# Cortes de Dedekind

**Gustavo H. M. Garcia**

Email: gustavo-marques1@hotmail.com

## Resumo

*O presente trabalho faz uma introdução e apresenta os principais resultados relacionados a teoria de Cortes de Dedekind. O conceito de Cortes de Dedekind é abordado para construir o conjunto dos números reais. Após, fala-se sobre cardinalidade e números transcendentais. O foco é direcionado para a apresentação dos resultados, muitas vezes abstendo demonstrações.*

## Introducão

Os números racionais são todos aqueles da forma $q = \frac{m}{n}$, com $m \in \mathbb{Z}$ e $n \in \mathbb{N}^*$. Considere, agora, um triângulo retângulo de catetos de comprimento $1$ e denote por $p$ o comprimento da hipotenusa desse triângulo. Pelo Teorema de Pitágoras, $p^2 = 2$. Escrevemos então $p = \sqrt{2}$.
Agora, suponha que $p \in \mathbb{Q}$. Logo existem $m \in \mathbb{Z}$ $n \in \mathbb{N}^*$, primos entre sí, tais que $p = \frac{m}{n}$. Logo $p^2 = 2 = \frac{m^2}{n^2}$, portanto $2n^2 = m^2$. Daí concluímos que $m$ e $n$ são pares, contradizendo a hipótese inicial.
Esse simples problema nos conta que existem outros números além dos racionais. O conjunto desses números é chamado de Irracionais. Da união desse dois últimos conjuntos é formado o conjunto dos Números Reais. Uma maneira de tratar os números irracionais é defini-los como certos subconjunto dos números racionais chamados cortes de Dedekind.
Essa forma de construção também é capaz de incluir os números racionais, portanto podemos definir os números Reais a partir do conjunto de todos os cortes. A forma como isso é feito faz com que muitas propriedades dos números reais sejam decorrente das propriedades dos números racionais.

## Cortes de Dedekind

**Definição 1 (Cortes de Dedekind)** *Um corte é definido como sendo um conjunto $\alpha \subset \mathbb{Q}$ que satisfaz as seguinte propriedades:*

(i) $\alpha$ é não vazio, $\alpha \neq \mathbb{Q}$;

(ii) Se $p \in \alpha$, $q \in \mathbb{Q}$ e $p > q$, então $q \in \alpha$ ;

(iii) Se $p \in \alpha$, então existe algum $r \in \alpha$ tal que $p < r$;

É usual denotar cortes por letras gregas.

**Proposição 1** *Seja $r \in \mathbb{Q}$ e $r^*$ o conjunto $\{p \in \mathbb{Q}$ tal que $p < r\}$. Então $r^*$ é um corte.*

Por exemplo o conjunto $0^* = \{p \in \mathbb{Q}$ tal que $p < 0\}$ é um corte racional e veremos que podemos associar a ele o número racional 0. Já o conjunto $\{p \in \mathbb{Q}$ tal que $p^2 < 2\}$ também é um corte, associamos ele ao número $\sqrt{2}$, mas não é um corte racional.

**Definição 2 (Soma em $\mathbb{R}$)** *Sejam $\alpha$ e $\beta$ dois cortes. Definiremos $\alpha + \beta$ como sendo o conjunto de todas as somas $r + s$, onde $r \in \alpha$ e $s \in \beta$.*

**Proposição 2** *A soma em $\mathbb{R}$ possui as seguintes propriedades:*

1. A soma de dois cortes também é um corte.
2. A soma de cortes é comutativa.
3. A soma de cortes é associativa.
4. O conjunto dos números reais possui um elemento neutro aditivo.
5. O conjunto dos números reais possui elemento oposto.

