Universidade Estadual Paulista "Júlio de Mesquita Filho"
Instituto de Geociências e Ciências Exatas
Campus de Rio Claro

Números Transcendentes e de Liouville

Roberto Miachon Marchiori

Dissertação apresentada ao Programa de Pós-Graduação – Mestrado Profissional em Matemática em Rede Nacional como requisito parcial para a obtenção do grau de Mestre

Orientadora
Profa. Dra. Elíris Cristina Rizziolli

2013

512.7 Marchiori, Roberto Miachon
M317n Números Transcendentes e de Liouville/ Roberto Miachon Marchiori- Rio Claro: [s.n.], 2013.
36 f. : il.

Dissertação (mestrado) - Universidade Estadual Paulista, Instituto de Geociências e Ciências Exatas.
Orientadora: Elíris Cristina Rizziolli

1. Teoria dos números. 2. Álgebra. 3. Números Álgébricos. 4. Números de Liouville. I. Título

Ficha Catalográfica elaborada pela STATI - Biblioteca da UNESP
Campus de Rio Claro/SP

TERMO DE APROVAÇÃO

Roberto Miachon Marchiori

Números Transcendentes e de Liouville

Dissertação aprovada como requisito parcial para a obtenção do grau de Mestre no Curso de Pós-Graduação Mestrado Profissional em Matemática em Rede Nacional do Instituto de Geociências e Ciências Exatas da Universidade Estadual Paulista "Júlio de Mesquita Filho", pela seguinte banca examinadora:

Profa. Dra. Elíris Cristina Rizziolli
Orientadora

Prof. Dr. Aldício José Miranda
Instituto de Ciências Exatas - UNIFAL-MG - ALFENAS/MG

Profa. Dra. Marta Cilene Gadotti
Departamento de Matemática - IGCE - UNESP - RIO CLARO/SP

Rio Claro, 28 de Janeiro de 2013

Dedico essa dissertação à minha esposa, família, amigos e alunos.

Agradecimentos

Em primeiro lugar agradeço a Deus por ter me dado força nos momentos de maior dificuldade, e seguir em frente para tornar este momento possível.

Em seguida tenho muito a agradecer a minha esposa pelo incentivo para que me inscrevesse ao Programa de Mestrado Profissional em Matemática em Rede Nacional - Profmat. Foram incontáveis horas de estudos, noites em claro, trabalhos para entregar e avaliações para me preparar, sem contar os sábados longe de casa. Em todos os momentos tive o apoio total de minha esposa, sempre presente e acreditando em mim e no meu potencial, mesmo diante das adversidades que encontrei pela frente como, por exemplo, conciliar o mestrado com o trabalho nas escolas onde leciono e também no Fórum (acumulo duas profissões).

Obrigado também a minha família e amigos que me incentivaram e, é claro, não poderia deixar de citar meus alunos, principal fonte inspiradora para que voltasse a estudar e me aperfeiçoar para me tornar um professor um pouco melhor.

Finalmente agradeço a todos os professores do Departamento de Matemática da Unesp de Rio Claro, em especial à minha orientadora Profa. Eliris e à coordenadora Profa. Suzinei que sempre estiveram presentes para me auxiliar e aos amigos de curso Luis Henrique, Ronaldo, Ricardo e Pedro com os quais aprendi muito principalmente o valor de uma amizade.

O único lugar em que sucesso vem antes de trabalho é no dicionário.

Albert Einstein

Resumo

Tudo é número, diria o famoso matemático grego Pitágoras. Os números estão a nossa volta, como o oxigênio que respiramos. Primeiro vieram os naturais, depois os inteiros, os racionais e os incríveis irracionais, que deixaram os pitagóricos tão perplexos a ponto de escondê-los. Números primos, perfeitos e outros vieram. E quando tudo parecia ser real apareceram os imaginários. Que imaginação tem esses matemáticos! Vamos nos aprofundar em um grupo intrigante de números chamados transcendentes e aos números estudados por um matemático francês chamado Liouville.

Palavras-chave: Teoria dos números, Álgebra, Números Álgébricos, Números de Liouville.

Abstract

All is number, say the famous Greek mathematician Pythagoras. The numbers are all around us, like the oxygen we breathe. First came the natural, then the integers, the rational and the irrational incredible that left perplexed the Pythagoreans so as to hide them. Prime numbers, perfect and others came. And when everything seemed to be real the imaginary appeared. What have these mathematical imagination! Let's delve in a group of intriguing numbers called transcendental numbers and studied by a French mathematician named Liouville.

Keywords: Number Theory, Algebra, Algebraic Numbers, Liouville's Numbers.

Sumário

1 Introdução

Os números acompanham os passos do homem desde a Antiguidade e seu desenvolvimento está ligado inicialmente a duas funções básicas: a contagem e a medição. Contar envolve a comparação entre grandezas discretas e para tal são usados os números inteiros.

Por vezes medir envolve a comparação entre grandezas contínuas e assim são usados os números reais. Com o aprimoramento dos números foi possível classificá-los em conjuntos.

A humanidade desenvolveu lentamente o princípio de contagem como a comparação entre grandezas discretas. Neste contexto podemos citar o exemplo clássico do homem que conta seu rebanho utilizando pedras, daí a origem da palavra *cálculo*.

A caracterização formal do conjunto dos **Números Naturais** representado por $\mathbb{N}$, por incrível que possa parecer, é recente (início do século XX) e foi feita pelo matemático italiano Giuseppe Peano. Tal caracterização é feita de forma axiomática e baseada na ideia de sucessor. Assim os números naturais são descritos pelo conjunto a seguir:

$$\mathbb{N} = \{1, 2, 3, 4, 5, ...\}.$$

Com relação ao número zero não estar representado se deve ao fato de que alguns autores não o consideram natural, sendo facultativa sua representação. Também podemos citar o fato histórico de que o zero surgiu bem depois dos números naturais. O conjunto dos números naturais é munido de duas operações básicas: a adição e a multiplicação. A adição associa a cada dois números $x, y \in \mathbb{N}$ a soma $x + y$. A multiplicação por sua vez associa a cada dois números $x, y \in \mathbb{N}$ o produto $x.y$.

Em seguida, temos o conjunto dos **Números Inteiros**, representado por $\mathbb{Z}$, o qual é formado pelos números naturais, pelo zero e pelos números negativos. A necessidade da criação deste conjunto se deve ao fato de que dados $a, b \in \mathbb{N}$, a diferença $a - b \notin \mathbb{N}$ se $a < b$. Assim representamos os números inteiros da seguinte forma

$$\mathbb{Z} = \{..., -3, -2, -1, 0, 1, 2, 3, ...\}.$$

O conjunto dos **Números Racionais**, representado por $\mathbb{Q}$, é definido como o quociente de dois números inteiros, sendo o denominador diferente de zero e sua representação é dada por

$$\mathbb{Q} = \left\{ \frac{p}{q} : \ p \ , \ q \in \mathbb{Z} \ \ e \ q \neq 0 \right\}.$$

Todo número que pode ser escrito como a razão entre dois números inteiros, exceto o zero como denominador, é chamado de número racional. Em particular, os números naturais e inteiros são racionais pois podem ser escritos com denominador 1. Assim concluímos que o conjunto dos números naturais e o dos números inteiros podem ser vistos como subconjuntos do conjunto dos números racionais. Além dos naturais e dos inteiros, as frações, os decimais finitos e os decimais infinitos periódicos são números racionais. Por exemplo,

$$2 = \frac{2}{1} \ \ ; \ \ -3 = \frac{-3}{1} \ \ ; \ \ 1,5 = \frac{3}{2} \ \ ; \ \ 0,44444... = \frac{4}{9}$$

A crença de que todo número poderia ser escrito como a razão entre dois inteiros começou a cair na Grécia Antiga, mais precisamente na sociedade pitagórica. Foi surpreendente e perturbador para os pitagóricos o fato de que a medida do comprimento de sua diagonal de um quadrado de lado unitário não poderia ser expressa como um número racional. Por mais que se tentasse encontrar, não havia qualquer fração que multiplicada por ela mesma resulta 2. Foi um golpe mortal na filosofia pitagórica segundo a qual tudo dependia dos números inteiros. A descoberta da irracionalidade de $\sqrt{2}$ provocou tamanha consternação entre os pitagóricos que, por algum tempo, se fizeram esforços para manter a questão em sigilo. Alguns historiadores dizem que o pitagórico Hipaso foi expulso da sociedade por revelar o segredo e teria sido lançado ao mar.

Hoje os **Números Irracionais** são bem compreendidos. São definidos como números que não podem ser expressos como a razão entre dois inteiros. Os números racionais parecem ilhas de ordem num interminável oceano de desordem representado pelos irracionais. Há um número infinito de racionais, porém os irracionais são bem mais numerosos. Enquanto os números racionais tem um padrão como as dízimas periódicas os irracionais são desprovidos de padrão. Veja os exemplos:

$$\frac{3}{7} = 0,428571 \ 428571 \ 428571... \ \left(\frac{3}{7} \in \mathbb{Q} \right).$$

$$\sqrt{2} = 1,414213562373095... \ (\sqrt{2} \text{ irracional }).$$

Os números irracionais formam espaços entre os padrões. Foi o matemático Georg Cantor que estudou os conjuntos infinitos e se era possível contá-los. Ele descobriu que os conjuntos dos números naturais, inteiros e racionais são enumeráveis (ou contáveis), pois era possível estabelecer uma bijeção entre estes conjuntos e o conjunto dos números naturais. Porém o conjunto dos números irracionais não é enumerável (incontável).

A união dos conjuntos dos números racionais e dos irracionais forma o conjunto dos **Números Reais**, representado por $\mathbb{R}$, que não é enumerável como veremos no próximo capítulo.

Nosso objeto de estudo será a classificação dos números em **Algébricos** e **Transcendentes**. Dizemos que um número é algébrico se o mesmo é solução de uma equação polinomial com coeficientes inteiros. Caso contrário ele é dito transcendente. Deste fato já podemos concluir que todo número racional p/q com $p, q \in \mathbb{Z},\ q \neq 0,$ é algébrico pois é solução da equação polinomial de coeficientes inteiros $qx - p = 0$. Além disso alguns irracionais também são algébricos como por exemplo $\sqrt{2}$ que é solução da equação $x^2 - 2 = 0$.

