/\sim$. Construímos dessa forma o plano projetivo $\mathbb{RP}^2 = (S^2/\sim, \tau_{S^2/\sim})$.

Exemplo 2 Seja T $\subset \mathbb{R}^3$ um toro de revolução (vide observação a seguir) com centro em (0, 0, 0) $\in \mathbb{R}^3$ e seja A : T → T definida por A(x, y, z) = (- x, - y, - z) (ver figura seguinte). Sendo K o espaço quociente de T pela relação de equivalência p ~ A(p) e denotemos por $\pi : T \to K$ a aplicação π(p) = $\{p, A(p)\}$. Cubramos T com parametrizações $x_\alpha : U_\alpha \to T$ tais que $x_\alpha(U_\alpha) \cap (A \circ x_\alpha)(U_\alpha) = \emptyset$. Como antes, é possível mostrar que K com a família $\{U_\alpha, \pi \circ x_\alpha\}$ é uma superfície abstrata, que é chamada de garrafa de Klein.

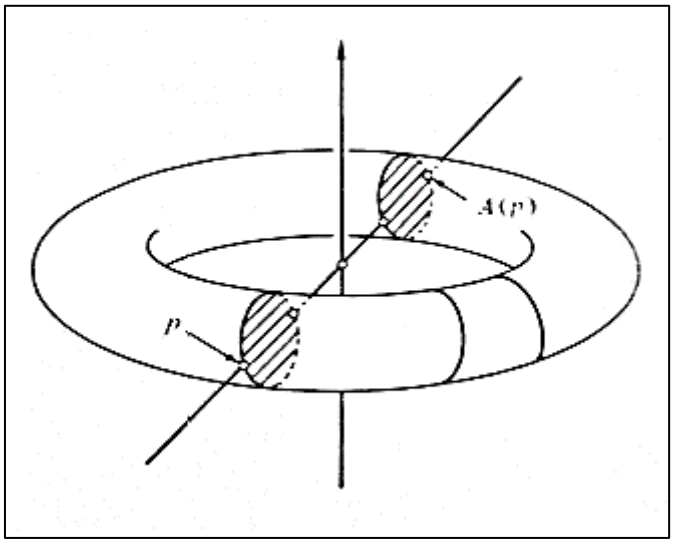

Figura 3: A(x, y, z) = (- x, - y, - z)

Associemos agora um plano tangente a cada ponto de uma superfície abstrata S. O plano tangente, nesse caso, é o conjunto de vetores tangentes em um ponto, sendo um vetor tangente em um ponto definido como a velocidade neste ponto de uma curva na superfície. Precisamos definir o que é o vetor tangente de uma curva em uma superfície abstrata. Como não podemos contar com o $\mathbb{R}^3$, o que é onde vivem os vetores tangente às curvas, é necessário buscar uma propriedade característica de tais vetores que não dependa do $\mathbb{R}^3$.

Seja $\alpha : (-\varepsilon, \varepsilon) \to \mathbb{R}^2$ uma curva diferenciável em $\mathbb{R}^2$, com $\alpha(0) = p$. Escrevendo $\alpha(t) = \big(u(t), v(t)\big), t \in (-\varepsilon, \varepsilon)$, e $\alpha'(0) = \Big(u'(0), v'(0)\Big) = w$. Seja f diferenciável definida em uma vizinhança de p. Podemos restringir f a α e escrever a derivada direcional de f com relação a w da seguinte maneira:

$$\frac{d(f\circ\alpha)}{dt}\Big|_{t=o} = \left(\frac{\partial f}{\partial u}\frac{du}{dt} + \frac{\partial f}{\partial v}\frac{dv}{dt}\right)\Big|_{t=0} = \left\{u'(0)\frac{\partial}{\partial u} + v'(0)\frac{\partial}{\partial v}\right\}.\text{f}$$

Desta forma, a derivada direcional na direção do vetor w é um operador sobre funções diferenciáveis que depende apenas de w. Esta é a propriedade característica dos vetores tangentes.

OBSERVAÇÂO: O toro é a *superfície regular* gerada pela rotação de um círculo S de raio r e em torno de uma reta pertencente ao plano do círculo e a uma distância a > r do centro do círculo.

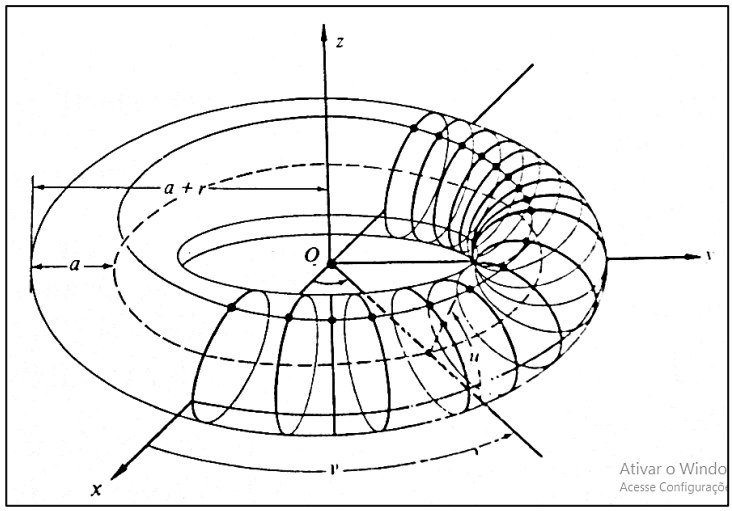

Figura 4: conceito de toro

<u>Definição 1</u> Uma aplicação diferenciável $\alpha : (-\varepsilon, \varepsilon) \to S$ recebe o nome de curva em S. Suponhamos que $\alpha(0) = p$ e seja D o conjunto de funções em S que são diferenciáveis em p. O vetor tangente à curva α em t = 0 é a função $\alpha'(0) : D \to \mathbb{R}$ dada por:

$$\alpha'(0)(f) = \frac{d(f\circ\alpha)}{dt}\Big|_{t=o}, \text{ f} \in \text{D}$$

Um vetor tangente em um ponto p ∈ S é o vetor tangente em t = 0 de alguma curva $\alpha : (-\varepsilon, \varepsilon) \to S$ com $\alpha(0) = p$.

