PONTIFÍCIA UNIVERSIDADE CATÓLICA DE SÃO PAULO
PUC/SP

ALOÍSIO DANIEL VENDEMIATTI

A QUADRATURA DO CÍRCULO E A GÊNESE DO NÚMERO π

MESTRADO PROFISSIONAL EM ENSINO DE MATEMÁTICA

São Paulo

2009

PONTIFÍCIA UNIVERSIDADE CATÓLICA DE SÃO PAULO
PUC/SP

ALOÍSIO DANIEL VENDEMIATTI

A QUADRATURA DO CÍRCULO E A GÊNESE DO NÚMERO π

Dissertação apresentada à Banca Examinadora da Pontifícia Universidade Católica de São Paulo, como exigência parcial para obtenção do título de ***MESTRE PROFISSIONAL EM ENSINO DE MATEMÁTICA****, sob a orientação do* ***Prof. Dr. Benedito Antonio da Silva****.*

São Paulo

2009

Errata

p. 22, linha 26: onde se lê: do decágono, leia-se: dodecágono.
p.25, linha 15: onde se lê: tabela abaixo, leia-se: tabela 1.

p.28, linha 1: onde se lê: A desigualdade $\frac{p_n}{2r} < \frac{C}{2r} < \frac{P_n}{2r}$ determina uma seqüência de intervalos encaixados, leia-se: A desigualdade $\frac{p_n}{2r} < \frac{C}{2r} < \frac{P_n}{2r}$ determina uma seqüência $I_n = \left[\frac{p_n}{2r}, \frac{P_n}{2r}\right]$ de intervalos fechados e encaixados.

p.31, linha 11: onde se lê: tabela abaixo, leia-se: tabela 2.

p.34, linha 21: onde se lê: Achamos necessário justificá-la, leia-se: Achamos necessário justificá-la sem a pretensão de demonstrá-la.

p.44, linha 16: onde se lê: casas decimais do número π, leia-se: casas decimais da representação decimal do número π.

p.63, linha 28: onde se lê: conhecendo-se dois de seus pontos, leia-se: determinada por dois pontos construtíveis do plano.

p.65, linha 13: onde se lê: $(b_{n-1}, \ldots, b_1, b_0 \in Q)$, leia-se: $(b_{m-1}, \ldots, b_1, b_0 \in Q)$.

p.70, linha 4: onde se lê: $\forall\ \alpha \in |,\ 1.\alpha = \alpha$, leia-se: $\forall \alpha \in \mathrm{R},\ 1.\alpha = \alpha$.

p.81, linha 11: Onde se lê: $|\alpha - \frac{p_m}{q_m}| > \frac{1}{q^{n+1}}$, leia-se: $|\alpha - \frac{p_m}{q_m}| > \frac{1}{q_m^{n+1}}$.

p.83, linha 15: Onde se lê: $b_n = \begin{cases} a_{nn}+1\ ,\ se\ a_{nn} \neq 9 \\ 0\ \ ,\ se\ a_{nn} = 9 \end{cases}$, leia-se: $b_n = \begin{cases} a_{nn}+1\ ,\ se\ a_{nn} \neq 9 \\ 1\ \ ,\ se\ a_{nn} = 9 \end{cases}$.

p.84, linha 18: onde se lê: a união de conjuntos enumeráveis é enumerável, leia-se: a união de dois conjuntos enumeráveis é enumerável.

p.85, linha 16: onde se lê: o número α^β é transcendente, se α é algébrico $(\alpha \neq 0\ e\ \alpha \neq 1)$ e β é algébrico e não racional, leia-se: *Sejam α e β números algébricos (reais ou complexos). Se $\alpha \neq 0, \alpha \neq 1$ e β não for um número racional (real), então α^β é transcendente* (FIGUEIREDO, 1985, p.96).

p.85, linha 25: onde se lê: $\log_{10} 2$ não é racional, leia-se: $\log_{10} 2$ não é racional (NIVEN, 1984, p.110).

p.86, linha 1: onde se lê: e^π é transcendente. $e^\pi = \frac{1}{e^{-\pi}}$. Como $e^{i\pi} = -1$ e $i^2 = -1$, temos $e^{i\pi} = i^2 \Rightarrow (e^{i\pi})^i = (i^2)^i \Rightarrow e^{i^2\pi} = i^{2i} \Rightarrow e^{-\pi} = i^{2i}$. Então $e^\pi = \frac{1}{e^{-\pi}} = \frac{1}{i^{2i}} = i^{-2i}$ e i^{-2i} é transcendente pelo Teorema de Gelfond, leia-se: e^π é transcendente, pois $e^\pi = \frac{1}{e^{-\pi}} = \frac{1}{i^{2i}}$, e i^{2i} é transcendente pelo Teorema de Gelfond (BOYER, 1974, p. 445).

p.93, linha 12: onde se lê: $P_n(t_1, t_2) = t_1^n - t_2^n$, leia-se: $P_n(t_1, t_2) = t_1^n + t_2^n$.

p.105, linha 2: onde se lê: $\binom{n}{m} = \frac{n!}{m.(n-m)!}$, leia-se: $\binom{n}{m} = \frac{n!}{m!.(n-m)!}$.

p.147, linha 5: onde se lê: (FIGUEIREDO, 1885, p. 59-65), leia-se: (FIGUEIREDO, 1985, p. 59-65).

Banca Examinadora

_____

_____

_____

Autorizo, exclusivamente para fins acadêmicos e científicos, a reprodução total ou parcial desta Dissertação por processos de fotocopiadoras ou eletrônicos.

