O Corpo completo dos Números Reais

Márcio Nascimento da Silva

15 de janeiro de 2009

Resumo

Neste trabalho definimos uma estrutura algébrica chamada **corpo** e a partir de fatos elementares (axiomas), deduzimos certas propriedades (teoremas). Com mais algumas definições chegaremos até o conceito de corpo completo e veremos que esse tipo de estrutura algébrica é "muito parecida" com o conjunto dos números reais. Boa parte deste trabalho é praticamente uma transcrição de parte do terceiro capítulo de [1], com alguns comentários que tentam deixar mais claro os exemplos e conceitos ali apresentados.

1 Grupos

Seja G um conjunto não vazio e $*$ uma operação em G que satisfaz os seguintes axiomas:

(G1) (Associatividade) Dados $x, y, z \in G$, tem-se $x * (y * z) = (x * y) * z$.

(G2) Existe em G um elemento σ tal que $x * \sigma = x$ para qualquer $x \in G$.

O elemento σ é chamado ***elemento neutro de*** G ***com relação a operação*** $*$.

(G3) Para cada $x \in G$, existe um outro elemento, $x' \in G$ tal que $x * x' = \sigma$.

O elemento x' é chamado ***simétrico de*** x ***com relação a operação*** $*$.

Nessas condições o par $(G, *)$ é chamado ***grupo***. Quando, além disso, tem-se

(G4) (Comutatividade) $x * y = y * x$ para quaisquer $x, y \in G$

Dizemos que $(G, *)$ é um grupo ***comutativo*** ou ***abeliano***.

Exemplo 1.1 *Considere o conjunto dos números inteiros* $\mathbb{Z} = \{0, \pm 1, \pm 2, \pm 3, \ldots\}$ *e a operação de adição.*

Como já sabemos, vale a associatividade e a comutatividade. Além disso, o elemento neutro de $\mathbb{Z}$ *é* $\sigma = 0$ *e para cada elemento* $x \in \mathbb{Z}$ *o seu simétrico é* $-x$*. Desta forma,* $\mathbb{Z}$ *é um grupo comutativo.*

■

Exemplo 1.2 *Considere o conjunto as matrizes* $\mathbb{M}(n, n)$ *com entradas reais e a operação de multiplição de matrizes.*

A associatividade é válida, uma vez que para quaisquer matrizes M, N, P*, temos* $M.(N.P) = (M.N).P$*. O elemento neutro para esta operação é a matriz identidade* $I_{n \times n}$*. No entanto, nem todo elemento de* $\mathbb{M}(n, n)$ *possui simétrico, isto é, dada uma matriz* M*, pode não existir uma matriz* M' *tal que* $M.M' = I$*. Sendo assim,* $(\mathbb{M}(n, n), \cdot)$ *não é um grupo.*

Exemplo 1.3 *Considere o conjunto de polinômios de grau 1, isto é,*

$$G = \{f : \mathbb{R} \longrightarrow \mathbb{R} \; ; \; f(x) = ax + b, \; a, b \in \mathbb{R}, a \neq 0\}$$

e a operação de composição de funções.

1. *Dadas $f, g, h \in G$, temos*

$$[(f \circ g) \circ h](x) = (f \circ g)(h(x)) = f(g(h(x))) = f((g \circ h)(x)) = [f \circ (g \circ h)](x)$$

2. *Seja $e(x) = x$. Então para qualquer $f \in G$, temos:*

$$(f \circ e)(x) = f(e(x)) = f(x)$$

   Assim, o elemento neutro de G é a função identidade $e(x) = x$.

3. *Dado um elemento $f \in G$, temos, $f(x) = ax + b$. Vejamos se existe $\tilde{f}$ tal que*

$$f \circ \tilde{f} = e$$

   Seja $\tilde{f}(x) = Ax + B$. Então

$$(f \circ \tilde{f})(x) = f(Ax + B) = a(AX + B) + b = aAx + aB + b$$

   Queremos que

$$aAx + aB + b = x$$

   Então $aA = 1$ e $aB + b = 0$. Desta forma, $A = 1/a$ e $B = -b/a$. Assim,

$$\tilde{f}(x) = \frac{1}{a}x - \frac{b}{a}$$

   é o simétrico de $f(x) = ax + b$.

Temos, então, que G é um grupo. No entanto, G não é comutativo, uma vez que se

$$f(x) = ax + b \qquad \text{e} \qquad g(x) = cx + d$$

temos

$$(f \circ g)(x) = f(g(x)) = a(cx + d) + b = acx + (ad + b)$$
$$(g \circ f)(x) = g(f(x)) = c(ax + b) + d = acx + (bc + d)$$

portanto, em geral, $f \circ g \neq g \circ f$.

■

2 Corpos

Seja K um conjunto não vazio no qual estão definidas duas operações $*$ e $\diamond$ (chamadas adição e multiplicação) tais que:

1. $(K, *)$ é um grupo comutativo;
2. Valem os seguintes axiomas de multiplicação

   (M1) Se $x, y, z \in K$ então $(x \diamond y) \diamond z = x \diamond (y \diamond z)$. (Associatividade)

(M2) Existe $e \in K$ tal que $x \diamond e = x$ para qualquer $x \in K$. (Elemento Neutro)

(M3) Para cada $x \in K$, $x \neq \sigma$, existe $\overline{x} \in K$ tal que $x \diamond \overline{x} = e$. (Inverso Multiplicativo)

(M4) Para quaisquer $x, y \in k$, temos $x \diamond y = y \diamond x$ (Comutatividade)

3. Vale o seguinte axioma de distributividade

   (D1) Dados $x, y, z \in K$, temos:

$$x \diamond (y * z) = x \diamond y * x \diamond z$$

Nessas condições, $(K, *, \diamond)$ é chamado ***corpo***, que denotaremos simplesmente por K. Já que por definição, $(K, *)$ é um grupo comutativo, chamaremos K de ***grupo abeliano aditivo***. Com relação a multiplicação, vemos que σ **não** possui inverso multiplicativo, no entanto, qualquer outro elemento possui. Neste caso, $K - \{\sigma\}$ é um grupo comutativo com relação a multiplicação, ou simplesmente dizemos que $K - \{\sigma\}$ é um ***grupo abeliano multiplicativo***.