Por exemplo, para mostrarmos que vale o último item fixemos $\alpha \in \mathbb{R}$ e escolher $\beta$ o conjunto de todos os $p$ com a seguinte propriedade: existe algum $r > 0$ tal que $-p-r \notin \alpha$. Isso significa que deve haver algum racional menor que $-p$ que não está em $\alpha$. Primeiro, vamos mostrar que $\beta$ é um corte e depois que $\alpha + \beta = 0^*$.

i) Escolha $s \notin \alpha$ e tome $p = -s - 1$. Assim $s = -p - 1$ e portanto $-p - 1 \notin \alpha$. Logo $p \in \beta$ e consequentemente $\beta$ não é vazio. Agora escolha $p$ de tal forma que $-p \in \alpha$. Assim $-p - r \in \alpha$, para todo $r > 0$. Logo $p \notin \beta$ e portanto $\beta \neq \mathbb{Q}$.

ii) Agora escolha $p \in \beta$ e seja $r$ tal que $-p - r \notin \alpha$. Se $q < p$, então $-q - r > -p - r$, assim $-q - r \notin \alpha$ e portanto $q \in \beta$.

iii) Tome $t = p + (r/2)$, $p$ e $r$ como no item anterior. Consequentemente $t > p$ e $-t - (r/2) = -p - r \notin \alpha$, portanto $t \in \beta$.

Concluímos então que $\beta \in \mathbb{R}$. Agora escolha $t \in \alpha$ e $s \in \beta$. Assim existe algum $r > 0$ tal que $-s - r \notin \alpha$. Veja que $-s > -s - r$, logo $-s \notin \alpha$. Dessa forma, $t < -s$ e $t + s < 0$. Desde que $r$ e $s$ são arbitrários, $\alpha + \beta \subset 0^*$.
Agora escolha $p \in 0^*$ . Sejam $q \in \alpha$ e $r \in \mathbb{Q}$ de tal forma que $-r \notin \alpha$ e $p = q - r$. Logo $-r = +p - q$ e portanto $-r \in \beta$ (note que $-p > 0$ ), logo $p = q + (-r)$ pertence a $\alpha + \beta$. Por fim, $0^* \subset \alpha + \beta$.
Concluímos que $0^* = \alpha + \beta$. Feito isso, passaremos a denotar $\beta$ por $-\alpha$ e chamaremos esse último conjunto de elemento oposto de $\alpha$.

**Definição 3** *Módulo em $\mathbb{R}$. O módulo de $\alpha$, denotado por $|\alpha|$, é dado por*

$$|\alpha| = \begin{cases} \alpha & \textit{se } 0^* \subset \alpha \\ -\alpha & \textit{se } 0^* \not\subset \alpha \end{cases}$$

Podemos notar então que se $\alpha \in \mathbb{R}$ então $|\alpha| \supset 0^*$.

**Proposição 3** *Sejam $0^* \subset \alpha$ e $0^* \subset \beta$ dois corte. Então o conjunto $\gamma = \{t \in \mathbb{Q}; t < 0$ ou $t \leq r \cdot s$, para $r, s \geq 0$, $r \in \alpha$, $s \in \beta\}$ é um corte.*

Denotamos $\gamma = \alpha \cdot \beta$.
Com isso podemos definir o produto de dois cortes:

**Definição 4** *Sejam $\alpha$ e $\beta$ dois cortes.O produto ou multiplicação entre eles é dado por:*

$$\alpha \cdot \beta = \begin{cases} |\alpha| \cdot |\beta|, & se\ \beta \subset 0^* \text{ e } \alpha \subset 0^* \text{ ou se } \beta \supset 0^* \text{ e } \alpha \supset 0^* \\ -|\alpha| \cdot |\beta|, & se\ \beta \supsetneq 0^* \text{ e } \alpha \subsetneq 0^* \text{ ou se } \beta \subsetneq 0^* \text{ e } \alpha \supsetneq 0^* \end{cases}$$

A proposição anterior já deixa implícita uma definição de produto, no entanto ela se restringe aos corte que satisfazem $\alpha \supset 0^*$. A definição por módulo estende a operação para quaisquer dois cortes. Dessa forma, podemos ver que a multiplicação em $\mathbb{R}$ satisfaz:

1. A multiplicação de dois cortes é um corte.
2. A multiplicação de cortes é comutativa.
3. A multiplicação de cortes é associativa.
4. O conjunto dos números reais possui um elemento neutro multiplicativo.
5. O conjunto dos números reais possui elemento inverso.