Assinatura: _____ Local e Data: _____

À minha esposa Andréia
Aos meus pais, Antonio e Margarida

AGRADECIMENTOS

À minha esposa Andréia Neme Prado Vendemiatti, engenheira civil e professora de Matemática, que sempre me acompanhou durante o curso, pela compreensão, paciência, apoio, ajuda e sugestões.

À minha família pelo incentivo, assim como à família de minha esposa.

Ao meu cunhado Adilson José Neme Prado pelo acolhimento em sua casa todas as vezes que precisei ficar na cidade de São Paulo durante o curso.

Ao meu irmão José Adriano Vendemiatti que sempre me ajudou com prontidão por esclarecer e ensinar a utilizar os recursos do computador para a digitalização deste trabalho.

Ao meu irmão Leandro Abel Vendemiatti que fez a revisão final do texto.

Ao meu orientador, professor Dr. Benedito Antonio da Silva, pelas horas de atendimento, sugestões, indicações de leituras, ensinamentos e discussões no grupo de estudos, e por sua experiência, conhecimento e sabedoria que ajudaram muito na elaboração deste trabalho.

Às professoras doutoras Cristina Cerri e Sonia Barbosa Camargo Igliori, pelas contribuições e comentários sobre o projeto deste trabalho durante o exame de qualificação.

Aos professores do Programa de Estudo Pós-Graduados em Educação Matemática da Pontifícia Universidade Católica de São Paulo, Dr. Benedito Antonio da Silva, Dra. Sandra Maria Pinto Magina, Dr. Vincenzo Bongiovanni, Dra. Laurizete Ferragut Passos, Dra. Cileda de Queiroz e Silva Coutinho, Dra. Bárbara Lutaif Bianchini, Dr. Antonio Carlos Brolezzi, Dra. Sonia Pitta e Dr. Gerson Pastre de Oliveira, com os quais cursei as disciplinas do programa.

Ao amigo Antonio Spanó Junior, que foi meu professor durante a graduação na PUC de Campinas, pelas conversas e contribuições para este texto.

À Secretaria de Educação do Estado de São Paulo pela bolsa de estudos concedida pelo Programa Bolsa Mestrado.

O Autor

RESUMO

O objetivo deste trabalho é apresentar aspectos da gênese do número π, inerentes à questão da quadratura do círculo, a qual consiste em construir um quadrado de área igual à área de um círculo de raio r dado. Esse problema não diz respeito a uma aplicação prática da matemática, mas sim a uma questão teórica que envolve uma distinção entre uma boa aproximação e a exatidão do pensamento. O registro da primeira tentativa de se quadrar o círculo remonta a Anaxágoras, no século V a.C. Posteriormente, ficou estabelecido que essa construção deveria ser realizada utilizando-se, um número finito de vezes, a régua não graduada e o compasso. Nas construções com régua e compasso, estamos nos referindo aos três primeiros postulados dos *Elementos* de Euclides: 1) é possível unir dois pontos por uma reta, 2) prolongar uma linha reta até onde seja necessário e 3) traçar uma circunferência em torno de qualquer ponto e com qualquer raio. Esses postulados são a base dessas construções, muitas vezes chamadas de *construções euclidianas.* Um número real α é construtível, se for possível "construir com régua e compasso um segmento de comprimento igual a α, a partir de um segmento tomado como unidade". Apresentamos a idéia de traduzir o problema geométrico das construções com régua e compasso para a linguagem algébrica, e isso permitiu solucionar o problema da quadratura do círculo. Expomos que todo número construtível é algébrico sobre os racionais, estabelecendo a impossibilidade de quadrar o círculo com a demonstração de Lindemann, em 1882, da transcendência do número π. Vemos que esse problema fascinou estudiosos por mais de 20 séculos. Procuramos fornecer todas as ferramentas matemáticas necessárias para essa demonstração. As demonstrações desempenham um papel fundamental no desenvolvimento deste trabalho, que tem por finalidade não só contribuir para a formação do professor de matemática, mas também detalhar a resolução do problema da quadratura do círculo.

Palavras-Chave: quadratura do círculo, número π, números algébricos, números construtíveis, transcendência do número π.

ABSTRACT

The goal of this essay is to show aspects of genesis of number π, inherent to the question of squaring the circle, which consists in constructing a square which has the same area as a given circle. This problem does not refer to a practical application of mathematics, but to the theoretic question that involves the distinction between a valid approach and thinking accuracy. The first attempt to squaring the circle dates back in the fifth century before Christ. After that, it was established that this construction should be carried through using a finite number of times, also the non-graduated ruler and the drawing compass itself. In the constructions with ruler and drawing compass we are referring to the first three postulates of Euclides Elements: 1) It´s possible to join two points by a straight line, 2) to expand a straight line until the necessary point, and 3) to draw a circumference around any point and with any radius. These postulates are the base of these constructions, sometimes called *euclidean´s constructions*. A real number α is constructible, if feasible building a segment of legth α with ruler and drawing compass, since a segment is taken as a unity. We show the idea of translating the geometrical problem of constructions made with ruler and drawing compass to the algebraic language and this allowed us to solve the problem of squaring the circle. We exposed that all constructible numbers are algebraic, over the rational numbers, establishing the impossibility of squaring the circle, with Lindemann´s demonstration, in 1882, of the number π transcendence. This problem has been fascinating people for more than twenty centuries. We tried to supply all mathematical tools needed for this demonstration. Demonstrations play a fundamental role in the development of this essay, which purpose is not only to contribute to the math teacher formation, but also to detail the resolution of the problem of squaring the circle.

