UNIVERSIDADE FEDERAL DE SANTA CATARINA
UNIVERSIDADE VIRTUAL DO MARANHÃO
DEPARTAMENTO DE MATEMÁTICA E FÍSICA
CURSO DE ESPECIALIZAÇÃO EM MATEMÁTICA

NÚMEROS IRRACIONAIS E TRANSCENDENTES

IMPERATRIZ
2009

JULIMAR CARLOS DE OLIVEIRA
CARLOS CRUZ GOMES

NÚMEROS IRRACIONAIS E TRANSCENDENTES

Monografia apresentada ao Departamento de Matemática e Física da UFSC, como requisito parcial para obtenção do grau de professor Especialista em Matemática.

Orientador: Prof.º Eliezer Batista

IMPERATRIZ
2009

Oliveira, Julimar Carlos

Números irracionais e transcendentes/ Julimar Carlos de Oliveira; Carlos Cruz Gomes.-Imperatriz, 2009.

Monografia (Especialização em Matemática) Universidade Federal de Santa Catarina e Universidade Virtual do Maranhão, 2009.

1.Números Irracionais. 2.Números Transcendentes. 3. Números Algébricos. I Gomes, Carlos Cruz. II.Título.

CDU 511.14

JULIMAR CARLOS DE OLIVEIRA
CARLOS CRUZ GOMES

NÚMEROS IRRACIONAIS E TRANSCENDENTES

Monografia apresentada ao Departamento de Matemática e Física da UFSC, como requisito parcial para obtenção do grau de Professor Especialista em Matemática.

Aprovada em ______/_______/________

BANCA EXAMINADORA

____
Prof.º Eliezer Batista (orientador)

____
Prof°. Dr. Lício Hernanes Bezerra

____
Prof°. Dr. Ivan Pontual Costa e Silva

A todos os professores do curso de especialização, em especial ao professor Eliezer Batista e à Coordenadora do curso, Neri Terezinha Both Carvalho, por terem se empenhado para o bom andamento deste curso.

Carlos Cruz

A todos os professores do curso de especialização em Matemática da UFSC e, em especial, ao professor Eliezer Batista por ter nos orientado de forma tão prestativa ao longo de todo o trabalho.

Julimar Carlos

AGRADECIMENTOS

A todos os professores do curso de especialização em matemática da UFSC que durante todo o curso nos proporcionaram os fundamentos necessários para a busca do conhecimento.

A Deus, pelo dom da vida, e por ter nos dado, até aqui, força, saúde e inteligência para que pudéssemos alcançar mais essa conquista.

A toda a equipe de funcionários da Univima por terem provido os meios necessários para facilitar o nosso acesso ao saber.

Aos nossos colegas de turma, pelos conhecimentos e experiências compartilhados no decorrer de todo o curso.

A todos aqueles que de uma forma direta ou indireta contribuíram para que pudéssemos alcançar nosso tão almejado objetivo.

A filosofia está escrita nesse grande livro, ou seja, o universo, que se encontra aberto continuamente ante os nossos olhos, mas ele não pode ser entendido a menos que se aprenda, primeiro, a ler sua linguagem e interpretar as letras com as quais o compuseram. Ele foi escrito no idioma da matemática e seus símbolos são triângulos, círculos e outras figuras geométricas sem as quais é humanamente impossível entender uma única palavra de seu texto.

–Galileu Galilei, Il Saggiatore (1623)

RESUMO

Este trabalho trata dos números irracionais e transcendentes caracterizando-os sob diferentes aspectos. Particularmente traz a demonstração da irracionalidade do número π e do número e de Euler, base do logaritmo natural. Também apresenta uma demonstração da transcendência do número e baseada no roteiro de exercícios propostos por D.G. de Figueiredo em [4], além de um pequeno apanhado histórico sobre π, e, números algébricos e transcendentes.

Palavras-chave: números racionais, números irracionais, números algébricos, números transcendentes, número π, numero e.

SUMÁRIO

INTRODUÇÃO 8

1. CAPÍTULO I   NÚMEROS RACIONAIS E IRRACIONAIS 11

1.1 Caracterização dos Números Racionais...11

1.2 Radiciação e Irracionalidade...15

1.3 Enumerabilidade dos Racionais..18

1.4 Não Enumerabilidade dos Irracionais...21

2. CAPÍTULO II   ALGUNS NÚMEROS IRRACIONAIS.......................................24

2.1 Irracionalidade do Número *e*...24

2.2 Um pouco da História do Número π...29

2.3 Irracionalidade do Número π...30

3. CAPÍTULO III   NÚMEROS ALGÉBRICOS TRANSCENDENTES......................35

3.1 Um Pouco Sobre Números Algébricos e Transcendentes...........................35

3.2 Caracterização dos Números Algébricos e Transcendentes.......................36

4. CAPÍTULO IV   A TRANSCÊNDENCIA DO NÚMERO *e*...................................43

5. CONCLUSÃO...53

6. REFERÊNCIAS...55

7. APÊNDICES..56

1. Algoritmo da Divisão de Euclides..57

2. Teorema Fundamental da Aritmética...58

INTRODUÇÃO

Desde a aurora da história escrita os seres humanos têm necessitado lidar com números. Para os antigos, e para algumas tribos ainda hoje, os números estão resumidos aos naturais. De fato, quando se torna necessário enumerar aquilo que possuímos, os números naturais são suficientes. Cedo ou tarde, porém, devemos lidar com medições, encontrar a área de um terreno, o volume de um recipiente ou a distância entre duas cidades e é altamente improvável que tais medidas resultem em valores exatos de unidades. Daí surge a necessidade de frações.

As frações já eram conhecidas pelos egípcios e babilônios que criaram meios engenhosos de registrá-las e de fazer cálculos com elas. Mas foram os gregos, influenciados pelos ensinamentos de Pitágoras, que fizeram das frações o centro de seu sistema matemático filosófico, elevando-as a uma condição quase mítica. Os pitagóricos acreditavam que tudo no mundo, da física e da cosmologia até a arte e a arquitetura, podia ser expresso em termos de frações, isto é, números racionais. Esta crença provavelmente originou-se do interesse de Pitágoras pelas leis da harmonia musical. Assim, Pitágoras raciocinou que se a música era baseada em números racionais, certamente o mesmo deveria acontecer com o universo inteiro. E os números racionais passaram a dominar a visão grega do mundo, exatamente como o pensamento racional dominou sua filosofia (de fato, a palavra grega para racional é *logos*, da qual deriva o termo moderno, *lógica*).

É claro que não foram apenas argumentos filosóficos que colocaram os números racionais tão no centro da matemática. Uma propriedade que distingue esses números dos inteiros é que os racionais formam um conjunto *denso* de números

A palavra *densa* reflete com precisão o modo como os racionais se distribuem ao longo da linha dos números. Pegue qualquer segmento de reta e, não importa o quão pequeno ele seja, estará sempre povoado por um número infinito de "pontos racionais". Assim parece natural concluir, como os gregos fizeram, que toda a linha dos números é povoada por pontos racionais. Mas na matemática o que *parece* ser uma conclusão natural muitas vezes se revela falsa. Um dos momentos mais importantes da história da matemática foi a descoberta de que os números racionais, apesar de sua densidade, deixam "buracos" ao longo da linha dos números, ou seja, pontos que não correspondem a nenhum número racional.

A descoberta desses buracos é atribuída a Pitágoras, embora possa ter sido feita por um de seus discípulos. A descoberta envolveu a diagonal de um quadrado unitário. Chamando o comprimento da diagonal de x, pelo Teorema de Pitágoras teremos

$x^2 = 1^2 + 1^2 = 2$**,** de modo que x é a raiz quadrada de 2, que escrevemos $\sqrt{2}$. Os pitagóricos, é claro, presumiram que este número era igual a alguma fração e tentaram pertinazmente encontrá-lo. Certo dia, porém, um deles fez a espantosa descoberta de que $\sqrt{2}$ não podia ser igual a uma fração. E assim foi descoberta a existência dos números *irracionais.*

A descoberta de que $\sqrt{2}$ é irracional deixou os pitagóricos num estado de choque, pois lá estava uma quantidade que podia claramente ser medida e até mesmo construída com esquadro e compasso e, no entanto, não se tratava de um número racional. Fiéis ao seu juramento de segredo, os pitagóricos se comprometeram a manter a descoberta somente entre eles.

Entretanto, o conhecimento da descoberta espalhou-se e logo outros números irracionais foram encontrados. Na época em que Euclides escreveu seus *Elementos*, no século III a.C., os números irracionais já tinham deixado de ser novidade. No entanto, uma teoria inteiramente satisfatória dos irracionais, destituída de considerações geométricas, só apareceu em 1872, quando Richard Dedekind (1831-1916) publicou seu famoso ensaio *Continuidade e números irracionais.*

Juntando o conjunto dos números racionais com o dos irracionais obtemos o conjunto maior dos *números reais.*

Caracterizar os números irracionais a partir da construção dos racionais será nosso objetivo no primeiro capítulo. Já no segundo, demonstraremos a irracionalidade de duas das mais importantes constantes matemáticas; π e *e*, além de um pequeno apanhado histórico sobre eles.

Outra alternativa de classificarmos os reais é em *algébricos* e *transcendentes.* Dizemos que um número x é algébrico quando satisfaz uma equação polinomial com coeficientes inteiros, ou seja, existem $a_0, ..., a_n \in \mathbb{Z}$ para os quais

$$a_0 + a_1 x + a_2 x^2 + ... + a_{n-1} x^{n-1} a_n x^n = 0 .$$

A grande maioria dos números que encontramos satisfaz essa condição. Não é difícil perceber que todo número racional é algébrico assim, se um número não satisfizer a equação acima necessariamente deve ser irracional. A recíproca dessa afirmação não é verdadeira pois, por exemplo, a raiz *n*-ésima de todo número primo é irracional sendo que tal número, no entanto, é algébrico. Quando um número não satisfaz uma equação polinomial com coeficientes inteiros dizemos que ele é um número *transcendental* indicando com isso apenas que esses números transcendem, ou seja, vão além no reino dos números algébricos. A questão que intrigou por muito tempo os matemáticos era a seguinte: existirão números irracionais não algébricos? Essa resposta só foi dada por volta da metade do século XIX.

No terceiro capítulo nosso objetivo será caracterizar os números algébricos bem como demonstrar indiretamente que números não algébricos, ou seja, transcendentes, de fato existem.

No último capítulo demonstraremos a transcendência do número *e*, base dos logaritmos naturais, seguindo o roteiro dos exercícios propostos pelo professor Djairo Guedes de Figueiredo apresentado em [4].

Ao longo de todo este trabalho suporemos estabelecidas a existência e propriedades do conjunto $\mathbb{R}$ dos números reais como feito, por exemplo, em $[11]$.

CAPÍTULO I

NÚMEROS RACIONAIS E IRRACIONAIS

1.1 Caracterização dos Números Racionais

Uma fração $\frac{a}{b}$, com $b \neq 0$, diz-se irredutível se $mdc(a,b)=1$.Os números racionais costumam ser representados por frações ordinárias, representação essa que é única se tomarmos as frações em forma irredutível e com denominadores positivos. Assim, podemos definir números racionais da seguinte forma:

Definição 1.1 *Um número real é dito racional se pode ser escrito na forma* $\frac{a}{b}$*, com* $a \in \mathbb{Z}$ *e* $b \in \mathbb{Z}^*$*. Simbolicamente* $\mathbb{Q} = \left\{ x \in \mathbb{R}; x = \frac{a}{b}, com\ a \in \mathbb{Z}\ e\ b \in \mathbb{Z}^* \right\}$.

Vamos considerar a conversão de frações ordinárias em decimais, com vistas a entender quando a representação decimal resulta ser finita ou periódica.

A conversão de uma fração ordinária em número decimal se faz dividindo o numerador pelo denominador. Assim, podemos estabelecer a seguinte proposição.

Proposição 1.1 *Toda fração irredutível representa um decimal finito ou periódico.*

Demonstração

Seja $\frac{a}{b}$ uma fração irredutível. Pelo algoritmo de Euclides existem a_0 e $r_0 \in \mathbb{Z}$ tais que $a = ba_0 + r_0 \Rightarrow \frac{a}{b} = a_0 + \frac{r_0}{b}$, com $0 \leq r_0 < b$.

Podemos expandir essa divisão da seguinte forma:

$$\frac{a}{b} = a_0 + \frac{1}{10}\left(\frac{10r_0}{b}\right) = a_0 + \frac{1}{10}\left(a_1 + \frac{r_1}{b}\right) = a_0 + \frac{a_1}{10} + \frac{1}{10}\cdot\frac{r_1}{b},\ \text{com } 10r_0 = ba_1 + r_1 \text{ e } 0 \leq r_1 < b.$$

Continuando com o mesmo raciocínio teremos,

$$\frac{a}{b} = a_0 + \frac{a_1}{10} + \frac{1}{10^2}\left(\frac{10r_1}{b}\right) = a_0 + \frac{a_1}{10} + \frac{1}{10^2}\left(a_2 + \frac{r_2}{b}\right) = a_0 + \frac{a_1}{10} + \frac{a_2}{10^2} + \frac{1}{10^2}\cdot\frac{r_2}{b},$$

com $10r_1 = ba_2 + r_2$ e $0 \leq r_2 < b$.

Continuando com o mesmo raciocínio, encontraremos $r_3, r_4, ..., r_i$, com $0 \leq r_i < b \ \forall_i$. Acontece que os possíveis restos da divisão de qualquer número por b só pode ser $0,1,2,...,b-1$. Diante disso, teremos duas possibilidades:

i) $r_i = 0$ para algum i

Neste caso, a expansão de $\frac{a}{b}$ será;

$\frac{a}{b} = a_0 + \frac{a_1}{10} + \frac{a_2}{10^2} + ... + \frac{a_i}{10^i} + \frac{1}{10^i} \cdot \frac{r_i}{b} = a_0 + \frac{a_1}{10} + \frac{a_2}{10^2} + ... + \frac{a_i}{10^i} = a_0, a_1 a_2 ... a_i$ que representará um decimal finito.

ii) $r_i \neq 0 \ \forall i$

Neste caso, como as classes de restos módulo b são finitas, em algum momento teremos um $j > i$ tal que $r_{i+j} = r_i$. Assim, a partir do momento em que isso ocorrer, os algarismos do quociente voltarão a se repetir. Dessa forma, teremos;

$\frac{a}{b} = a_0 + \frac{a_1}{10} + \frac{a_2}{10^2} + ... + \frac{a_i}{10^i} + \frac{1}{10^i} \cdot \frac{r_i}{b} + ... + \frac{a_j}{10^j} + \frac{1}{10^j} \cdot \frac{r_j}{b}$ com $a_{i+1} = a_{j+1}, \ a_{i+2} = a_{j+2}, ...$ que resultará em

$\frac{a}{b} = a_0 + \frac{a_1}{10} + \frac{a_2}{10^2} + ... + \frac{a_i}{10^i} + \frac{a_{i+1}}{10^{i+1}} + ... + \frac{a_j}{10^j} = a_0, a_1 a_2 ... a_i \overline{a_{i+1} a_{i+2} ... a_j}$ que representará um decimal periódico. A barra sobre a seqüência de números indica que estes números são repetidos infinitas vezes. □

Por esse caso, concluímos também que o período terá no máximo $b-1$ algarismos. A recíproca dessa proposição também é verdadeira, como veremos agora.