Por exemplo, para mostrar a existência do elemento inverso: Seja $\alpha \in \mathbb{R} \setminus 0^*$. Então o conjunto $\gamma = \{t \in q;\ t \leq 0$ ou existe $q \notin |\alpha|$ tal que $q < t^{-1}$ e $t^{-1} \notin |\alpha|\}$ é um corte e $|\alpha| \cdot \gamma = 1^*$. Primeiro mostraremos que valem os requerimentos da definição 1 para $\gamma$.

i) Veja que se $t^{-1} \in |\alpha|$ então $t \notin \gamma$ logo $\gamma \neq \mathbb{Q}$. Note ainda que $0^* \subset \gamma$.

ii) Seja $p \in \gamma$ e $q < p$. Se $q \leq 0$ então é imediato que $q \in \gamma$. Se $q > 0$ então seja $r \notin |\alpha|$ tal que $1/p > r$. Então temos que $1/q > 1/p > 0$ e portanto $q \in \gamma$.

iii) Sejam $p$ e $r$ como anteriormente e seja $q$ tal que $\frac{1}{p} > q > r$ . Então $\frac{1}{q} \in \gamma$ e $\frac{1}{q} > p$.

Com isso concluímos que $\gamma$ é um corte. Agora seja $r \in |\alpha| \cdot \gamma$ e suponha $r \leq 0$ Então existem $s \in |\alpha|$, $p \in \gamma$ e $q \notin \alpha$ tais que $r = s \cdot p$ e $\frac{1}{p} > q$. Portanto $q > s$ e $1/q > p$. Segue então que $1 > \frac{s}{q} > s \cdot p = r$. Portanto $r \in 1^*$. Se $r < 0$ é imediato que $r \in 1^*$. Logo $|\alpha| \cdot \gamma \subset 1^*$.
Seja agora $p \in 1^*$. Se $p \leq 0$ então basta notar que segue de $0^* \subsetneq \gamma$ que $0 \in |\alpha| \cdot \gamma$. Suponha então $0 < p < 1$. Escolha $s > 0 \in \alpha$ e denote $r_1 = s \cdot (p^{-1})^{n-1}$, $t = s \cdot (p^{-1})^n$. Desde que $p^{-1} > 0$ existe $n \in \mathbb{N}$ tal que $t \notin |\alpha|$. Escolha então $n$ o menor deles, de modo que $r_1 \in |\alpha|$. Seja $r \in \alpha$ tal que $r > r_1$ e $q = t^{-1} \cdot r^{-1} \cdot r_{-1}$. Temos então que $q^{-1} = t \cdot r \cdot {r_{-1}}^{-1} > t$ (pois $r > r_1$ ) portanto $q \in \gamma$. Logo $q \cdot r = p$ e portanto $p \in |\alpha| \cdot \gamma$. Então $1^* \subset |\alpha| \cdot \gamma$. Feito isso, podemos definir $\alpha^{-}1$, o elemento inverso de $\alpha$:

- se $\alpha \subsetneq 0^*$ então defina $\alpha^{-1} = -\gamma$, onde $\gamma$ é o conjunto da construção anterior.
- se $\alpha \supsetneq 0^*$ então $\alpha^{-1} = \gamma$.

Observação: da mesma forma que não está definido $0^{-1}$ não definimos $0^{*-1}$. Note que em ambos os caso, $\alpha \cdot \alpha^{-1} = 1^*$.

**Proposição 4** *A multiplicação em $\mathbb{R}$ é distributiva em relação a soma.*

Isso é o mesmo que mostrar que

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

para quaisquer $\alpha, \beta$ e $\gamma \in \mathbb{R}$.
Com isso, já podemos concluir que $\mathbb{R}$ é um corpo.

**Definição 5** *Sejam $\alpha$ e $\beta$ dois cortes. Se $\alpha \subsetneq \beta$ dizemos que $\alpha$ é menor que $\beta$ e denotamos $\alpha < \beta$. É equivalente escrever $\beta > \alpha$ e dizer $\beta$ é maior que $\alpha$.*

**Proposição 5 ( $\mathbb{R}$ é um conjunto ordenado)** *Sejam $\alpha, \beta, \gamma$ cortes. Então entre dois cortes vale uma e apenas umas das seguintes relações:*

$$\alpha < \beta, \qquad \alpha = \beta, \qquad \alpha > \beta.$$

*Além disso, se tivermos $\gamma < \alpha$ e $\alpha < \beta$ então teremos $\alpha < \beta$.*

Sejam $\alpha, \beta$ e $\gamma$ cortes quaisquer. Temos que

i) $\alpha + \beta < \alpha + \gamma$ se $\beta < \gamma$;

ii) $\alpha \cdot \beta > 0$ se $\alpha > 0^*$ e $\beta > 0^*$ .