Key words: squaring the circle, number π, algebraic numbers, constructible numbers, transcendence of number π.

SUMÁRIO

APRESENTAÇÃO 13

CAPÍTULO 1 19
1.1 O problema da quadratura do círculo 19
1.2 O método de Arquimedes para o cálculo do π 22
1.3 Comprimento da Circunferência 24
1.4 Área do Círculo 30
1.5 A expressão de Viète para o número π 34
1.6 A expressão de John Wallis para o número π 37
1.7 Outras maneiras de se obter uma estimativa para o π 42

CAPÍTULO 2 47
2.1 Os números algébricos 47
2.2 O conjunto dos números algébricos é enumerável 52
2.3 Todo número construtível é algébrico 53
2.4 A aritmética dos números algébricos 64
2.4.1 A soma de dois números algébricos é algébrico 65
2.4.2 O produto de dois números algébricos é algébrico 69
2.4.3 O simétrico de um número algébrico é algébrico 69
2.4.4 O inverso de um número algébrico $\alpha \neq 0$ é algébrico 70

CAPÍTULO 3 73
3.1 Os números transcendentes: considerações iniciais 73
3.2 O Teorema de Liouville 75
3.3 Os números de Liouville 80
3.4. Prova de Cantor para a existência de números transcendentes 82
3.5. O conjunto dos números transcendentes não é enumerável 84
3.6 Outros exemplos de números transcendentes 85

CAPÍTULO 4 89
4.1 Relações entre os coeficientes e as raízes de uma equação 89
4.2 Polinômios Simétricos 92
4.2.1 Polinômios simétricos elementares 95
4.2.2 Teorema 96
4.2.3 Teorema 98

CAPÍTULO 5 103
5.1 Demonstração da transcendência do número π 103

CONSIDERAÇÕES FINAIS 119

REFERÊNCIAS 123

Anexo I 127

Anexo II 139
A Fórmula de Euler 139
Cálculo da soma $\sum_{i=1}^{n}\binom{n}{i}$ 140

Anexo III 141

Anexo IV 145
Desigualdade do valor médio para funções de uma variável complexa 145

LISTA DE FIGURAS

Figura 1 24
Figura 2 25
Figura 3 28
Figura 4 30
Figura 5 31
Figura 6 55
Figura 7 55
Figura 8 56
Figura 9 57
Figura 10 58

LISTA DE TABELAS

Tabela 1 26
Tabela 2 32
Tabela 3 45

APRESENTAÇÃO

A ciência grega fundamenta-se numa curiosidade altamente intelectual contrastando com o espírito prático do pensamento pré-helênico. A menção da primeira tentativa de se quadrar o círculo remonta a Anaxágoras, no século V a.C. Posteriormente ficou estabelecido que o quadrado de área exatamente igual à do círculo deveria ser construído utilizando-se apenas os instrumentos platônicos, a saber, régua e compasso. Essa questão que iria fascinar estudiosos por mais de vinte séculos, retrata uma matemática muito diferente da dos babilônios e egípcios, uma vez que não se trata de uma aplicação prática da ciência dos números mas sim de uma questão teórica envolvendo uma clara distinção entre uma boa aproximação e a exatidão do pensamento (Boyer, 1974, p. 48)

Como veremos, a quadratura do círculo pode ser expressa por meio de um enunciado muito simples, mas que se revelou como um grande desafio para várias gerações de matemáticos. As tentativas de resolvê-lo ou de demonstrar a impossibilidade de sua resolução serviram como motivação à criação de novas teorias e ao desenvolvimento da matemática, notadamente, no que se refere à gênese do número π.

Esse problema teve origem na geometria da Grécia antiga, mas sua resolução necessitou de um tratamento no âmbito da moderna geometria algébrica. Sua resolução, ou seja, a prova de sua impossibilidade, precisou ir muito além da régua, do compasso e das fronteiras da Grécia. Envolveu o trabalho de muitos matemáticos durante um longo período de tempo.

A dificuldade para resolver a questão da quadratura do círculo está na natureza do número π que, além de ser irracional, também é transcendente, porém computável.

O estudo do número π permite fazer uma articulação entre as várias áreas da matemática, como a geometria, a álgebra e a análise, necessitando naturalmente muitas mudanças de quadros, como veremos neste trabalho.

Muitos livros de matemática do ensino fundamental e médio apenas apresentam o número π como a razão entre o comprimento de uma circunferência qualquer pelo seu diâmetro e que é aproximadamente igual a 3,14. Esses livros não apresentam uma maneira de se obter essa estimativa para o número π. Além disso, propõem como uma aplicação o cálculo do comprimento da circunferência e da área do círculo, apresentando as fórmulas $C = 2 \cdot \pi \cdot r$ e $A = \pi \cdot r^2$, também sem nenhuma justificativa.

Com este trabalho objetivamos apresentar aspectos da gênese do número π, inerentes à questão da quadratura do círculo e mostrar a impossibilidade da construção de tal quadrado, fundamentando todas as etapas envolvidas, inclusive a demonstração do resultado definitivo, a saber, a transcendência do número π.

Esperamos que esta pesquisa também venha contribuir para a formação dos professores de matemática, ampliando a visão sobre a natureza dos números e complementando, dessa forma, a teoria apresentada na maioria dos livros didáticos sobre os números, especialmente sobre o número π.