Proposição 1.2 *Todo decimal finito ou periódico é racional.*

Demonstração:

Se x é decimal finito, então $x = a_0, a_1 a_2 ... a_r$, com $0 \leq a_i \leq 9 (i = 1, 2, ... r)$ e $a_0 \in \mathbb{Z}$. Multiplicando ambos os membros da igualdade por 10^r, obtemos:

$10^r x = a_0 a_1 a_2 ... a_r \Rightarrow x = \frac{a_0 a_1 a_2 ... a_r}{10^r}$ que é racional.

Considerando x um número decimal periódico, então $x = a_0, a_1 \dots a_r \overline{b_1 \dots b_s}$, com $0 \le a_i \le 9,\ 0 \le b_j \le 9,\ i = 1, 2, ..., r,\ j = 1, 2, ..., s\ e\ a_0 \in \mathbb{N}$. Multiplicando ambos os membros da igualdade por 10^r e 10^{r+s} respectivamente, obtemos:

α : $10^r x = a_0 a_1 a_2 ... a_r \overline{b_1 ... b_s}$

β : $10^{r+s} x = a_0 a_1 ... a_r b_1 ... b_s \overline{b_1 ... b_s}$.

Fazendo $a_0 a_1 a_2 ... a_r = a$, $a_0 a_1 \dots a_r b_1 \dots b_s = b$ e subtraindo α de β, obtemos:

$$10^{r+s} x - 10^r x = b - a \Rightarrow x\left(10^{r+s} - 10^r\right) = b - a \Rightarrow x = \frac{b-a}{10^{r+s} - 10^r},$$

que é racional. $\square$

Outra importante característica das frações irredutíveis se refere à decomposição do denominador em fatores primos, como veremos agora.

Proposição 1.3 *Se uma fração irredutível contém somente fatores primos 2 e/ou 5 no denominador, então representará um decimal finito.*

Demonstração:

Seja $x = \frac{a}{b}$ uma fração irredutível com a decomposição do denominador somente em fatores primos 2 e/ou 5. Então $\frac{a}{b}$ será da forma $\frac{a}{2^r \cdot 5^s}$ $(r, s \in \mathbb{N})$.

Se $r = s$, então $\frac{a}{2^r \cdot 5^r} = \frac{a}{10^r}$ e x é decimal finito. Se $r \ne s$, tomemos $n = \min(r, s)$ e $m = \max(r, s)$ e, assim, podemos introduzir fatores 2 e/ou 5 no denominador em numero suficiente para torná-lo potência de 10 e, dessa forma, teremos $x = \frac{a}{2^r \cdot 5^s} = \frac{a.q^{|r-s|}}{10^m}$ (com $q = 2$ se $n = r$ ou $q = 5$ se $n = s$) e novamente x é decimal finito. $\square$

Outra alternativa de representarmos um número racional é através de frações contínuas. Esse será o objetivo de nossa próxima proposição. Basicamente, para essa representação, utilizamos o algoritmo da divisão de Euclides que, como vimos na Proposição 1.1, após um número finito de passos nos fornecerá resto 1.

Proposição 1.4 *Um número é racional se, e somente se, representa uma fração contínua finita.*

Demonstração:

$\Rightarrow$ Considere o racional $\frac{a}{b}$ irredutível. Pelo algoritmo de Euclides existem a_0 e $r_1 \in$

tais que $a = ba_0 + r_1$, ou seja, $\frac{a}{b} = a_0 + \frac{r_1}{b}$, com $0 \le r_1 < b$. Se $r_1 = 1$, procedimento encerrado e teremos $\frac{a}{b} = a_0 + \frac{1}{b}$. Caso contrário, continuamos o procedimento, fazendo: $\frac{a}{b} = a_0 + \frac{1}{\frac{b}{r_1}} = a_0 + \cfrac{1}{a_1 + \frac{r_2}{r_1}}$, com $b = r_1 a_1 + r_2$ e $0 \le r_2 < r_1$. Se $r_2 = 1$, procedimento encerrado e teremos, $\frac{a}{b} = a_0 + \cfrac{1}{a_1 + \frac{1}{r_1}}$. Caso contrário, continuamos o procedimento, fazendo:

$$\frac{a}{b} = a_0 + \cfrac{1}{a_1 + \cfrac{1}{\frac{r_1}{r_2}}} = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \frac{r_3}{r_2}}},$$ com $r_1 = r_2 a_2 + r_3$ e $0 \le r_3 < r_2$.

Acontece que existem apenas $b-1$ naturais menores que b e como temos $b > r_1 > r_2 > r_3 > \dots$, teremos necessariamente um $r_n = 1$ que finalizará o procedimento e tornará $$\frac{a}{b} = a_0 + \cfrac{1}{a_1 + \cfrac{1}{\ddots + \cfrac{1}{a_{n-1} + \cfrac{1}{a_n}}}}$$

$\Leftarrow$ Por outro lado, dada uma fração contínua finita $$a_0 + \cfrac{1}{a_1 + \cfrac{1}{\ddots + \cfrac{1}{a_{n-3} + \cfrac{1}{a_{n-2} + \cfrac{1}{a_{n-1} + \cfrac{1}{a_n}}}}}},$$

podemos estabelecer o processo inverso fazendo

$b_n = a_{n-1} + \frac{1}{a_n}$, $b_{n-1} = a_{n-2} + \frac{1}{b_n}, \dots, b_2 = a_1 + \frac{1}{b_3}$ até obtermos o racional $b_1 = a_0 + \frac{1}{b_2}$.

$\square$

Convém observar que, nesse processo de divisões sucessivas, somente o primeiro quociente é possivelmente negativo e os demais são todos positivos. Disso concluímos que na fração contínua todos os a_i's são inteiros positivos, com a possível exceção de a_0.

Definiremos agora números cuja representação decimal não é nem finita nem periódica. Números como esses são chamados de irracionais. De forma mais precisa podemos estabelecer a seguinte definição:

Definição 1.2 *Todo número decimal que não pode ser escrito na forma* $\frac{a}{b}$, *com* $a \in \mathbb{Z}$ *e* $b \in \mathbb{Z}^*$ *é irracional. Simbolicamente* $\mathbb{R} \setminus \mathbb{Q} = \{x \in \mathbb{R}; x \in \mathbb{R} \text{ e } x \notin \mathbb{Q}\}$.

A partir dessa definição e das proposições anteriores, podemos concluir que todos os números irracionais são decimais não periódicos e, ainda, sua representação em forma de fração resulta em uma fração contínua infinita.

A seção seguinte tratará da radiciação de inteiros positivos, basicamente estabeleceremos quando a raiz *n*-ésima de um inteiro positivo será racional ou irracional.

1.2 Radiciação e irracionalidade

Para nossos próximos resultados será necessário considerar o polinômio $p(x) = a_0 + a_1x + a_2x^2 + ... + a_nx^n$, com $a_0, a_1, a_2, ...a_n \in \mathbb{Z}$. É preciso também estabelecer a seguinte proposição que fundamentará todos os resultados posteriores.

Proposição 1.5 *Se um número racional* $\frac{r}{s}$, *na forma irredutível, é raiz de* $p(x)$, *então* $r \mid a_0$ *e* $s \mid a_n$.

Demonstração:

Se o racional $\frac{r}{s}$ é raiz do polinômio $p(x)$ teremos $p\left(\frac{r}{s}\right) = 0$, ou seja, $a_0 + a_1\left(\frac{r}{s}\right) + a_2\left(\frac{r}{s}\right)^2 + ... + a_n\left(\frac{r}{s}\right)^n = 0$. Multiplicando ambos os membros por s^n fica: $a_0s^n + a_1rs^{n-1} + a_2r^2s^{n-2} + ...a_{n-1}r^{n-1}s + a_nr^n = 0$. Pondo s em evidência na soma dos n termos do primeiro membro e passando para o segundo o último termo, obtemos: $s\left(a_0s^{n-1} + a_1rs^{n-2} + ... + a_{n-1}r^{n-1}\right) = -a_nr^n$.

Isso mostra que $s \mid a_n r^n \Rightarrow s \mid a_n$ ou $s \mid r^n$. Como s não divide r, pois são primos entre si, s também não divide r^n. Logo, $s \mid a_n$.

Analogamente, pondo r em evidência nos n termos do primeiro membro e passando $a_0 s^n$ para o segundo, fica:

$$r\left(a_1 s^{n-1} + a_2 r s^{n-2} + \ldots + a_{n-1} r^{n-2} s + a_n r^{n-1}\right) = -a_0 s^n.$$

Pelo mesmo raciocínio, concluímos que $r \mid a_0$. $\square$

Considerando agora $p(x)$ como polinômio mônico podemos estabelecer o importante corolário.

Corolário 1.1 *Se* $p(x) = a_0 + a_1 x + a_2 x^2 + \ldots + x^n$, *com* $a_0, a_1, a_2, \ldots a_{n-1} \in \mathbb{Z}$, *então as eventuais raízes racionais de* $p(x)$ *são números inteiros divisores de* a_0.

Demonstração:

Se o número racional $\frac{r}{s}$ é raiz de $p(x)$, então pela Proposição 1.4 $s \mid 1$, ou seja, $s = 1$ ou $s = -1$. Logo $\frac{r}{s} = \pm r$ e, portanto $\in \mathbb{Z}$. Ainda pela Proposição 1.4, $r \mid a_0$ e, portanto, o mesmo acontece com $-r$. $\square$

Através da próxima proposição estabeleceremos nosso primeiro importante resultado sobre radiciação. Basicamente estabeleceremos que a raiz *n*-ésima de um inteiro positivo a é irracional sempre que os expoentes dos fatores na decomposição do radicando a, em fatores primos, forem menores que o índice do radical, mas nem todos nulos.

Proposição 1.5 *Se* $p_1, p_2, \ldots, p_r$ *são primos distintos,* $r_i < n (n \geq 2,\ i = 1, 2, \ldots, r)$ *e pelo menos um* $r_i \neq 0$, *então* $\sqrt[n]{p_1^{r_1}.p_2^{r_2} \ldots p_r^{r_r}}$ *é irracional.*

Demonstração:

Observamos que $\sqrt[n]{p_1^{r_1}.p_2^{r_2} \ldots p_r^{r_r}}$ é raiz do polinômio $p(x) = x^n - \left(p_1^{r_1}.p_2^{r_2} \ldots p_r^{r_r}\right)$.

Se $p(x)$ possui alguma raiz racional, pelo Corolário 1.1, essa raiz será um inteiro divisor de $p_1^{r_1}.p_2^{r_2}...p_r^{r_r}$. Por outro lado, todo inteiro positivo q que divide $p_1^{r_1}.p_2^{r_2}...p_r^{r_r}$ é da forma $q = p_1^{s_1}.p_2^{s_2}...p_r^{s_r}$ em que $0 \leq s_i \leq r_i (i = 1, 2, ..., r)$ .Dessa forma teremos:

$p(q) = \left(p_1^{s_1}.p_2^{s_2}...p_r^{s_r}\right)^n - \left(p_1^{r_1}.p_2^{r_2}...p_r^{r_r}\right) = 0$, ou seja,

$\left(p_1^{s_1}.p_2^{s_2}...p_r^{s_r}\right)^n = \left(p_1^{r_1}.p_2^{r_2}...p_r^{r_r}\right) \Rightarrow p_1^{n.s_1}.p_2^{n.s_2}...p_r^{n.s_r} = p_1^{r_1}.p_2^{r_2}...p_r^{r_r}$.

Mas como $p_1, p_2, ...p_r$ são primos distintos, para que essa igualdade faça sentido, devemos ter $n \cdot s_i = r_i$, ou seja, $s_i = \frac{r_i}{n}$ para todo $i = 1, 2, ..., r$. No entanto, $s_i = \frac{r_i}{n}$ somente quando $r_i = s_i = 0$ para todo i, o que contraria a hipótese inicial de que pelo menos um r_i é diferente de zero. Para as demais possibilidades, $s_i = \frac{r_i}{n}$ é um absurdo, pois por hipótese, $r_i < n$ para todo i. Logo $p(x)$ não possui raízes inteiras e, portanto $\sqrt[n]{p_1^{r_1}.p_2^{r_2}...p_r^{r_r}}$ só pode ser irracional. □

Como conseqüência dessa proposição podemos estabelecer o seguinte corolário.

Corolário 1.2 *Se p é primo, então $\sqrt{p}$ é irracional.*

Demonstração:

Basta observar que o expoente de p é menor que o índice do radical. Logo, pela Proposição 1.5, $\sqrt{p}$ é irracional. □

Mas o que acontece quando pelo menos um expoente dos fatores da decomposição do radicando a é maior ou igual ao índice do radical? Para responder a essa pergunta precisaremos ainda de uma proposição simples, mas de grande importância.

Proposição 1.6 *O produto de um número irracional por um racional diferente de zero é um número irracional.*

Demonstração:

Sejam α irracional e $\frac{a}{b}$ um racional diferente de zero. Se $x = \alpha\frac{a}{b}$ fosse racional, então teríamos

$\alpha = \frac{x.b}{a}$, o que é um absurdo pois α é irracional. Logo x só pode ser irracional.

□

Vamos agora ao principal resultado dessa seção que definiremos como um Teorema.

Teorema 1.1 *Se n e a são inteiros positivos, então $\sqrt[n]{a}$ é um número irracional ou inteiro positivo.*

Demonstração:

Decompondo a de forma canônica em fatores primos, obteremos $a = p_1^{\alpha_1} p_2^{\alpha_2} ... p_r^{\alpha_r}$ com $p_1, p_2, ... p_r$ aparecendo $\alpha_1, \alpha_2, ... \alpha_r$ vezes respectivamente $(\alpha_i \geq 1,\ i = 1, 2, ..., r)$. Além disso, pelo algoritmo de Euclides, podemos expressar cada $\alpha_i = nq_i + r_i$ com $0 \leq r_i < n.$ Assim,

$$\sqrt[n]{a} = \sqrt[n]{p_1^{\alpha_1} p_2^{\alpha_2} ... p_r^{\alpha_r}} = \sqrt[n]{p_1^{n.q_1+r_1} p_2^{n.q_2+r_2} ... p_r^{n.q_r+r_r}} \Rightarrow$$

$$\sqrt[n]{p_1^{n.q_1} . p_1^{r_1} . p_2^{n.q_2} p_2^{r_2} ... p_r^{n.q_r} p_r^{r_r}} = \sqrt[n]{(p_1^{n.q_1} p_2^{n.q_2} ... p_r^{n.q_r})(p_1^{r_1} . p_2^{r_2} ... p_r^{r_r})} \Rightarrow$$

$$\sqrt[n]{(p_1^{q_1} p_2^{q_2} ... p_r^{q_r})^n (p_1^{r_1} . p_2^{r_2} ... p_r^{r_r})} = p_1^{q_1} p_2^{q_2} ... p_r^{q_r} \sqrt[n]{(p_1^{r_1} p_2^{r_2} ... p_r^{r_r})}.$$

Se $r_i = 0$ para todo $i = 1, 2, ..., r,$ teremos $\sqrt[n]{a}$ igual ao inteiro positivo $p_1^{q_1} . p_2^{q_2} ... p_r^{q_r}$. Porém, se pelo menos um $r_i \neq 0,$ pela Proposição 1.5, $\sqrt[n]{p_1^{r_1} . p_2^{r_2} ... p_r^{r_r}}$ é um número irracional e teremos pela Proposição 1.6, $\sqrt[n]{a}$ como o produto de um irracional por um racional diferente de zero, que será irracional. □

Desse Teorema concluímos que a raiz *n*-ésima de qualquer inteiro positivo é um inteiro positivo ou um número irracional

Em nossa próxima seção, nosso objetivo será caracterizar os números racionais sob o ponto de vista de sua enumeração.