Com isso concluímos que $\mathbb{R}$ é um corpo ordenado.

**Definição 6** *Seja $A \in \Omega$, onde $\Omega$ é um conjunto ordenado. Se para todo $a \in A$ tivermos $a \leq b$, então dizemos que $b$ é um limitante superior de $A$.*

**Definição 7** *Seja $A$ um conjunto ordenado e suponha que existe $b$ tal que:*

*i) $b$ é um limitante superior de $A$;*

*ii) se $c < b$ então $c$ não é um limitante superior de $A$.*

*Dizemos que $b$ é o supremo de $A$ e denotamos $b = \sup A$.*

Por exemplo, para todo corte racional $r^*$, $r = \sup r^*$. O supremo também pode ser chamado de menor limitante superior de um conjunto.

**Proposição 6** *$\mathbb{R}$ tem a propriedade do supremo.*

Isso significa que todo subconjunto de $\mathbb{R}$ possui supremo e que o supremo de todos esses conjuntos são elementos do $\mathbb{R}$. O que não ocorre em geral, por exemplo $\mathbb{Q}$ é conjunto que não possui a propriedade do supremo. Para ver isso, basta notar que o conjunto $\alpha = \{p \in \mathbb{Q}$ tal que $p^2 < 2\}$ não possui supremo em $\mathbb{Q}$. Se supomos o contrário, veremos que $\sqrt{2} = \sup \alpha$, mas $\sqrt{2}$ não é um elemento de $\mathbb{Q}$.

**Proposição 7** *Seja $\mathbb{Q}^*$ o conjunto de todos os cortes racionais. Então cada elemento de $\mathbb{Q}$ pode ser associado a um único elemento de $\mathbb{Q}^*$.*

Para isso mostramos que valem as seguintes relações:

(a) $r^* + s^* = (r + s)^*$;

(b) $r^* s^* = (rs)^*$;

(c) $r^* < s^* \Leftrightarrow r < s$;

Com isso, resolve-se o problema dos números irracionais.

## Cardinalidade

A Cardinalidade traduz a ideia de associar um tamanho a um conjunto. Suponha então que exista uma função bijetiva entre um conjunto $A$ e $\mathbb{N}$, o conjunto dos naturais. Isso significa que cada elemento de $A$ é associado a um e somente um número natural e vice-versa. Quando isso acontece dizemos que $A$ é contável. Isso é o mesmo que dizer que a cardinalidade de $A$ e $\mathbb{N}$ são as mesmas.

**Teorema 1** *Todo subconjunto infinito de um conjunto contável é contável.*

**Teorema 2** *O conjunto dos números racionais é contável.*

Quando um conjunto não é contável e também não é finito dizemos que esse conjunto é incontável.

**Teorema 3** *O conjunto dos números reais é incontável.*

Esses resultados nos trazem outra evidência de que há outros números além dos racionais. Note que se isso não acontecesse deveríamos ter que $\mathbb{R}$ é contável.

### Números transcendentais

Um número é dito algébrico quando ele é raíz de alguma equação polinomial com coeficientes inteiros. Por exemplo, todo número racional é algébrico. De fato, seja $q = \frac{a}{b}$, $a \in \mathbb{Z}, b \in \mathbb{N}^*$, então $q$ é raíz da equação $bx - a = 0$.
Podemos mostrar que o conjunto de todos os números algébricos é contável. Como $\mathbb{R}$ é incontável, os resultados anteriores nos mostram que existem números que não são algébricos. Esses são os chamados números transcendentais.
Decorre dos números transcendentais não serem contáveis que eles existem em um número muito maior que os números algébricos. Como exemplos de números transcendentais temos o número $\pi$ e $e$.

## Conclusão

Os cortes de Dedekind são uma forma de definir os números reais. Embora a construção os trate como conjunto de números, as operações definidas entre esses conjuntos satisfazem exatamente o que era de se esperar para números. O processo construtivo soluciona o problema de definir números como $\sqrt{2}$ e outros irracionais. A teoria de cardinalidade nos dá outra pista sobre a existência dos números racionais e permite concluir que existem números não algébricos.