Descrevemos o método de Arquimedes para estimar uma aproximação do número π e justificamos as fórmulas do comprimento da circunferência e da área do círculo. Isso será realizado com o auxílio de uma calculadora científica para o cálculo do seno e da tangente de vários ângulos. Também apresentamos algumas sequências que convergem para o número π, com suas respectivas demonstrações.

A escolha do objeto de pesquisa deste trabalho foi motivada por uma das discussões surgida no grupo de pesquisas, sob a orientação do professor Benedito Antonio da Silva, referente aos três problemas clássicos gregos: a quadratura do círculo, a duplicação do cubo e a trissecção de um ângulo.

Segundo Laville e Dionne (1999, p. 11), “chegar a possíveis explicações ou soluções para um problema pode significar não apenas aquisição de novos conhecimentos, mas, também, favorecer uma determinada intervenção. Um problema é sempre uma falta de conhecimento”.

Esse foi o espírito do desenvolvimento deste trabalho: a busca de explicações e a intervenção nas demonstrações com a finalidade de deixá-las mais detalhadas. Isso sempre pensando na elaboração de um material que possa contribuir para a formação do professor de matemática e para sua prática no exercício do magistério. Para isso foi necessária a aquisição de novos conhecimentos, principalmente sobre os polinômios simétricos.

Durante a elaboração deste trabalho, reconhecemos a importância da pesquisa em nossa área e a necessidade de incorporá-la ao exercício de nossa profissão, tendo em vista o desempenho de um alto nível de qualificação profissional. Além disso, percebemos também a importância da procura por uma informação que não sabemos e que precisamos saber, desenvolvendo dessa maneira certa autonomia em nossa formação.

A maioria dos livros consultados sobre o problema da quadratura do círculo não apresenta a demonstração da transcendência do número π por ser muito técnica. Por outro lado, os que a apresentam, fazem-na de uma forma muito concisa, tornando sua leitura muitas vezes difícil de ser compreendida. Além disso, não justificam outros resultados envolvidos na demonstração.

Como tornar a leitura da demonstração da transcendência do número π mais acessível aos professores e aos alunos dos cursos de licenciatura em matemática? Como apresentar a demonstração da impossibilidade da quadratura do círculo de forma mais detalhada em um único texto, com todos os resultados necessários envolvidos para tal demonstração?

Neste trabalho, procuramos fazer uma explicação da demonstração da transcendência do número π com essa finalidade. Também justificamos todos os passos das demonstrações dos resultados e das afirmações que são utilizados no decorrer dessa demonstração.

As demonstrações desempenharão um papel fundamental no desenvolvimento do trabalho. A preocupação com o entendimento dos raciocínios nelas utilizados foi um ponto ao qual procuramos dar muita importância.

Serão utilizadas várias técnicas de demonstração em matemática: a demonstração por indução, demonstrações diretas e principalmente as demonstrações por redução ao absurdo.

Achamos necessário incluir um capítulo sobre os números transcendentes para ampliarmos as informações sobre a natureza desses números. Veremos que além da classificação dos números reais em racionais e irracionais que sempre é apresentada nos livros didáticos, podemos também fazer uma separação dos números reais em algébricos e transcendentes ou, ainda, em computáveis e não computáveis.

O trabalho é apresentado em cinco capítulos e quatro anexos.

No capítulo 1, descrevemos o problema da quadratura do círculo e a impossibilidade da construção; a forma como Arquimedes tratou a questão e algumas maneiras de se estimar uma aproximação para o número π. Mostramos ainda não só como se obter a fórmula do comprimento da circunferência, mas também como se obter a fórmula para o cálculo da área do círculo.

No capítulo 2, depois da apresentação do conjunto dos números algébricos e suas propriedades, mostramos que esse conjunto é enumerável. Expomos a idéia de traduzir o problema geométrico das construções com régua e compasso para a linguagem algébrica, o que proporcionou um avanço no estudo do problema da quadratura do círculo. Neste capítulo, também mostramos que todo número construtível por régua e compasso é algébrico.

No capítulo 3, apresentamos elementos da teoria dos números transcendentes e como Liouville e Cantor provaram a existência de tais números. Também expomos a prova de Cantor da não-enumerabilidade do conjunto dos números transcendentes, assim como outros exemplos desses números.

No capítulo 4, revisamos as relações métricas entre os coeficientes e as raízes de uma equação polinomial. Esse capítulo é essencialmente dedicado ao estudo dos polinômios simétricos e de suas propriedades.

No capítulo 5, desenvolvemos um estudo elucidativo da demonstração da transcendência do número π.

No anexo I mostramos que dada uma altura *h* fixa, existe um número finito de equações polinomiais com coeficientes inteiros com essa altura.

Nos anexos II e III, demonstramos outros resultados utilizados na demonstração da transcendência do π que não foram contemplados no corpo da dissertação. No anexo IV, expomos uma breve teoria sobre os números complexos, necessária para demonstrar a desigualdade do valor médio para funções de uma variável complexa. Essa desigualdade será utilizada na demonstração da transcendência do número π apresentada neste trabalho.

CAPÍTULO 1

Neste primeiro capítulo, vamos descrever de forma suscinta o problema da quadratura do círculo e sua relação com o número π. Apresentaremos uma justificativa de como se pode obter a fórmula do comprimento da circunferência e da área do círculo. Veremos também algumas maneiras de se estimar o valor do π utilizando processos geométricos e algébricos.