Existem porém alguns números irracionais que não são solução de nenhuma equação polinomial com coeficientes inteiros. É o caso do π, do e e dos números de Liouville. Estes são chamados números transcendentes. Aliás, o matemático francês Joseph Liouville foi o autor da primeira demonstração da existência de números transcendentes estabelecendo um critério para que um número seja transcendente. Este resultado permitiu a construção da famosa **constante de Liouville**, qual seja: 0,110001000000000000000001...

Este trabalho está composto por quatro capítulos, a saber, a Introdução no capítulo 1, reservamos o capítulo 2 para explorar números irracionais e transcendentes, o capítulo 3 irá apresentar os números de Liouville e apresentamos no capítulo 4 uma aula sobre números racionais e irracionais.

Finalmente observamos que são necessárias para a leitura deste trabalho noções básicas sobre Análise Real como prerrequisito.

2 Números Algébricos e Transcendentes

A seguir exploramos os Números Algébricos e Transcendentes. Iniciamos com definições e propriedades que envolvem os Números Inteiros, uma vez que estes estabelecem a base para os próximos conceitos.

2.1 Números Inteiros

Definição 2.1. *Dados $a, b \in \mathbb{Z}$, dizemos que* ***a divide b****, e escrevemos $a|b$, se existir $q \in \mathbb{Z}$ tal que $b = qa$. Neste caso, diremos que a é um fator ou divisor de b ou ainda que b é um múltiplo de a.*

Exemplo 2.1. $3|12$, pois $12 = q3 \Longrightarrow q = 4$.

Definição 2.2. ***(a)*** *Um número $p \in \mathbb{N}$, $p > 1$, é chamado* ***primo*** *se este só admite dois divisores naturais: o 1 e si próprio. Assim p é primo se para todo $d \in \mathbb{N}$ tal que $d|p$, então $d = p$ ou $d = 1$.*

(b) *Um número $p \in \mathbb{Z}$, $p \neq 0$ e $p \neq \pm 1$, é* ***primo*** *se os únicos números inteiros que o dividem são $\pm p$ e ± 1.*

Exemplo 2.2. $p = 5$ e $d|5 \Longrightarrow d = 5 \;\; ou \;\; d = 1$.

Definição 2.3. *Seja $a \in \mathbb{Z}$. Um número inteiro b é chamado* ***múltiplo*** *de a se $b = aq$, para algum $q \in \mathbb{Z}$.*

Exemplo 2.3. $a = 5$, $q = 4$; $\quad b = 5.4 \Longrightarrow b = 20 \quad$ (20 é múltiplo de 5).

Definição 2.4. *Dados $a, b \in \mathbb{Z}$, um número natural d é chamado o* ***máximo divisor comum*** *de a e b, denotado por $d := mdc(a, b)$, se satisfaz as afirmações abaixo:*

(i) *$d|a$ e $d|b$;*

(ii) *se $r \in \mathbb{Z}$,é tal que $r|a$ e $r|b$, então $r|d$.*

Exemplo 2.4. Se $a = 30$, $b = 75$ então $mdc(30, 75) = 15$, pois $15|30$ *e* $15|75$ e além disso se $r|30$ *e* $r|75$ então $r|15$ (por exemplo se $r = 3$, temos que $3|30$, $3|75$ e ainda que $3|15$).

Observação 2.1. O $mdc(a,0)$ não existe caso a seja **nulo**. Além disso, assumimos que $mdc(a,0)=a$, se $a \neq 0$.

Teorema 2.1. ***(Algoritmo da Divisão)*** *Se $a, b \in \mathbb{Z}$, com $b \neq 0$, então existem (e são únicos) $q, r \in \mathbb{Z}$ com $0 \leq\ r <\ |b|$, tais que,*

$$a = qb + r. \tag{2.1}$$

Demonstração. (i) **Existência.**

($\mathbf{b > 0}$) Consideremos o conjunto dos números múltiplos de b ordenados de acordo com a ordem natural da reta, isto é, o conjunto ..., $-3b$, $-2b$, $-b$, 0, b, $2b$, $3b$, ..., com,

$$... - 3b \ \leq \ -2b \ \leq \ -b \ \leq \ 0 \ \leq \ b \ \leq \ 2b \ \leq \ 3b...$$

Note que disso decorre uma decomposição da reta em intervalos disjuntos da forma

$$[qb, (q+1)b) = \{x \in \mathbb{R} : qb \leq x < (q+1)b\},$$

com $q \in \mathbb{Z}$. Para $q = -3$, temos por exemplo,

$$[-3b, -2b) = [-3b, (-3+1)b) = \{x \in \mathbb{R} : -3b \leq x < -2b\}.$$

Assim, dado $a \in \mathbb{Z}$, este pertence a apenas um desses intervalos e portanto necessariamente é da forma $a = qb + r$, com $q \in \mathbb{Z}$ e $r \geq 0$. É claro que $r < (q+1)b - qb = b$.

($\mathbf{b < 0}$) Aplicamos o teorema para $|b|$, logo existem $q', r \in \mathbb{Z}$, com $0 \leq r < |b|$ tais que

$$a = q'|b| + r. \tag{2.2}$$

Fazendo $q = -q'$, como $|b| = -b$, (pois $b < 0$), obtemos de (2.2) $a = qb + r$, onde $q, r \in \mathbb{Z}$ e $0 \leq r < |b|$.

(ii) **Unicidade**. Resta demonstrar que q e r, os quais satisfazem (2.1) são únicos. De fato, suponha que $a = qb + r$ e $a = q_1 b + r_1$, com $0 \ \leq \ r < |b|$ e $0 \leq r_1 < |b|$. Assim,

$$qb + r = q_1 b + r_1 \Rightarrow$$
$$r - r_1 = (q_1 - q)b. \tag{2.3}$$

Afirmamos que $r = r_1$. Com efeito, se $r \neq r_1$, então: $0 \ < \ |r_1 - r|$.

Além disso, $|r_1 - r| \ < \ b$. De fato, vamos admitir, sem perda de generalidade, que $r < r_1$, consequentemente $r_1 - r \ > \ 0$ e $|r_1 - r| = r_1 - r$. Assim, se $r_1 - r = |b|$, então $r_1 = |b| + r$ e portanto $r_1 > |b|$, que é absurdo. Também, se $r_1 - r \ > \ |b|$, então $r_1 > |b| + r > |b|$, gerando novamente o absurdo $r_1 > b$. Logo pela Lei da Tricotomia,

$$|r_1 - r| = r_1 - r < |b|.$$

Segue que

$$0 < \ |r_1 - r| \ < \ |b|. \tag{2.4}$$

Agora de (2.3) obtemos,

$$|r_1 - r| = |q_1 - q||b|. \tag{2.5}$$

Substituindo (2.5) em (2.4), obtemos,

$$0 < |q_1 - q||b| < |b|.$$

Logo, $0 < |q_1 - q| < 1$, o que é um absurdo, pois $|q_1 - q|$ é um número inteiro (pois q e $q_1 \in \mathbb{Z}$ e em $\mathbb{Z}$ vale a Lei do Fechamento da Adição). Portanto $r = r_1$. Note que essa igualdade combinada com (2.3) implica $q_1 = q$, já que $0 = (q_1 - q)b$ e $b \neq 0$ por hipótese.

□

Exemplo 2.5. Se $a = 17$ e $b = 5$ então obtemos $q = 3$ e $r = 2$ pois $17 = 3.5 + 2$.

Teorema 2.2. *Dados $a, b \in \mathbb{Z}$, pelo menos um deles não nulo, existem $x_0, y_0 \in \mathbb{Z}$ tais que*

$$ax_0 + by_0 = d$$

onde $d = mdc(a, b)$.

Demonstração. Considere o conjunto C de todos os inteiros positivos da forma $ax+by$, isto é, $C = \{n \in \mathbb{N} : n > 0 \ \ e \ \ n = ax + by, \text{ para algum } x \text{ e algum } y\}$. O conjunto C não é vazio, pois tomando $x = a$ e $y = b$ temos $n = aa+bb \in C$. Utilizando o Princípio da Boa Ordenação podemos afirmar que C tem um menor elemento.

Dessa forma, existe $d \geq 1$ tal que $d = ax_0 + by_0$, com $x_0, y_0 \in \mathbb{Z}$, e

$$d \leq ax + by \tag{2.6}$$

para todo $ax + by \in C$. A seguir afirmamos que

$$d \mid ax + by \tag{2.7}$$

para todo $ax + by \in C$. Para demonstrar (2.7) suponhamos, por contradição, que $d \nmid ax + by$. Logo, existem $q, r \in \mathbb{Z}$ com $0 < r < d$ tais que

$$ax + by = qd + r = q(ax_0 + by_0) + r,$$

de onde segue que

$$r = a(x - qx_0) + b(y - qy_0) \tag{2.8}$$

Como $r > 0$, a expressão (2.8) diz que $r \in C$. Porém isso é um absurdo pois $r < d$, contrariando o fato de assurmirmos d como o menor elemento do conjunto C. Logo $d \mid ax + by$.

A relação $d \mid ax + by$ implica $d \mid |a|$ e $d \mid |b|$ pois, ou um deles é zero e $d \mid 0$, ou ambos são positivos e, nesse caso, ambos estão em C. De fato,

$$|a| = a(sgn\{a\}) + b.0 \tag{2.9}$$

e analogamente para $|b|$; em (2.9) $sgn\{a\} = +1$ se $a > 0$ e $sgn\{a\} = -1$ se $a < 0$, e em ambos os casos $sgn\{a\} \in \mathbb{Z}$. Consequentemente,

$$d \mid a \quad e \quad d \mid b. \tag{2.10}$$

Por outro lado, se $n \in \mathbb{N}$ é tal que $n \mid a$ e $n \mid b$, então $n \mid (ax_0 + by_0)$, ou seja, $n \mid d$. Portanto, $d \mid a \;\; e \;\; d \mid b$ e também para $n \in \mathbb{N}, n \mid a$ e $n \mid b$, então $n \mid d$, concluímos que d é o máximo divisor comum de a e b. Logo,

$$d = ax_0 + by_0 = mdc(a, b),$$

o que finaliza a demonstração.