Tratando com a parametrização x : U → S em torno de p = x(0, 0), podemos expressar a função f e a curva α em x por f(u, v) e $(u(t), v(t))$, respectivamente. Logo,

$$\alpha'(0)(f) = \frac{d(f\circ\alpha)}{dt}\Big|_{t=o} = \frac{d(f(u(t),v(t)))}{dt}\Big|_{t=o} =$$

$$= u'(0)\left(\frac{\partial f}{\partial u}\right)_0 + v'(0)\left(\frac{\partial f}{\partial u}\right)_0 =$$

$$= \left\{u'(0)\left(\frac{\partial f}{\partial u}\right)_0 + v'(0)\left(\frac{\partial f}{\partial u}\right)_0\right\}(f).$$

Isto sugere, dadas as coordenadas (u, v) em torno de p, que denotamos por $\left(\frac{\partial}{\partial u}\right)_0$ o vetor tangente em p que aplica a função f em $\left(\frac{\partial f}{\partial u}\right)_0$; um significado análogo será referente a $\left(\frac{\partial f}{\partial v}\right)_0$. Observamos que $\left(\frac{\partial f}{\partial u}\right)_0, \left(\frac{\partial f}{\partial v}\right)_0$ podem ser interpretados como vetores tangentes em p das *curvas coordenadas* $u \to x(u, 0), v \to x(0, v)$, respectivamente.

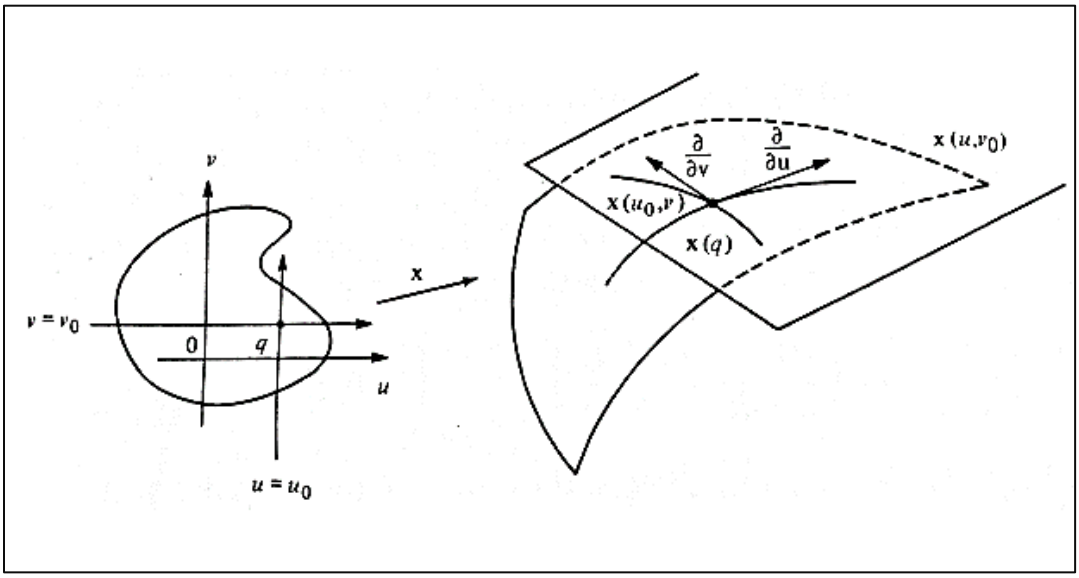

Figura 5: $u \to x(u, 0), v \to x(0, v)$

O conjunto de vetores tangentes em p, com as operações usuais para funções, é um espaço vetorial bi-dimensional T_pS chamado de *espaço tangente* de S em p. Vemos também que a escolha de uma parametrização x : U → T em torno de p determina uma *base associada* $\left\{\left(\frac{\partial}{\partial u}\right)_q + \left(\frac{\partial}{\partial u}\right)_q\right\}$ de T_pS para todo q ∈ x(U).

Definição 2 Sejam S_1 e S_2 superfícies abstratas e seja $\varphi : S_1 \to S_2$ uma aplicação diferenciável. Para cada p $\in S_1$ e cada $w \in T_pS_1$, considere a curva diferenciável $\alpha : (-\varepsilon, \varepsilon) \to S_1$, com $\alpha(0) = p$, $\alpha'(0) = w$. Faça $\beta = \varphi \circ \alpha$. A aplicação $d\varphi_p : T_pS_1 \to T_{\alpha(p)}S_2$ dada por $d\varphi_p(w) = \beta'(0)$ é uma aplicação linear bem definida, que recebe o nome de diferencial de φ em p.