1.1 O problema da quadratura do círculo

Talvez um dos mais famosos problemas da história da matemática seja o da "Quadratura do Círculo", que consiste em construir um quadrado de área igual à área de um círculo de raio *r* dado, utilizando apenas régua sem escala e compasso, sendo que esses instrumentos devem ser usados um número finito de vezes. Portanto, não podem ser empregados limites ou processos de convergência, com um número infinito de operações em tais construções.

Esse problema obcecou matemáticos desde Platão no século III a.C.

Segundo Boyer (1974, p. 64),

> Platão pode ter sido o grande responsável pela restrição, que prevalecia nas construções geométricas gregas, às que podem ser efetuadas só com régua e compasso. A razão desta limitação provavelmente não foi a simplicidade dos instrumentos usados na construção de retas e círculos, mas antes a simetria das construções. Qualquer dos infinitos diâmetros de um círculo é um eixo de simetria da figura; qualquer ponto de uma reta pode ser considerado um centro de simetria, assim como qualquer reta perpendicular a uma reta dada é uma reta em relação à qual a reta dada é simétrica.

No entanto, ao falarmos em construções com régua não graduada e compasso, estamos nos referindo aos três primeiros postulados dos *Elementos* de Euclides:

1. É possível unir dois pontos por uma reta
2. Prolongar uma linha reta até onde seja necessário
3. Traçar uma circunferência em torno de qualquer ponto e com qualquer raio.

Esses postulados são a base destas construções, muitas vezes chamadas de *construções euclidianas.* Para os geômetras gregos, um problema que podia ser resolvido com régua sem escala e compasso era um problema cuja solução consistia em construir os elementos desconhecidos, utilizando apenas a régua sem escala e o compasso, a partir dos elementos geométricos conhecidos. Isso significava fazer construções fundamentadas nos três primeiros postulados de Euclides.

Ainda, segundo Boyer (1974, p. 271),

> Em 1672 o matemático dinamarquês Georg Mohr (1640-1697) publicou um livro em que mostrou que toda construção ponto a ponto que possa ser realizada com régua e compasso (isto é, todo problema "plano") pode ser feita só com compasso. Evidentemente não se pode traçar uma reta com compasso; mas se considerarmos uma reta como conhecida sempre que dois pontos distintos sobre ela são conhecidos, então o uso de régua em geometria euclidiana é supérfluo. Tão pouca atenção prestaram os matemáticos da época a essa notável descoberta que a geometria que usa apenas compasso tem o nome não de Mohr mas de Lorenzo Mascheroni, que redescobriu o princípio 125 anos depois. O livro de Mohr desapareceu tão completamente que só em 1928, quando um exemplar foi acidentalmente descoberto por um matemático numa livraria de Copenhagem é que se soube que alguém havia provado antes de Mascheroni a superfluidade da régua.

O problema da "Quadratura do Círculo" pode ser enunciado em termos atuais, da seguinte maneira:

Construir um quadrado de área igual à área de um círculo de raio r dado, utilizando apenas uma régua sem escala e um compasso. Dado um círculo de raio *r*, sua área é dada por $\pi \cdot r^2$. Vamos considerar um círculo de raio unitário, ou seja, $r = 1$. Então a área deste círculo será igual a $\pi \cdot 1^2 = \pi \cdot 1 = \pi$. Assim, se a área de um quadrado de lado l for igual à de um círculo de raio unitário, devemos ter $l^2 = \pi$, o que nos dá $l = \sqrt{\pi}$.

Para resolver o problema da "Quadratura do Círculo", seria necessário, então, construir um segmento de reta de comprimento igual a $l = \sqrt{\pi}$, utilizando apenas uma régua sem escala e um compasso. Mas se $\sqrt{\pi}$ fosse construtível[1], então π também o seria.

Se fosse possível construir um segmento de reta de comprimento igual a π, o número π seria construtível. Porém, todos os números construtíveis, como veremos, são algébricos[2]. E o matemático alemão Lindemann (1852-1939) demonstrou em 1882 que o número π não é algébrico[3]. Portanto, a possibilidade de se construir um segmento de reta com medida igual a π é falsa, ou seja, tal construção não é possível. Com isso, fica demonstrada a impossibilidade da quadratura do círculo.

Enquanto não se apresentou uma prova dessa impossibilidade, muitos matemáticos tentaram quadrar o círculo utilizando régua e compasso. Como veremos adiante, todas as construções com régua e compasso são equivalentes geométricos de equações algébricas de primeiro e segundo grau e de combinações de tais equações. Como π é um número transcendente, qualquer equação que seja satisfeita por ele não pode ser algébrica (KASNER e NEWMAN, 1968, p. 77).

A solução do problema da quadratura do círculo, que intrigara os matemáticos desde a antiguidade, fez de Lindemann um homem famoso. No entanto, foi a prova do matemático francês Charles Hermite (1822-1901) para a transcendência do número *e*, publicada em 1873, que possibilitou a Lindemann provar a transcendência do π, nove anos mais tarde (MAOR, p. 249).

A transcendência de π estabeleceu finalmente a impossibilidade de se construir , usando régua e compasso, um quadrado com uma área igual à do círculo.

A questão de quadrar o círculo consiste na realidade, no estudo da natureza do π.