1.3 Enumerabilidade dos Racionais

Uma característica importante do conjunto dos racionais é que ele é enumerável, ou seja, possui a mesma cardinalidade dos naturais. De forma mais precisa definimos conjunto enumerável da seguinte forma:

Definição 1.3 *Um conjunto* X *diz-se enumerável quando é finito ou quando existe uma bijeção* $f:\mathbb{N}\rightarrow X$. *No segundo caso, o conjunto* X *diz-se infinito enumerável.*

Nosso objetivo a partir de agora será demonstrar que os números racionais formam um conjunto infinito enumerável e para isso, precisaremos da seguinte proposição.

Proposição 1.7 *Se* $f:X\rightarrow Y$ *é injetiva e* Y *é enumerável, então* X *é enumerável.*

Demonstração:

Basta considerar o caso em que existe uma bijeção $\varphi:Y\rightarrow\mathbb{N}$. Então $\varphi\circ f:X\rightarrow\mathbb{N}$ é uma bijeção de X sobre um subconjunto de $\mathbb{N}$, o qual é enumerável. $\square$

Outra proposição de grande importância será a seguinte:

Proposição 1.8 *Se* $f:E\rightarrow F$ *e* $g:F\rightarrow G$ *são injetivas, então* $g\circ f$ *é injetiva.*

Demonstração:

Sejam x_1 e $x_2\in E$ tais que $\left(g\circ f\right)(x_1)=\left(g\circ f\right)(x_2)$. Então $g(f(x_1))=g(f(x_2))$ e, como g é injetiva, $f(x_1)=f(x_2)$. Usando-se agora a hipótese de que f é injetiva, conclui-se que $x_1=x_2$.

Logo, $g\circ f$ é injetora. $\square$

Por fim, precisaremos ainda de dois lemas.

Lema 1.1 *O conjunto* $\mathbb{Z}$ *é enumerável.*

Demonstração:

Consideremos a aplicação $f:\mathbb{Z}\rightarrow\mathbb{N}$ definida por $f(a)=2a$, se $a\geq 0$ e $f(a)=-2a-1$, se $a<0$. Claramente f é injetiva. De fato, seja a_1 e $a_2\in\mathbb{Z}$.

Se a_1 e a_2 são positivos, temos que $f(a_1)=f(a_2)\Rightarrow 2a_1=2a_2\Rightarrow a_1=a_2$. Porém, se a_1 e a_2 forem números negativos, temos que

$f(a_1)=f(a_2)\Rightarrow -2a_1-1=-2a_2-1\Rightarrow -2a_1=-2a_2\Rightarrow a_1=a_2$.

Se $a_1 \geq 0$ e $a_2 < 0$, então $f(a_1) \neq f(a_2)$. De fato, se for $f(a_1) = f(a_2)$, teremos $f(a_1) = f(a_2) \Rightarrow 2a_1 = -2a_2 - 1$. O que é um absurdo, pois o primeiro membro é um natural par, enquanto o segundo, é um natural ímpar. □

Lema 1.2 *Sejam* X, Y *conjuntos enumeráveis. O produto cartesiano* $X \times Y$ *é enumerável.*

Demonstração:

Como X, Y são enumeráveis, então existem aplicações injetivas $\varphi : X \to \mathbb{N}$ e $\psi : Y \to \mathbb{N}$.

Temos que a aplicação $h : X \times Y \to \mathbb{N}$ definida por $h(x,y) = 2^{\varphi(x)}3^{\psi(y)}$ é injetiva pois a decomposição em fatores primos é única e $\varphi(x)$ e $\psi(x)$ também o são. Além disso, h fornece uma bijeção de $X \times Y$ sobre o conjunto enumerável $h(X \times Y) \subset \mathbb{N}$. □

Vamos agora à demonstração de que o conjunto $\mathbb{Q}$ dos números racionais é enumerável.

Teorema 1.2 *O conjunto dos números racionais é enumerável.*

Demonstração:

Consideremos a aplicação $f : \mathbb{Q} \to \mathbb{Z} \times \mathbb{Z}^*$ definida por $f(x) = (m,n)$, com $x = \dfrac{m}{n}$ irredutível. Acontece que f é injetiva pois, se $x = \dfrac{m}{n}$ *e* $x_1 = \dfrac{m_1}{n_1} \in \mathbb{Q}$ e $f(x) = f(x_1)$, então $(m,n) = (m_1,n_1) \Rightarrow m = m_1$ *e* $n = n_1$.

Da Proposição 1.8, temos que a aplicação h composta por f definida por $h \circ f : \mathbb{Q} \to \mathbb{N}$ é injetiva. Assim, $h \circ f$ fornece uma bijeção de $\mathbb{Q}$ sobre o conjunto enumerável $(h \circ f)(\mathbb{Q}) \subset \mathbb{N}$.

Logo, $\mathbb{Q}$ é enumerável. □

1.4 Não Enumerabilidade dos Irracionais

Mostramos pouco atrás que o conjunto dos números racionais é enumerável. Esse resultado poderia nos levar a acreditar que todos os conjuntos infinitos também o são. Mostraremos agora que os irracionais formam um conjunto não enumerável, ou seja, possui cardinalidade diferente dos naturais e estabeleceremos este resultado como uma conseqüência da não enumerabilidade dos reais. Mas antes, precisaremos da seguinte proposição:

Proposição 1.9 *Uma reunião enumerável de conjuntos enumeráveis é enumerável.*

Demonstração:

Considere os conjuntos $A_1, A_2, A_3,....$ Como todos eles são enumeráveis, podemos escrevê-los na forma:

$$\begin{array}{l} A_1 = \{a_{11}a_{12}a_{13}a_{14}....a_{1n}....\} \\ A_2 = \{a_{21}a_{22}a_{23}a_{24}...a_{2n}...\} \\ A_3 = \{a_{31}a_{32}a_{33}a_{34}....a_{3n}...\} \\ \vdots \qquad\quad \vdots \qquad\quad \vdots \\ A_n = \{a_{n1}a_{n2}a_{n3}a_{n4}...a_{nn}...\} \\ \vdots \qquad\quad \vdots \qquad\quad \vdots \end{array}$$

A união $\bigcup_{i=1}^{\infty} A_i$ está contida na união disjunta $\bigcup_{i=1}^{\infty} A_i$ destes mesmos conjuntos(pode ser que algum elemento pertença a vários conjuntos A_i, na união disjunta, este elemento é repetido em cada A_i ao qual ele pertence).

Definamos, agora, uma função

$$\phi : \bigcup_{i=1}^{\infty} A_i \text{(união disjunta)} \to \mathbb{N} \times \mathbb{N}$$

$$a_{ij} \to (i, j)$$

É fácil ver que ϕ e injetiva. Finalmente, pelo Lema 1.2, sabemos que $\mathbb{N} \times \mathbb{N}$ é enumerável pela função

$$h : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$$

$$(i, j) \to 2^i \cdot 3^j$$

Logo, podemos compor as diversas funções injetivas

$$\bigcup_{i=1}^{\infty} A_i \xrightarrow{I} \bigcup_{i=1}^{\infty} A_i \,\text{(união disjunta)} \xrightarrow{\phi} \mathbb{N} \times \mathbb{N} \xrightarrow{h} \mathbb{N}$$

e obtemos uma função injetiva de $\bigcup_{i=1}^{\infty} A_i$ nos naturais, garantindo, assim a sua enumerabilidade. $\square$

Demonstraremos agora a não enumerabilidade dos reais.

Proposição 1.10 *O conjunto $\mathbb{R}$ dos números reais não é enumerável.*

Demonstração:

Para demonstrar esse resultado, usaremos o fato de que o intervalo (0,1) possui a mesma cardinalidade de toda a reta. Observe que alguns números desse intervalo possuem mais de uma representação decimal como por exemplo, 0,7 e 0,6999....Para excluir essa possibilidade, adotaremos para cada número sua representação decimal infinita. Assim, por exemplo;

$$0{,}7 = 0{,}6999...; \;\; 0{,}0343 = 0{,}342999...; etc\,.$$

Suponhamos agora que seja possível estabelecer uma bijeção entre os números do intervalo (0,1) e os naturais. Podemos então supor que os números desse intervalo sejam os elementos de uma seqüência infinita, $x_1, x_2, ..., x_n, ...$ Assim podemos listá-los da seguinte forma:

$$\begin{array}{l}
x_1 = 0, a_{11}a_{12}a_{13}...\ a_{1n}... \\
x_2 = 0, a_{21}a_{22}a_{23}...\ a_{2n}... \\
x_3 = 0, a_{31}a_{32}a_{33}...\ a_{3n}... \\
\vdots \qquad \vdots \qquad \vdots \\
x_n = 0, a_{n1}a_{n2}a_{n3}...\ a_{nn}... \\
\vdots \qquad \vdots \qquad \vdots
\end{array}$$

Nas quais a_{ij} são algarismos de 0 a 9. No entanto, por mais extensa que seja nossa lista, podemos produzir um número que não pertença a ela através do processo diagonal de Cantor. Esse processo consiste em construir um número que seja diferente de x_1 na primeira casa decimal, diferente de x_2 na segunda casa decimal, diferente de x_3 na terceira casa, e assim por diante, de sorte que, esse número, não será igual a nenhum dos números da lista acima. Para tanto, definimos $x = 0, a_1 a_2 ...$ do seguinte modo: $a_i = 1$ se $a_{ii} = 5$ e $a_i = 5$ se $a_{ii} \neq 5$.

Dessa forma, cada x_i será diferente de x ao menos pelo elemento a_{ii} e como esse elemento não está em nossa lista, chegamos a um absurdo, o que nos leva a concluir que o conjunto dos números reais não é enumerável. $\square$

Corolário 1.3 *O conjunto dos números irracionais não é enumerável.*

Demonstração:

Sendo $\mathbb{R} = \mathbb{Q} \cup (\mathbb{R} \setminus \mathbb{Q})$, se o conjunto dos irracionais fosse enumerável, pela Proposição 1.9, os reais também o seriam, como reunião de dois conjuntos enumeráveis. Também pela Proposição 1.9, conclui-se que os irracionais formam a maioria dos reais, pois o conjunto enumerável é o "menor" dos conjuntos infinitos. $\square$

CAPÍTULO II

ALGUNS NÚMEROS IRRACIONAIS

Acabamos de demonstrar a existência do conjunto dos números irracionais, sua não enumerabilidade bem como sua maioria dentre os reais. Devida a sua importância na análise matemática, neste capítulo daremos ênfase a duas constantes: π e e. Demonstraremos também que são irracionais.

2.1 A Irracionalidade do Número e

A origem de e não é tão clara, ela parece recuar ao século XVI, quando se percebeu que a expressão $\left(1+\frac{1}{n}\right)^n$, que aparecia na fórmula dos juros compostos, tendia a um certo limite – cerca de 2,71828 – à medida que n aumenta. Assim e tornou-se o primeiro número a ser *definido* por um processo de limite, $e = \lim\left(1+\frac{1}{n}\right)^n$ conforme $n \to \infty$. Durante algum tempo o novo número foi considerado uma curiosidade. O passo crucial para colocá-lo na vanguarda da matemática foi dado com a invenção do cálculo, quando se percebeu que o inverso da função logarítmica – que depois seria denotado como e^x – era igual à sua própria derivada. Isto imediatamente deu ao número e e a função e^x um papel central na análise.

Existem muitas fórmulas envolvendo o número e, dentre as quais:

$$e = 1 + \frac{1}{1!} + \frac{1}{2!} + \frac{1}{3!} + \frac{1}{4!} + ...$$

Esta série infinita foi descoberta por Newton em 1665, e pode ser obtida da expansão binomial de $\left(1+\frac{1}{n}\right)^n$, deixando $n \to \infty$. Ela converge muito rapidamente, devido ao aumento rápido dos valores dos fatoriais nos denominadores. Por exemplo, a soma dos primeiros onze termos (terminados com $\frac{1}{10!}$) é 2,718281801, o que já é uma boa aproximação.

O número e também pode ser representado por uma fração continua infinita. Esta forma de representação, descrita a seguir, foi descoberta por Euler em 1737.

$$e = 2 + \cfrac{1}{1 + \cfrac{1}{2 + \cfrac{2}{3 + \cfrac{3}{4 + \cfrac{4}{5 + \ldots}}}}}$$

Euler provou também que todo número racional pode ser escrito como uma fração contínua finita; inversamente, toda fração contínua infinita sempre representa um número irracional. O número e também pode ser encontrado usando série de Maclaurin(1698-1746), como veremos a seguir.

Seja $f(x) = e^x$. Calculemos diversas derivadas sucessivas de f no ponto $x = 0$:

$$\begin{array}{lll} f(x) = e^x & \Rightarrow & f(0) = 1 \\ f'(x) = e^x & \Rightarrow & f'(0) = 1 \\ f''(x) = e^x & \Rightarrow & f''(0) = 1 \\ f'''(x) = e^x & \Rightarrow & f'''(0) = 1 \\ \vdots & \vdots & \vdots \end{array}$$

Logo, $f^n(0) = 1$. Então, a série de Maclaurin $\sum_{n=0}^{\infty} \frac{f^{(n)}(0)x^n}{n!}$ de $f(x) = e^x$ é:

$$e^x = f(0) + \frac{f'(0)x}{1!} + \frac{f''(0)x^2}{2!} + \frac{f'''(0)x^3}{3!} + \ldots.$$

$$e^x = 1 + x + \frac{x^2}{2!} + \frac{x^3}{3!} + \ldots.$$

$e^x = \sum_{n=0}^{\infty} \frac{x^n}{n!}$. Para $x = 1$, temos:

$$e = 1 + \frac{1}{1!} + \frac{1}{2!} + \frac{1}{3!} + \ldots.$$

Demonstraremos agora uma importante característica desse número. Sua irracionalidade. Inicialmente precisaremos de um resultado simples mas muito importante na análise matemática expressado pela seguinte proposição.