Definição 3 Uma superfície geométrica (Variedade Riemanniana de dimensão 2) é uma superfície abstrata S munida de uma escolha de um produto interno $\langle\ ,\ \rangle_p$

em cada T_pS, $p \in S$, que varia diferencialmente com p no seguinte sentido. Para alguma parametrização x : U → S em torno de p, as funções

$$E(u,v) = \left\langle \frac{\partial}{\partial u}, \frac{\partial}{\partial u} \right\rangle,\ F(u,v) = \left\langle \frac{\partial}{\partial u}, \frac{\partial}{\partial v} \right\rangle,\ G(u,v) = \left\langle \frac{\partial}{\partial v}, \frac{\partial}{\partial v} \right\rangle$$

são funções diferenciáveis em U. O produto interno $\langle\ ,\ \rangle$ é frequentemente chamado de métrica Riemanniana em S.

Definição 4 Uma aplicação diferenciável $\varphi : S \to \mathbb{R}^3$ de uma superfície abstrata S em $\mathbb{R}^3$ é uma imersão se a diferencial $d\varphi_p : T_pS \to T_p\mathbb{R}^3$ é injetiva. Se, além disto, S tiver uma métrica $\langle\ ,\ \rangle$ e $\langle d\varphi_p(v), d\varphi_p(w)\rangle_{\varphi(p)} = \langle\ ,\ \rangle_p$, $v, w \in T_pS$, dizemos que φ é uma imersão isométrica.

Vemos que o primeiro produto interno apresentado é usual do $\mathbb{R}^3$, já o segundo é a métrica Riemanniana dada sobre S. Chegando assim que para uma imersão isométrica a métrica *induzida* por $\mathbb{R}^3$ sobre S coincide com a métrica dada sobre S.

Exemplo 3 Seja $\mathbb{R}^2$ um plano com coordenadas (x, y) e $T_{m,n} : \mathbb{R}^2 \to \mathbb{R}^2$ a aplicação (translação) $T_{m,n}$(x, y) = (x + m, y + n), onde m e n são inteiros. Definamos uma relação de equivalência em $\mathbb{R}^2$ por (x, y) ~ (x_1, y_1) se existem inteiros m, n tais que $T_{m,n}$(x, y) = (x_1, y_1). Seja T o espaço quociente de $\mathbb{R}^2$ por esta relação de equivalência e seja $\pi : \mathbb{R}^2 \to T$ a projeção natural $\pi(x,y) = \{T_{m,n}(\mathrm{x},\mathrm{y});\ \text{para todos m, n inteiros}\}$. Observamos que em cada quadrado unitário aberto cujos vértices tenham coordenadas inteiras, teremos apenas um representante de um elemento T, e T pode ser pensado como um quadrado fechado com os lados opostos identificados (ver figura a seguir, nela temos que todos os pontos de $\mathbb{R}^2$ denotados por x representam o mesmo ponto p em T).

Temos que $i_\alpha : U_\alpha \subset \mathbb{R}^2 \to \mathbb{R}^2$ é uma família de parametrização $\mathbb{R}^2$, sendo i_α aplicação identidade, onde $U_\alpha \cap T_{m,n}(U_\alpha) = \emptyset$ em quaisquer m, n inteiros. Sabendo que $T_{m,n}$ é um difeomorfismo, então a família $(U_\alpha, \pi \circ i_\alpha)$ é uma estrutura diferenciável pata T . T é chamado um toro (diferenciável). Seguimos da própria definição de estrutura diferenciável em T que $\pi : \mathbb{R}^2 \to T$ é uma aplicação diferenciável e um difeomorfismo local (vemos isso na figura seguinte onde temos que T é diomorfo ao toro usual em $\mathbb{R}^3$.

Vejamos agora que $T_{m,n}$ é uma isomeria de $\mathbb{R}^2$ e introduz uma estrutura geométrica (Riemanniana) em T da seguinte maneira. Sejam $p \in T$ e $v \in T_pT$. Sejam

$q_1, q_2 \in \mathbb{R}^2$ *e* $w_1, w_2 \in \mathbb{R}^2$ tais que $\pi(q_1) = \pi(q_2) = p$ e $d\pi_{q_1}(w_1) = d\pi_{q_2}(w_2) = v$. Então $q_1 \sim q_2$; logo existe $T_{m,n}$ tal que $T_{m,n}(q_1) = q_2$, $d(T_{m,n}) = q_2$, $d(T_{m,n})_{q_1}(w_1) = w_2$. Como $T_{m,n}$ é uma isomeria, $|w_1| = |w_2|$. Definamos agora o comprimento de v em T_pT por $|v| = \left|d\pi_q(w_1)\right| = |w_1|$. Pelo que acabamos de ver, isto está bem definido. Evidentemente, tal definição dá origem a um produto interno $\langle\ ,\ \rangle_p$ em T_pT para cada $p \in T$. Como este é essencialmente o produto interno usual do $\mathbb{R}^2$ e π é um difeomorfismo local, $\langle\ ,\ \rangle_p$ varia diferencialmente com p.

Observemos que os coeficientes da primeira forma fundamental de T, em qualquer uma das parametrizações da família $\{U_\propto, \pi \circ i_\alpha\}$, são E = G = 1, F = 0. Assim, este toro se comporta localmente como um espaço euclidiano. Por exemplo, a sua curvatura Guassiana é identicamente nula. Isto justifica o nome *toro plano*, que usualmente é dado a T munido do produto interno que acabamos de descrever.

Evidentemente o toro plano não pode ser isometricamente imerso em $\mathbb{R}^3$, pois, por compacidade, ele teria um plano com curvatura positiva. No entanto, ele pode ser imerso isometricamente em $\mathbb{R}^4$.