Exemplo 2.1 $(\mathbb{Q}, +, \cdot)$ *é um corpo.*

Exemplo 2.2 *Considere o conjunto* $\mathbb{Z}_2 = \{\overline{0}, \overline{1}\}$, *onde*

$$\overline{0} = \{0, \pm 2, \pm 4, \pm 6, \ldots\}$$

$$\overline{1} = \{\ldots, -5, -3, -1, 1, 3, 5, \ldots\}$$

isto é, $\mathbb{Z}_2$ *é uma partição de* $\mathbb{Z}$. *Defina em* $\mathbb{Z}_2$ *a soma da seguinte forma:*

$$\overline{0} + \overline{0} = \overline{0} \qquad \overline{0} + \overline{1} = \overline{1} \qquad \overline{1} + \overline{0} = \overline{1} \qquad \overline{1} + \overline{1} = \overline{0}$$

Já o produto, definimos por

$$\overline{0}.\overline{0} = \overline{0} \qquad \overline{0}.\overline{1} = \overline{0} \qquad \overline{1}.\overline{0} = \overline{0} \qquad \overline{1}.\overline{1} = \overline{1}$$

Nessas condições, $(\mathbb{Z}_2, +, \cdot)$ *é um corpo.*

$\blacksquare$

Exercícios

1. Defina a *diferença* no corpo K por $x - y = x + (-y)$

   (a) Mostre que $x - y = z \Longleftrightarrow x = y + z$.

   (b) Mostre que o elemento neutro de K com relação a adição é único.

   (c) Mostre que cada elemeto de K possui um único simétrico.

   (d) Mostre que se $x + z = y + z$ então $x = y$ (Lei do corte para adição).

2. Defina a *divisão* no corpo K por $x/y = x.\overline{y}$. Considere σ o elemento neutro da adição.

   (a) Mostre que se $y \neq \sigma$ então $x/y = z \Longrightarrow x = y.z$

   (b) Mostre que se $z \neq \sigma$ e $x.z = y.z$ então $x = z$ (Lei do corte para multiplicação).

   (c) Mostre que o elemento neutro de K com relação a multiplicação é único.

   (d) Mostre que cada elemeto de K diferente de σ possui um único inverso multiplicativo.

3. Mostre que num corpo K, se $x.y = 0$ então $x = 0$ ou $y = 0$.

4. Mostre que num corpo K,

   (a) $(-x).y = x.(-y) = -(x.y)$

   (b) $(-x).(-y) = x.y$

5. Mostre que $\mathbb{R}, \mathbb{Q}$ são corpos.

2.1 Corpos Ordenados

Um *Corpo Ordenado* é um corpo K, no qual está contido um subcojunto (próprio) $P \subset K$ para o qual valem as seguintes condições:

(P1) P é fechado com relação a adição e a multiplicação, isto é, se $x, y \in P$ então $x + y \in P$ e $x.y \in P$.

(P2) Dado um elemento qualquer de K, então: ou $x = \sigma$ ou $x \in P$ ou $-x \in P$, onde σ é o elemento neutro da adição.

Se K é um corpo ordenado, então podemos definir o conjunto $-P$ formado pelos elementos $-x$ tal que $x \in P$ e assim

$$K = P\dot{\cup}(-P)\dot{\cup}\{\sigma\}$$

Observe ainda que o elemento neutro da operação adição **não pertence** a P.

Proposição 2.1 *Seja K um corpo ordenado. Se $a \neq \sigma$ e $a \in K$ então $a^2 \in P$.*

Prova: De fato, sendo $a \neq \sigma$ então $a \in P$ ou $-a \in P$. Daí $a.a \in P$ ou $(-a).(-a) \in P$. Como $(-a).(-a) = a.a$, segue que, de qualquer forma, $a.a = a^2 \in P$.

■

Proposição 2.2

Exemplo 2.3 $(\mathbb{Q}, +, \cdot)$ *é um corpo ordenado.*

De fato, considere $P = \{p/q \in \mathbb{Q}\ ;\ p.q \in \mathbb{N}\}$. Se x, y são elementos quaisquer em $\mathbb{Q}$, temos

(P1)

$$x + y = \frac{p}{q} + \frac{r}{s} = \frac{ps + rq}{qs}$$

Sendo $(ps + rq)(qs) = pqs^2 + rsq^2$ e $pq, rs \in \mathbb{N}$, segue que $(ps + rq)(qs) \in \mathbb{N}$ uma vez que $s^2 \in \mathbb{N}$. Logo, $x + y \in \mathbb{Q}$.

$$x.y = \frac{p}{q}.\frac{r}{s} = \frac{p.r}{q.s}$$

Como $(pr).(qs) = (pq).(rs)$ e $pq, rs \in \mathbb{N}$, segue que $xy \in \mathbb{Q}$.

(P2) *Seja $p/q \in \mathbb{Q}$ e suponha que $p/q \notin \mathbb{Q}$. Então $p.q \notin \mathbb{N}$, isto é, $p.q \leq 0$. Desta forma $p.q = 0$ ou $p.q < 0$. Se $p.q < 0$ entao $(-p).q > 0$, ou seja, $(-p).q \in \mathbb{N}$ e portanto $(-p)/q \in P$. Mas então $-(p/q) \in P$.*

Veja que nesse exemplo, o conjunto P é exatamente $\mathbb{Q}_+^*$.

$\blacksquare$

Exemplo 2.4 $(\mathbb{Z}_2, +, \cdot)$ *não é um corpo ordenado.*

Com efeito, os subconjuntos de $\mathbb{Z}_2$ são:

$$\varnothing \qquad \{\overline{0}\} \qquad \{\overline{1}\} \qquad \mathbb{Z}_2$$

assim, a única possibilidade para P é:

$$P = \{\overline{1}\}$$

Mas, como já vimos, $\overline{1} + \overline{1} = \overline{0} \notin P$.

$\blacksquare$

Dado um corpo ordenado K e dois elementos quaisquer $x, y \in P$, temos que $-y \notin P$. Logo $x + (-y)$ pode não pertencer a P. Quando isso ocorrer, escrevemos $x - y \notin P$. Denotaremos essa **não pertinência** com a seguinte simbologia:

$$x < y \qquad \text{ou} \qquad y > x$$

Chamaremos o símbolo $<$ de **menor que** e o símbolo $>$ de **maior que**. Assim, dados x, y elementos de um corpo ordenado K, se $x - y \notin P$ então

x é menor que y
ou
y é maior que x

Se σ é o elemento neutro de K com relação a operação de adição, então usaremos essa simbologia para dizer se um dado elemento $x \in K$ pertence ou não a P:

Se $x \in P$, então escreveremos $x > \sigma$
Se $x \notin P$, escreveremos $x < \sigma$

Observação 2.1 (Os corpos ordenados se manifestam no dia-a-dia!)