□

Lema 2.1. *Sejam $a, x_0, b, y_0, d \in \mathbb{Z}$, se $d|a$ e $d|b$, então $d|(ax_0 + by_0)$.*

Demonstração. Como $d|a$ (pela definição 2.1) implica que existe $q \in \mathbb{Z}$, tal que $a = qd$. Também (pela definição 2.1) $d|b$ implica que existe $p \in \mathbb{Z}$, tal que $b = pd$. Logo,

$$ax_0 + by_0 = qdx_0 + pdy_0 = d(qx_0 + py_0).$$

Observe que $K = (qx_0 + py_0) \in \mathbb{Z}$, (pois vale a lei do fechamento da adição e multiplicação em $\mathbb{Z}$ e $q, x_0, p, y_0 \in \mathbb{Z}$). Portanto, $ax_0 + by_0 = dK, K \in \mathbb{Z}$, ou seja,

$$d|(ax_0 + by_0).$$

□

Exemplo 2.6. $3|6$ e $3|9 \Rightarrow 3|(6x_0 + 9y_0), \forall \; x_0, \; y_0 \; \in \; \mathbb{Z}$.

Lema 2.2. *Seja $p \in \mathbb{N}$ um número primo, e $a, b \in \mathbb{Z}$. Se p divide o produto $\boldsymbol{ab}$ então p divide $\boldsymbol{a}$ ou $\boldsymbol{b}$.*

Demonstração. Se $p|a$, nada temos que provar. Suponhamos que p não divide a, ou seja, p e a são primos entre si. Logo, pelo Teorema 2.2, existem $x_0, y_0 \in \mathbb{Z}$ tais que $ax_0 + py_0 = 1$. Assim,

$$abx_0 + pby_0 = b. \tag{2.11}$$

Como $p|ab$ (por hipótese) e claramente $p|pb$, logo pelo Lema 2.1, segue que,

$$p|(abx_0 + pby_0).$$

Portanto de (2.11) segue que $p|b$. □

Exemplo 2.7. 1. Sejam $p = 3$, $a = 9$, $b = 5$, assim $3|9.5$ e também $3|9$.

2. $p = 3$, $a = 9$, $b = 6$, temos que $3|9.6$ e também $3|9$ e $3|6$.

Corolário 2.1. *Seja $p \in \mathbb{N}$ um número primo e $a \in \mathbb{Z}$. Se $p|a^n$, então $p|a$.*

Demonstração. Esse resultado segue usando o Princípio da Indução Finita. Queremos mostrar a veracidade da sentença.

$$\mathcal{P}(n) : p|a^n \implies p|a, \forall n \in \mathbb{N}.$$

Note que, obviamente, $\mathcal{P}(1)$ é válida,

$$\mathcal{P}(1) : p|a^1 \Longrightarrow p|a.$$

Além disso, observe que $\mathcal{P}(2)$ também é válida pois se $p|a^2$, pelo Lema 2.2, se $p|a.a$, então $p|a$ ou $p|a$, isto é, $p|a$.

Suponha agora que para qualquer $k \in \mathbb{N}$,

$$\mathcal{P}(k) : \text{“Se } \ p|a^k, \text{ então } p|a.\text{”}$$

Queremos mostrar que $\mathcal{P}(k+1)$ é válida, ou seja,

$$''\text{Se } p|a^{k+1}, \text{ então } p|a.\text{”}$$

Observe que $p|a^{k+1}$ é o mesmo que $p|a^k.a$. Agora, do Lema 2.2, segue que $p|a^k$ ou $p|a$. Se $p|a$, o resultado está provado. Por outro lado, se $p|a^k$ temos por Hipótese de Indução que $p|a^k$ implica que $p|a$ e também está provado. Portanto, $p|a^{k+1}$ implica $p|a$.

□

Uma vez explorados os Números Inteiros, apresentamos os Números Algébricos.

2.2 Números Algébricos

Um número real ou complexo é dito algébrico quando é solução de uma equação polinomial com coeficientes inteiros, conforme a definição abaixo:

Definição 2.5. *Qualquer solução de uma equação da forma*

$$x^n + a_{n-1}x^{n-1} + ... + a_1x + a_0 = 0 \tag{2.12}$$

*em que cada coeficiente $a_i \in \mathbb{Z}, \forall i \in \{0, 1, ..., n-1\}$, é chamado de **inteiro algébrico**.*

Exemplo 2.8. 1. Seja $a \in \mathbb{Z}$, então a é um inteiro algébrico, pois a é solução da equação $x - a = 0$, a qual é do tipo (2.12), para $n = 1$ e $a_0 = -a$.

2. $\sqrt{5}$ é um inteiro algébrico, já que é solução de $x^2 - 5 = 0$.

3. $\sqrt{2+\sqrt{3}}$ é um inteiro algébrico, uma vez que é solução de uma equação do tipo (2.12). A seguir descrevemos como obtê-la.

Para obtermos uma equação do tipo (2.12), precisamos aplicar duas quadraturas. Aplicando a primeira quadratura, temos

$$x = \sqrt{2+\sqrt{3}} \Rightarrow x^2 = (\sqrt{2+\sqrt{3}})^2 \Rightarrow x^2 = 2+\sqrt{3}.$$

Para eliminar o radical que restou, aplicamos outra quadratura,

$$x^2 = 2+\sqrt{3} \Rightarrow$$

$$x^2 - 2 = \sqrt{3} \Rightarrow$$

$$(x^2-2)^2 = (\sqrt{3})^2 \Rightarrow$$

$$x^4 - 4x^2 + 4 = 3 \Rightarrow$$

$$x^4 - 4x^2 + 1 = 0.$$

Portanto, $x^4 - 4x^2 + 1 = 0$, é a equação procurada.

4. Todo número da forma $\sqrt{b}$, com $b \in \mathbb{N}$, é um inteiro algébrico. De fato,

$$x = \sqrt{b} \Rightarrow x^2 = (\sqrt{b})^2 \Rightarrow x^2 = b \Rightarrow x^2 - b = 0,$$

e esta última é uma equação do tipo (2.12), para $n = 2,\ a_0 = -b$.

5. Para cada $a \in \mathbb{Z}^*$, o número complexo $i\sqrt{a}$ é um inteiro algébrico, pois é solução da equação $x^2 + a = 0$.

Observação 2.2. Dos exemplos acima, podemos observar que todos os Números Inteiros são Inteiros Algébricos. Também, existem Inteiros Algébricos **Irracionais** e **Complexos**. O Teorema a seguir caracteriza os Inteiros Algébricos **Reais**.

Teorema 2.3. *Todo número inteiro algébrico (real) é um número inteiro ou irracional.*

Demonstração. Para provar que um inteiro algébrico não pode ser um número racional não inteiro, usaremos o tipo de demonstração indireta, a saber, redução ao absurdo. Suponha por absurdo, que o número racional $x = \dfrac{p}{q}$, em que $p, q \in \mathbb{Z}$, $q > 1$ e $mdc(p, q) = 1$, satisfaça a equação do tipo (2.12), ou seja,

$$x^n + a_{n-1}x^{n-1} + ... + a_1x + a_0 = 0.$$

Então,

$$\left(\frac{p}{q}\right)^n + a_{n-1}\left(\frac{p}{q}\right)^{n-1} + ... + a_1\left(\frac{p}{q}\right) + a_0 = 0 \Rightarrow$$

$$\frac{p^n}{q^n} + a_{n-1}\frac{p^{n-1}}{q^{n-1}} + ... + a_1\frac{p}{q} + a_0 = 0 \Rightarrow$$
$$\frac{p^n}{q^n} = -a_{n-1}\frac{p^{n-1}}{q^{n-1}} - ... - a_1\frac{p}{q} - a_0 \Rightarrow$$
$$p^n = q^n\left(-a_{n-1}\frac{p^{n-1}}{q^{n-1}} - ... - a_1\frac{p}{q} - a_0\right) \Rightarrow$$
$$p^n = (-a_{n-1}p^{n-1}q - ... - a_1pq^{n-1} - a_0q^n) \Rightarrow$$
$$p^n = q(-a_{n-1}p^{n-1} - ... - a_1pq^{n-2} - a_0q^{n-1}).$$

Considerando, $j = (-a_{n-1}p^{n-1} - ... - a_1pq^{n-2} - a_0q^{n-1})$, temos que $j \in \mathbb{Z}$ (pois vale a lei do fechamento, da adição e multiplicação em $\mathbb{Z}$) e que $p^n = qj$, ou seja, $q|p^n$. Agora, seja r um fator primo de q, $r \neq 1$ (observe que se r for primo podemos considerar $r = q$); então r divide p^n e pelo Corolário 2.1 isso implica que $r|p$. Obtemos assim que, $r|q$ e $r|p$, o que contradiz o fato de $mdc(p,q) = 1$ (o absurdo ocorre quando admitimos que $\frac{p}{q}$ é solução da equação do tipo (2.12)). □

No próximo exemplo mostraremos a irracionalidade de algumas raízes quadradas.

Exemplo 2.9. **(a)** $\sqrt{2}$ é irracional. De fato, supomos $\sqrt{2}$ racional, então este pode ser escrito como $\frac{a}{b}$, com $a, b \in \mathbb{Z}$ e $b \neq 0$ e a, b irredutíveis, ou seja, primos entre si. Então temos: $\sqrt{2} = \frac{a}{b} \Rightarrow 2 = \frac{a^2}{b^2} \Rightarrow a^2 = 2b^2$. Como a^2 é par, então a é par (pois se a fosse ímpar, então $a = 2k+1, k \in \mathbb{Z} \Rightarrow a^2 = 4k^2 + 4k + 1$ então a^2 seria ímpar). Assim, sendo a par, então $a = 2k \Rightarrow a^2 = 4k^2 \Rightarrow 2b^2 = 4k^2 \Rightarrow b^2 = 2k^2 \Rightarrow b^2$ é par, daí b é par. Contradição, pois a e b são primos entre si.