De fato, seja $F: \mathbb{R}^2 \to \mathbb{R}^4$ dado por

$$F(x, y) = \frac{1}{2\pi}(cos2\pi x, cos2\pi y, sen2\pi y).$$

Como $F(x + m, y + n) = F(x, y)$ para quaisquer m, n inteiros, podemos definir uma aplicação $\varphi: T \to \mathbb{R}^4$, por $\varphi(p) = F(q)$, onde $q \in \pi^{-1}(q)$. É claro que $\varphi \circ \pi = F$ e, como $\pi: \mathbb{R}^2 \to T$ é um difeomorfismo local, φ é diferenciável. Além disto, o posto $d\varphi$ é igual ao posto de dF que, por sua vez, verifica – se facilmente, é igual a 2. Assim, φ é uma imersao. Para ver que a imersão é isométrica, observamos primeiro que se $e_1 = (1, 0), e_2$= (0, 1) são os vetores da base canônica em $\mathbb{R}^2$, os vetores $d\pi_{q_1}(e_1) = f_1$, $d\pi_{q_1}(e_2) = f_2, q \in IR^2$, formam uma base para $T_{\pi_{(q)}}T$. Pela definição do produto interno em T, $\langle f_i, f_j\rangle = \langle e_i, e_j\rangle, i, j = 1, 2$. Em seguida, calculamos

$$\frac{\partial F}{\partial x} = dF(e_1) = (-sen2\pi x, cos2\pi x, 0, 0),$$

$$\frac{\partial F}{\partial y} = dF(e_2) = (0, 0, -sen2\pi y, cos2\pi y),$$

E obtemos que

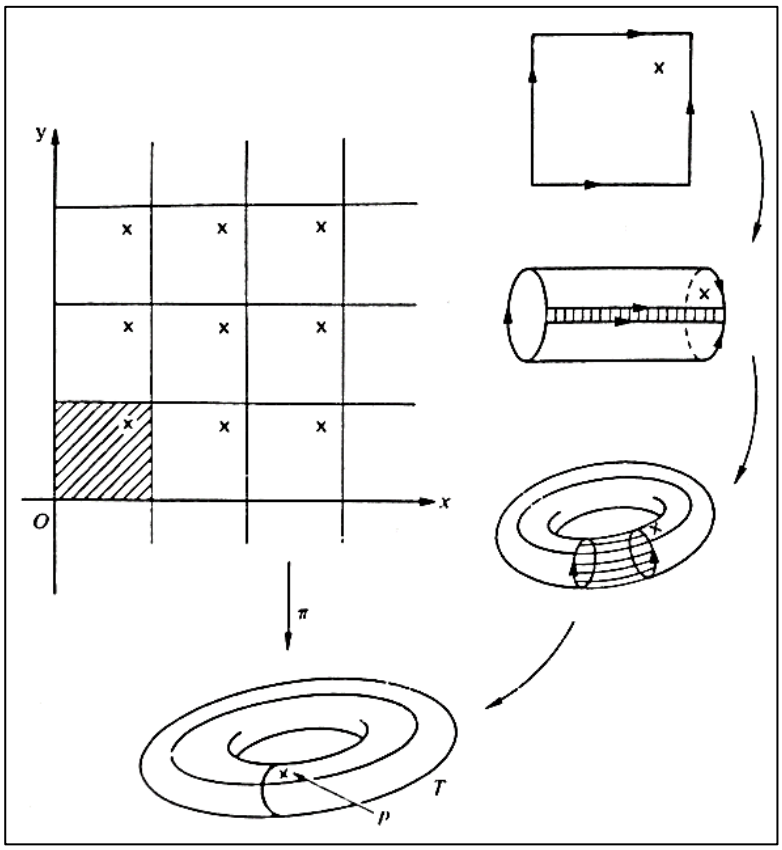

Figura 6: O toro

Assim, $\langle \mathrm{d}\varphi(f_i), \mathrm{d}\varphi(f_j)\rangle = \langle \mathrm{d}\varphi\left(d\pi(e_i), \mathrm{d}\varphi\left(d\pi(e_j)\right)\right)\rangle = \langle f_i, f_j\rangle$. Segue-se que φ é uma imersão isométrica, como havíamos afirmado.

Observemos que a imagem $\varphi(S)$ de uma imersão $\varphi : S \to \mathbb{R}^n$ pode ser auto-interseções. No último exemplo, $\varphi : T \to \mathbb{R}^4$ é injetiva e, além disto, φ é um homeomorfismo sobre sua imagem. Convém utilizar a seguinte terminologia.

Definição 5 Seja S uma superfície abstrata. Uma aplicação diferenciável $\varphi : S \to \mathbb{R}^n$ é um mergulho se φ é uma imersão e um homeomorfismo sobre a sua imagem.

Por exemplo, uma superfície regular em $\mathbb{R}^3$ pode ser caracterizada como a imagem de uma superfície abstrata S por um mergulho $\varphi : S \to \mathbb{R}^3$. Isto significa que apenas aquelas superfícies abstratas que podem ser mergulhadas em $\mathbb{R}^3$ poderiam ter sido detectadas em nosso estudo das superfícies regulares em $\mathbb{R}^3$. O exemplo abaixo mostra que tal fato é uma séria restrição.

Exemplo 4 Observamos primeiramente que a definição de orientabilidade pode ser estendida, sem mudar uma única palavra, às superfícies abstratas. Considere agora o plano projetivo real P^2 do exemplo 5.3. Afirmamos que P^2 é não – orientável.