Suponha que você encontra na rua o atleta Oscar (ex-jogador de basquete da seleção brasileira) e o artilheiro Romário. Por quê dizemos que o Oscar é maior que o Romário? Primeiro, estamos associando a cada um deles um número racional chamado ***altura****. Suponha que a altura do Oscar seja $2,10m$ e a do Romário $1,69m$. Estes números correspondem aos racionais $21/10$ e $169/100$ respectivamente. Como o conjunto dos números racionais é um corpo ordenado, então, temos condições de comparar dois números. Neste caso, como*

$$169/100 - 21/10 \notin P = \mathbb{Q}^*_+$$

então podemos dizer que

$$69/100 < 21/10 \qquad \text{ou} \qquad 21/10 > 69/100$$

isto é, podemos dizer que o Romário é menor que o Oscar ou que o Oscar é maior que o Romário.

Doravente, chamaremos P de ***conjunto dos elementos positivos de*** K e o conjunto $-P$ será chamado de ***conjunto dos elementos negativos de*** K. Chamaremos o elemento σ de ***zero*** e o denotaremos por 0. Se $x \in K$ é tal que $x > 0$ então diremos que x é um elemento ***positivo***. Caso $x < 0$, diremos que x é um elemento ***negativo***.

O elemento neutro da operação multiplicação será chamado ***um*** e denotado por 1. Dado $x \in K$, denotaremos o inverso multiplicativo de x por x^{-1} ou $1/x$.

As notações $x > 0$ e $x < 0$ nos dizem se o elemento $x \in K$ é positivo ou negativo, isto é, posiciona x dentro do conjunto

$$K = (-P) * \dot{\cup}\{0\}\dot{\cup}P^*$$

Chamaremos $x > y$ e $x < y$ de ***relações de ordem*** em K.

A relação de ordem $x < y$ em K satisfaz as seguintes propriedades:

(O1) (Transitividade) Se $x < y$ e $y < z$ então $x < z$.

Prova: Se $x < y$ e $y < z$ então $y - x, z - y \in P$. Daí, $(y - x) + (z - y) \in P$. Como $(y - x) + (z - y) = z - x$, segue $z - x \in P$ e portanto $x < z$.

(O2) (Tricotomia) Dados $x, y \in K$ ocorre exatamente um dos casos: $x = y$, $x < y$, $y < x$.

Prova: Dados $x, y \in K$ e sendo K ordenado, então ou $x - y = 0$ ou $x - y \in P$ ou $-(x - y) \in P$. Se $x - y = 0$ então $x = y$. Se $x - y \in P$ então $y < x$ e se $-(x - y) \in P$, então $y - x \in P$ e portanto $x < y$.

(O3) (Monotonicidade da adição) Se $x < y$ então para qualquer z, vale $x + z < y + z$.

Prova: Se $x < y$ então $y - x \in P$. Sendo 0 elemento neutro da adição e $0 = z + (-z)$ temos que $y + z + (-z) - x \in P$, isto é, $y + z - (x + z) \in P$ e portanto $x + z < y + z$.

(O4) (Monotonicidade da multiplicação) Sejam $x, y \in K$ tais que $x < y$. Se $0 < z$ então $x.z < y.z$. Se $z < 0$ então $y.z < x.z$.

Prova: Sendo $x < y$ segue que $y - x \in P$. Se $0 < z$ então $z \in P$. Daí, $(y - x).z \in P$, ou seja, $y.z - x.z \in P$ e portanto $x.z < y.z$.

Se $z < 0$ então $-z \in P$ e portanto $(y - x).(-z) \in P$. Isso significa que $xz - yz \in P$ e portanto $y.z < x.z$.

Exercícios

Seja K um corpo ordenado.

1. Mostre que $x < y$ é equivalente a $-y < -x$.
2. Mostre que $x < y$ e $x' < y'$ implicam em $x = x' < y + y'$.
3. Mostre que $0 < x < y$ e $0 < x' < y'$ implicam em $0 < x.x' < y.y'$.
4. Mostre que se $0 < x$ e $y < 0$ então $x.y < 0$.
5. Mostre que o inverso multiplicativo de um número positivo é também positivo.
6. Mostre que se $x < y$ e x, y ambos positivos, então $y^{-1} < x^{-1}$.

Observação 2.2 *A relação $x > y$ também é uma relação de ordem em K e valem propriedades análogas às da relação $x < y$ (as propriedades (O1) à (O4)).*

Uma outra relação de ordem que existente num corpo ordenado K é a relação $x \leq y$. Essa notação indica que $x < y$ ou $x = y$. Isso significa, então, que:

$$x \leq y \Longleftrightarrow y - x \in P \cup \{0\}$$

Diremos que $P \cup \{0\}$ é o conjunto dos ***elementos não-negativos*** de K. O denotaremos por K_+. Já o conjunto $-P \cup \{0\}$ será chamado conjunto dos ***elementos não-positivos*** de K e será denotado por K_-. Observe que

$$K_- \cup K_+ = K$$

no entanto, $\{K_-, K_+\}$ não é uma partição de K, uma vez que $K_- \cap K_+ \neq \varnothing$.

Esta relação satisfaz as seguinte propriedades:

1. (Transitividade) $x \leq y$, $y \leq z \Longrightarrow x \leq z$.
2. (Reflexividade) $x \leq x$ para qualquer $x \in K$
3. (Anti-simetria) $x \leq y$, $y \leq x \Longrightarrow x = y$
4. (Monotonicidade da adição) Se $x \leq y$ e $z \in K$, então $x + z \leq y + z$.
5. (Monotonicidade da multiplicação) Sejam $x, y \in K$ tais que $x \leq y$. Se $0 \leq z$, então $x.z \leq y.z$. Se $z \leq 0$, então $y.z \leq x.z$.