A idéia do número π não nasceu pronta, muito menos a constatação de que ele é um número representado por infinitas casas decimais não periódicas. A busca pelo valor do π ocupou os matemáticos desde a Antiguidade. Em papiros egípcios, escritos antes de

---

[1] Um número real α é um número construtível, se for possível "construir com régua e compasso, a partir de um segmento tomado para unidade, um segmento de comprimento igual a α"

[2] Um número real α se diz algébrico se for solução de uma equação polinomial da forma $a_n \cdot x^n + a_{n-1} \cdot x^{n-1} + ... + a_1 \cdot x + a_0 = 0$, em que os coeficientes $a_n, a_{n-1}, ..., a_1, a_0$ são números inteiros.

[3] Um número que não seja algébrico é chamado de transcendente.

1700 a.C, encontra-se que a área de um círculo é igual a área de um quadrado de lado igual a $\frac{8}{9}$ do diâmetro, e o papiro de Ahmes, cerca de 1600 a.C, dá à relação existente entre o comprimento da circunferência e do seu diâmetro, o valor de 3,16.

No Velho Testamento, 2Cr, 4, 2, na descrição da construção do templo de Salomão, aproximadamente em 950 a.C, podemos ver uma aproximação hebraica para o número π que diz o seguinte: "Fez também um mar fundido, que tinha dez côvados duma borda à outra, redondo em toda a volta; tinha cinco côvados de alto e um cordão de trinta côvados abraçava toda a sua circunferência". Neste versículo, podemos observar uma aproximação igual a 3 para o número π, pois $\frac{TRINTA\ côvados}{DEZ\ côvados} = 3$.

Em seguida veremos o método de Arquimedes (287-212 a.C) para estimar uma aproximação para o número π.

1.2 O método de Arquimedes para o cálculo do π

A primeira tentativa científica de calcular π e o comprimento da circunferência parece ter sido a de Arquimedes, 240 a.C. (EVES, 2006, p. 141). Em sua obra *As medidas do círculo*, Arquimedes desenvolveu um método de aproximação para o cálculo da medida do comprimento da circunferência. Esse método envolvia a construção de polígonos regulares inscritos e circunscritos a uma dada circunferência. Conhecidos os perímetros dos polígonos inscritos e circunscritos a ela, ele tentou definir um intervalo no qual estaria contida a medida do comprimento da circunferência.

Começaremos então descrevendo o seu método.

O comprimento de uma circunferência é um número entre o perímetro de qualquer polígono regular inscrito e de qualquer polígono regular circunscrito.

Numa circunferência de raio r inscreve-se um triângulo equilátero. Em seguida, divide-se cada um dos três arcos da circunferência em duas partes iguais, unem-se estes pontos e assim obtém-se um hexágono regular de perímetro igual a $6 \cdot r$. Com sucessivas divisões dos arcos ao meio, constrói-se a partir do hexágono regular um dodecágono

regular. Em seguida, polígonos regulares de 24 lados, de 48 lados e, finalmente, de 96 lados. Aqui Arquimedes fez uma primeira parada (KARLSON, 1961, p. 137).

Considerou que o comprimento da circunferência ainda será maior que o perímetro do polígono de noventa e seis lados, pois, entre cada dois vértices sucessivos, a medida do lado do polígono é menor que a medida do arco de circunferência correspondente a esse lado. Tanto mais verdadeira será essa afirmação para a soma de todos os lados. Passa a calcular, então, o perímetro desse polígono, concluindo que é maior que $3\frac{10}{71}.d$, onde d é o diâmetro da circunferência e, com mais forte razão, o comprimento da circunferência será maior que $3\frac{10}{71}.d$ (KARLSON, 1961, p. 137), ou seja, maior que $3{,}14084507.d$.

Em seguida, Arquimedes circunscreve de maneira semelhante à circunferência, uma sequência de polígonos, prosseguindo, também aqui, até o de 96 lados. Cada um desses polígonos tem perímetro maior que a circunferência. O cálculo numérico conduz ao seguinte resultado: o polígono regular de 96 lados circunscrito à circunferência de diâmetro d é menor que $3\frac{1}{7}.d$, ou seja, menor que $3{,}142857143.d$. Resulta, assim, que o comprimento da circunferência deve estar compreendido entre $3\frac{10}{71}.d$ e $3\frac{1}{7}.d$, isto é, que π é maior que $3\frac{10}{71}$ e menor que $3\frac{1}{7}$, ou seja, $3{,}14084507 < \pi < 3{,}142857143$, obtendo, assim, $\pi \approx 3{,}14$ (KARLSON, 1961, p. 138).

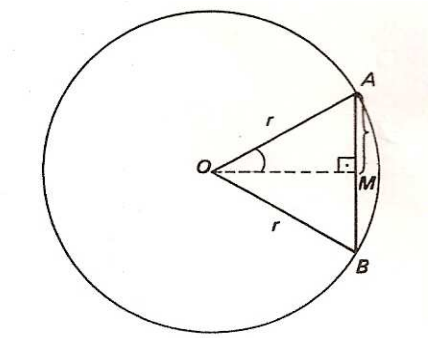
Arquimedes estabelece dois limites, um inferior e um superior, entre os quais deve se encontrar o número π. Ele não afirma mais nada além disso. Utiliza o cálculo numérico, e esse é, possivelmente, seu maior feito, considerando-se as limitações enormes do sistema de numeração de sua época. Uma conclusão inevitável é que Arquimedes era um exímio calculista. O método fundamentado nos polígonos regulares inscritos e circunscritos à circunferência, é conhecido como *método clássico* de cálculo do π (EVES, 2004, p. 142).