Para provar isto, fazemos primeiro a seguinte consideração geral. Sempre uma superfície abstrata S contenha um conjunto aberto M difeomorfo a uma faixa de Mobius, ela é não-orientável. Caso contrário, existe uma família de parametrização cobrindo S com a propriedade de que todas as mudanças de coordenadas têm Jacobiano positivo; a restrição de uma tal família a M induzirá uma orientação em M, o que é uma contradição.

P^2 é obtido a partir da esfera S^2 pela identificação de pontos antípodas. Consideremos em S^2 uma faixa fina B formada por segmentos abertos de meridianos cujos centros estão sobre metade de um equador(ver figura seguinte). Através da identificação dos pontos antípodas, é claro que B se torna uma faixa de Mobius em P^2. Assim, P^2 é não-orientável.

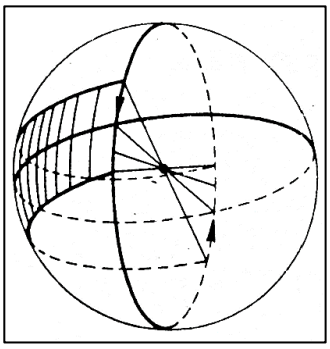

Figura 7: O plano projetivo contém uma faixa de M*ö*bius

Por um argumento análogo, pode-se mostrar que a garrafa de Klein K do Exemplo 2 também é não-orientável. Em geral, sempre que uma superfície regular $S \subset \mathbb{R}^3$ é simétrica em relação à origem de $\mathbb{R}^3$, a identificação dos pontos simétricos dá origem a uma superfície abstrata não-orientável.

Pode-se provar que uma superfície regular compacta em $\mathbb{R}^3$ é orientada. Assim, P^2 e K não podem ser mergulhados em $\mathbb{R}^3$, e o mesmo acontece para as superfícies não-orientáveis geradas da maneira descrita acima. Desta maneira, se nos limitarmos a superfícies regulares em $\mathbb{R}^3$ teremos que deixar de lado muitas superfícies.

No entanto, P^2 e K^2 podem ser mergulhados em $\mathbb{R}^4$. Para garrafa de Klein K, consideremos a aplicação G : $\mathbb{R}^2 \rightarrow \mathbb{R}^4$ dada por

$$G(u,v) = \left((r.\cos v + a).\cos u, (r.\cos v + a).sen\, u, R.sen\, v.cos\, \frac{u}{2}, r.sen\, \frac{u}{2}\right).$$

Notemos que $G(u,v) = G(u + 2m\pi, 2n\pi - v)$, onde m e n são inteiros. Desta forma, G induz uma aplicação ψ da superfície que é obtida a partir do quadrado

$$[0, 2\pi]\ x\ [0, 2\pi] \subset \mathbb{R}^2$$

quando consideramos primeiro a reflexão de um de seus lados em relação ao centro deste lado e depois se faz a identificação dos lados opostos (ver figura seguinte). Podemos ver que tal conjunto é a garrafa de Klein, como foi apresentado no exemplo 6.4., se desprezamos uma metade aberta do toro no qual os pontos simétricos estão sendo identificados e observamos que ambos os processos fornecem a mesma superfície (ver figura seguinte).

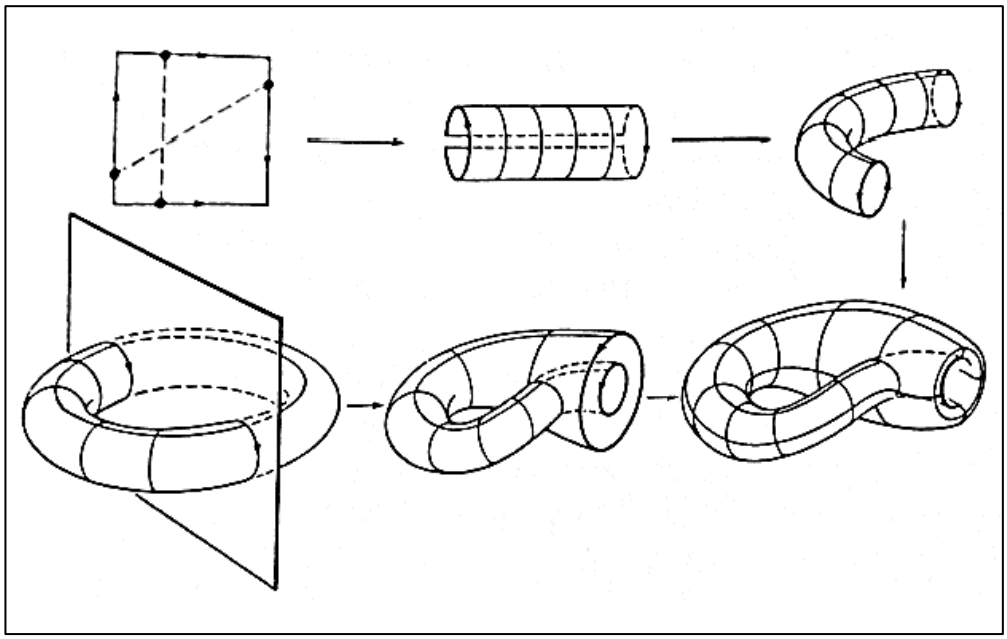

Figura 8: Imagem em $\mathbb{R}^3$ da garrafa de Klein por uma imersão

Desta forma, ψ é uma aplicação de K em $\mathbb{R}^4$. Observe também que

$$G(u + 4m\pi, v + 2m\pi) = G(u,v)$$

Temos ainda que G = $\psi \circ \pi_1 \circ \pi$, onde $\pi : \mathbb{R}^2 \to T$ é essencialmente a projeção natural do toro T e $\pi_1 : T \to K$ corresponde a identificar pontos antípodas em T. Temos que π e π_1 são, por definição de estruturas diferenciáveis em T e K, difeomorfismos locais. Logo, $\psi : K \to \mathbb{R}^4$ é diferenciável e o posto de dψ coincide com o posto de dG. Calculamos facilmente que este último é 2, então, ψ é uma imersão. Como K é compacto e ψ é injetiva, vemos sem dificuldades que ψ^{-1} é contínua em $\psi(K)$. Assim, ψ é um mergulho, como desejamos.