Observação 2.3 *Num corpo ordenado K, $x.0 = 0$ para qualquer $x \in K$. Com efeito,*

$$x.0 = x.(y + (-y)) = x.y + x.(-y) = x.y + (-x.y) = 0$$

Observação 2.4 *Num corpo ordenado K, o elemento neutro da multiplicação pertence a $K_+ \backslash \{0\}$, isto é, é positivo. De fato, suponha por absurdo que $1 \leq 0$. Então dado $x > 0$, temos*

$$x = 1.x \leq 0.x = 0 \Longrightarrow x \leq 0$$

2.1.1 Números Naturais

Dado um corpo ordenado K. Por um momento, voltemos a denotar o elemento neutro da multiplicação por e. Já sabemos que $0 < e$. Daí, somando e aos dois membros da desigualdade (já que $<$ é uma relação de ordem), temos:

$$e < e + e$$

Novamente somando e aos dois membros da última desigualdade, teremos

$$e + e < e + e + e \Longrightarrow e < e + e < e + e + e$$

Repetindo esse processo, teremos

$$e < e < e + e < e + e + e < e + e + e + e < \dots$$

Veja que dessa forma, $e, (e+e), (e+e+e), (e+e+e+e), \dots$ são todos elementos diferentes entre si. Considere o conjunto dos números naturais

$$\mathbb{N} = \{1, 2, 3, 4, \dots\}$$

Definindo a função $f : \mathbb{N} \longrightarrow K$ por

$$f(1) = e, f(2) = e + e, f(3) = e + e + e, f(4) = e + e + e + e, \ldots$$

temos uma bijeção do conjunto $\mathbb{N}$ sobre o subconjunto $f(\mathbb{N})$ de K. Isso significa dizer que dentro de um corpo ordenado existe um conjunto "muito parecido" com $\mathbb{N}$. Na verdade, dado um corpo ordenado K, costuma-se dizer que $K \supset \mathbb{N}$. Observe ainda que todos os elementos de $f(\mathbb{N})$ são positivos, isto é, $f(\mathbb{N}) \subset P$ se considerarmos P como o conjunto dos elementos positivos de K.

A função f também confirma que todo corpo ordenado é um conjunto infinito, uma vez que $f(\mathbb{N})$ é um subconjunto infinito.

2.1.2 Números inteiros

Uma vez que $f(\mathbb{N}) \subset P \subset K$, e $(K, +)$ é grupo, segue que para cada $f(n) \in f(\mathbb{N})$ existe $-f(n) \in K$, mas não pertencente a $f(\mathbb{N})$. Denotemos por $-f(\mathbb{N})$ o conjunto de todos os simétricos de elementos de $f(\mathbb{N})$. Desta forma, o conjunto $-f(\mathbb{N}) \cup \{0\} \cup f(\mathbb{N})$ é um grupo abeliano "muito parecido" com o conjunto dos números inteiros. Na verdade, se definirmos a função $g : \mathbb{Z} \longrightarrow K$ por

$$g(n) = \begin{cases} -f(n) & \text{se } n < 0 \\ 0 & \text{se } n = 0 \\ f(n) & \text{se } n > 0 \end{cases}$$

então g é uma bijeção do conjunto $\mathbb{Z}$ sobre o conjunto $g(\mathbb{Z}) = -f(\mathbb{N}) \cup \{0\} \cup f(\mathbb{N})$ e também dizemos que $\mathbb{Z} \subset K$.

2.1.3 Números Racionais

Sendo K um corpo ordenado, cada elemento (diferente de zero) de $g(\mathbb{Z})$ possui inverso multiplicativo. Também é fato que K é fechado para a multiplicação. Assim, dados $g(m), g(n) \in g(\mathbb{Z}) \subset K$, $g(n) \neq 0$, temos:

$$g(m), [g(n)]^{-1} \in K \Longrightarrow g(m).[g(n)]^{-1} = \frac{g(m)}{g(n)} \in K$$

Podemos, desta forma, considerar a função $h : \mathbb{Q} \longrightarrow K$ definida por

$$h\left(\frac{m}{n}\right) = \frac{g(m)}{g(n)}$$

ou seja, h é uma bijeção do conjunto $\mathbb{Q}$ no conjunto

$$h(\mathbb{Q}) = \left\{x \in K \ ; \ x = g(m).[g(n)]^{-1}, \ m, n \in \mathbb{Z}\right\}$$

Analogamente ao caso dos números naturais e inteiros, costuma-se dizer que um corpo ordenado K contém o conjunto dos números racionais $\mathbb{Q}$.

Proposição 2.3 *O conjunto $h(\mathbb{Q})$ é o menor subcorpo de um corpo ordenado K.*

Prova: Um subcorpo de um corpo K, como o próprio nome diz, é um corpo K' contido dentro de um corpo K. Desta forma, devemos mostrar inicialmente que $h(\mathbb{Q})$ é um corpo. De fato, se tomarmos dois elementos em $h(\mathbb{Q})$, a soma e o produto continuam em $h(\mathbb{Q})$ (verifique!). Desta forma, $h(\mathbb{Q})$ é fechado para adição e multiplicação e herda, naturalmente, as propriedades de K.

Agora provemos que $h(\mathbb{Q})$ é o menor subcorpo de K. Sendo K' um subcorpo de K, temos que $0, 1 \in K'$. Se $1 \in K'$ então por somas sucessivas, $(1+1+1...)$, $f(\mathbb{N}) \subset K'$. Mas para cada elemento de $f(\mathbb{N})$, seu simétrico deve pertencer também a K', isto é, $g(\mathbb{Z}) \subset K'$. Além disso, K' deve conter o inverso multiplicativo de cada elemento de $g(\mathbb{Z})$ (exceto o de 0, que não é definido), isto é, $h(\mathbb{Q}) \subset K'$. Logo, $h(\mathbb{Q})$ está contido em qualquer subcorpo de K. Como já vimos que $h(\mathbb{Q})$ é um subcorpo, então $h(\mathbb{Q})$ é o menor subcorpo de K.