Proposição 2.1 *Toda seqüência monótona limitada é convergente.*

Demonstração:

Sem perda de generalidade, suponhamos x_n monótona não-decrescente e limitada. Podemos escrever $X = \{x_1, x_2, x_3, \ldots, x_n, \ldots\}$. Seja $a = \sup X$ (que existe pelo axioma do supremo). Afirmamos que $a = \lim x_n$. Segue que, dado $\varepsilon > 0$, o número $a - \varepsilon$ não é cota superior de X. Logo, existe $n_0 \in \mathbb{N}$ tal que $a - \varepsilon < x_{n_0} \leq a$. Assim, $\forall n > n_0 \Rightarrow a - \varepsilon < x_{n_0} \leq x_n < a + \varepsilon$ e, portanto, $\lim x_n = a.$ $\square$

Dessa forma, podemos estabelecer a seguinte proposição.

Proposição 2.2 *A seqüência cujo termo geral é* $a_n = 1 + \frac{1}{1!} + \frac{1}{2!} + \frac{1}{3!} + ... + \frac{1}{n!}$ *é convergente.*

Demonstração:

Esta seqüência é evidentemente monótona crescente pois $a_{n+1} > a_n$ para todo $n \in \mathbb{N}$. Resta-nos mostrar que é limitada.

Começando com $n = 3,$ teremos:

$n! = 1 \cdot 2 \cdot 3 ... n > 1 \cdot 2 \cdot 2 ... 2 = 2^{n-1}$, portanto, $a_n < 1 + 1 + \frac{1}{2} + \frac{1}{2^2} + ... + \frac{1}{2^{n-1}}$.

Nesta soma, a partir do segundo termo, temos uma progressão geométrica de razão $\frac{1}{2}$. Aplicando a fórmula $S = \frac{a_1}{1-q}$, fica: $S = \frac{1}{1-1/2} = 2.$ Daí teremos $a_n < 1 + 2 = 3.$ Logo, a seqüência a_n é limitada superiormente por 3 e, pela Proposição 2.1, é convergente. $\square$

Escreveremos $\lim a_n = e$ e mostraremos que a seqüência cujo termo geral é $b_n = \left(1 + \frac{1}{n}\right)^n$ converge para o mesmo limite que a_n.

Proposição 2.3 *Se* $b_n = \left(1 + \frac{1}{n}\right)^n$*, então* $\lim b_n = e.$

Demonstração:

Pelo teorema binomial temos:

$$b_n = 1 + n.\frac{1}{n} + \frac{n(n-1)}{2!}.\frac{1}{n^2} + ... + \frac{n(n-1)(n-2)...3.2.1}{n!}.\frac{1}{n^n}$$
$$b_n = 1 + 1 + \frac{1}{2!}\left(1 - \frac{1}{n}\right) + \frac{1}{3!}\left(1 - \frac{1}{n}\right)\left(1 - \frac{2}{n}\right) + ... + \frac{1}{n!}\left(1 - \frac{1}{n}\right)\left(1 - \frac{2}{n}\right)...\left(1 - \frac{n-1}{n}\right).$$

Como a expressão dentro de cada parêntese é menor que 1, teremos que $b_n \leq a_n$, assim, $b_n \leq \lim a_n$. Portanto, a seqüência b_n também tem um limite superior. Além disso, b_n é monótona crescente pois $b_{n+1} > b_n$ para todo n. De fato;

$$b_{n+1}=1+1+\frac{1}{2!}\left(1-\frac{1}{n+1}\right)+...+\frac{1}{n!}\left(1-\frac{1}{n+1}\right)...\left(1-\frac{n-1}{n+1}\right)+\frac{1}{(n+1)!}\left(1-\frac{1}{n+1}\right)...\left(1-\frac{n}{n+1}\right)>$$
$$>1+1+\frac{1}{2!}\left(1-\frac{1}{n+1}\right)+\frac{1}{3!}\left(1-\frac{1}{n+1}\right)\left(1-\frac{2}{n+1}\right)+...+\frac{1}{n!}\left(1-\frac{1}{n+1}\right)\left(1-\frac{2}{n+1}\right)...\left(1-\frac{n-1}{n+1}\right)$$

pois o último termo de b_{n+1} é positivo. Acontece que $n+1>n\Rightarrow\frac{1}{n+1}<\frac{1}{n}\Rightarrow 1-\frac{a}{n+1}>1-\frac{a}{n}\ \forall\ 0<a<n.$ Assim, teremos;

$$b_{n+1}>1+1+\frac{1}{2!}\left(1-\frac{1}{n+1}\right)+...+\frac{1}{n!}\left(1-\frac{1}{n+1}\right)\left(1-\frac{2}{n+1}\right)...\left(1-\frac{n-1}{n+1}\right)+>$$
$$>1+1+\frac{1}{2!}\left(1-\frac{1}{n}\right)+\frac{1}{3!}\left(1-\frac{1}{n}\right)\left(1-\frac{2}{n}\right)+...+\frac{1}{n!}\left(1-\frac{1}{n}\right)\left(1-\frac{2}{n}\right)...\left(1-\frac{n-1}{n}\right)=b_n$$

Logo, $b_{n+1}>b_n$. Assim, pela Proposição 2.1, b_n também é convergente e $\lim\limits_{n\to\infty}b_n\le\lim\limits_{n\to\infty}a_n$.

Por outro lado, quando $p<n$, vale:

$$b_n\ge 1+1+\frac{1}{2!}\left(1-\frac{1}{n}\right)+...+\frac{1}{p}\left(1-\frac{1}{n}\right)\left(1-\frac{2}{n}\right)...\left(1-\frac{p-1}{n}\right).$$

Agora vamos deixar n aumentar sem limites enquanto mantemos p fixo. Da desigualdade acima obtemos $\lim b_n\ge 1+1+\frac{1}{2!}+\frac{1}{3!}+...+\frac{1}{p!}=a_p$. Como esta desigualdade vale para todo $p\in\mathbb{N}$, segue que $\lim\limits_{n\to\infty}b_n\ge\lim\limits_{p\to\infty}a_p$. Mas já vimos que $\lim b_n\le\lim a_n$. Logo, só podemos ter $\lim b_n=\lim a_n=e.$ $\square$

Nossa prova também mostra que $\lim a_n=e$ encontra-se entre 2 e 3. Na realidade vale $e\cong 2{,}7182,$ com quatro decimais exatas.

Para finalmente demonstrarmos a irracionalidade de e uma última proposição será necessária.

Proposição 2.4 *Se* $q\ge 2,$ *então o somatório* $S=\lim S_n,$ *em que*
$$S=\frac{1}{q+1}+\frac{1}{(q+1)(q+2)}+...+\frac{1}{(q+1)(q+2)...(q+n)}+...,$$ *não é um inteiro.*

Demonstração:

Claramente $S_n>0$ para todo n. Como $q\ge 2$, temos que:

$$\frac{1}{q+1}+\frac{1}{(q+1)(q+2)}+\frac{1}{(q+1)(q+2)(q+3)}+...\leq\frac{1}{3}+\frac{1}{3.4}+\frac{1}{3.4.5}+...<\frac{1}{3}+\frac{1}{3^2}+\frac{1}{3^3}+...$$

Usando a fórmula para a soma de uma série geométrica infinita, na última desigualdade obtemos: $S=\frac{1/3}{1-1/3}=\frac{1}{3}.\frac{3}{2}=\frac{1}{2}$. Logo, $0<S_n<\frac{1}{2}$. □

Finalmente;

Teorema 2.1 *e é irracional.*

Demonstração:

Suponhamos que e seja racional e então mostramos que esta suposição leva a uma contradição. Vamos fazer $e=\frac{p}{q}$, em que p e q são inteiros. Já mostramos que $2<e<3$, assim e não pode se um inteiro e consequentemente o denominador q deve ser pelo menos 2. Assim;

$$\frac{p}{q}=1+1+\frac{1}{2!}+\frac{1}{3!}+......+\frac{1}{n!}.$$

Multiplicando ambos os membros por $q!$ fica:

$$\frac{p\cdot q!}{q}=q!\left(1+1+\frac{1}{2!}+\frac{1}{3!}+...+\frac{1}{(q-1)!}+\frac{1}{q!}+\frac{1}{(q+1)!}+...+\frac{1}{n!}+...\right)$$

$$p(q-1)(q-2)...2\cdot 1=q!+q!+\frac{q!}{2!}+\frac{q!}{3!}+...+\frac{q!}{(q-1)!}+\frac{q!}{q!}+\frac{q!}{(q+1)!}+...+\frac{q!}{n!}+...$$

$$p(q-1)(q-2)...2\cdot 1=\left[q!+q!+q(q-1)(q-2)...4.3+q(q-1)(q-2)...5\cdot 4+...q+1\right]+\frac{1}{q+1}+$$

$$\frac{1}{(q+1)(q+2)}+...+\frac{1}{(q+1)(q+2)...(q+n)}+....$$

O primeiro membro é obviamente um inteiro pois trata-se de um produto de inteiros. O segundo membro não é um inteiro, pois a expressão dentro das chaves também é um inteiro, mas o somatório dos termos remanescentes, pela proposição 2.4, não é. Esse absurdo completa a demonstração. □

2.2 Um pouco da história do Número π

O número mais famoso da história, π, representa a razão constante entre o perímetro de um círculo e o seu diâmetro. A história do número π tem início cerca de 4.000 anos atrás, sendo que a existência de uma relação constante entre "a circunferência e o seu diâmetro" era conhecida por muitas das civilizações antigas.

Muitas civilizações antigas observaram através de medições que a razão entre o perímetro de diferentes círculos e seus respectivos diâmetros era sempre um mesmo valor. No entanto, foram os gregos que conseguiram compreender e explicar a lógica desta relação, que advém das propriedades de figuras semelhantes. Os gregos antigos compreenderam que números como π e $\sqrt{2}$ são diferentes dos números inteiros e dos números racionais utilizados em suas matemáticas e, mesmo tendo conseguido provar a irracionalidade de $\sqrt{2}$, o mesmo não ocorreu para π.

Arquimedes de Siracusa(287-212 a.C.) conseguiu melhorar a aproximação dada ao número π, aproximando a circunferência por polígonos regulares de 12, 24, 48 e 96 lados e descobrindo as seguintes limitações para π: $3\frac{10}{71} < \pi < 3\frac{1}{7}$, isto é, $3{,}14085 < \pi < 3{,}142857$.

Cerca de dezoito séculos depois de Arquimedes, um matemático francês chamado François Viète(1540-1603), no curso de seu trabalho em trigonometria, encontrou uma fórmula notável envolvendo o número π:

$$\frac{2}{\pi} = \frac{\sqrt{2}}{2} \cdot \frac{\sqrt{2+\sqrt{2}}}{2} \cdot \frac{\sqrt{2+\sqrt{2+\sqrt{2}}}}{2} \cdots\cdots$$

A descoberta desse *produto infinito* em 1593 foi um marco na história da matemática, pois pela primeira vez um processo infinito era escrito explicitamente como uma fórmula matemática. De fato, a característica mais extraordinária na fórmula de Viète, além de sua elegância, são os três pontos no final, indicando que ela continua e continua...*ad infinitum.* Ela mostra que o valor de π pode ser encontrado, pelo menos em princípio, usando-se repetidamente quatro operações da matemática elementar: adição, multiplicação, divisão e a extração da raiz quadrada, todas aplicadas ao número 2.

A fórmula de Viète quebrou uma importante barreira psicológica, já que o mero ato de escrever os três pontos no final sinalizava a aceitação dos processos infinitos na matemática e abria o caminho para seu uso generalizado. O grande matemático Isaac Newton descobriu outro produto infinito envolvendo π influenciado pelo trabalho de outro inglês, John Wallis(1616-1703). Eis o produto infinito de Newton para π:

$$\frac{\pi}{2}=\frac{2}{1}\cdot\frac{2}{3}\cdot\frac{4}{3}\cdot\frac{4}{5}\cdot\frac{6}{5}\cdot\frac{6}{7}.....$$

E, em 1671, o escocês James Gregory(1638-1675) descobriu a série infinita:

$$\frac{\pi}{4}=\frac{1}{1}-\frac{1}{3}+\frac{1}{5}-\frac{1}{7}+-....$$

O que torna essas fórmulas tão notáveis é que o número π, originalmente definido em relação ao círculo, pode ser expresso somente através de inteiros, ainda que através de um processo infinito. Até hoje, essas fórmulas estão entre as mais belas de toda a matemática.

Sabe-se hoje que π é um número irracional, no entanto, essa característica só foi demonstrada em 1761 por Johann Heinrich Lambert(1728-1777).

2.3 A Irracionalidade do Número π

Nosso objetivo agora será demonstrar a irracionalidade de π, para tanto, necessitaremos de algumas propriedades da função $f_n(x)=\dfrac{x^n(1-x)^n}{n!}$. Observe que $0<f_n(x)<\dfrac{1}{n!}, \forall x\in(0,1)$ e que $f(x)=f(1-x)$.

Vamos iniciar nossa demonstração supondo que π^2 seja racional, assim, $\pi^2=\dfrac{a}{b}$ com a e b primos entre si. Nosso objetivo é chegar a um absurdo, mostrando assim que π^2 não é racional. E consequentemente π não pode ser racional, pois o quadrado de um racional é também um racional.

Para a conclusão da demonstração, vamos precisar da seguinte proposição.

Proposição 2.5 *Para um n suficientemente grande e a um número positivo,* $\dfrac{2a^n}{n!}<1$.

Demonstração:

Sendo $N<n$, notamos que; $\dfrac{2a^n}{n!}=2\left(\dfrac{a}{1}\cdot\dfrac{a}{2}\cdot...\cdot\dfrac{a}{N}\right)\left(\dfrac{a}{N+1}\cdot\dfrac{a}{N+2}\cdot...\cdot\dfrac{a}{n}\right)$. Fixando N tal que $\dfrac{a}{N}<\dfrac{1}{2}$, cada um dos $n-N$ fatores do segundo parêntese será inferior a $\dfrac{1}{2}$. Logo;

$\frac{2a^n}{n!} < 2\left(\frac{a}{1}\cdot\frac{a}{2}\cdot\ldots\cdot\frac{a}{N}\right)\frac{1}{2^{n-N}} = 2\left(\frac{a}{1}\cdot\frac{a}{2}\cdot\ldots\cdot\frac{a}{N}\right)\frac{2^N}{2^n} = \frac{2(2a)^N}{N!}\cdot\frac{1}{2^n} = \frac{C}{2^n}$, em que C é uma constante que só depende de N, que já está fixado. Assim, para um n suficientemente grande teremos $\frac{2a^n}{n!} < 1$. □

Um importante resultado sobre a função $f_n(x) = \frac{x^n(1-x)^n}{n!}$ é dado pela seguinte proposição.