Para o plano projetivo P^2, considere a aplicação F : $\mathbb{R}^3 \to \mathbb{R}^4$ dada por

F(x, y, z) = ($x^2 - y^2$, xy, xz, yz).

Seja $S^2 \subset \mathbb{R}^2$ a esfera unitária com centro na origem de $\mathbb{R}^3$. A restrição $\varphi = F|\, S^2$é tal que φ(p) = φ(-p). Assim, φ induz uma aplicação

$\tilde{\varphi} : P^2 \to \mathbb{R}^4$ por $\tilde{\varphi}(\{p, -p\}) =$ φ(p).

Consideremos a parametrização x de S^2, para ver que φ (logo, $\tilde{\varphi}$) é uma imersão, como x(x, y) = (x, y, $+\sqrt{1 - x^2 - y^2}$), onde $x^2 + y^2 < 1$. Logo

$\varphi \circ x(x, y) = (x^2 - y^2, xy, xD, yD)$, D = $\sqrt{1 - x^2 - y^2}$.

Analisamos que a matriz de d($\varphi \circ x$) tem posto 2. Desta maneira, $\tilde{\varphi}$ é imersão.

Para ver que $\tilde{\varphi}$ é injetiva, faça

$x^2 - y^2 = a$, $xy = b$, $xz = c$, $yz = d$. (equações*)

Precisamos apenas mostrar que, sob a condição $x^2 + y^2 + z^2 = 1$, as equações acima têm apenas duas soluções que são da forma (x, y, z) e (- x, - y, - z). Podemos então escrever

$x^2 d = bc, y^2 c = bd, z^2 b = cd, x^2 - y^2 = a,\ \ x^2 + y^2 + z^2 = 1$ (equações**), onde as três primeiras equações vêm das três últimas equações*.

Se um dos números b, c, d é não nulo, as equações ** nos dão x^2, y^2, z^2 e as equações* determinam o sinal de duas coordenadas, uma vez dado o sinal da coordenada restante. Se b = c = d = 0, as equações* e a última equação** mostram que exatamente duas coordenadas serão nulas, e a restante será $\pm$1.Por compacidade, φ é um mergulho, e isto conclui o exemplo.

Uma variável diferenciável de dimensão n é um conjunto M munido de uma família de aplicações bijetivas x_α: $U_\alpha \to M$ de conjuntos abertos $U_\alpha \subset \mathbb{R}^n$ em M tal que

1. $U_\alpha x_\alpha(U_\alpha) = M$.

2. Para cada par α, β com $x_\alpha(U_\alpha) \cap x_\beta(U_\beta) = W = \emptyset$, temos que x_α^{-1}(W), x_β^{-1}(W) são conjuntos abertos em $\mathbb{R}^n$ e $x_\beta^{-1} \circ x_\alpha, x_\alpha^{-1} \circ x_\beta$ são aplicações diferenciáveis.

3. A família $\{U_\alpha, x_\alpha\}$ é máxima em relação às condições 1 e 2.

A família $\{U_\alpha, x_\alpha\}$, satisfazendo as condições 1 e 2 é chamada uma estrutura diferenciável em M. Sendo assim, podemos completar esta estrutura em uma máxima agregando a ela todas as possíveis parametrizações que, junto com alguma parametrização da família $\{U_\alpha, x_\alpha\}$, satisfazem a condição 2. Podemos então dizer que uma variedade diferenciável é um conjunto munido de uma estrutura diferenciável.

OBSERVAÇÃO: Podemos definir em M uma família de conjuntos abertos pela regra a seguir: V ⊂ M é um conjunto aberto se para todo α, $x_\alpha^{-1}(\mathrm{V} \cap x_\alpha(U_\alpha))$ é um conjunto aberto em $\mathbb{R}^n$. Notemos que uma tal família define uma topologia natural em M. Nesta topologia, as aplicações x_α são contínuas e os conjuntos $x_\alpha(U_\alpha)$ são abertos em M.

Para variedades diferenciáveis, as definições de aplicações diferenciáveis e de vetor tangente se generalizam. Sabemos que o espaço tangente é agora um espaço vetorial n-dimensional. As definições de diferencial e orientabilidade também se estendem imediatamente para esta situação mais geral.

Uma variedade Riemanniana é uma variedade diferenciável n-dimensional M munida de uma escolha de um produto interno $\langle\ ,\ \rangle_p$ em cada $T_pM, p \in M$, que varia diferenciavelmente com p no seguinte sentido. Para alguma, ou melhor, para todas as parametrizações $x_\alpha : U_\alpha \to M$ com $p \in x_\alpha(U_\alpha)$, as funções $g_{ij}(u_1, \dots, u_n) = \left\langle \frac{\partial}{\partial u_i}, \frac{\partial}{\partial u_j} \right\rangle, i, j = 1, \dots, n$, são diferenciáveis em $x_\alpha^{-1}(p)$; aqui $(u_1, \dots, u_n)$ são as coordenadas de $U_\alpha \subset \mathbb{R}^n$.