(b) $\sqrt{3}$ é irracional.
Observe primeiramente que se p^2 *é múltiplo de* 3, *então* p *é múltiplo de* 3. De fato, vamos provar, usando a contrapositiva, que se p não é múltiplo de 3, então p^2 não é múltiplo de 3.

Note que p não múltiplo de 3, pelo Teorema 2.1, significa que $p = 3q + r$, onde $q \in \mathbb{Z}$ e $0 < r < 3$.

Daí,

$$p^2 = (3q+r)^2 \Rightarrow$$
$$p^2 = 9q^2 + 6qr + r^2 \Rightarrow$$
$$p^2 = 3(3q^2 + 2qr) + r^2 \Rightarrow$$
$$p^2 = 3q' + r^2$$

onde $q' = (3q^2 + 2qr) \in \mathbb{Z}$.

Estudemos o resto r, $0 < r < 3$,

(i) $r = 1$

$$p^2 = 3q' + 1$$

Logo, neste caso, p^2 não é múltiplo de 3.

(ii) $r = 2$

$$p^2 = 3q' + 4 \Rightarrow p^2 = 3q' + 3 + 1 \Rightarrow p^2 = 3q'' + 1$$

onde $q'' = (q' + 1) \in \mathbb{Z}$. Também, neste caso, p^2 não é múltiplo de 3.

Agora sim mostraremos que $\sqrt{3}$ é um número irracional. Para tanto, suponhamos por absurdo que $\sqrt{3}$ é um número racional. Logo, existem $p, q \in \mathbb{Z}$, com $q > 1$ e $mdc(p, q) = 1$, tal que $x = \dfrac{p}{q}$.

Assim:

$$x^2 = \left(\frac{p}{q}\right)^2 \Rightarrow 3 = \frac{p^2}{q^2} \Rightarrow 3q^2 = p^2.$$

Segue que p^2 é múltiplo de 3. Logo p é múltiplo de 3. Consequentemente, p pode ser escrito da forma $p = 3a$, para algum $a \in \mathbb{Z}$.
Substituindo $p = 3a$, temos,

$$3q^2 = 9a^2 \Rightarrow \frac{3q^2}{3} = \frac{9a^2}{3} \Rightarrow q^2 = 3a^2.$$

Logo, q^2 é múltiplo de 3, e assim, q é múltiplo de 3.
Portanto, p e q são múltiplos de 3, o que é absurdo, já que por hipótese p e q são primos entre si.

(c) Se um número natural não é o quadrado de um outro número natural, sua raiz quadrada é um número irracional. Para provar este fato, seja $n \in \mathbb{N}$. Se $\dfrac{p}{q} \in \mathbb{Q}$ é tal que

$$\left(\frac{p}{q}\right)^2 = n \Longrightarrow p^2 = nq^2$$

Como os fatores primos de p^2 e q^2 aparecem todos com expoente par, o mesmo deve ocorrer com os fatores primos de n. Então n é o quadrado de algum número natural.

Além dos números racionais e irracionais, outros importantes números reais são os números algébricos e transcedentes, os quais são definidos a seguir.

Definição 2.6. ***(a)*** *Qualquer solução de uma equação polinomial da forma*

$$a_n x^n + a_{n-1} x^{n-1} + ... + a_1 x + a_0 = 0, \ a_i \in \mathbb{Z}, \ \forall \ i \in \{0, ..., n\} \tag{2.13}$$

*é chamado um **número algébrico**. Ou seja, um número α é algébrico quando é possível encontrar uma equação polinomial com coeficientes inteiros, da qual α seja raiz.*

(b) *Um número que não seja algébrico é chamado **transcendente**.*

Exemplo 2.10. (i) Qualquer número racional $\alpha = \dfrac{p}{q}$, é algébrico porque α é a raiz da equação $qx - p = 0$.

(ii) Qualquer inteiro algébrico é um número algébrico.

Os números algébricos possuem algumas propriedades de fechamento, as quais são listadas no Teorema a seguir.

Teorema 2.4. *Valem as seguintes propriedades:*

(i) A soma de dois números algébricos é um algébrico;

(ii) O produto de dois números algébricos é um algébrico;

(iii) O simétrico $-\alpha$ de um número algébrico α é algébrico;

(iv) O inverso α^{-1} de um número algébrico $\alpha \neq 0$ é um inteiro algébrico.

Demonstração. **(i)** e **(ii)** Vide [1].

(iii) Se α é algébrico, então ele é raiz de uma equação do tipo (2.13). Portanto $-\alpha$ é raiz da equação

$$(-1)^n a_n x^n + (-1)^{n-1} a_{n-1} x^{n-1} + ... + (-1) a_1 x + a_0 = 0.$$

(iv) Se α satisfaz a equação (2.13) e $\alpha \neq 0$, então α^{-1} satisfaz à equação

$$a_0 x^n + a_1 x^{n-1} + ... + a_{n-1} x + a_n = 0.$$

□

2.3 Números Transcendentes

Como na seção 2.2, um número é transcendente quando este não é algébrico, ou seja, quando tal número não é raiz de alguma equação polinomial de coeficientes inteiros não nulos. No que segue, estamos interessados em mostrar a existência de números transcendentes. Para tal necessitamos de alguns conceitos.

Definição 2.7. *Um conjunto A é enumerável se seus elementos podem ser colocados em correspondência biunívoca com os números naturais. Mais precisamente, A é enumerável se existir uma função bijetiva, (isto é, uma função injetiva e sobrejetiva), $f : \mathbb{N} \to A$.*

Exemplo 2.11. **(a)** O conjunto dos números pares positivos é enumerável. Seja $P = \{2n, n \in \mathbb{N}\}$, e considere a seguinte função

$$\begin{array}{rccc} f: & \mathbb{N} & \longrightarrow & P \\ & n & \longmapsto & 2n \end{array}$$

(i) f é injetora. Suponha que $f(x) = f(y)$. Queremos mostrar que $x = y$. Como

$$f(x) = f(y) \Rightarrow 2x = 2y \Rightarrow x = y.$$

Portanto f, é injetora.

(ii) f é sobrejetora, isto é $f(\mathbb{N}) = P$. De fato,

- $f(\mathbb{N}) \subset P$ pela definição de imagem;
- $P \subset f(\mathbb{N})$, pois, seja $b \in P$ qualquer, então $b = 2n_0$ para algum $n_0 \in \mathbb{N}$. Tomando $x = n_0$, temos que $f(x) = f(n_0) = 2n_0 = b$, ou seja, $b \in f(\mathbb{N})$, logo $b = f(x)$. Portanto f é sobrejetora.

Logo por (i) e (ii), f é bijetora.

(b) O conjunto dos números ímpares positivos é enumerável. Basta considerar a função

$$f: \mathbb{N} \longrightarrow I$$

$$n \longmapsto 2n - 1$$

onde $I = \{2n-1, n \in \mathbb{N}\}$. A demontração pode ser feita de modo análogo ao exemplo (a).

(c) O conjunto $\mathbb{Z}$ é enumerável. Observe a correspondência abaixo

$$\begin{array}{cccccccc} ..., & -3, & -2, & -1, & 0, & 1, & 2, & 3, & ... \\ & \updownarrow & \updownarrow & \updownarrow & \updownarrow & \updownarrow & \updownarrow & \updownarrow & \\ ... & 7, & 5, & 3, & 1, & 2, & 4, & 6, & ... \end{array}$$

Esta correspondência pode ser descrita pela função definida por partes

$$\begin{array}{rccc} f: & \mathbb{Z} & \longrightarrow & \mathbb{N} \\ & n & \longmapsto & f(n), \end{array}$$

onde

$$f(n) = \begin{cases} 2n, & \text{se } n > 0, \\ -2n+1, & \text{se } n \leq 0. \end{cases}$$

(i) f é injetora, isto é, $x \neq y \Rightarrow f(x) \neq f(y)$, pois:
- se $x, y > 0$, $f(x) = 2x \neq 2y = f(y)$
- se $x, y < 0$, $f(x) = -2x + 1 \neq -2y + 1 = f(y)$
- se $x > 0$ e $y < 0$, temos que $f(x) = 2x$ e$f(y) = -2y + 1$ daí, $f(x) = 2x \neq 2y \neq -2y \neq -2y + 1 = f(y)$;
- se $x < 0$ e $y > 0$, idem item anterior;
- se $x = 0$ e $y > 0$ (ou $y = 0$ e $x > 0$), então $f(x) = f(0) = 1$ e $f(y) = 2y$, daí $f(y) = 2y \neq 1 = f(0) = f(x)$
- se $x = 0$ e $y < 0$ (ou $y = 0$ e $x < 0$), então $f(x) = f(0) = 1$ e $f(y) = -2y + 1$, daí $f(y) = -2y + 1 \neq 1 = f(0) = f(x)$

Portanto, pelos casos considerados acima, f é injetora.

(ii) f é sobrejetora, isto é, $f(\mathbb{Z}) = \mathbb{N}$. De fato,
- $f(\mathbb{Z}) \subset \mathbb{N}$ pela definição de imagem;
- $\mathbb{N} \subset f(\mathbb{Z})$, pois, seja $n \in \mathbb{N}$. Se n é **par**, então $n = 2k, k \in \mathbb{N}$. Logo, tomando $x = k$, temos

$$n = 2k = f(k) = f(x).$$

Se n é **ímpar**, então $n = 2k+1, k \in \mathbb{N}$, logo tomando $x = -k$, temos

$$n = 2k+1 = -2(-k)+1 = f(-k) = f(x) \ \in f(\mathbb{Z}).$$

Portanto f é sobrejetora.

Por (i) e (ii) f é bijetora. Como f é bijetora, existe $g^{-1} : \mathbb{N} \to \mathbb{Z}$, assim basta tomarmos $f = g^{-1}$.