Proposição 2.6 $f_n(x) = \frac{1}{n!}\sum_{j=0}^{n}\binom{n}{j}(-1)^j x^{n+j}$.

Demonstração:

$f(x) = \frac{x^n(1-x)^n}{n!}$. Desenvolvendo $(1-x)^n$ fica:

$$f_n(x) = \frac{x^n}{n!}\left[\binom{n}{0}1^n(-x)^0 + \binom{n}{1}1^{n-1}(-x)^1 + \binom{n}{2}1^{n-2}(-x)^2 + \ldots + \binom{n}{n-1}(-x)^{n-1} + \binom{n}{n}(-x)^n\right]$$

$$f_n(x) = \frac{1}{n!}\left[\binom{n}{0}x^n + \binom{n}{1}(-1).x^{n+1} + \binom{n}{2}(-1)^2x^{n+2} + \ldots + \binom{n}{n-1}(-1)^{n-1}x^{2n-1} + \binom{n}{n}(-1)^n x^{2n}\right],$$ ou

seja, $f_n(x) = \frac{1}{n!}\sum_{j=0}^{n}\binom{n}{j}(-1)^j x^{n+j}$. □

Estabeleceremos uma importante conseqüência dessa proposição no seguinte corolário.

Corolário 2.1 *Seja* $f_n^{(m)}(x)$ *a m-ésima derivada de* $f_n(x)$. *Então:*

i) $f_n^{(m)}(0) = 0$ *se* $0 \le m < n$ *ou* $m > 2n$.

ii) $f_n^{(m)}(0)$ *é um número inteiro se* $n \le m \le 2n$.

Demonstração:

1ª Parte: $f_n^{(m)}(0) = 0$ se $0 \le m < n$ ou $m > 2n$.

Basta observar que para $0 \le m < n$ todos os termos são multiplicados por x e como zero é raiz de $f_n(x)$ com multiplicidade n, $f_n^{(m)}(0) = 0$.

De fato:

$$f_n(x) = \frac{x^n}{n!}(1-x)^n$$

$$f_n'(x) = \frac{1}{n!}\left[n.x^{n-1}(1-x)^n + n.x^n(1-x)^{n-1}\right] = \frac{x^{n-1}}{n!}\left[n(1-x)^n - n.x(1-x)^{n-1}\right]$$

$$f_n'(x) = \frac{x^{n-1}}{n!} g_1(x), \text{ sendo } g_1(x) = n(1-x)^n - n.x(1-x)^{n-1}.$$

Generalizando:

$f_n^{(m)}(x) = \dfrac{x^{n-m}}{n!} g_m(x)$ que é tal que $f_n^{(m)}(0) = 0$ para $0 \le m < n$.

Para $m > 2n$, obviamente $f_n^{(m)}(x) = 0$ pois o grau de $f_n(x)$ é $2n$.

2ª Parte:

Desenvolvendo $f_n(x)$, obtemos;

$f_n(x) = \dfrac{1}{n!}\left[c_0 x^n - c_1 x^{n+1} + c_2 x^{n+2} - \ldots + (-1)^{n-1} c_{n-1} x^{2n-1} + (-1)^n c_n x^{2n}\right]$ para convenientes $c_0, c_1, c_2 \ldots c_n \in \mathbb{Z}$. Assim:

$$f_n^{(n)}(0) = \frac{n! c_0}{n!} \in \mathbb{Z}$$

$$f_n^{(n+1)}(0) = -\frac{(n+1)! c_1}{n!} \in \mathbb{Z}$$

$$\vdots \qquad \vdots \qquad \vdots$$

$$f_n^{(2n)}(0) = \frac{(-1)^n (2n)! c_n}{n!} \in \mathbb{Z}.$$

Portanto, $f_n^{(m)}(0)$ é um inteiro para $n \le m \le 2n$. Utilizando o mesmo raciocínio concluímos que o corolário também vale para $f_n^{(m)}(1)$. $\square$

Supondo $\pi^2 = \dfrac{a}{b}$, definiremos agora a função $H(x)$ da seguinte forma:

Definição 2.1 $H(x) = b^n\left[\pi^{2n} f_n(x) - \pi^{2n-2} f_n''(x) + \ldots + (-1)^{n-1}\pi^2 f_n^{(2n-2)}(x) + (-1)^n f_n^{(2n)}(x)\right]$

Assim, se $\pi^2 = \dfrac{a}{b}$, podemos estabelecer a seguinte proposição.

Proposição 2.7 $\dfrac{d}{dx}\left[H'(x) sen\pi x - \pi H(x)\cos\pi x\right] = \pi^2 a^n f_n(x) sen\pi x.$

Demonstração:

Aplicando a regra do produto, fica:

$\frac{d}{dx}\left[H'(x)sen\pi.x - \pi H(x)\cos\pi.x\right] = \left[H''(x)sen\pi x + \pi H'(x)\cos\pi x - \pi H'(x)\cos\pi x + \pi^2 H(x)sen\pi x\right] =$
$\left[H''(x) + \pi^2 H(x)\right]sen\pi x.$

Mas $H''(x) = b^n\left[\pi^{2n} f''(x) - \pi^{2n-2} f^{(4)}(x) + ... + (-1)^{n-2}\pi^4 f^{(2n-2)}(x) + (-1)^{n-1}\pi^2 f^{(2n)}(x)\right]$ e

$\pi^2 H(x) = b^n\left[\pi^{2n+2} f(x) - \pi^{2n} f''(x) + ... + (-1)^{n-1}\pi^4 f^{(2n-2)}(x) + (-1)^n \pi^2 f^{(2n)}(x)\right]$. Assim, teremos:

$\left[H''(x) + \pi^2 H(x)\right]sen\pi x = b^n\left[\pi^{2n+2} f(x) + \pi^{2n} f''(x) + \pi^{2n-2} f^{(4)}(x) - \pi^{2n-2} f^{(4)}(x) + ...\right.$
$\left.(-1)^{n-1}\pi^2 f^{(2n)}(x) + (-1)^n \pi^2 f^{(2n)}(x)\right] = \pi^{2n+2} b^n f(x) sen\pi x = (\pi^2)^n.\pi^2 b^n f(x) sen\pi x.$

Como supomos inicialmente $\pi^2 = \frac{a}{b}$, vem;

$\frac{a^n}{b^n}\pi^2 b^n f(x) sen\pi x = \pi^2 a^n f(x) sen\pi x.$

Logo $\frac{d}{dx}\left[H'(x)sen\pi x - \pi H(x)\cos\pi x\right] = \pi^2 a^n f(x) sen\pi x.$ ∎

Proposição 2.8 $H(0)$ *e* $H(1)$ *são inteiros.*

Demonstração:

Nas condições da definição, temos:
$H(0) = b^n\left[\pi^{2n} f(0) - \pi^{2n-2} f''(0) + ... + (-1)^{n-1}\pi^2 f^{(2n-2)}(0) + (-1)^n f^{(2n)}(0)\right].$

Acontece que para $m < n$, pelo Corolário, 2.1 teremos;
$f(0) = 0$, $f''(0) = 0, ..., f^{(n)}(0) = 0$ de onde $H(0)$ fica resumida a $b^n \sum_{j=0}^{n} (-1)^{n-j}\pi^{2j} f^{(2n-2j)}(0)$ para $n \le 2n - 2j \le 2n.$ Mas ainda pelo corolário, $f^{(m)}(0) \in \mathbb{Z}$ para $n \le m \le 2n$. Já para o fator $b^n \pi^{2j}$, lembrando que $\pi^2 = \frac{a}{b}$, temos:
$b^n \pi^{2j} = a^j b^{n-j} \in \mathbb{Z}$.

Logo, $b^n \sum_{j=0}^{n} (-1)^{n-j}\pi^{2j} f^{(2n-2j)}(0)$ para $n \le 2n - 2j \le 2n,$ e, portanto $H(0) \in \mathbb{Z}$.

Pelo mesmo raciocínio concluímos que $H(1)$ também é inteiro. ∎

Proposição 2.9 *Se* $\pi^2 = \dfrac{a}{b}$, *então* $\int_0^1 \pi^2 a^n f(x) sen\pi x dx = \pi\left[H(1)+H(0)\right]$.

Demonstração:

Aplicando o teorema fundamental do cálculo, fica:

$$\int_0^1 \pi^2 a^n f(x) sen\pi x = \left[H'(x) sen\pi x - \pi H(x)\cos \pi x\right]_0^1 = \left[(H'(1) sen\pi - \pi H(1)\cos \pi) - (H'(0) sen0 - \pi H(0)\cos 0)\right] = \left[\pi H(1)+\pi H(0)\right] = \pi\left[H(1)+H(0)\right].$$ ∎

Finalmente, diante de todas as conclusões anteriores, podemos estabelecer o seguinte Teorema:

Teorema 2.2 π *é irracional.*

Demonstração:

Como $0 < f(x) < \dfrac{1}{n!}$ em (0,1), de todas as conclusões temos que:

$$\int_0^1 \pi^2 a^n f(x) sen\pi x dx \le \pi^2 a^n \int_0^1 \frac{sen\pi x}{n!} dx = \frac{\pi^2 a^n}{n!}\int_0^1 sen\pi x dx = \frac{\pi^2 a^n}{n!}\cdot\frac{2}{\pi} = \frac{2\pi a^n}{n!},$$

ou seja,

$0 < \int_0^1 \pi^2 a^n f(x) sen\pi x dx \le \dfrac{2\pi a^n}{n!}$. Como $\int_0^1 \pi^2 a^n f(x) sen\pi x dx = \pi\left[H(0)+H(1)\right]$, fica

$$0 < \pi\left[H(0)+H(1)\right] \le \frac{2\pi a^n}{n!} \Rightarrow 0 < H(0)+H(1) < \frac{2a^n}{n!} < 1 \Rightarrow 0 < H(0)+H(1) < 1.$$

E isso é um absurdo, pois não existe número inteiro maior que zero e menor que um. Somos assim obrigados a abandonar a hipótese inicial que π^2 é racional e consequentemente π. ∎

CAPÍTULO III

NÚMEROS ALGÉBRICOS E TRANSCENDENTES

3.1 Um Pouco Sobre Números Algébricos e Transcendentes

Tendo em vista os resultados obtidos no capítulo II, classificamos os números reais em dois conjuntos disjuntos: os racionais e os irracionais. Além dessa classificação, existe uma outra, em números algébricos e transcendentes.

Definição 3.1: *Se um número real* x *satisfizer uma equação da forma*

$$a_0 + a_1x + a_2x^2 + ... + a_nx^n = 0,$$

com coeficientes inteiros, dizemos que este número é algébrico.

Sobre a definição acima, duas observações devem ser feitas: Tendo em vista resultados posteriores, sempre que tomarmos um polinômio para o qual um número α é raiz suporemos o polinômio de menor grau possível para o qual isso ocorre. A outra observação é que, se dividirmos todos os termos da equação pelo coeficiente dominante, teremos x satisfazendo agora uma equação com coeficientes racionais. Assim, uma definição equivalente seria "*Se um número real* x *satisfizer uma equação da forma*

$$a_0 + a_1x + a_2x^2 + ... + x^n = 0,$$

com coeficientes racionais, dizemos que este número é algébrico."

A maioria dos números encontrados na álgebra elementar podem ser imaginados como soluções para equações simples; mais especificamente, são números algébricos. Por exemplo, os números -1, $2/3$ e $\sqrt{2}$ são soluções, respectivamente, das equações polinomiais $x+1=0$, $3x-2=0$ e $x^2-2=0$. O número $i=\sqrt{-1}$ também pertence a esse grupo, visto que ele satisfaz a equação $x^2+1=0$; entretanto, vamos restringir nossa discussão aos números reais.

Até mesmo um número de "aparência" complicada como $\sqrt[3]{(1-\sqrt{2})}$ pertence a essa classe, já que ele satisfaz a equação $x^6-2x^3-1=0$, como se pode constatar facilmente.

Claramente todo número racional a/b é algébrico, já que ele satisfaz a equação $bx-a=0$. Assim, se um número não for algébrico, deve ser irracional. A recíproca dessa afirmação, contudo, não é verdadeira; um número irracional pode ser algébrico, como mostra o exemplo de $\sqrt{2}$. Surge agora uma questão importante: existirão números irracionais *não algébricos*? Por volta do início do século XIX os matemáticos começaram a suspeitar que a resposta fosse sim, mas nenhum número desse tipo tinha sido encontrado. Parecia que um número não algébrico se fosse encontrado, seria uma singularidade.

Foi em 1844 que o matemático francês Joseph Liouville (1809-1882) provou que os números não algébricos de fato existiam. Sua prova, embora não fosse simples, permitiu que ele produzisse vários exemplos de tais números. Um dos exemplos, conhecido como número de Liouville, é

$$\frac{1}{10^{1!}}+\frac{1}{10^{2!}}+\frac{1}{10^{3!}}+\frac{1}{10^{4!}}+....$$

cuja expansão decimal é 0,110001000000000000000000100... onde os blocos cada vez maiores de zeros são devidos à presença de $n!$ no expoente do denominador do número de Liouville, o que faz com que os termos diminuam de um modo extremamente rápido. Outro exemplo é 0,12345678910111213..., em que os dígitos são os números naturais em ordem. Um número real não algébrico é chamado de *transcendente*. Não há nada de místico nessa palavra, ela indica apenas que esses números transcendem, ou seja, vão além no reino dos números algébricos. A seguir definimos de forma mais precisa números transcendentes.

Definição 3.2 *Todo número real que não é raiz de nenhuma equação da forma* $a_0+a_1x+a_2x^2+...+a_nx^n=0$ *com coeficientes inteiro é transcendente.*

Em contraste com os números irracionais, cuja descoberta surgiu de um problema comum na geometria, os números transcendentes foram “criados” especificamente com o propósito de demonstrar que tais números existiam.

Nosso objetivo nesse capítulo será demonstrar algumas características importantes do conjunto dos números algébricos.

3.2 Caracterização dos Números Algébricos e Transcendentes

Proposição 3.1 *O conjunto dos algébricos é denso em* $\mathbb{R}$.

Demonstração:

Basta observar que o conjunto dos números algébricos contém todos os racionais e, como os racionais são densos em $\mathbb{R}$, conclui-se trivialmente que os algébricos são densos. $\square$

Nosso objetivo agora será demonstrar a enumerabilidade dos números algébricos, para isso, vamos considerar, sem demonstração, o teorema fundamental da álgebra que afirma: *Todo polinômio não constante de grau* n*, com coeficientes complexos, tem* n *raízes complexas.*

Precisaremos também da seguinte proposição:

Proposição 3.2 *Uma reunião enumerável de conjuntos finitos é enumerável*

Demonstração:

No capítulo I demonstramos que uma reunião enumerável de conjuntos enumeráveis é enumerável. Como todo conjunto finito é enumerável temos, portanto, um caso particular da Proposição 2.4. □

Teorema 3.1 *O conjunto dos números algébricos é enumerável.*

Demonstração:

Considere um polinômio com coeficientes inteiros

$p(x) = a_0 + a_1 x + a_2 x^2 + ... + a_n x^n$.