$\blacksquare$

Proposição 2.4 (A desigualdade de Bernouilli) *Seja K um corpo ordenado e $n \in \mathbb{N}$. Se $x \geq -1$ então $(1+x)^n \geq 1 + nx$.*

Prova: Façamos indução sobre n. Se $n = 1$, então

$$(1+x)^1 = 1 + 1.x \geq 1 + 1.x$$

Se $n > 1$ suponha que $(1+x)^n \geq 1 + n.x$ e mostremos que

$$(1+x)^{n+1} \geq 1 + (n+1).x$$

Temos

$$\begin{aligned}
(1+x)^{n+1} &= (1+x)^n.(1+x) \\
&\geq (1+n.x).(1+x) \\
&= 1 + x + n.x + n.x^2 \\
&= 1 + (n+1)x + n.x^2 \\
&\geq 1 + (n+1).x
\end{aligned}$$

$\blacksquare$

2.1.4 Intervalos

Dado um corpo ordenado K, alguns conjuntos recebem notação especial. Sejam $a, b \in K$ com $a < b$.

1. (Intervalo aberto) $\{x \in K \ ; \ a < x < b\} = (a, b)$
2. (Intervalo fechado) $\{x \in K \ ; \ a \leq x \leq b\} = [a, b]$
3. (Intervalo aberto à direita) $\{x \in K \ ; \ a \leq x < b\} = [a, b)$
4. (Intervalo aberto à esquerda) $\{x \in K \ ; \ a < x \leq b\} = (a, b]$
5. $\{x \in K \ ; \ x \geq a\} = [a, +\infty)$
6. $\{x \in K \ ; \ x \leq b\} = (+\infty, b]$
7. $\{x \in K \ ; \ x > a\} = (a, +\infty)$
8. $\{x \in K \ ; \ x < b\} = (+\infty, b)$
9. $K = (-\infty, +\infty)$

Poderíamos considerar o caso em que $a = b$. Neste caso, o intervalo $[a, b] = [a, a] = \{a\}$ é chamado ***intervalo degenerado***.

Os intervalos do tipo (1) à (4) são chamados ***limitados*** e os demais ***ilimitados***. O símbolo $+\infty$ foi introduzido como uma maneira de indicar que um intervalo é ilimitado.

Proposição 2.5 *Todo invervalo limitado não degenerado possui infinitos elementos.*

Prova: Sejam $x, y \in K$ tais que $x < y$. Sendo 1 o elemento neutro da multiplicação, temos:

$$x + x < y + x \Longrightarrow \frac{1}{(1+1)}.x.(1+1) < \frac{1}{1+1}(y+x) \Longrightarrow x < \frac{1}{1+1}(y+x)$$

Analogamente

$$x < y \Longrightarrow y + x < y + y \Longrightarrow \frac{1}{1+1}y + x < \frac{1}{1+1}.y.(1+1) \Longrightarrow \frac{1}{1+1}(y+x) < y$$

Desta forma,

$$x < \frac{1}{1+1}(y+x) < y$$

Isto é, dados dois elementos quaisquer $x, y \in K$ com $x \neq y$, obtemos um terceiro, digamos, z, tal que $x < z < y$ onde $z = \dfrac{1}{1+1}(x+y)$. Se repertirmos o processo para x e z, obteremos z'. Se fizermos o mesmo para x e z' obteremos z'' e assim por diante. Podemos fazer isso infinitas vezes.

$\blacksquare$

2.1.5 Valor Absoluto

Um outro conceito que pode ser definido num corpo ordenado K é o de ***valor absoluto***. Dado $x \in K$, o valor absoluto (ou módulo) de x é denotado por $|x|$ e definido por

$$|x| = \begin{cases} x & \text{se } x \geq 0 \\ -x & \text{se } x < 0 \end{cases}$$

Com essa definição $|x| \in K_+$. De fato, se $x \geq 0$ então $|x| = x \geq 0$. Se $x < 0$ então $-x > 0$ e $|x| = -x > 0$. Observe ainda que $|x| = \max\{-x, x\}$. De fato, se $x > 0$ então $|x| = x$. Além disso $-x < 0$ e portanto, $-x < x$. Se $x < 0$, então $|x| = -x$ e $-x > 0$, isto é, $x < -x$. Nos dois casos, $|x|$ é o máximo valor entre $-x$ e x. Com isso, temos $|x| \geq x$ e $|x| \geq -x$ (ou equivalentemente, $-|x| \leq x$). Daí

$$-|x| \leq x \leq |x|$$

para qualquer $x \in K$.

Teorema 2.1 *Sejam a, x elementode de um corpo ordenado K. São equivalentes:*

(i) $-a \leq x \leq a$

(ii) $x \leq a$ *e* $-x \leq a$

(iii) $|x| \leq a$.

Prova:

$(i) \Longrightarrow (ii)$ $-a \leq x \leq a \Longrightarrow -a \leq x$ e $\underline{x \leq a}$. Daí, $a \geq -x$, ou seja, $\underline{-x \leq a}$.

$(ii) \Longrightarrow (iii)$ Sendo $x \leq a$ e $-x \leq a$, segue que $\max\{-x, x\} \leq a$, isto é, $|x| \leq a$.

$(iii) \Longrightarrow (i)$ Sendo $|x| = \max\{-x, x\}$ segue que $|x| \geq x$ e $|x| \geq -x$, isto é, $a \geq x$ (que equivale a $x \leq a$) e $a \geq -x$ (que equivale a $-a \leq x$). Assim, $-a \leq x \leq a$.

■

Teorema 2.2 *Seja ϵ um elemento positivo e a um elemento qualquer, ambos de um corpo ordenado K. As seguintes sentenças são equivalentes:*

(i) $x \in (a - \epsilon, a + \epsilon)$

(ii) $a - \epsilon < x < a + \epsilon$

(iii) $|x - a| < \epsilon$

Prova:

$(i) \Longrightarrow (ii)$ Segue da própria definição de intervalo.

$(ii) \Longrightarrow (iii)$ Se $a - \epsilon < x < a + \epsilon$ então somando $-a$ em todos os membros, temos

$$-\epsilon < x - a < \epsilon$$

e pelo teorema anterior,

$$|x - a| < \epsilon$$

$(iii) \Longrightarrow (i)$ Também pelo teorema anterior, $|x - a| < \epsilon \Longrightarrow -\epsilon < x - a < \epsilon$ e somando a a todos os membros, temos $a - \epsilon < x < a + \epsilon$ o que significa que $x \in (a - \epsilon, a + \epsilon)$.