(d) O conjunto dos números racionais é enumerável. Mostremos primeiramente que o conjunto dos números racionais positivos é enumerável.

$$\begin{array}{ccccccccccc}
\frac{1}{1} & \to & \frac{1}{2} & & \frac{1}{3} & \to & \frac{1}{4} & & \frac{1}{5} & \to & \cdots \\
 & \swarrow & & \nearrow & & \swarrow & & \nearrow & & & \\
\frac{2}{1} & & \frac{2}{2} & & \frac{2}{3} & & \frac{2}{4} & & \frac{2}{5} & & \cdots \\
 & \nearrow & & \swarrow & & \nearrow & & \swarrow & & & \\
\frac{3}{1} & & \frac{3}{2} & & \frac{3}{3} & & \frac{3}{4} & & \frac{3}{5} & & \cdots \\
 & \swarrow & & \nearrow & & \swarrow & & \nearrow & & & \\
\frac{4}{1} & & \frac{4}{2} & & \frac{4}{3} & & \frac{4}{4} & & \frac{4}{5} & & \cdots \\
 & \nearrow & & \swarrow & & \nearrow & & \swarrow & & & \\
\frac{5}{1} & & \frac{5}{2} & & \frac{5}{3} & & \frac{5}{4} & & \frac{5}{5} & & \cdots \\
 & \swarrow & & & & & & & & & \\
\vdots & & \vdots & & \vdots & & \vdots & & \vdots & &
\end{array}$$

Observe que todos os números da forma $\frac{p}{q}$, com $p, q \in \mathbb{N}$ e $q \neq 0$ aparecem no quadro acima. Se o percorrermos seguindo as flechas temos uma ordenação desse conjunto, a função f

$$\begin{array}{rccc}
f: & \mathbb{N} & \longrightarrow & \mathbb{Q}^+ \\
 & n & \longmapsto & f(n)
\end{array}$$

é definida como $f(n) = n$-ésimo elemento que encontramos seguindo as flechas. Não é difícil ver que f é bijeção e que portanto o conjunto $\mathbb{Q}^+ = \{x \in \mathbb{Q}, \quad x > 0\}$ é enumerável.

A enumerabilidade de $\mathbb{Q}$ segue do item (i) do próximo Teorema, lembrando que $\mathbb{Q} = \mathbb{Q}^+ \cup \mathbb{Q}^- \cup \{0\}$, onde $\mathbb{Q}^- = \{x \in \mathbb{Q} : x < 0\}$.

A seguir demonstramos algumas propriedades sobre conjuntos enumeráveis.

Teorema 2.5. ***(i)*** *A união de um conjunto finito e um conjunto enumerável é enumerável;*

(ii) *A união de dois conjuntos enumeráveis é enumerável;*

(iii) *A união de um número finito de conjuntos enumeráveis é enumerável;*

(iv) *A união de um conjunto enumerável de conjuntos finitos é enumerável;*

(v) *A união de um conjunto enumerável de conjuntos enumeráveis é enumerável.*

Demonstração. **(i)** Seja $A = \{a_1, a_2, ..., a_n\}$ um conjunto finito e $B = \{b_1, b_2, ...\}$ um conjunto enumerável. O conjunto $A \cup B$ é enumerável. De fato, basta considerar a correspondência biunívoca entre $A \cup B$ e $\mathbb{N}$ dada por

$$\begin{array}{cccccc} a_1, & ..., & a_n, & b_1, & b_2, & ... \\ \updownarrow & & \updownarrow & \updownarrow & \updownarrow & \\ 1 & & n & n+1 & n+2 & ... \end{array}$$

(ii) Sejam $A = \{a_1, a_2, ...\}$ e $B = \{b_1, b_2, ...\}$ dois conjuntos enumeráveis, então $A \cup B$ é enumerável, já que possui a seguinte correspondência biunívoca,

$$\begin{array}{cccccc} a_1, & b_1, & a_2, & b_2, & a_3, & ... \\ \updownarrow & \updownarrow & \updownarrow & \updownarrow & \updownarrow & \\ 1 & 2 & 3 & 4 & 5 & ... \end{array}$$

(iii) Sejam $A_1, A_2, ..., A_n$ conjuntos enumeráveis, queremos mostrar que $A_1 \cup A_2 \cup ... \cup A_n$, é enumerável, $\forall\, n \in \mathbb{N}$. Para isto usamos o Princípio de Indução Finita. Note que para $k = 1$ a propriedade é válida pois A_1 é enumerável. Para $k = 2$ é válida pelo item (ii). Suponha que seja válida para k, ou seja, se $A_1, A_2, ..., A_k$ são enumeráveis, então $A_1 \cup A_2 \cup ... \cup A_k$ é enumerável. Provemos então que a propriedade é válida para $k+1$. $A_1, ..., A_k, A_{k+1}$ são enumeráveis, então

$$A_1 \cup A_2 \cup ... \cup A_k \cup A_{k+1}$$

é enumerável. Note que

$$A_1 \cup A_2 \cup ... \cup A_k \cup A_{k+1} = (A_1 \cup ... \cup A_k) \cup A_{k+1}$$

Considere $A = (A_1 \cup ... \cup A_k)$, então

$$A_1 \cup A_2 \cup ... \cup A_k \cup A_{k+1} = A \cup A_{k+1}.$$

Agora A é enumerável por Hipótese de Indução e $A \cup A_{k+1}$ é enumerável por (ii). Portanto $A_1 \cup ... \cup A_k \cup A_{k+1}$ é enumerável.

(iv) Seja $\{A_1, A_2, ..., A_n, ...\}$ um conjunto enumerável onde cada A_i é um conjunto finito, para qualquer $i \in \{1, ..., n, ...\}$.

Queremos mostrar que $A_1 \cup A_2 \cup ... \cup A_n \cup ...$ é enumerável. Suponha que $A_1 = \{a_{11}, a_{12}, ..., a_{1l_1}\}$, $A_2 = \{a_{21}, a_{22}, ..., a_{2l_2}\}$ e $A_n = \{a_{n1}, a_{n2}, ..., a_{nl_n}\}$. Então,

$$A_1 \cup A_2 \cup ... \cup A_n \cup ... = \{a_{11}, a_{12}, ..., a_{1l_1}, a_{21}, a_{22}, ..., a_{2l_2}, ..., a_{n1}, a_{n2}, ..., a_{nl_n}, ...\}$$

Defina a seguinte correspondência entre $A_1 \cup A_2 \cup ... \cup A_n \cup ...$ e $\mathbb{N}$:

$$\begin{array}{cccccccccccc} a_{11}, & ..., & a_{1_{l1}}, & a_{21}, & ..., & a_{2_{l2}}, & ..., & a_{n1}, & ..., & a_{n_{ln}}, & ... \\ \updownarrow & & \updownarrow & \updownarrow & & \updownarrow & & \updownarrow & & \updownarrow & \\ 1, & ..., & l_1, & l_1+1, & ..., & l_1+l_2, & ..., & l_1+l_2+...+l_{n-1}+1, & ... & l_{n+1} & ... \end{array}$$

Logo, $A_1 \cup A_2 \cup ... \cup A_n \cup ...$ é enumerável.

(v) Seja $\{A_1, A_2, ..., A_n, ...\}$ um conjunto enumerável onde cada A_i é um conjunto enumerável para qualquer $i \in \{1, .., n, ...\}$. Suponha que

$$A_1 = \{a_{11}, a_{12}, a_{13}, ...\},$$

$$A_2 = \{a_{21}, a_{22}, a_{23}, ...\},$$

$$A_n = \{a_{n1}, a_{n2}, a_{n3}, ...\}...$$

Disponha os elementos de $A_1, A_2, ..., A_n, ...$ como na tabela

$$\begin{array}{cccc} a_{11}, & a_{12}, & a_{13}, & \cdots \\ a_{21}, & a_{22}, & a_{23}, & \cdots \\ \cdots & \cdots & \cdots & \cdots \\ a_{n1}, & a_{n2}, & a_{n3}, & \cdots \\ \cdots & \cdots & \cdots & \cdots \\ \cdots & \cdots & \cdots & \cdots \\ \cdots & \cdots & \cdots & \cdots \end{array}$$

Formando flechas como feito em $\mathbb{Q}^+$ definimos f por $f(n) = n$-ésimo elemento que encontramos seguindo as flechas. Dessa forma definimos uma correspondência biunívoca entre $A_1 \cup A_2 \cup ... \cup A_n \cup ...$ e $\mathbb{N}$ e consequentemente provamos que é um conjunto enumerável. □

Observação 2.3. Se A é enumerável e $B \subset A$ é um conjunto infinito, então B também é enumerável, pois como A é enumerável existe uma correspondência biunívoca, f, entre $\mathbb{N}$ e A, então basta considerar a restrição $f|_B : B \to \mathbb{N}$.

Teorema 2.6. *O conjunto $\mathbb{R}$ dos números reais não é enumerável.*

Demonstração. Demonstraremos que o conjunto dos números reais $x \in [0, 1)$, (isto é, $0 \leq x < 1$) não é enumerável e, em virtude da observação acima, segue que $\mathbb{R}$ também não é enumerável. Primeiro note que os números $x \in [0, 1)$ tem uma representação decimal da forma

$$0, a_1 a_2 a_3 ... \tag{2.14}$$

onde a_j é um dos algarismos $0, 1, 2, 3, 4, 5, 6, 7, 8$ ou 9. Alguns números tem duas representações da forma (2.14), por exemplo, $\frac{1}{2}$ é igual $0, 50...$ ou $0, 499...$ Para tais números, escolhemos a representação decimal que termina. Em outras palavras, eliminamos os decimais (2.14) que a partir de uma certa ordem todos os elementos são 9. Suponhamos que os decimais tipo (2.14), ou que os números reais no intervalo $[0, 1)$, formam um conjunto enumerável.

$$\begin{aligned}
&0, a_{11}a_{12}a_{13}... \\
&0, a_{21}a_{22}a_{23}... \\
&0, a_{31}a_{32}a_{33}... \\
&...
\end{aligned} \tag{2.15}$$

Agora considerando o decimal $0, b_1b_2b_3...$ do seguinte modo: todos os b_i's são diferentes de 0 ou 9 e $b_1 \neq a_{11}$, $b_2 \neq a_{22}, ...$. É claro que $0, b_1b_2b_3 \ldots \neq 0, a_{n1}a_{n2}a_{n3} \ldots$, para todo n, pois $b_n \neq a_{nn}$. Logo $0, b_1b_2b_3 \ldots$ não está na tabela (2.15) o que é um absurdo, já que é um número real entre 0 e 1. □

Com os resultados anteriores provamos a existência de números transcedentes garantido pelo seguinte teorema.