Vamos definir altura do polinômio como sendo o número natural $h(P) = |a_0| + |a_1| + |a_2| + ... |a_n| + n - 1$.

Pelo teorema fundamental da álgebra, para cada polinômio de grau n, teremos no máximo n raízes complexas. Eventualmente todas, algumas ou nenhuma podem ser reais. Reciprocamente, para cada altura $h(P)$ teremos um número finito de polinômios. Seja $\varphi(P)$ esse número. Assim teremos:

$\varphi(1) = 2,\ \varphi(2) = 8, ...$

Mais precisamente,

$\varphi(1) = \#\{p_1(x) = x,\ p_2(x) = -x\}$

$$\varphi(2) = \#\{p_1(x) = x+1,\ p_2(x) = x-1,\ p_3(x) = -x+1,\ p_4(x) = -x-1,\ p_5(x) = x^2,\ p_6(x) = -x^2,\ p_7(x) = 2x,\ p_8(x) = -2x\}$$

e assim por diante.

Temos, portanto, que as raízes de todos os polinômios com uma dada altura formam um conjunto finito e como podemos enumerar todas essas alturas, segue da Proposição 3.2 que o conjunto A de todos os números algébricos reais é enumerável. $\square$

Corolário 3.1 *Existem números transcendentes e estes são não enumeráveis.*

Demonstração:

Como o conjunto $\mathbb{R}$ é não enumerável (Proposição 1.10, Cap.I) e o conjunto A é enumerável, segue que existe um conjunto $\mathcal{T} = \mathbb{R} \setminus A$ não enumerável, pois $\mathbb{R} = A \bigcup (\mathbb{R} \setminus A)$.

De fato, se $\mathcal{T}$ fosse enumerável teríamos que $\mathbb{R}$ também o era contrariando a Proposição 1.10 de que $\mathbb{R}$ é não enumerável. $\square$

O objetivo do nosso próximo teorema é demonstrar que os algébricos formam um corpo, para isso, vamos necessitar de alguns resultados da álgebra linear.

Consideraremos, a partir de agora, V como sendo espaço vetorial sobre o corpo dos racionais.

Sejam V um espaço vetorial e $S = \{v_1, v_2, ..., v_n\} \subset V$.

Consideremos a equação

$a_1v_1 + a_2v_2 + ... + a_nv_n = 0$

Sabemos que essa equação admite pelo menos uma solução:

$a_1 = 0, a_2 = 0, ..., a_n = 0$

Chamada solução trivial.

Definição 3.3 (1) O subconjunto S diz-se *linearmente independente* (LI) se admite *apenas a solução trivial.*

(2) Se existirem soluções não triviais, isto é, soluções com alguns $a_i \neq 0$, diz-se que o conjunto S é *linearmente dependente* (LD).

Definição 3.4 Um subconjunto $B = \{v_1, v_2, ..., v_n\} \subset V$ é uma base de espaço vetorial V se:

i) B é LI

ii) B gera V

A dimensão de um espaço vetorial V é a cardinalidade de qualquer base de V.

Seja V um espaço vetorial tal que $\dim V = n.$ Se S é um subespaço de V, então $\dim S \leq n$. No caso de $\dim S = n,$ tem-se $S = V$. Assim, podemos estabelecer a seguinte proposição.

Proposição 3.3 *Se V é um espaço vetorial de dimensão n, então qualquer subconjunto de V com mais de n vetores é linearmente dependente (LD).*

Demonstração:

Seja $B = \{v_1, v_2, ..., v_n\}$ uma base de um espaço vetorial V e $B' = \{w_1, w_2, ..., w_m\}$ um conjunto qualquer de m vetores de V, com $m > n$. Pretende-se mostrar que B' é LD. Para tanto, basta mostrar que existem escalares $x_1, x_2, ..., x_n$ não todos nulos tais que:

$$x_1 w_1 + x_2 w_2 + ..., x_m w_m = 0 \qquad (1)$$

Como B é uma base de V, cada vetor w_i pertencente a B' é uma combinação linear dos vetores de B, isto é, existem números $\alpha_i, \beta_i, ..., \delta_i$ tais que:

$$\begin{aligned} w_1 &= \alpha_1 v_1 + \alpha_2 v_2 + ... + \alpha_n v_n \\ w_2 &= \beta_1 v_1 + \beta_2 v_2 + ... + \beta_n v_n \\ &\vdots \qquad \vdots \qquad \vdots \qquad \vdots \\ w_m &= \delta_1 v_1 + \delta_2 v_2 + ... + \delta_n v_n \end{aligned} \qquad (2)$$

Substituindo as relações (2) em (1), obtemos:

$$\begin{aligned} &x_1 \left(\alpha_1 v_1 + \alpha_2 v_2 + ... + \alpha_n v_n \right) + \\ &x_2 \left(\beta_1 v_1 + \beta_2 v_2 + ... + \beta_n v_n \right) + \\ &\vdots \qquad \vdots \qquad \vdots \qquad \vdots \\ &x_m \left(\delta_1 v_1 + \delta_2 v_2 + ... + \delta_n v_n \right) = 0 \end{aligned}$$

Ordenando os termos convenientemente:

$$\begin{aligned} &\left(\alpha_1 x_1 + \beta_1 x_2 + ... + \delta_1 x_m \right) v_1 + \\ &\left(\alpha_2 x_2 + \beta_2 x_2 + ... + \delta_2 x_m \right) v_2 + \\ &\vdots \qquad \vdots \qquad \vdots \qquad \vdots \\ &\left(\alpha_n x_1 + \beta_n x_2 + ... + \delta_n x_m \right) v_n = 0 \end{aligned}$$

Tendo em vista que $v_1, v_2, ..., v_n$ são LI, os coeficientes dessa combinação linear são nulos, ou seja:

$$\alpha_1 x_1 + \beta_1 x_2 + ... + \delta_1 x_m = 0$$
$$\alpha_2 x_1 + \beta_2 x_2 + ... + \delta_2 x_m = 0$$
$$\vdots \quad \vdots \quad \vdots \quad \vdots$$
$$\alpha_n x_1 + \beta_n x_2 + ... + \delta_n x_m = 0$$

Esse sistema linear homogêneo possui m variáveis $x_1, x_2, ...x_m$ e n equações. Como $m > n$, existem soluções não triviais, isto é, existe $x_i \neq 0$. Logo $B' = \{w_1, w_2, ..., w_m\}$ é LD.

∎

Vamos agora a demonstração de que A é corpo.

Teorema 3.2 *A forma um corpo.*

Demonstração:

Precisamos demonstrar as seguintes propriedades:

(i) $\alpha, \beta \in A \Rightarrow \alpha + \beta \in A$

(ii) $\alpha, \beta \in A \Rightarrow \alpha.\beta \in A$

(iii) $\alpha \in A \Rightarrow -\alpha \in A$

(iv) $\alpha \in A, \alpha \neq 0 \Rightarrow \dfrac{1}{\alpha} \in A$

Demonstração de (iii):

Se α é algébrico então ele é raiz de uma equação com coeficientes inteiros do tipo

$$a_0 + a_1 x + a_2 x^2 + ... + a_{n-1} x^{n-1} + a_n x^n = 0$$

Portanto $-\alpha$ é raiz da equação

$$a_0 - a_1 x + a_2 x^2 - ... + (-1)^{n-1} a_{n-1} x^{n-1} + (-1)^n a_n x^n = 0$$ ∎

Demonstração de (iv):

Se α satisfaz a equação

$$a_0 + a_1 x + a_2 x^2 + ... + a_{n-1} x^{n-1} + a_n x^n = 0$$

e $\alpha \neq 0$, então $\dfrac{1}{\alpha}$ satisfaz a equação

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

De fato temos,

$$a_0 + a_1\alpha + a_2\alpha^2 + ... + a_{n-1}\alpha^{n-1} + a_n\alpha^n = 0.$$

Multiplicando por $\frac{1}{\alpha^n}$ obtemos,

$$a_0\frac{1}{\alpha^n} + a_1\frac{1}{\alpha^{n-1}} + a_2\frac{1}{\alpha^{n-2}} + ... + a_{n-1}\frac{1}{\alpha} + a_n =$$
$$\frac{1}{\alpha^n}\left(a_0 + a_1\alpha + a_2\alpha^2 + ... + a_{n-1}\alpha^{n-1} + a_n\alpha^n\right) =$$
$$\frac{1}{\alpha^n}.0 = 0$$

□

Para as demonstrações de (i) e (ii) vamos considerar os números algébricos como raízes de polinômios com coeficientes racionais, além disso, suporemos o polinômio de menor grau para o qual isso ocorre.

Demonstração de (i):

Considere os polinômios p_1 e p_2 com coeficientes racionais obtidos a partir da divisão pelo coeficiente do termo de maior grau.

$$p_1(x) = a_0 + a_1x + a_2x^2 + ... + a_{n-1}x^{n-1} + x^n$$
$$p_2(x) = b_0 + b_1x + b_2x^2 + ... + b_{n-1}x^{m-1} + x^m$$

Sejam α e β algébricos, raízes das equações polinomiais $p_1 = 0$ e $p_2 = 0$ respectivamente. Assim,

$$\alpha^n + a_{n-1}\alpha^{n-1} + ... + a_2\alpha^2 + a_1\alpha + a_0 = 0 \qquad \text{e} \tag{3.10}$$

$$\beta^m + b_{m-1}\beta^{m-1} + ... + b_2\beta^2 + b_1\beta + b_0 = 0 \tag{3.11}$$

ou seja,

$$\alpha^n = -a_{n-1}\alpha^{n-1} - ... - a_2\alpha^2 - a_1\alpha - a_0 \text{ e} \tag{3.12}$$

$$\beta^m = -b_{m-1}\beta^{m-1} - ... - b_2\beta^2 - b_1\beta - b_0 \tag{3.13}$$

isto é, α^n está expresso como uma combinação linear de $1, \alpha, ..., \alpha^{n-1}$, usando coeficientes racionais e β^m como combinação linear de $1, \beta, ..., \beta^{m-1}$. Multiplicando (3.10) por α e substituindo-se o α^n obtido na expressão pelo seu valor dado em (3.12), obtemos α^{n+1} expresso ainda como combinação linear de $1, \alpha, ..., \alpha^{n-1}$ usando coeficientes racionais. E assim sucessivamente todas as potencias α^j para $j \geq n$, são expressas como combinações lineares de $1, \alpha, ..., \alpha^{n-1}$, usando-se coeficientes racionais.

O mesmo se conclui para β^k, para $k \geq m$ como combinações lineares de $1, \beta, ..., \beta^{m-1}$.

Nosso objetivo agora será mostrar que $\alpha + \beta$ satisfaz uma equação polinomial de grau mn com coeficientes racionais, implicando então que $\alpha + \beta$ seja algébrico.

Consideremos os $m.n+1$ números

$$1, \alpha+\beta, (\alpha+\beta)^2, ..., (\alpha+\beta)^{mn}$$

e o espaço vetorial sobre $\mathbb{Q}$ gerado pelos elementos

$$B = \{1, \alpha, \beta, \alpha^2, \beta^2, \alpha\beta, ..., \alpha^{n-1}\beta^{m-1}\}$$

Como B é um conjunto de geradores de $m \cdot n$ elementos, então possui uma base com cardinalidade menor ou igual a $m \cdot n$. Então a dimensão deste espaço é menor ou igual a $m \cdot n$, logo, os $m \cdot n + 1$ números acima são L.D.. Portanto, existem racionais $(r_0, ..., r_{m \cdot n})$ nem todos nulos, tais que

$$r_0 + r_1(\alpha+\beta) + r_2(\alpha+\beta)^2 + ... + r_{mn}(\alpha+\beta)^{mn} = 0.$$

O que mostra que $\alpha + \beta$ satisfaz uma equação polinomial de grau mn. $\square$

Demonstração de (ii):

Utilizamos o mesmo raciocínio da demonstração de (i). No entanto consideramos agora os $m.n+1$ números

$$1, \alpha\beta, (\alpha\beta)^2, ..., (\alpha\beta)^{m.n}$$

Seguindo o mesmo argumento de (i), pela Proposição 3.3, os $w_i s$ são os $m.n+1$ números $1, \alpha\beta, (\alpha\beta)^2, ..., (\alpha\beta)^{m.n}$ e os $v_i s$ são os mn números $\alpha^j \beta^k$. Assim, existem $(s_0, s_1, ..., s_{mn})$ racionais, nem todos nulos, tais que

$$s_0 + s_1(\alpha\beta) + s_2(\alpha\beta)^2 + ... + s_{mn}(\alpha\beta)^{mn} = 0$$

O que mostra que $\alpha\beta$ é raiz de uma equação polinomial de grau mn. $\square$

CAPÍTULO IV

A TRANSCENDÊNCIA DO NÚMERO e

No capítulo II, demonstramos a irracionalidade do número e bem como o caracterizamos de diferentes formas. Nosso objetivo, nesse capitulo, será demonstrar a transcendência do número e.

Inicialmente vamos considerar um polinômio $F(x)$ definido como a soma de um polinômio $P(x)$ de grau r com suas respectivas derivadas.

Proposição 4.1 *Seja a função* $F(x)=P(x)+P'(x)+...+P^{(r)}(x)$*; em que* $P(x)$ *é um polinômio de grau* r *e* $P^{(r)}(x)$ *representa a derivada de ordem* r *de* $P(x)$*. Então,*

$$\frac{d}{dx}\left(e^{-x}F(x)\right)=-e^{-x}P(x).$$

Demonstração:

Temos $e^{-x}F(x)=e^{-x}P(x)+e^{-x}P'(x)+...+e^{-x}P^{(r)}(x)$. Então,

$$\frac{d}{dx}\left(e^{-x}F(x)\right)=-e^{-x}P(x)+e^{-x}P'(x)-e^{-x}P'(x)+e^{-x}P''(x)-e^{-x}P''(x)...$$

$$+e^{-x}P^{(r)}(x)-e^{-x}P^{(r)}(x)+e^{-x}P^{(r+1)}(x),$$

como $P^{(r+1)}(x)=0$, pois $P(x)$ tem grau r, temos

$$\frac{d}{dx}\left(e^{-x}F(x)\right)=-e^{-x}P(x).$$

□

Proposição 4.2 *Temos que,* $F(k)-e^{k}F(0)=-ke^{k(1-\theta_k)}P(k\theta_k)$*, para todo* $k>0$*, onde* θ_k *é um número entre 0 e 1.*

Demonstração:

Uma vez que $0<\theta_k<1$, vamos aplicar o Teorema do Valor Médio à função $e^{-x}F(x)$. Temos então:

$$\frac{e^{-k}F(k)-e^{-0}F(0)}{k-0}=\frac{d}{dx}\left(e^{-k.\theta_k}F(k\theta_k)\right)\Rightarrow$$
$$e^{-k}F(k)-F(0)=-ke^{-k.\theta_k}P(k\theta_k)\Rightarrow$$
$$F(k)-e^{k}F(0)=-ke^{k(1-\theta_k)}P(k\theta_k),$$

sendo que na segunda linha usamos a proposição 4.1. $\square$

Devido à importância dessa expressão para a demonstração, vamos definir a constante do segundo membro como:

Definição 4.1 $\varepsilon_k=-ke^{k(1-\theta_k)}P(k\theta_k)$.