■

Teorema 2.3 (Propriedades do Valor Absoluto) *Sejam x, y, z elementos quaisquer num corpo ordenado K. Valem as seguintes propriedades:*

(i) $|x + y| \leq |x| + |y|$

(ii) $|x.y| = |x|.|y|$

(iii) $|x| - |y| \leq \Big||x| - |y|\Big| \leq |x - y|$

(iv) $|x - z| \leq |x - y| + |y - z|$

Prova:

(i) *Já vimos que* $-|x| \leq x \leq |x|$ *e* $-|y| \leq y \leq |y|$. *Somando membro a membro, temos:*

$$-|x| - |y| \leq x + y \leq |x| + |y|$$

ou seja $-(|x| + |y|) \leq x + y \leq (|x| + |y|)$ *e portanto*

$$|x + y| \leq |x| + |y|$$

(*ii*) *Observe que* $|x| = x$ *ou* $|x| = -x$. *Como* K *é um corpo ordenado, segue que* $|x|^2 = x^2$. *Assim*

$$|x.y|^2 = (x.y)^2 = (x.y).(x.y) = (x.x).(y.y) = x^2.y^2 = |x|^2.|y|^2 = \ldots = (|x|.|y|)^2$$

Assim, temos duas possibilidades a princípio:

$$|x.y| = |x|.|y| \qquad \text{ou} \qquad |x.y| = -(|x|.|y|)$$

Como da definição de valor absoluto, $|x.y|, |x|, |y| \in K_+$ *e* $|x|, |y| \in K_+ \Longrightarrow |x|.|y| \in K_+$, *segue que ocorre, com certeza,* $|x.y| = |x|.|y|$.

(*iii*) *Inicialmente, pela definição de valor absoluto,*

$$\Big||x| - |y|\Big| = \max\{-(|x| - |y|), |x| - |y|\} \geq |x| - |y|$$

e temos a primeira desigualdade. Para ver a segunda desigualdade, observe que do item (*i*), *temos*

$$|x| = |x - y + y| \leq |x - y| + |y| \Longrightarrow |x| - |y| \leq |x - y|$$

$$|y| = |y - x + x| \leq |y - x| + |x| \Longrightarrow |y| - |x| \leq |y - x| \Longrightarrow -(|x| - |y|) \leq |y - x|$$

Por outro lado,

$$|x - y| = |(-1).(y - x)| = |-1|.|y - x| = 1.|y - x| = |y - x|$$

Daí

$$|x| - |y| \leq |x - y| \qquad \text{e} \qquad -(|x| - |y|) \leq |x - y|$$

Pelo Teorema 2.1, segue que

$$\Big||x| - |y|\Big| \leq |x - y|$$

(*iv*) *Usando o item* (*i*), *temos:*

$$|x - z| = |(x - y) + (y - z)| \leq |x - y| + |y - z|$$

■

2.1.6 Ínfimo e Supremo

Um subsconjunto X de um corpo ordenado K diz-se ***limitado superiormente*** quando existe $b \in K$ tal que $X \subset (-\infty, b]$. Se existe $a \in K$ tal que $X \subset [a, +\infty)$, dizemos que X é ***limitado inferiormente***. Se X é limitado inferiormente e superiormente, isto é, existem $a, b \in K$ tais que $X \subset [a, b]$, dizemos que X é ***limitado***.

Os elementos a, b citados acima são chamados ***cota inferior para*** X e ***cota superior para*** X, respectivamente.

Observação 2.5 *Considere o corpo dos números racionais* $\mathbb{Q}$. *O conjunto dos números naturais* $\mathbb{N}$ *é limitado inferiormente mas não superiormente, uma vez que* $\mathbb{N} \subset [1, +\infty)$. *Observe que qualquer* $a < 1$ *é uma cota inferior para* $\mathbb{N}$. *Já o conjunto dos números inteiros* $\mathbb{Z}$ *não é limitado nem superiormente nem inferiormente.*

Observação 2.6 *Dependendo do corpo K, $\mathbb{N}$ pode não ter um limitante superior. Vejamos no exemplo a seguir.*

Exemplo 2.5 *Considere o conjunto $\mathbb{Q}(t) = \{r(t) = p(t)/q(t)\}$ onde $p(t), q(t)$ são polinômios com coeficientes inteiros e q é não identicamente nulo. Tal conjunto é um corpo ordenado quando consideramos $r(t)$ positivo se, no polinômio $p.q$, o coeficiente de mais alto grau for positivo. Por exemplo, se $r(t) = (3x^2+x)/(2x-1)$, então $p(t).q(t) = 6x^3 - x^2 - x$ e o coeficiente de mais alto grau é $6 > 0$. Portanto, $r(t) \in P$. Claro, agora falta mostrar que realmente $\mathbb{Q}(t)$ é um corpo ordeando.*

Veja que $r(t) = t \in \mathbb{Q}(t)$, pois neste caso, $p(t) = t$ e $q(t) = 1$. Além disso, se considerarmos os polinômios da forma $n(t) = n$, temos $n(t) \in \mathbb{Q}(t)$. Daí, $u_n(t) = p(t) - n(t) = t - n \in \mathbb{Q}(t)$ e o coeficiente do termo de mais alto grau é sempre igual a 1. Portanto, $u_n(t) \in P$, isto é,

$$u_n(t) > 0 \Longrightarrow t - n > 0 \Longrightarrow t > n$$

para todo $n \in \mathbb{N}$. Dessa forma, em $\mathbb{Q}(t)$, o elemento $p(t)$ é uma cota superior para $\mathbb{N}$, ou seja, $\mathbb{N}$ é limitado superiormente.

Teorema 2.4 *Num corpo ordenado K, são equivalentes*

(i) *$\mathbb{N} \subset K$ limitado superiormente;*

(ii) *Dados $a, b \in K$, com $a > 0$, existe $n \in \mathbb{N}$ tal que $n.a > b$*

(iii) *Dado $a \in K$, $a > 0$, existe $n \in \mathbb{N}$ tal que $0 < 1/n < a$*

Quando num corpo ordenado K vale qualquer uma das condições do Teorema acima (portanto valem as três), dizemos que K é um ***corpo arquimediano***. Desta forma, como visto nos exemplos acima, $\mathbb{Q}$ é um corpo arquimediano e $\mathbb{Q}(t)$ não.