Estrutura Riemanniana (ou métrica Riemanniana) em M é o nome que se dá a família diferenciável $\{\langle\ ,\ \rangle_p, p \in M\}$. Para o caso das superfícies utilizamos a notação tradicional $g_{11} = E, g_{12} = g_{21} = F, g_{22} = G$.

A extensão das noções da geometria intrínseca a variedades Riemannianas não é tão direta quanto no caso das variedades diferenciáveis.

Definamos primeiramente a noção de derivada covariante para variedades Riemannianas. Para isto, seja x : U → M uma parametrização com coordenadas $(u_1, \dots, u_n)$ e coloque $x_i = \frac{\partial}{\partial u_i}$. Desta forma, $g_{ij} = \langle x_i, x_j \rangle$.

Desejamos definir a derivada covariante D_w^v de um campo de vetores v com relação a um campo de vetores w. Primeiramente, ela deve ter as propriedades distributivas da derivada covariante tradicional. Assim, se u, v, w são campos de vetores em M e f, g são funções diferenciáveis em M, queremos

$$D_{fu+gw}(v) = fD_u^v + gD_w^v, (*)$$

$$D_u(fv + gw) = fD_u^v + \frac{\partial \mathrm{f}}{\partial u}v + gD_u^w + \frac{\partial \mathrm{g}}{\partial u}w, (**)$$

onde $\frac{\partial \mathrm{f}}{\partial u}$, por exemplo, é uma função cujo valor em $p \in M$ é a derivada $(f \circ \alpha)'(0)$ da restrição de f a uma curva $\alpha : (-\varepsilon, \varepsilon) \to M, \alpha(0) = p, \alpha'(0) = u$.

As equações (*) e (**) mostram que a derivada covariante D fica inteiramente definida se conhecemos seus valores em uma base de vetores

$$D_{x_i}x_j = \sum_{k=1}^{n} \Gamma_{ij}^k x_k, \quad i, j, k = 1, \dots, n,$$

onde os coeficiente Γ_{ij}^{k} são funções ainda a determinar.

Em segundo lugar, queremos que os Γ_{ij}^{k} sejam simétricos em i e j ($\Gamma_{ij}^{k} = \Gamma_{ji}^{k}$); isto é

$$D_{x_i}x_j = D_{x_j}x_i \text{ para todo } i \text{ e } j. \ (***)$$

Em terceiro lugar, faremos com que a lei do produto seja válida; isto é,

$$\frac{\partial}{\partial u_k}\langle x_i, x_j\rangle = \langle D_{x_k}x_i, x_j\rangle + \langle x_i, D_{x_k}\, x_j\rangle. \ (****)$$

Segue-se das equações $(***)$ e $(****)$ que:

$$\frac{\partial}{\partial u_k}\langle x_i, x_j\rangle + \frac{\partial}{\partial u_i}\langle x_j, x_k\rangle - \frac{\partial}{\partial u_j}\langle x_k, x_i\rangle = 2\langle D_{x_i}x_k, x_j\rangle,$$

ou, de forma equivalente,

$$\frac{\partial}{\partial u_k}g_{ij} + \frac{\partial}{\partial u_i}g_{jk} - \frac{\partial}{\partial u_j}g_{ki} = 2\sum_l \Gamma_{ik}^{l} g_{lj}.$$

Sabendo que $\det(g_{ij}) \neq 0$, podemos resolver este último sistema e obtermos os Γ_{ij}^{k} como funções da métrica Riemanniana g_{ij} e de suas derivadas. Se pensarmos em g_{ij} como uma matriz e escrevermos a sua inversa como g^{ij}, a solução do sistema acima é

$$\Gamma_{ij}^{k} = \frac{1}{2}\sum_l g^{kl}\left(\frac{\partial g_{il}}{\partial u_j} + \frac{\partial g_{jl}}{\partial u_i} - \frac{\partial g_{ij}}{\partial u_l}\right).$$

Desta forma, dada a métrica Riemanniana em M, existe uma única derivada covariante em M, também conhecidas como conexão de Levi-Civita da estrutura Riemanniana dada, satisfazendo as equações apresentadas $(*,**,***,****)$.

6.2 A Faixa de Möbius como Espaço Quociente

Seja $I^2 \subset R^2$ com a topologia induzida (quando em f: X → Y sobrejetiva, temos um V ⊂ Y tal que a inversa de f(V) pertence a topologia) pela topologia usual de R^2. Consideremos em I^2 a relação de equivalência:

(x, y) ~ (x_1, y_1) ⇔ (x, y) = (x_1, y_1) ou (0, y) ~ (1, 1 − y), para todo (x, y), (x_1, y_1) ∈ I^2

Observemos que se $x \neq 0, 1$, então $[(x, y)] = \{(x, y)\}$ e $[(0, y)] = [(1,1 - y)]$. Em particular,é $[(0, 0)] = [(1, 1)]$ e $[(0, 1)] = [(1, 0)]$. Então, $\prod : I^2 \to (I^2/\sim)$ é uma identificação. Note que $\prod$ é bijetiva salvo para $(0,y)$ e $(1,1 - y)$ e $(I^2/\sim) \cong M$, onde M é a faixa de Möbius.