A fim de generalizarmos resultados posteriores, precisaremos de um importante resultado sobre o polinômio $Q(x)=\sum_{j=0}^{r}a_jx^j$ que será exposto na seguinte proposição.

Proposição 4.3 *Seja* $Q(x)=\sum_{j=0}^{r}a_jx^j$ *um polinômio com coeficientes inteiros e seja* $p<r$ *um inteiro primo. Então*:

(i) $Q^{(i)}(x)=\sum_{j=i}^{r}\frac{j!}{(j-i)!}a_jx^{j-i}, i\le r.$

(ii) $\frac{1}{(p-1)!}Q^{(i)}(x), p\le i,$ *é um polinômio com coeficientes inteiros divisíveis por* p.

Demonstração:

Temos que $Q(x)=\sum_{j=0}^{r}a_jx^j=a_0+a_1x+...+a_rx^r$.

Então,

$$Q^{(1)}(x)=a_1+2a_2x+...+ra_rx^{r-1}$$
$$Q^{(2)}(x)=2a_2+6a_3x+...+r(r-1)a_rx^{r-2}$$
$$Q^{(3)}(x)=6a_3+24a_4x+...+r(r-1)(r-2)a_rx^{r-3}$$
$$=\frac{3!}{0!}a_3+\frac{4!}{1!}a_4x+...+\frac{r!}{(r-3)!}a_rx^{r-3}$$
$$\vdots \qquad\qquad \vdots$$

Logo, $Q^{(i)}(x)=\frac{i!}{0!}a_1+\frac{(i+1)!}{1!}a_{i+1}x+\frac{(i+2)!}{2!}a_{i+2}x^2+...+\frac{r!}{(r-i)!}a_rx^{r-i}$, ou seja,

$$Q^{(i)}\left(x\right)=\sum_{j=i}^{r}\frac{j!}{(j-i)!}a_j x^{j-i}, i\le r$$

o que prova a primeira parte.

Quanto a segunda, observemos que os coeficientes de $\frac{1}{(p-1)!}Q^{(i)}\left(x\right)$ serão da forma

$\frac{j!}{(j-1)!}.\frac{1}{(p-1)!}a_j$, onde a_j é inteiro.

Temos $p\le i$, p fixo e $j=i,\dots,r.$

No primeiro coeficiente, temos $j=i$ e, consequentemente,

$$\frac{j!}{0!}.\frac{1}{(p-1)!}=\frac{j(j-1)\dots p(p-1)!}{(p-1)!}=j(j-1)\dots p.$$

No segundo coeficiente, temos $j=i+1,$ portanto,

$$\frac{j!}{1!}.\frac{1}{(p-1)!}=\frac{j(j-1)\dots p(p-1)!}{(p-1)!}=j(j-1)\dots p.$$

No terceiro coeficiente, temos $j=i+2,$ portanto,

$$\frac{j!}{2!}.\frac{1}{(p-1)!}=\frac{j(j-1)\dots p(p-1)!}{2.1(p-1)!}=\frac{j(j-1)\dots p}{2}.$$

Observemos que o numerador tem $j-(p-1)=j-p+1$ fatores. Como $i+2\ge p+2,$ temos $j\ge p+2,$ ou seja, $j-p\ge 2,$ o que implica $j-p+1\ge 3.$ Assim, podemos concluir que o numerador terá pelo menos 3 fatores, logo é divisível por 2 e por p.

No quarto coeficiente, temos $j=i+3,$ portanto,

$$\frac{j!}{3!}.\frac{1}{(p-1)!}=\frac{j(j-1)\dots p(p-1)!}{3.2.1(p-1)!}=\frac{j(j-1)\dots p}{3!}$$

e, nesse caso, o numerador terá pelo menos 4 fatores, logo é divisível por 6 e por p.

Generalizando, teremos para $j=i+k, k\in\mathbb{N}$,

$$\frac{j!}{k!}.\frac{1}{(p-1)!}=\frac{j(j-1)\dots p(p-1)!}{k!(p-1)!}=\frac{j(j-1)\dots p}{k!},$$

sendo que o numerador tem pelo menos $k+1$ fatores, ou seja,

$$j-p+1\ge k+1\Rightarrow$$
$$j-k+1\ge p+1.$$

Dessa forma,

$$\begin{aligned}\frac{j!}{k!}\cdot\frac{1}{(p-1)!} &= \frac{j(j-1)...(j-k+1)(j-k)...p}{k!}\\ &= \frac{j(j-1)...(j-k+1)}{k!}\cdot\frac{(j-k)!}{(j-k)!}(j-k)...p\\ &= \frac{j!}{k!(j-k)!}(j-k)...p\\ &= \binom{j}{k}(j-k)...p,\end{aligned}$$

sendo $\binom{j}{k}$ um número binomial, o que implica $\binom{j}{k}\in\mathbb{Z}$, ou seja, $\binom{j}{k}(j-k)...p\in\mathbb{Z}$ e, portanto, $\frac{j!}{k!}\cdot\frac{1}{(p-1)!}\in\mathbb{Z}$ e é divisível por p. Dessa forma, os coeficientes de $\frac{1}{(p-1)!}Q^{(i)}(x)$ são todos inteiros divisíveis por p. ∎

Definiremos agora o polinômio $P(x)$, da proposição 4.1, como sendo

Definição 4.2 $P(x)=\frac{1}{(p-1)!}x^{p-1}(1-x)^p...(n-x)^p$

Diante dessa definição, podemos estabelecer importantes propriedades expressadas na seguinte proposição e nos corolários que seguem.

Proposição 4.4 *O polinômio* $P(x)=\frac{1}{(p-1)!}x^{p-1}(1-x)^p...(n-x)^p$*, sendo p um número primo tal que* $p>n\in\mathbb{N}^*$ *e* $p>c_0$*, pode ser escrito na forma*

$$P(x)=\frac{(n!)^p}{(p-1)!}x^{p-1}+\frac{b_1}{(p-1)!}x^p+...$$

Sendo b_1 *uma constante.*

Demonstração:

Temos

$$P(x)=\frac{1}{(p-1)!}x^{p-1}(1-x)^p...(n-x)^p.$$

Façamos

$$H(x)=(1-x)(2-x)...(n-x)$$

e observemos que $H(x)$ é da forma $a_n x^n + a_{n-1}x^{n-1} + ... + a_1 x + n!,$ sendo $a_1,...,a_n$ constantes e consequentemente, teremos

$$[H(x)]^p = b_{np}x^{np} + b_{n-1}x^{np-1} + ... + b_1 x + (n!)^p,$$

sendo $b_1,...,b_{np}$ constantes.

Voltando a $P(x),$ temos,

$$P(x) = \frac{x^{p-1}}{(p-1)!}\left[H(x)\right]^p \Rightarrow$$

$$P(x) = \frac{b_{np}}{(p-1)!}x^{np+p-1} + ... + \frac{b_1}{(p-1)!}x^p + \frac{(n!)^p}{(p-1)!}$$

ou seja,

$$P(x) = \frac{(n!)^p}{(p-1)!}x^{p-1} + \frac{b_1}{(p-1)!}x^p + ... + \frac{b_{np}}{(p-1)!}x^{np+p-1},$$

□

Corolário 4.1 *Nas condições da Proposição 4.4, temos* $P^{(i)}(k) = 0; k = 1,...,n;$ *sendo* $i < p$.

Demonstração:

Basta observar que $1,...,n$ são raízes de multiplicidade p do polinômio $P.$ Como o grau de P é maior que p (Proposição 4.4), temos que $1,...,n$ são raízes das derivadas de ordens menores que p.

De fato:

$$P(x) = (k-x)^p g(x),$$

sendo $g(x) = \dfrac{1}{(p-1)!}x^{p-1}(1-x)^p...(k-1-x)^p(k+1-x)^p...(n-x)^p.$

Logo:

$$P'(x) = -p(k-x)^{p-1}g(x) + (k-x)^p g'(x)$$
$$= (k-x)^{p-1}\left(-pg(x) + (k-x)g'(x)\right)$$
$$= (k-x)^{p-1}g_1(x),$$

sendo $g_1(x) = -pg(x) + (k-x)g'(x).$

Generalizando, teremos:

$$P^{(i)}(x) = (k-x)^{p-i}g_i(x),$$

que é tal que $P^{(i)}\left(k\right)=0; k=1,...,n;$ sendo $i<p$. □

Corolário 4.2 *Nas condições da Proposição 4.4,* $P^{(p-1)}\left(0\right)=(n!)^p$ *e* $P^{(i)}\left(0\right)=0,\ i<p-1.$

Demonstração:

1^a Parte: $P^{(p-1)}\left(0\right)=(n!)^p$.

De $P\left(x\right)=\dfrac{(n!)^p}{(p-1)!}x^{p-1}+\dfrac{b_1}{(p-1)!}x^p+...$, temos $P^{(p-1)}\left(x\right)=(n!)^p+b_1px+...$ e, assim, o único termo que não é fatorado por x é $(n!)^p$. Daí, ao aplicarmos $x=0$, esse é o único termo que não se anulará.

2^a Parte: $P^{(i)}\left(0\right)=0,\ i<p-1.$

Nesse caso, qualquer $i<p-1$ será menor que o menor expoente de x em $P,$ o que fará com que todos os termos do polinômio $P^{(i)}\left(x\right)$ estejam fatorados por x e, consequentemente, se tornem nulos ao aplicarmos $x=0$. □

A partir de agora vamos supor que e seja algébrico, ou seja, é raiz de uma equação polinomial com coeficientes inteiros e de menor grau possível (tomaremos também $c_0>0$). Assim,

$$c_ne^n+c_{n-1}e^{n-1}+...+c_1e+c_0=0. \qquad (4.1)$$

Nosso objetivo agora é chegar a alguma contradição com essa hipótese.

Proposição 4.5 *Se* e *é algébrico, satisfazendo à equação (4.1), então* $c_0F\left(0\right)+c_1F\left(1\right)+...+c_nF\left(n\right)=c_1\varepsilon_1+...+c_n\varepsilon_n.$

Demonstração:

Da Proposição 4.2, temos

$$\begin{aligned}
F\left(1\right)&=-e^{(1-\theta_1)}P\left(\theta_1\right)+eF\left(0\right)=\varepsilon_1+eF\left(0\right)\\
F\left(2\right)&=-2e^{2(1-\theta_2)}P\left(2\theta_2\right)+e^2F\left(0\right)=\varepsilon_2+e^2F\left(0\right)\\
&\ \vdots \qquad\qquad\qquad\qquad \vdots\\
F\left(n\right)&=-ne^{n(1-\theta_n)}P\left(n\theta_n\right)+e^nF\left(0\right)=\varepsilon_n+e^nF\left(0\right).
\end{aligned}$$

Então,

$$c_0F(0)+c_1F(1)+...+c_nF(n)=c_0F(0)+c_1\varepsilon_1+c_1eF(0)+...+c_n\varepsilon_n+c_ne^nF(0)$$

$$=F(0)\left(c_0+c_1e+...+c_ne^n\right)+c_1\varepsilon_1+...+c_n\varepsilon_n,$$

ou seja,

$$c_0F(0)+c_1F(1)+...+c_nF(n)=c_1\varepsilon_1+...+c_n\varepsilon_n, \qquad (4.2)$$

Devido à hipótese assumida acima que e satisfaz (4.1). □

Nosso objetivo agora será demonstrar que para um determinado polinômio $P(x)$ o lado esquerdo dessa igualdade é um inteiro não divisível por um primo p enquanto o lado direito pode se tornar menor que 1, em valor absoluto, para um primo p suficientemente grande. O que nos dará um absurdo.

Proposição 4.6 *Seja* $F(x)=P(x)+P'(x)+......+P^{(np+p-1)}(x)$, *conforme definido na Proposição 4.1, então* $F(k)$, *para* $k=1,...,n$, *é um inteiro divisível por* p *e* $F(0)$ *é um inteiro não divisível por* p. *O polinômio* $P(x)$ *é o da definição 4.2.*

Demonstração:

Vamos considerar os seguintes fatos:

1. $P(k)=0, k=1,...,n.$ Pois $P(x)=\dfrac{1}{(p-1)!}x^{p-1}(1-x)^p...(n-x)^p$.

2. Do Corolário 4.1, temos que $P^{(i)}(k)=0$; $i<p$.

3. Todo $P^{(i)}(x)$ pode ser escrito na forma $\dfrac{1}{(p-1)!}Q^{(i)}(x)$, sendo $Q^{(i)}(x)$ definido de acordo com a Proposição 4.3 (para ver isso, basta derivar P na forma não fatorada, conforme Proposição 4.4). Daí, $P^{(i)}(k)$, para $i\geq p$ é um inteiro divisível por p.

Portanto, $F(k)$ fica resumida ao somatório dos $P^{(i)}(k)$, onde $i\geq p$, os quais são inteiros e divisíveis por p.

Para $F(0)$ consideramos também que:

4. $P(0)=0$.

5. Do Corolário 4.2, temos que $P^{(p-1)}(0)=(n!)^p$ e $P^{(i)}(0)=0,\ i<p-1$.

6. $(n!)^p$ não é divisível por p pois p é primo e $p<n \Rightarrow n$ não é divisível por $p \Rightarrow n!$ não é divisível por $p \Rightarrow (n!)^p$ também não é divisível por p.

Portanto, $F(0)$ é um somatório de números inteiros, em que um dos termos ($P^{(p-1)}(0)=(n!)^p$) não é divisível por p e os demais são divisível por p. Logo $F(0)$ é um inteiro não divisível por p. ∎

Considerando a igualdade 4.2 da Proposição 4.5, podemos estabelecer o seguinte corolário.

Corolário 4.3 *O número* $c_0F(0)+c_1F(1)+...+c_nF(n)$ *é um inteiro não divisível por* p, *sendo* $0<c_0<p$.

Demonstração:

Como $p>c_0$, então c_0 não é divisível por p, e da Proposição 4.6, temos que $F(0)$ também não é divisível por p. Portanto, $c_0F(0)$ não é divisível por p, pois p é primo.

Se supusermos que p divide $c_0F(0)+c_1F(1)+...+c_nF(n)$, então p dividirá todos os termos do somatório, o que não é verdade, pois $c_0F(0)$ não é divisível por p. Logo, p não divide $c_0F(0)+c_1F(1)+...+c_nF(n)$. ∎

Para as duas próximas proposições, utilizaremos a constante da definição 4.1.