Agora vamos, finalmente, definir o ínfimo e o supremo de um subconjunto de um corpo ordenado K. Considere $X \subset K$ um subconjunto limitado superiormente. Quando existir a menor cota superior para X, ela será chamada ***supremo do conjunto*** X e denotamos por $\sup X$, isto é

$$\sup X = \min\{a \in K \ ; \ a \geq x, x \in X\}$$

Analogamente, se $X \subset K$ é limitado inferiormente, definimos o ***ínfimo de*** X sendo a maior cota inferior (quando existir!) de X, isto é,

$$\inf X = \max\{b \in K \ ; \ b \leq x, x \in X\}$$

Para $\sup X$, decorrem da definição

(i) Se $x \in X$ então $x \leq \sup X$.

(ii) Se $c \geq x$ para todo $x \in X$ então $c \geq \sup X$.

(iii) Se $c < \sup X$ então existe $x \in X$ tal que $c < x < \sup X$.

Analogamente, para $\inf X$,

(i) Se $x \in X$ então $x \geq \inf X$.

(ii) Se $c \leq x$ para todo $x \in X$, então $c \leq \inf X$.

(iii) Se $\inf X > c$ então existe $x \in X$ tal que $\inf X > x > c$.

Observe que $\sup X$ e $\inf X$ podem não pertencer a X. De fato, considere o intervalo $X = (a, b)$ de um corpo ordenado K. Então $\inf X = a \notin X$ e $\sup X = b \notin X$.

Seja X um conjunto não vazio. Dizemos que $a \in X$ é o ***elemento mínimo*** de X se $a \leq x$ para qualquer $x \in X$. Analogamente, se existe $b \in X$ tal que $x \leq b$ para qualquer $x \in X$, então b é o ***elemento máximo*** de X.

Observação 2.7 *Quando X possui um elemento mínimo a, então $a = \inf X$. Da mesma forma, se X possui um elemento máximo, digamos b, então $b = \sup X$. Reciprocamente, se $\inf X \in X$, então $\inf X$ é o menor elemento de X. O mesmo vale para o $\sup X$.*

Lema 2.1 (Lema de Pitágoras) *Não existe um número racional cujo quadrado seja igual a 2.*

Prova: Suponha, por absurdo, que existe $p/q \in \mathbb{Q}$ tal que $(p/q)^2 = 2$. Então $p^2 = 2q^2$. Considerando a decomposição em fatores primos de p e q temos

$$p = p_1.p_2.\cdots.p_n, \quad p_1 \leq p_2 \leq \ldots \leq p_n$$

$$q = q_1.q_2.\cdots.q_m, \quad q_1 \leq q_2 \leq \ldots \leq q_n$$

$$(p_1.p_2.\cdots.p_n)^2 = 2.(q_1.q_2.\cdots.q_m)^2$$

isto é,

$$p_1.p_1.p_2.p_2.\cdots.p_n.p_n = 2.q_1.q_1.q_2.q_2.\cdots.q_m.q_m$$

Portanto p^2 possui um número par de fatores primos iguais a 2, enquanto q^2 possui um número ímpar desses fatores. Absurdo.

■

Exemplo 2.6 *Seja $X \subset \mathbb{Q}$ o conjunto das frações do tipo $1/2^n$ com $n \in \mathbb{N}$. Observe que*

$$\frac{1}{2} > \frac{1}{2^2} > \frac{1}{2^3} > \ldots\ldots$$

Portanto, $1/2 > x$ para qualquer $x \in X$ e $1/2 \in X$, isto é, $1/2$ é uma cota superior para X que pertence a X. Isso significa que $1/2 = \sup X$. Com mais alguns passos, podemos mostrar que $0 = \inf X$ (vide [1], página 62).

■

Exemplo 2.7 *Existem conjuntos limitados de números racionais que não possuem supremo (ou ínfimo). Considere o corpo $\mathbb{Q}$ e o conjunto $X = \{x \in \mathbb{Q}\ ;\ x \geq 0 \text{ e } x^2 < 2\}$. Observe que $X \subset [0, 2]$, portanto, X é um conjunto limitado de números* ***racionais****. O supremo desse conjunto seria $\sqrt{2}$, mas este não é racional.*

Afirmação 1: *O conjunto X não possui elemento máximo.*

Provaremos essa afirmação verificando que dado $x \in X$, existe um número $x + r$ ainda pertence a X. Isso nos diz que ainda existe um elemento um "pouco mais a frente" ainda pertencente a X, ou seja, X não possui elemento máximo.

De fato, considere um número racional $r < 1$ tal que $0 < r < \dfrac{2 - x^2}{2x + 1}$ com $x \in X$. Observe que $x \geq 0$ e $x^2 < 2$ implica em $2 - x^2 > 0$ e $2x + 1 \geq 1$, portanto, $\dfrac{2 - x^2}{2x + 1} > 0$.

Temos:

$$r < 1 \Longrightarrow r^2 < r$$
$$r < \frac{2 - x^2}{2x + 1} \Longrightarrow r(2x + 1) < 2 - x^2$$

Portanto

$$(x + r)^2 = x^2 + 2xr + r^2 < x^2 + 2rx + r = x^2 + r(2x + 1) < x^2 + (2 - x^2) = 2$$

isto é, $x + r \in X$.

Afirmação 2: *O conjunto* $Y = \{y \in \mathbb{Q} \ ; \ y > 0 \text{ e } y^2 > 2\}$ *não possui elemento mínimo.*

Analogamente a Afirmação 1, provaremos esse fato verificando que dado um elemento $y \in Y$*, existe um outro um "pouco mais atrás" ainda pertencente a* Y.

Se $y^2 > 2$ *e* $y > 0$ *então* $y^2 - 2 > 0$ *e* $2y > 0$*, isto é,* $\dfrac{y^2 - 2}{2y} > 0$*. Logo, existe um racional* $r >$ *tal que* $0 < r < \dfrac{y^2 - 2}{2y}$*. Daí* $2yr < y^2 - 2$ *e*

$$(y - r)^2 = y^2 - 2yr + r^2 > y^2 - (y^2 - 2) + r^2 = r^2 + 2 > 2$$

Além disso, $\dfrac{y^2 - 2}{2y} = \dfrac{y}{2} - \dfrac{1}{y}$*, portanto* $y - r > y - \dfrac{y}{2} + \dfrac{1}{y} = \dfrac{y}{2} + \dfrac{1}{y} > 0$*. Assim*

$$(y - r) > 0 \qquad \text{e} \qquad (y - r)^2 > 0$$

ou seja, $y - r \in Y$.