Vamos, agora, calcular o comprimento da circunferência, utilizando esse método clássico, com os recursos que dispomos atualmente.

1.3 Comprimento da Circunferência

Consideremos uma circunferência de raio r e um polígono regular de n lados inscrito nessa circunferência. Representaremos o lado desse polígono por l_n e o seu perímetro por p_n. Desse modo temos:

Figura 1



Sendo $AB = l_n$, a medida do ângulo central AÔB é igual a $\frac{360^o}{n}$.

Então $AM = \frac{l_n}{2}$ e $med(A\hat{O}M) = \frac{A\hat{O}B}{2} = \frac{\frac{360^o}{n}}{2} = \frac{180^o}{n}$.

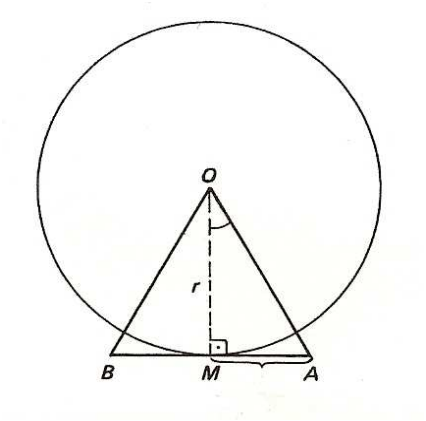
No triângulo retângulo AOM, temos: $sen\left(\frac{180^o}{n}\right) = \frac{\frac{l_n}{2}}{r} = \frac{l_n}{2r}$.

Portanto $l_n = 2r \cdot sen\left(\frac{180^o}{n}\right)$. Como o polígono possui n lados, então o seu perímetro será dado em função de n por $p_n = n \cdot 2r \cdot sen\left(\frac{180^o}{n}\right)$ ou seja $p_n = 2 \cdot n \cdot r \cdot sen\left(\frac{180^o}{n}\right)$.

Notemos que o perímetro do polígono regular inscrito à circunferência é igual ao produto do número $n \cdot sen\left(\frac{180^o}{n}\right)$ pelo diâmetro da circunferência. O número $n \cdot sen\left(\frac{180^o}{n}\right)$ depende exclusivamente do polígono.

Consideremos agora um polígono regular de n lados circunscrito nessa circunferência de raio r. Representaremos o lado desse polígono por L_n e o seu perímetro por P_n. Desse modo, temos:

Figura 2



Sendo $AB = L_n$, a medida do ângulo AÔB é igual a $\frac{360^o}{n}$.

Então $AM = \frac{L_n}{2}$ e $med(A\hat{O}M) = \frac{180^o}{n}$.

No triângulo retângulo AOM, temos: $tg\left(\frac{180^o}{n}\right) = \frac{\frac{L_n}{2}}{r} = \frac{L_n}{2r}$.

Portanto $L_n = 2r \cdot tg\left(\frac{180^o}{n}\right)$.

Logo o seu perímetro será dado em função de *n* por $P_n = 2r \cdot n \cdot tg\left(\frac{180^o}{n}\right)$.

O perímetro do polígono regular circunscrito à circunferência é igual ao produto do número $n \cdot tg\left(\frac{180^o}{n}\right)$ pelo diâmetro da circunferência. O número $n \cdot tg\left(\frac{180^o}{n}\right)$ depende exclusivamente do polígono.

Com o auxílio de uma calculadora científica, podemos obter os valores $n \cdot sen\left(\frac{180^o}{n}\right) = \frac{p_n}{2r}$ e os valores de $n \cdot tg\left(\frac{180^o}{n}\right) = \frac{P_n}{2r}$ para vários polígonos.

Esses valores estão calculados na tabela 1, com aproximação de 8 casas decimais, obtidas por truncamento.

Tabela 1

n	$\frac{p_n}{2r}$	$\frac{P_n}{2r}$	$\frac{P_n}{2r} - \frac{p_n}{2r}$
3	**2,59807621**	**5,19615242**	**2,59807621**
4	2,82842712	4,00000000	1,17157288
5	2,93892626	3,63271264	0,69378638
6	**3,00000000**	**3,46410161**	**0,46410161**
10	3,09016994	3,24919696	0,15902702
12	**3,10582854**	**3,21539030**	**0,10956176**
24	**3,13262861**	**3,15965994**	**0,02703133**
48	**3,13935020**	**3,14608621**	**0,00673601**
96	**3,14103195**	**3,1427146**	**0,00168264**
500	3,14157198	3,14163399	0,00006201
1000	3,14158748	3,14160298	0,00001550

Os valores em negrito correspondem aos polígonos utilizados por Arquimedes para se obter a aproximação $3\frac{10}{71} < \pi < 3\frac{1}{7}$.

Consideremos agora as duas sequências:

1. A sequência dos perímetros dos polígonos regulares inscritos em uma circunferência de raio *r*, dada por $p_n = 2 \cdot r \cdot n \cdot sen\left(\frac{180\,^{\circ}}{n}\right),\ n \geq 3$.

2. A sequência dos perímetros dos polígonos regulares circunscritos em uma circunferência de raio *r*, dada por $P_n = 2 \cdot r \cdot n \cdot tg\left(\frac{180\,^{\circ}}{n}\right),\ n \geq 3$.