6.3 O Toro como Espaço Quociente

Seja $I^2 \subset R^2$ com a topologia induzida pela topologia usual de R^2. Consideremos em I^2 a relação de equivalência:

$(x,y) \sim (x_1,y_1) \Leftrightarrow (x,y) = (x_1,y_1)$ ou $(0,y) \sim (1,y)$ e $(x,0) \sim (x,1)$, para todo (x,y), $(x_1,y_1) \in I^2$

Observemos que se $x \neq 0, 1$, então $[(x,y)] = \{(x,y)\}$ e $[(0,y)] = [(1,y)]$ e se $y = 0$, então $[(x,0)] = [(x,1)]$. Em particular, $[(0,0)] = [(1,0)] = [(0,1)] = [(1,1)]$. Então, $\prod : I^2 \to (I^2/\sim)$ é uma identificação. Note que $\prod$ é bijetiva salvo para $(0,y)$, $(1,y)$, $(x,0)$ e $(x,1)$ e $(I^2/\sim) \cong S^1 x\, S^1$.

6.4 A Garrafa de Klein

Seja $I^2 \subset R^2$ com a topologia induzida pela topologia usual de R^2. Consideremos em I^2 a seguinte relação de equivalência:

$(x,y) \sim (x_1,y_1) \Leftrightarrow (x,y) = (x_1,y_1)$, ou $(0,y) \sim (1,y)$ e $(x,0) \sim (1 - x,1)$, para todo (x,y), $(x_1,y_1) \in I^2$.

Se x, y $\neq 0, 1$, então $[(x,y)] = \{(x,y)\}$ e $[(0,y)] = [(1,y)]$ e $[(x,0)] = [(1 - x,1)]$. Em particular, $[(0,0)] = [(1,0)] = [(0,1)] = [(1,1)]$. Então, $\prod : I^2 \to (I^2/\sim)$ é uma identificação. Note que $\prod$ é bijetiva salvo para $(0,y)$, $(1,y)$, $(x,0)$ e $(1 - x,1)$.

$(I^2/\sim)$ é chamada garrafa de Klein. A garrafa de Klein contém uma faixa de *Möbius.*

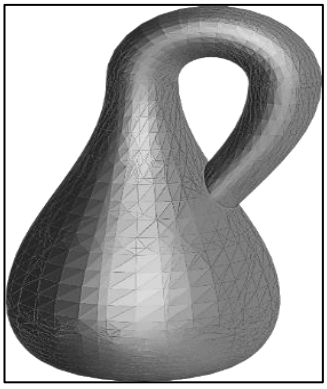

Figura 9: Garrafa de Klein

7 CONSIDERAÇÕES FINAIS

Este trabalho trouxe um maior conhecimento sobre a construção dos números inteiros, racionais e reais, assim como suas operações e relações de ordem. Estudamos os espaços vetoriais em classes de equivalência, analisando teoremas e definições. Observamos também as superfícies abstratas, com seus conceitos e exemplos de planos projetivos reais e garrafas de Klein, proporcionando um maior esclarecimento a respeito do assunto.

REFERÊNCIAS

FERREIRA, Jamil. **A Construção dos Números.** Rio de Janeiro: Sociedade Brasileira de Matemática, 2013.

CARMO, Manfredo Perdigão do; ROITMAN, Pedro. **Geometria diferencial de curvas e superfícies.** Rio de Janeiro: Sociedade Brasileira de Matemática, 2012.

BUENO, Hamilton Prado. **Álgebra linear:** um segundo curso. Rio de Janeiro: Sociedade Brasileira de Matematica, 2006.

COELHO, Flávio Ulhoa; LOURENÇO, Mary Lilian. **Um Curso de álgebra linear.** 2. ed. rev. e ampl. São Paulo: EDUSP, 2010.

APÊNDICE A – DEFINIÇÃO

Relação de equivalência: Seja dado um conjunto *A* e uma relação *R* sobre ele. Diz-se que *R* é uma relação de equivalência se possuir as seguintes propriedades:

1. Reflexiva: aRa, para todo $a \in A$;
2. Simétrica: se $a, b \in A$, e aRb, então bRa;
3. Transitiva: para $a, b, c \in A$, se aRb e bRc, então aRc.

Isomorfismo: Quando em T: X→Y, tivermos dim X = dim Y e T é bijetora.

Difeomorfismo: Quando uma aplicação f: U→V for uma bijeção diferenciável e sua inversa também.

Espaço métrico: Uma métrica sobre um conjunto X é uma função d: X×X → IR que associa a cada par ordenado de elementos x, y ∈ X um número real d(x, y) chamado a distância de x a y, de modo que se tenha, para todos x, y, z ∈ X:

d.1) d(x, x) = 0

d.2) Se x ≠ y então d(x, y) > 0

d.3) d(x, y) = d(y, x) (Simetria)

d.4) d(x, z) ≤ d(x, y) + d(y, z) (Desigualdade Triangular)

Um conjunto X munido de uma métrica d (fixada) é chamado espaço métrico.

Homeomorfismo: Sendo M e N espaços métricos, um homeomorfismo de M sobre N é uma bijeção contínua f: M→N, cuja inversa f^{-1}: N→M também o é.

Plano projetivo real: É o conjunto P^2 das retas de R^3 que passam pela origem. É um exemplo de superfície abstrata.

Imersão: Diz-se que f: M → N é imersão se qualquer p que pertença a M for um ponto regular para f, ou seja, a derivada de f em $TM_p \to TN_{f(p)}$ é injetiva para cada p pertencente a M.

Mergulho: Para f ser mergulho precisa primeiramente ser imersão e também ser homeomorfismo de M sobre um subespaço f(M) contido em N.

Métrica Riemanniana: É uma correspondência que associa a cada ponto p pertencente a M, um produto interno no espaço tangente TM_p.