Teorema 2.7. *Existem números transcendentes.*

Demonstração. Dado um polinômio com coeficientes inteiros,

$$P(x) = a_n x^n + ... + a_1 x + a_0 \tag{2.16}$$

Definimos sua altura como sendo o número natural

$$|P| = |a_n| + ... + |a_1| + |a_0| + n \tag{2.17}$$

O Teorema Fundamental da Álgebra nos diz que $P(x) = 0$, tem exatamente n raízes complexas. Todas, algumas ou nenhuma delas podem ser reais. Agora o número de polinômios do tipo (2.16) com uma dada altura é apenas um número finito (observe que é para essa afirmação que incluímos a parcela n na definição da altura em (2.17)). Logo, as raízes de todos os polinômios de uma dada altura formam um conjunto finito, consequentemente o conjunto de todas as raízes de todos os polinômios de todas as alturas formam um conjunto enumerável de conjuntos finitos. (Por exemplo, se $P(x) = 3x^4 - x^3 + x - 5$, então $|P| = |3| + |-1| + |0| + |1| + |-5| + 4$, pelo Teorema Fundamental da Álgebra $P(x)$ possui quatro raízes complexas e com essa altura podem existir até treze polinômios). Portanto, podemos concluir que o conjunto dos números algébricos reais é enumerável.

Agora, o conjunto dos números reais pode ser considerado como a união do conjunto dos números algébricos reais com o conjunto dos números transcendentes reais. Assim, como o conjunto $\mathbb{R}$ não é enumerável, o conjunto dos transcendentes reais deve ser não enumerável, já que, caso contrário, pelo item (ii) do Teorema 2.5, $\mathbb{R}$ seria enumerável. Consequentemente, existe um conjunto infinito não enumerável de números reais transcendentes. □

3 Os Números de Liouville

O Teorema 2.7 apresentado no capítulo anterior garante a existência de números transcendentes e, de fato, existem em abundância, mas não fornece explicitamente nenhum número transcendente. Foi o matemático francês Joseph Liouville, em 1851, que estebeleceu um critério para que um número real seja transcendente. Com o seu trabalho, passou a ser possível escrever explicitamente alguns números transcendentes.

Definição 3.1. *Um número algébrico α é de grau n se ele for raiz de uma equação polinomial de grau n com coeficientes inteiros, e se não existir uma equação desse tipo, de menor grau, da qual α seja raiz.*

Exemplo 3.1. Os Números Racionais coincidem com os números algébricos de grau 1, pois qualquer número racional da forma p/q, com $p, q \in \mathbb{Z}$ e $q \neq 0$ é raiz da equação polinomial de grau 1

$$qx - p = 0.$$

Definição 3.2. *Dizemos que um número real α é aproximável na ordem n por racionais se existirem uma constante $c > 0$ e uma sucessão $\{p_j/q_j\}$ de racionais distintos, com $q_j > 0$ e $mdc\,(p_j, q_j) = 1$ tais que*

$$\left|\alpha - \frac{p_j}{q_j}\right| < \frac{c}{q_j^n}\ . \tag{3.1}$$

Observação 3.1. Segue que, se um número α for aproximável na ordem n, então ele é aproximável em qualquer ordem k, com $k < n$. De (3.1) obtemos que

$$\left|\alpha - \frac{p_j}{q_j}\right| < c\ , \tag{3.2}$$

o que mostra que a sucessão $\{q_j\}$ não se mantém limitada. Podemos, portanto, deduzir que $q_j \to +\infty$. Logo, de (3.1) concluímos que

$$\lim_{j\to\infty}\left(\frac{p_j}{q_j}\right) = \alpha. \tag{3.3}$$

Ainda, veja que a importância da Definição 3.2 não está na existência de uma sucessão de racionais convergindo para α (tais sucessões sempre existem qualquer que seja o real

α, essa é a chamada densidade dos racionais no conjunto dos reais), mas no fato de que uma sucessão particular de racionais converge para α de acordo com (3.1). Outro ponto relevante na Definição 3.2 é que podemos tomar racionais todos diferentes, o que acarretará, em particular, que possamos torná-los diferentes de α, mesmo no caso deste ser racional.

Na sequência vamos estabelecer as relações entre os dois conceitos introduzidos nas Definições 3.1 e 3.2 dadas anteriormente.

Teorema 3.1. *Todo número racional (número algébrico de grau* 1*) é aproximável na ordem* 1*, e não é aproximável na ordem* k*, para* $k > 1$*.*

Demonstração. (i) (todo número racional é aproximável na ordem 1)

Seja p/q um número racional, com $q > 0$ e $mdc(p, q) = 1$. Pelo Teorema 2.2 existem $x_0, y_0 \in \mathbb{Z}$ tais que

$$px_0 - qy_0 = 1. \tag{3.4}$$

Na verdade a equação

$$px - qy = 1 \tag{3.5}$$

tem um número infinito de soluções da forma

$$x_t = x_0 + qt, \quad y_t = y_0 + pt, \tag{3.6}$$

para qualquer $t \in \mathbb{Z}$, as quais satisfazem (3.5), isto é,

$$px_t - qy_t = 1. \tag{3.7}$$

Fixando $k \in \mathbb{N}$, tal que $k > -x_0/q$, considere as sucessões $\{x_j\}, \{y_j\}$, definidas a partir de (3.6) por

$$x_j = x_0 + q(k + j), \quad y_j = y_0 + p(k + j), \quad j \in \mathbb{N}. \tag{3.8}$$

Pela restrição sobre k, temos $x_j > qj$ e daí $x_j > 0$, pois $q > 0$. Agora, afirmamos que

$$\frac{y_j}{x_j} \neq \frac{y_{j'}}{x_{j'}}, \quad se \quad j \neq j' \ , \tag{3.9}$$

pois caso houvesse igualdade entre os racionais em (3.9), por (3.6) e (3.4) teríamos $j = j'$. Em virtude de (3.7), os x_j's e os y_j's, definidos em (3.8), satisfazem a desigualdade

$$\left|\frac{p}{q} - \frac{y_j}{x_j}\right| = \frac{1}{qx_j} < \frac{2}{x_j},$$

o que prova que p/q é aproximável na ordem 1.

(ii) (todo número racional não é aproximável na ordem k, para $k > 1$) Para qualquer racional $v/u \neq p/q$ com $u > 0$, tem-se

$$\left|\frac{p}{q} - \frac{v}{u}\right| = \frac{|pu - qv|}{qu} \geq \frac{1}{qu}. \tag{3.10}$$

Ora, se p/q fosse aproximável na ordem 2, teríamos a existência de um $c > 0$, e de uma sucessão de racionais v_j/u_j diferentes, tais que

$$\left|\frac{p}{q} - \frac{v_j}{u_j}\right| < \frac{c}{u_j^2}. \tag{3.11}$$

De (3.10) e (3.11), segue-se que $1/qu_j < c/u_j^2$, isto é, $u_j < qc$, o que, entretanto, não pode ser verdade, pois $u_j \to +\infty$. Dessa forma, p/q não é aproximável na ordem 2, e portanto, também não é aproximável em nenhuma ordem superior. $\square$

Observação 3.2. A parte (ii) do Teorema 3.1 é consequência de um resultado mais geral demonstrado abaixo, a saber Corolário 3.1.

Teorema 3.2. *Todo número irracional é aproximável na ordem 2, isto é, existe uma constante $c > 0$ tal que a desigualdade abaixo se verifica para um número infinito de racionais p/q distintos,*

$$\left|\lambda - \frac{p}{q}\right| < \frac{c}{q^2}.$$

Demonstração. Seja α um número irracional e $n \in \mathbb{N}$. Representamos por $[x]$ a parte inteira de um número real x, isto é, o maior inteiro menor ou igual a x. Considere agora os $n+1$ números reais

$$0, \alpha - [\alpha], 2\alpha - [2\alpha], ..., n\alpha - [n\alpha], \tag{3.12}$$

os quais pertencem ao intervalo $[0,1) = \{x : 0 \leq x < 1\}$. Considere em seguida a partição do intervalo $[0,1)$ em n intervalos, disjuntos dois a dois, e da forma

$$\left[\frac{j}{n}, \frac{j+1}{n}\right), j = 0, 1, ..., n-1. \tag{3.13}$$

É claro que, pelo menos, dois dos reais em (3.12) estão em um mesmo intervalo do tipo (3.13). Digamos que eles sejam $n_1\alpha - [n_1\alpha]$ e $n_2\alpha - [n_2\alpha]$, com $0 \leq n_1 < n_2 \leq n$, para os quais temos então

$$|n_2\alpha - [n_2\alpha] - n_1\alpha + [n_1\alpha]| < \frac{1}{n}. \tag{3.14}$$

Seja agora $k = n_2 - n_1$ e $h = [n_2\alpha] - [n_1\alpha]$, os quais são inteiros com $k > 0, h \geq 0$. Logo, (3.14) pode ser escrito como

$$|k\alpha - h| < \frac{1}{n} \quad ou \quad \left|\alpha - \frac{h}{k}\right| < \frac{1}{nk},$$

segue que

$$\left|\alpha - \frac{h}{k}\right| < \frac{1}{k^2}, \tag{3.15}$$

para $k < n$. Em síntese, mostramos que, para cada n, existe um racional da forma h/k, com $k < n$, para o qual (3.15) se verifica. Agora, afirmamos que (3.15) se verifica para um número infinito de racionais h/k distintos. Suponha que tal não seja verdade, isto é, há apenas $h_1/k_1, ..., h_r/k_r$, racionais distintos satisfazendo (3.15).