Proposição 4.7 *Para* $k \le n$ *inteiro positivo,* $|\varepsilon_k| \le \dfrac{e^n n^p (n!)^p}{(p-1)!}$. *Sendo* ε_k *da Definição 4.1, calculado para o polinômio* $P(x)$ *da proposição 4.5.*

Demonstração:

$$\varepsilon_k = -ke^{k(1-\theta_k)}\frac{1}{(p-1)!}(k\theta_k)^{p-1}(1-k\theta_k)^p...(n-k\theta_k)^p,$$

sendo $0<\theta_k<1$ e $k \le n$. Daí,

$$|\varepsilon_k|(p-1)! = \left|ke^{k(1-\theta_k)}k^{p-1}\theta_k^{p-1}(1-k\theta_k)^p...(n-k\theta_k)^p\right|.$$

Como $0<\theta_k<1 \Rightarrow j-k\theta_k<j;\ j=1,...,n.$ Então,

$$|\varepsilon_k|(p-1)! < \left|k^p e^{k(1-\theta_k)}(\theta_k)^{p-1}1^p2^p...n^p\right|$$

ainda de $0 < \theta_k < 1 \Rightarrow k(1-\theta_k) < k$. Daí

$$|\varepsilon_k|(p-1)! < \left|k^p e^k (\theta_k)^{p-1}(n!)^p\right|$$

e mais uma vez, de $0 < \theta_k < 1$,

$$|\varepsilon_k|(p-1)! < \left|k^p e^k (1)^{p-1}(n!)^p\right|.$$

Assim, $|\varepsilon_k| < \dfrac{\left|k^p e^k (n!)^p\right|}{(p-1)!}$. Como $k \le n$, então $|\varepsilon_k| < \dfrac{n^p e^n (n!)^p}{(p-1)!}$. Portanto,

$$|\varepsilon_k| \le \frac{e^n n^p (n!)^p}{(p-1)!}. \qquad \square$$

Proposição 4.8 *Existe* p *primo tal que* $|c_1\varepsilon_1 + ... + c_n\varepsilon_n| < 1$, *sendo* $\varepsilon_1,...,\varepsilon_n$ *da Proposição anterior.*

Demonstração:

Temos
$$|c_1\varepsilon_1 + ... + c_n\varepsilon_n| \le |c_1\varepsilon_1| + ... + |c_n\varepsilon_n|$$
$$= |c_1||\varepsilon_1| + ... + |c_n||\varepsilon_n|.$$

Como $|\varepsilon_k| \le \dfrac{e^n n^p (n!)^p}{(p-1)!}$, então

$$|c_1\varepsilon_1 + ... + c_n\varepsilon_n| < (|c_1| + ... + |c_n|)\frac{n^p e^n (n!)^p}{(p-1)!} = \frac{Cn^p e^n (n!)^p}{(p-1)!},$$

sendo $C = |c_1| + ... + |c_n|$.

Vamos mostrar que existe p primo, suficientemente grande, tal que $\dfrac{Cn^p e^n (n!)^p}{(p-1)!} < 1$.

Para isso, vamos fazer $x_p = \dfrac{Cn^p e^n (n!)^p}{(p-1)!}$ e mostrar que essa seqüência converge para 0.

Tomemos $\left(\dfrac{x_{p+1}}{x_p}\right) = \dfrac{Cn^{p+1} e^n (n!)^{p+1}}{[(p+1)-1]!} \cdot \dfrac{(p-1)!}{Cn^p e^n (n!)^p} = \dfrac{Cn^p n e^n (n!)^p (n!)(p-1)!}{p(p-1)! Cn^p e^n (n!)^p} = \dfrac{n!.n}{p}$.

Logo, $\lim\limits_{p\to\infty}\left(\dfrac{x_{p+1}}{x_p}\right) = \dfrac{n!.n}{p} = 0$, Portanto, a série $\sum\limits_{p \ge n} x_p$ converge, ou seja, a sequência do termo geral x_p converge para 0. Assim, para um primo p suficientemente grande, teremos

$$x_p = \frac{Cn^p e^n (n!)^p}{(p-1)!} < 1 \Rightarrow |c_1\varepsilon_1 + ... + c_n\varepsilon_n| < 1. \qquad \square$$

Teorema 4.1 *e é transcendente.*

Demonstração:

Consideremos os seguintes resultados:

(1) Da Proposição 4.3, temos $c_0F(0)+c_1F(1)+...+c_nF(n)=c_1\varepsilon_1+...+c_n\varepsilon_n$.

(2) Do Corolário 4.3, temos que $c_0F(0)+c_1F(1)+...+c_nF(n)$ é um inteiro não divisível por p.

(3) Da Proposição 4.8, temos que para algum primo p, $|c_1\varepsilon_1+...+c_n\varepsilon_n|<1$.

Chegamos, assim, a uma contradição! Por (1), $|c_0F(0)+c_1F(1)+...+c_nF(n)|$ é um inteiro menor que um, ou seja, zero. Por (2), temos que esse inteiro não é divisível por p. Logo, não pode ser zero!

Essa contradição surgiu do fato de termos admitido que e fosse algébrico, ou seja, que poderia ser raiz de uma equação polinomial com coeficientes inteiros. Logo, e não é algébrico, sendo, portanto, transcendente. $\square$

CONCLUSÃO

Para propósitos de medições nós não precisamos dos números irracionais, pois sempre poderemos aproximar o número irracional através de uma serie de *aproximações racionais*, cuja precisão pode ser tão boa quanto desejarmos. É o aspecto *teórico* dos números irracionais que os tornam tão importantes para a matemática: eles são necessários para preencher os "buracos" deixados na linha dos números pela existência de pontos não racionais; e fazem do conjunto de números reais um sistema completo, um *continuum numérico.* O primeiro número transcendente só foi exibido em 1844 por Joseph Liouville embora a teoria dos números transcendentes tenha nascido na Grécia antiga com os três famosos problemas gregos de construção com régua e compasso: a quadratura de um círculo, a trisecção de um ângulo e a duplicação de um cubo. O estudo desses problemas recai na construção (com régua sem escala e compasso) de um segmento com certa medida que não é "construtível" a partir de um segmento dado como unidade. Temos aí a teoria dos *Números Construtíveis* que, hoje sabemos, são todos números algébricos.

No congresso internacional de Matemática, realizado em Paris, em 1900, um dos maiores matemáticos da época, David Hilbert (1892-1943), desafiou a comunidade matemática com uma lista de vinte e três problemas não resolvidos, cuja solução ele considerava da maior importância. O sétimo problema da lista de Hilbert era provar ou negar a hipótese de que, para qualquer número algébrico $a \neq 0$, 1 e para qualquer número algébrico irracional b, a expressão a^b é sempre transcendente. Como exemplo específico ele deu o número $2^{\sqrt{2}}$. Hilbert previu que esse problema levaria mais tempo para ser resolvido que o Último Teorema de Fermat, mas foi excessivamente pessimista. Em 1930 o matemático russo Alexandr Osipavich Gelfond (1906-1968) provou a sua transcendência. A hipótese geral de Hilbert, em relação a a^b, foi demonstrada em 1934 por Gelfond e também, independentemente, por T. Schneider na Alemanha.

Não é fácil provar que um número é transcendente: é preciso provar que o número *não* preenche certas exigências. **Entre os números cuja condição ainda não foi estabelecida temos π^e, π^π e e^e.**

A descoberta dos números transcendentes não provocou o mesmo choque intelectual que os números irracionais tinham causado, dois mil e quinhentos anos antes, mas suas conseqüências foram igualmente significativas. Ela mostrou que, por trás da aparente simplicidade do sistema de números reais, ocultam-se muitas sutilezas que não podem ser notadas simplesmente olhando-se a expansão decimal de um número. Mas a maior surpresa ainda estava por vir. Em 1874 o matemático alemão Georg Cantor (1845-1918) fez a espantosa descoberta de que existem mais números irracionais do que racionais, e mais números transcendentes do que algébricos. Em outras palavras, longe de serem excentricidade, a maioria dos números reais é irracional e, entre os números irracionais, a maioria é transcendente!

E isso no leva a campos ainda mais elevados de abstração. Se nos concentrarmos em apenas calcular os valores de π^e e e^π, descobriremos que eles são surpreendentemente próximos: 22,459157... e 23,140692..., respectivamente. É claro que π e e não estão demasiado separados numericamente. Pense nisso: entre a infinidade de números reais, aqueles que são mais importantes para a matemática – $0,1,\sqrt{2}$, e e π – estão localizados dentro de menos de quatro unidades na linha numérica. Uma coincidência extraordinária? Ou um mero detalhe de um projeto maior?

REFERÊNCIAS

[1] ÁVILA, Geraldo Severo de Sousa. Análise Matemática para Licenciatura, São Paulo: Edgard Blucher, 2006.

[2] LIMA, Elon Lages. Análise Real vol 1, Rio de Janeiro: IMPA, 2008.

[3] MAOR, Eli. *e:* a História de um Número; tradução de Jorge Luiz Calife – 4º ed,–Rio de Janeiro: Record, 2008.

[4] FIGUEIREDO D.G.. Números Irracionais e Transcendentes, Rio de Janeiro: Publicação da Sociedade Brasileira de Matemática (SBM). Coleção Fundamentos da Matemática elementar, 1985.

[5] CANTOR, Georg. Caracterização dos Números Reais; tradução de Denise Silva Vilela. Revista da Sociedade Brasileira da História da Ciência, nº 10, pg.85-94, 1993.

[6] DOMINGUES, Hygino H.. Álgebra Moderna: São Paulo: Atual, 2003.

[7] SANTOS, José Plínio de Oliveira. Introdução à Teoria dos Números, Rio de Janeiro: IMPA, 2006.

[8] STEINBRUCH, Alfredo. Álgebra Linear, São Paulo: Makron Books, 1987.

[9]OLIVEIRA, Anselmo A de A.(2004) Famat em Revista nº 03, setembro de 2004<www.famat.ufu.br/revista/revistaset2004/index.htm>Acessado em 20 de maio de 2009.

[10]SINGH, Simon. O Último Teorema de Fermat; tradução de Jorge Luiz Calife, Rio de Janeiro.

[11]SPIVAK, M. Calculos, 3ª Edição: Editora Publish or Perish, 1994.

APÊNDICES

Apêndice 1

Algoritmo da Divisão de Euclides

Dados dois inteiros a *e* b, $b \neq 0$ *existe um único par de inteiros* q *e* r *tais que* $a = qb + r$ *com* $0 \leq r < b$.

Há duas possibilidades:

(i) b é múltiplo de a e, portanto, $b = aq$ para um conveniente inteiro q.

(ii) b está situado entre dois múltiplos consecutivos de a, isto é, existe um inteiro q tal que $aq < b < a(q+1)$. Daí, $0 < b - aq < a$. Então, fazendo $b - aq = r$, obtemos $b = aq + r$, em que $0 < r < a$.

Juntando as duas possibilidades, podemos garantir o seguinte: dados dois números inteiros, a e b, com $a > 0$, então sempre se pode encontrar dói inteiros q e r tais que $b = aq + r$, em que $0 \leq r < a$.

Evidentemente, $r = 0$ corresponde ao caso em que b é múltiplo de a.

Vamos imaginar, por outro lado, que se pudesse determinar outro par de inteiros, q_1 e r_1, tais que $b = aq_1 + r_1$, com $0 \leq r_1 < a$. Então, $aq + r = aq_1 + r_1$ e, portanto. $a(q - q_1) = r_1 - r$. Suponhamos que $r \neq r_1$ digamos $r > r_1$. Daí, o segundo membro da ultima igualdade seria estritamente negativo e, como $a > 0$, então $q - q_1$ também seria estritamente negativo e, portanto, $q_1 - q > 0$, ou seja, $q_1 - q \geq 1$. Mas de $a(q - q_1) = r_1 - r$ segue que:

$$r = r_1 + a(q_1 - q)$$

Levando-se em conta que $a > 0$, $r_1 \geq 0$ e $q_1 - q \geq 1$, da ultima igualdade seguiria que $r \geq a$, o que é absurdo.

Da mesma forma, prova-se que a desigualdade $r_1 > r$ também é impossível. De onde $r = r_1$ e, consequentemente, $q = q_1$.

Apêndice 2

Teorema Fundamental da Aritmética

Todo inteiro maior do que 1 pode ser representado de maneira única (a menos de ordem) como um produto de fatores primos.

Sendo n um inteiro maior que 1, se n é primo não há nada a ser demonstrado, suponhamos pois, n composto. Seja $p_1 (p_1 > 1)$ o menor dos divisores positivos de n. Afirmamos que p_1 é primo. Isto é verdade, pois, caso contrário existiria $p, 1 < p < p_1$ com $p \mid n$, contradizendo a escolha de p_1. Logo, $n = p_1 n_1$.

Se n_1 for primo a prova está completa. Caso contrário, tomamos p_2 como o menor fator de n_1. Pelo argumento anterior, p_2 é primo e temos que $n = p_1 p_2 n_2$.

Repetindo este procedimento, obtemos uma seqüência decrescente de inteiros positivos $n_1, n_2, ..., n_r$. Como todos eles são inteiros maiores do que 1, este procedimento deve terminar. Como os primos na seqüência $p_1, p_2, ..., p_k$ não são, necessariamente distintos, n terá em geral, a forma:

$$n = p_1^{\alpha_1} p_2^{\alpha_2} ... p_k^{\alpha_k}.$$

Para mostrarmos a unicidade usamos indução em n. Para $n = 2$ a afirmação é verdadeira. Assumimos, então, que ela se verifica para todos os inteiros maiores do que 1 e menores do que n. Vamos provar que ela também é verdadeira para n. Se n é primo, não há nada a provar. Vamos supor, então, que n seja composto e que tenha duas fatorações, isto é,

$$n = p_1 p_2 ... p_s = q_1 q_2 ... q_r.$$

Vamos provar que $r = s$ e que cada p_i é igual a algum q_j. Como p_1 divide o produto $q_1 q_2 ... q_r$ ele divide pelo menos um dos fatores q_j. Sem perda de generalidade podemos supor que $p_1 \mid q_1$. Como são ambos primos, isto implica $p_1 = q_1$. Logo $n \mid p_1 = p_2 ... p_s = q_2 ... q_r$. Como $1 < n \mid p_1 < n$, a hipótese de indução nos diz que as duas fatorações são idênticas, isto é $s = r$ e, a menos de ordem, as fatorações $p_1 p_2 ... p_s$ e $q_1 q_2 ... q_s$ são iguais.

JULIMAR CARLOS DE OLIVEIRA
CARLOS CRUZ GOMES

NÚMEROS IRRACIONAIS E TRANSCENDENTES

Monografia apresentada ao Departamento de Matemática e Física da UFSC, como requisito parcial para obtenção do grau de Professor Especialista em Matemática.

Aprovada em ______/_______/________

BANCA EXAMINADORA

____

Prof.º Eliezer Batista (orientador)

____

____