Afirmação 3: *Se* $x \in X$ *e* $y \in Y$ *então* $x < y$.

Pela própria definição dos conjuntos X Y*, temos* $x^2 < 2 < y^2$ *para quaisquer* $x \in X$, $y \in Y$*. Como, além disso,* x, y *são positivos, segue que* $x^2 < y^2 \Longrightarrow x < y$.

Afirmação 4: *Não existe* $\sup X$ ***nos números racionais***.

Suponha, por absurdo, que existe $a = \sup X$*. Veja que* $a > 0$ *e não poderia ser* $a^2 < 2$*, pois do contrário,* $\sup X \in X$*, isto é,* $\sup X = \max X$*, mas* X *não possui elemento máximo.*

Suponha $a^2 > 2$*. Desta forma,* $a \in Y$*. Vimos na Afirmação 2, que* Y *não possui elemento mínimo, logo, existe* $b \in Y$ *tal que* $b < a$*. Usando a Afirmação 3, para qualquer* $x \in X$*, teríamos* $x < b < a$*, isto é, teríamos uma cota superior para* X *menor que* $a = \sup X$*. Contradição.*

Só resta dizer que $a^2 = 2$*. Isso também não ocorre, uma vez que não existe racional* a *tal que* $a^2 = 2$*. Logo, não existe* $\sup X$.

■

O exemplo acima deixa claro que se um corpo ordenado K é tal que todo subconjunto X limitado superiormente possui supremo, isto é, para todo $X \subset K$ existe $\sup X$, em particular, K contém $\mathbb{Q}$ (ou $h(\mathbb{Q})$) que contém $X = \{x \in \mathbb{Q} \ ; \ x \geq 0 \text{ e } x^2 < 2\}$. Como X é limitado superiormente e em K subconjuntos desse tipo possuem supremo, segue que existe $a = \sup X \in K$ tal que $a^2 = 2$. Denota-se a por $\sqrt{2}$.

Definição 2.1 *Um corpo ordenado diz-se **completo** quando todo subconjunto não vazio limitado superiormente possui supremo.*

Lema 2.2 *Seja K um corpo ordenado. Se K é completo, então é arquimediano.*

Prova: Considere um corpo não arquimediano qualquer K. Então em K o conjunto $\mathbb{N}$ (ou $f(\mathbb{N})$) é limitado superiormente. Se b é uma cota superior para $\mathbb{N}$ então $n \leq b$ para qualquer $n \in \mathbb{N}$, em particular, $n+1 \leq b$ para qualquer $n \in \mathbb{N}$ e portanto $n \leq b-1$ $\forall n \in \mathbb{N}$. Assim, se b é uma cota superior para $\mathbb{N}$ então $b-1$ também o é. Mas se $b-1$ o é, então $(b-1)-1$ também o é e assim sucessivamente. Portanto, não se pode determinar a menor cota superior e assim não existe $\sup \mathbb{N}$ em K. Assim, K não é completo.

■

Axioma 1 (Axioma Fundamental da Análise Matemática) *Existe um corpo ordenado completo. Ele será chamado conjunto dos números reais e será denotado por $\mathbb{R}$.*

3 Propriedades dos números reais

3.1 O elemento $\sqrt{2}$

Vimos que num corpo ordenado completo (que contém $\mathbb{Q}$!) existe um elemento positivo $a \notin \mathbb{Q}$ tal que $a^2 = 2$ e que será representado por $\sqrt{2}$. Este número é único. De fato, suponha $a^2 = b^2$ com $a \neq b$. Então

$$0 = a^2 - b^2 = (a-b)(a+b) \Longrightarrow a-b=0 \qquad \text{ou} \qquad a+b=0$$

Mas então $a = b$ ou $a = -b$. Ocorre que se $a = -b$ então um deles não é positivo, logo, $a = b$.

3.2 Os números irracionais

Sendo $\mathbb{R}$ um corpo completo e $\mathbb{Q} \subset \mathbb{R}$, existem elementos em $\mathbb{R}$ que não estão em $\mathbb{Q}$. Tais elementos formam o conjunto dos números irracionais $\mathbb{R} - \mathbb{Q}$. Desta forma, $\sqrt{2}$ é irracional.

Raiz n-ésima

Dados $a > 0$ elemento de $\mathbb{R}$ e $n \in \mathbb{N}$, existe um único número real $b > 0$ tal que $b^n = a$. O número b chama-se raiz n-ésima de a e é representado pelo símbolo $\sqrt[n]{a}$. Qualquer número natural que não possua uma raíz n-ésima também natural, é um número irracional.

Os números racionais e irracionais estão "espalhados" por toda parte do conjunto dos números reais.

Definição 3.1 *Um conjunto $X \subset \mathbb{R}$ chama-se denso em $\mathbb{R}$ quando todo intervalo aberto (a, b) contém algum ponto de X.*

Exemplo 3.1 *Seja $X = \mathbb{Z}^C$. Dado um intervalo qualquer em $\mathbb{R}$, digamos, (a, b), então*

$$(a,b) \cap \mathbb{Z} = \{[a]+1, [a]+2, \ldots, [b]\} \qquad \text{ou} \qquad (a,b) \cap \mathbb{Z} = \varnothing$$

Como (a, b) possui infinitos elementos, segue que $(a, b) \cap \mathbb{Z}^C$ é sempre não vazio.

Teorema 3.1 *Os conjuntos $\mathbb{Q}$ e $\mathbb{R} - \mathbb{Q}$ são densos em $\mathbb{R}$.*

Referências

[1] LIMA, Elon Lages. CURSO DE ANÁLISE, vol. 1. Publicação IMPA, Rio de Janeiro, 1995.

[2] ÁVILA, Geraldo. INTRODUÇÃO À ANÁLISE MATEMÁTICA. 2ª ed. Edgard Blücher. São Paulo, 1999.

[3] GONÇALVES, Adilson. INTRODUÇÃO À ÁLGEBRA. 4ª ed. Publicação IMPA, Rio de Janeiro, 1999.

[4] LEQUAIN, Yves. GARCIA, Arnaldo. ELEMENTOS DE ÁLGEBRA. Publicação IMPA, Rio de Janeiro, 2002.