Agora seja

$$\epsilon = min\{|\alpha - h_1/k_1|, ..., |\alpha - h_r/k_r|\}$$

e tome $n \in \mathbb{N}$ tal que $1/n < \epsilon$. Vimos que existe um racional h/k tal que

$$\left|\alpha - \frac{h}{k}\right| < \frac{1}{nk}.$$

Como $1/nk < 1/n < \epsilon$, segue que $h/k \neq h_i/k_i$, para i = 1, ... , r. Isso é uma contradição, pois h/k satisfaz (3.15). □

Observação 3.3. (i) O Teorema 3.2 afirma que um número irracional é aproximável, pelo menos, na ordem 2. Dependendo do número irracional ele poderá ser aproximável numa ordem superior a 2. O Teorema 3.3 abaixo fornece informações mais precisas sobre essas ordens de aproximação.

(ii) Hurwitz provou que a menor constante c que é válida para todos os irracionais na desigualdade acima é $1\sqrt{5}$. Mais precisamente, se $A < \dfrac{1}{\sqrt{5}}$, então existe um número irracional λ tal que para todos os racionais p/q, exceptuando-se um número finito deles. Para mais detalhes, confira I. Niven, *"Diophantine Approximations"*.

$$\left|\lambda - \frac{p}{q}\right| > \frac{A}{q^2}.$$

Teorema 3.3. *Seja α um número algébrico real de grau n. Então existe uma constante $A > 0$ tal que*

$$\left|\alpha - \frac{p}{q}\right| > \frac{1}{Aq^n} \tag{3.16}$$

para todo racional p/q. (Se $n = 1$, tome $p/q \neq \alpha$)

Demonstração. Uma vez que α é um número algébrico real de grau n, segue que α é uma solução de uma equação polinomial da forma

$$f(x) = a_n x^n + a_{n-1}x^{n-1} + ... + a_1 x + a_0 = 0. \tag{3.17}$$

Seja $d > 0$ tal que, no intervalo $[\alpha - d, \alpha + d]$ a única raiz de $f(x) = 0$ é α. A existência de um tal d segue do fato que a equação polinomial tem no máximo n raízes reais. Portanto d pode ser qualquer número menor que a menor das distâncias de α as demais raízes reais.

A seguir observamos que a derivada $f'(x)$ de $f(x)$ é um polinômio de grau $n - 1$, e, portanto, ela é limitada em qualquer intervalo finito. Seja pois $M > 0$ tal que

$$|f'(x)| < M, \text{ para } x \in [\alpha - d, \alpha + d]. \tag{3.18}$$

Para qualquer racional p/q, com $q > 0$, em $[\alpha - d, \alpha + d]$ temos, aplicando o Teorema do Valor Médio, que
$$f(\alpha) - f(p/q) = (\alpha - p/q)f'(\xi),$$
com $\xi \in (\alpha - d, \alpha + d)$. Como $f(\alpha) = 0$, obtemos
$$\left| f\left(\frac{p}{q}\right) \right| = \left| \alpha - \frac{p}{q} \right| |f'(\xi)| \leq M \left| \alpha - \frac{p}{q} \right|, \tag{3.19}$$
em que usamos a estimativa (3.18) no último passo. Para obter a desigualdade buscada, necessitamos de uma estimativa inferior para $f(p/q)$:
$$\left| f\left(\frac{p}{q}\right) \right| = \left| \frac{a_n p^n + a_{n-1} q p^{n-1} + ... + a_0 q^n}{q^n} \right| \geq \frac{1}{q^n}. \tag{3.20}$$
De (3.19) e (3.20) segue que
$$\left| \alpha - \frac{p}{q} \right| > \frac{1}{Mq^n},$$
para $p/q \in [\alpha - d, \alpha + d]$. Se p/q não estiver nesse intervalo teremos, então
$$\left| \alpha - \frac{p}{q} \right| > d,$$
e como $q \geq 1$ temos
$$\left| \alpha - \frac{p}{q} \right| > \frac{d}{q^n}.$$
Tomamos, finalmente, $1/A$ igual ao menor dos números $1/M$ e d, e obtemos a relação (3.16) para todos os racionais p/q. □

Corolário 3.1. *Se α é um número algébrico real de grau n, então α não é aproximável na ordem $n+1$.*

Demonstração. Por contradição, suponha que existe $c > 0$ e uma sucessão p_j/q_j de racionais distintos tais que
$$\left| \alpha - \frac{p_j}{q_j} \right| < \frac{c}{q_j^{n+1}}. \tag{3.21}$$
Para tais racionais, seguir-se-ia de (3.16) e (3.21) que
$$\frac{1}{Aq_j^n} < \frac{c}{q_j^{n+1}} \quad ou \quad q_j < Ac.$$
Mas a última desigualdade não é possível, pois $q_j \to +\infty$. □

Observação 3.4. Uma versão mais forte do Teorema (3.3) segue-se de um teorema de *Roth-Siegel-Thue*, que estabelece o seguinte: *"Seja λ um número algébrico; se houver uma infinidade de racionais distintos p/q, com $mdc(p,q) = 1, q > 0$, satisfazendo a desigualdade*
$$\left| \lambda - \frac{p}{q} \right| \leq \frac{1}{q^\nu},$$

*então $\nu \leq 2$". Segue-se daí que se $\mu > 2$, então há apenas um número finito de racionais p/q satisfazendo à desigualdade

$$\left|\lambda - \frac{p}{q}\right| \leq \frac{1}{q^{\mu}},$$

para um dado número algébrico λ. E finalmente, uma consequência imediata disso é o seguinte resultado. Dados um número algébrico λ e um número $\epsilon > 0$, existe uma constante $c > 0$ tal que

$$\left|\lambda - \frac{p}{q}\right| \geq \frac{C}{q^{2+\epsilon}}$$

para todos os números racionais p/q.

Definição 3.3. *Um número real α é chamado um número de Liouville se existir uma sucessão $\{p_j/q_j\}, q_j > 0, mdc(p_j, q_j) = 1$, com todos os elementos diferentes, e tal que*

$$\left|\alpha - \frac{p_j}{q_j}\right| < \frac{1}{q_j^j}. \tag{3.22}$$

Observação 3.5. Em particular podemos dizer que um número real α é chamado de número de Liouville se para todo número inteiro n existirem inteiros p e q tais que:

$$0 < \left|\alpha - \frac{p}{q}\right| < \frac{1}{q^n}, \quad q > 1.$$

Os números de Liouville são números que podem ser aproximados tanto quanto se queira por números racionais.

Vemos a seguir que os números de Liouville são irracionais e transcendentes.

Teorema 3.4. *Todo número de Liouville é irracional.*

Demonstração. Suponha, por contradição, que um certo número de Liouville $\alpha = \dfrac{a}{b}$ seja um inteiro positivo n tal que $2^{n-1} > b$. Como α é número de Liouville, então

$$0 < \left|\frac{a}{b} - \frac{p}{q}\right| < \frac{1}{q^n}.$$

A primeira desigualdade nos diz que $\dfrac{a}{b} \neq \dfrac{p}{q}$ o que equivale a $|aq - bp| \geq 1$, assim,

$$\left|\frac{a}{b} - \frac{p}{q}\right| = \left|\frac{aq - bp}{bq}\right| \geq \frac{1}{bq} > \frac{1}{2^{n-1}q} \geq \frac{1}{q^n},$$

o que leva a uma contradição. $\square$

Teorema 3.5. *Todo número de Liouville é transcendente.*

Demonstração. Suponha, por absurdo, que um certo número de Liouville α seja algébrico, digamos de grau n. Então, pelo Teorema 3.3, a relação (3.16) seria válida para todo racional. Em particular, para os p_j/q_j da Definição 3.3. Dessa forma teríamos

$$\frac{1}{Aq_j^n} < \left|\alpha - \frac{p_j}{q_j}\right| < \frac{1}{q_j^j},$$

de onde obtemos

$$q_j^{j-n} < A. \tag{3.23}$$

Como $q_j \to +\infty$, segue que (3.23) não é verificada para j suficientemente grande. A contradição está no fato de supormos que α seja algébrico. □

O resultado seguinte é útil nos exemplos.

Lema 3.1. *Seja α um número tal que*

$$\left|\alpha - \frac{v_j}{u_j}\right| < \frac{1}{u_j^j},$$

em que $\{v_j/u_j\}$ é uma sucessão de racionais diferentes com $u_j > 0$. (Atenção: não exigimos que $mdc(v_j, u_j)$ seja 1). Então α é um número de Liouville.

Demonstração. Considere a sucessão $\{p_j/q_j\}$, com $q_j > 0$ e $mdc(p_j, q_j) = 1$ definida por

$$\frac{p_n}{q_j} = \frac{v_n}{u_j}.$$

Então,

$$\left|\alpha - \frac{p_j}{q_j}\right| = \left|\alpha - \frac{v_j}{u_j}\right| < \frac{1}{u_j^j} \leq \frac{1}{q_j^j},$$

o que prova que α é um número de Liouville. □

Exemplo 3.2. Seja

$$\alpha = \sum_{k=1}^{\infty} \frac{1}{10^{k!}}. \tag{3.24}$$

Consideremos a sucessão de racionais definida por

$$\frac{v_j}{u_j} = \sum_{k=1}^{j} \frac{1}{10^{k!}}.$$

Temos,

$$\left|\alpha - \frac{v_j}{u_j}\right| = \sum_{k=j+1}^{\infty} \frac{1}{10^{k!}} = \frac{1}{10^{(j+1)!}}\left(1 + \frac{1}{10^{(j+2)!-(j+1)!}} + ...\right). \tag{3.25}$$

A expressão em parênteses é majorada por

$$1 + \frac{1}{10} + \frac{1}{10^2} + ... = \frac{10}{9}.$$

Logo, o último membro de (3.25) é majorado por

$$\frac{1}{(10^{j!})^j 10^{j!}} \cdot \frac{10}{9} < \frac{1}{(10^{j!})^j},$$

e portanto

$$\left|\alpha - \frac{v_j}{u_j}\right| < \frac{1}{(10^{j!})^j}.$$

Como $u_j = 10^{j!}$, segue que α definido em (3.24) é um número de Liouville.

Exemplo 3.3. Qualquer número da forma

$$\alpha = \sum_{k=1}^{\infty} \frac{a_k}{10^{k!}},$$

onde a_k é um qualquer dos números de 1 a 9, é um número de Liouville. Em particular, se $a_k = 1$ então α é a chamada constante de Liouville.

Definição 3.4. *A constante de Liouville foi o primeiro número transcendente historicamente reconhecido e é definida por*

$$L = \sum_{k=1}^{\infty} 10^{-k!} = 0,110001000000000000000001...$$

Note que a constante de Liouville corresponde a um decimal não periódico no qual o algarismo 1 ocupa a casa decimal correspondente a um fatorial $k!$ e as demais casas são ocupadas pelo algarismo 0.

Proposição 3.1. *A constante de Liouville é um número de Liouville.*

Demonstração. Considere um certo n inteiro e positivo fixo e defina p e q da seguinte forma: $p = \sum_{k=1}^{n} 10^{n!-k!}, \quad q = 10^{n!}$. Dessa forma,

$$\left|L - \frac{p}{q}\right| = \sum_{k=n+1}^{\infty} 10^{-k!} = \sum_{k=0}^{\infty} 10^{-(n+k+1)!} \leq \sum_{k=0}^{\infty} 10^{-(n+1)!-k} =$$

$$= 10^{-(n+1)!} \sum_{k=0}^{\infty} 10^{-k} < 10^{-n!n} = \frac{1}{q^n}$$

Portanto L é um número de Liouville. $\square$

4 Números Racionais e Irracionais: uma proposta didática na prática da sala de aula

Uma proposta didática na prática de uma aula no Ensino Médio seria o estudo dos Conjuntos Numéricos com ênfase na abordagem dos Números Racionais e Irracionais. Primeiramente vamos definir os Números Racionais.

Definimos **Números Racionais** todos aqueles que podem ser escritos como frações nas quais o numerador e o denominador são números inteiros e o denominador é diferente de zero. Representamos o conjunto dos Números Racionais pelo símbolo $\mathbb{Q}$.

Exemplos:

1. Os números inteiros: $3 = \dfrac{3}{1}$;
2. Os decimais exatos: $0,2 = \dfrac{2}{10}$;
3. Os decimais periódicos: $0,333... = \dfrac{3}{9} = \dfrac{1}{3}$.

Nos decimais periódicos, ou dízimas periódicas, chama-se **período** o algarismo ou grupo de algarismos que se repete infinitamente, e **geratriz** de uma dízima periódica a fração equivalente a ela.

Em uma dízima periódica simples, o período começa no primeiro algarismo após a vírgula.

Exemplo: Determinar a geratriz da dízima periódica $0,313131...$. Seja $x = 0,313131...$. Como há dois algarismos no período, multiplicamos ambos os membros da igualdade por 100 . Assim:

$$100x = 31,313131... \Rightarrow 100x - x = 31,313131... - 0,313131... \Rightarrow 99x = 31 \Rightarrow x = \frac{31}{99}.$$

Na dízima periódica composta, há um ou mais algarismos depois da vírgula que não fazem parte do período.

Exemplo: Determinar a geratriz da dízima periódica $0,5282828...$. Novamente, seja $x = 0,5282828...$. Primeiramente multiplicamos os dois membros da igualdade por 10, pois há apenas 1 algarismo antes do período. Assim obtemos $10x = 5,282828...$.

Em seguida, multiplicamos x por 1000 resultando em $1000x = 528,282828...$. Dessa forma:

$$1000x - 10x = 528,2828282... - 5,282828... \Rightarrow 990x = 523 \Rightarrow x = \frac{523}{990}.$$

Neste momento podem ser sugeridos alguns exercícios nos quais os alunos devem determinar a geratriz de algumas dízimas periódicas.

Exercício. Determine a geratriz da dízima periódica $1,23333...$.

Resolução. Considere $x = 1,23333...$. Multiplique x por 10 e por 100 obtendo, respectivamente, $10x = 12,3333...$ e $100x = 123,3333...$. Agora basta subtrair

$$100x - 10x = 123,3333... - 12,3333... \Rightarrow 90x = 111 \Rightarrow x = \frac{111}{90}.$$

Resposta: $1,23333... = \dfrac{111}{90}$.

Há números decimais que não são exatos e nem periódicos. Tais números decimais são impossíveis de se escrever na forma fracionária e, por isso, não são racionais. Esses números são chamados de **Números Irracionais**.

A história da origem dos Números Irracionais está no mundo grego clássico, no momento em que os pitagóricos resolveram calcular a medida da diagonal d de um quadrado de lado igual a 1. Ao utilizarem o Teorema de Pitágoras, encontraram:

$$d^2 = 1^2 + 1^2 \Rightarrow d^2 = 2,$$

e se questionaram: qual o número racional que elevado ao quadrado resulta 2? Após algumas tentativas perceberam que d possuía medida entre $1,414$ e $1,415$, pois $1,414^2 = 1,999396$ e $1,415^2 = 2,002225$. Mesmo tentando novas aproximações com mais casas decimais não foi possível determinar nenhum racional. Assim dizemos que $\sqrt{2}$ é um número irracional.

Exercício. Demonstre que $\sqrt{2}$ é irracional.

Resolução. De fato, supomos $\sqrt{2}$ racional, então este pode ser escrito como $\dfrac{a}{b}$, com $a, b \in \mathbb{Z}$ e $b \neq 0$ e a, b irredutíveis, ou seja, primos entre si. Então temos: $\sqrt{2} = \dfrac{a}{b} \Rightarrow 2 = \dfrac{a^2}{b^2} \Rightarrow a^2 = 2b^2$. Como a^2 é par, então a é par (pois se a fosse ímpar, então $a = 2k+1, k \in \mathbb{Z} \Rightarrow a^2 = 4k^2+4k+1$ então a^2 seria ímpar). Assim, sendo a par, então $a = 2k \Rightarrow a^2 = 4k^2 \Rightarrow 2b^2 = 4k^2 \Rightarrow b^2 = 2k^2 \Rightarrow b^2$ é par, daí b é par. Contradição, pois a e b são primos entre si.

De modo geral, as raízes quadradas de números naturais que não são quadrados perfeitos são números irracionais, como, por exemplo, $\sqrt{3} = 1,7320508...$.

Existem outros irracionais importantes como $\pi = 3,14159265358...$ (razão entre o comprimento de uma circunferência e o seu diâmetro) e o número $e = 2,7182818...$(base do logaritmo natural). O número π e o número e também são denominados números

transcendentes pois não são solução de nenhuma equação polinomial de coeficientes inteiros não nulos.

Observação:

i) Dados α irracional e r racional não nulo, então: $\alpha + r$; $\alpha.r$; $\dfrac{\alpha}{r}$ e $\dfrac{r}{\alpha}$ são todos números irracionais.

Exemplos:

$\sqrt{2}+1$; $3\sqrt{2}$; $\dfrac{\sqrt{3}}{2}$ e $\dfrac{3}{\sqrt{5}}$ são números irracionais.

ii) A soma, subtração, multiplicação ou divisão de dois irracionais pode resultar em um racional ou irracional.

Exemplos:

$\sqrt{2}+\sqrt{3}$; $\sqrt{2}.\sqrt{3}$; $\sqrt{2}-\sqrt{3}$ e $\dfrac{\sqrt{2}}{\sqrt{3}}$ são números irracionais.

$\left(2+\sqrt{3}\right) + \left(2-\sqrt{3}\right) = 4$; $\sqrt{3}.\sqrt{12} = 6$; $\sqrt{5}-\sqrt{5} = 0$ e $\dfrac{\sqrt{27}}{\sqrt{3}} = 3$ são números racionais.

Exercício. O número $x = \left[\left(\sqrt{2}\right)^{\sqrt{2}}\right]^{\sqrt{2}}$ é racional.

a) Usando propriedades das potências, calcule x.

b) Prove que existem dois números irracionais α e β tais que α^{β} é racional.

Resolução.

a) $x = \left[\left(\sqrt{2}\right)^{\sqrt{2}}\right]^{\sqrt{2}} = \left(\sqrt{2}\right)^{\sqrt{2}.\sqrt{2}} = \left(\sqrt{2}\right)^{2} = 2.$

b) Sabemos que $\sqrt{2}$ é irracional e que $\left[\left(\sqrt{2}\right)^{\sqrt{2}}\right]^{\sqrt{2}}$ é racional (por a). Ora, $\left(\sqrt{2}\right)^{\sqrt{2}}$ é racional ou irracional. Se $\left(\sqrt{2}\right)^{\sqrt{2}}$ é racional, então existem dois irracionais α e β tais que α^{β} é racional ($\alpha = \beta = \sqrt{2}$). Se $\left(\sqrt{2}\right)^{\sqrt{2}}$ é irracional, então existem dois irracionais α e β tais que α^{β} é racional ($\alpha = \left(\sqrt{2}\right)^{\sqrt{2}} e\ \beta = \sqrt{2}$).

A aula deve ser encerrada levando os alunos a refletir sobre o conjunto dos **Números Reais** (representado por $\mathbb{R}$) que é formado pela união dos números racionais com os números irracionais.

Referências

[1] FIGUEIREDO, D. G. *Números Irracionais e Transcendentes*. 3. ed. Rio de Janeiro: Sociedade Brasileira de Matemática, 2002.

[2] DOMINGUES, H. H. *Álgebra Moderna*. 2. ed. Rio de Janeiro: Editora Atual, 1982.

[3] HEFEZ, A. *Elementos de Aritmética*. 3. ed. Rio de Janeiro: Sociedade Brasileira de Matemática, 2002.

[4] EVES, H. *Introdução à História da Matemática*. 1. ed. Campinas: Editora Unicamp, 2004.

[5] BENTLEY, P. *O Livro dos Números*. 1. ed. Rio de Janeiro: Editora Zahar, 2010.