A sequência (p_n) é crescente[4], ou seja, quando o número de lados do polígono regular inscrito aumenta, o perímetro desse polígono também aumenta. Essa sequência é limitada inferiormente por p_3 e superiormente pela medida do comprimento da

[4] Diz-se que uma sequência $(a_n) = (a_1, a_2, a_3, \ldots, a_n, \ldots)$ é crescente se $a_1 < a_2 < a_3 < a_4 < \ldots < a_n \ldots$.

circunferência, portanto, (p_n) é uma sequência limitada[5]. Como toda sequência crescente e limitada é convergente[6], podemos concluir que a sequência (p_n) converge.

A sequência (P_n) é decrescente[7], ou seja, quando o número de lados do polígono regular circunscrito aumenta, o perímetro desse polígono diminui. Essa sequência é limitada superiormente por P_3 e inferiormente pela medida do comprimento da circunferência, portanto, (P_n) é uma sequência limitada. Como toda sequência decrescente e limitada é convergente, podemos concluir que a sequência (P_n) é convergente.

Nessa construção, qualquer que seja $n \geq 3$ tem-se $p_n < P_n$.

Além disso, sendo C o perímetro da circunferência de raio r, tem-se também que $p_n < C < P_n$, o que nos dá $\frac{p_n}{2r} < \frac{C}{2r} < \frac{P_n}{2r}$, $\forall n \in N,\ n \geq 3$.

A diferença $\frac{P_n}{2r} - \frac{p_n}{2r}$ pode tornar-se tão próxima de zero quanto quisermos, desde que se escolha um n adequado, suficientemente grande. A sequência $\left(\frac{P_n}{2r} - \frac{p_n}{2r}\right)$, que se aproxima de zero, quando n aumenta, indica que os perímetros dos polígonos circunscritos aproximam-se cada vez mais dos perímetros dos polígonos inscritos. Esse método é também chamado de método das aproximações sucessivas (IMENES, JAKUBOVIC, TROTTA, 1979, p. 105-106).

---

[5] Diz-se que uma sequência (a_n) é limitada quando o conjunto dos seus termos é limitado, isto é, quando existem números reais *c*, *d* tais que $c \leq a_n \leq d$ para todo $n \in$ N.

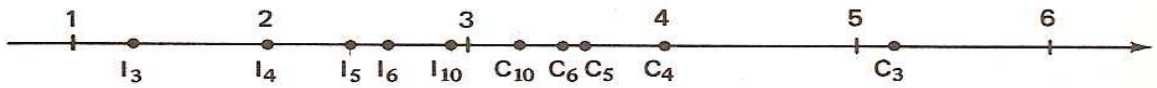
[6] Diz-se que uma sequência (a_n) converge para o número *L*, ou tem limite *L*, se, dado qualquer número $\varepsilon > 0$, sempre é possível encontrar um número *N* tal que $n > N \Rightarrow | a_n - L | < \varepsilon$. Uma sequência que converge é dita convergente.

[7] Diz-se que uma sequência $(a_n) = (a_1, a_2, a_3, \ldots, a_n, \ldots)$ é decrescente se $a_1 > a_2 > a_3 > a_4 > \ldots > a_n \ldots$.

A desigualdade $\frac{p_n}{2r} < \frac{C}{2r} < \frac{P_n}{2r}$ determina uma seqüência $I_n = \left[\frac{p_n}{2r}, \frac{P_n}{2r}\right]$ de intervalos fechados e encaixados[8], que se aproxima do ponto π. A compreensão do número π envolve a própria conceituação de número real como um corte[9] praticado na reta, introduzida por Richard Dedekind, em 1872.

Vamos fazer uma representação gráfica dos 5 primeiros valores destas sequências e observar o que acontece. Consideremos os pontos $I_n = \frac{p_n}{2r}$ e os pontos $C_n = \frac{P_n}{2r}$.

Figura 3



Observando a figura, podemos perceber que:

a) Todos os pontos I_n estão à esquerda de todos os pontos C_n, ou seja, $I_n < C_n$, $\forall n \in N,\ n \geq 3$.

b) À medida que n aumenta, a distância entre I_n e C_n diminui, tendendo a zero.

Podemos descrever essa situação, imaginando dois pontos distintos, deslocando-se sobre uma mesma reta com sentidos opostos, ou seja, um ao encontro do outro. Esses dois

---

[8] Seja $I_n = [a_n, b_n]$, $n = 1,2,...,$ uma família de intervalos fechados e encaixados, isto é, $I_1 \supset I_2 \supset ... \supset I_n \supset ...$. Então existe pelo menos um número *c* pertencendo a todos os intervalos I_n (ou, o que é o mesmo, $c \in I_1 \cap I_2 \cap ... \cap I_n \cap ...)$. Se além das hipóteses feitas, o comprimento $|I_n| = b_n - a_n$ do *n*-ésimo intervalo tender a zero, então, o número *c* será único, isto é, $I_1 \cap I_2 \cap ... \cap I_n \cap ... = \{c\}$.

[9] Seja uma reta e um ponto P sobre ela. Em relação ao ponto P, todos os pontos da reta se repartem em 2 classes: a classe (A) dos pontos que estão à esquerda de P, e a classe (B), dos pontos que estão à direita de P. O próprio ponto P, que produz a repartição, pode ser colocado indiferentemente na classe (A) ou na classe (B). Sempre que em uma reta, se tem uma repartição dos seus pontos em duas classes (A) e (B), satisfazendo às duas condições: *i*) nenhum ponto escapa à repartição; *ii*) todo ponto da classe (A) está à esquerda de todo ponto da classe (B), diz-se que se tem um corte, do qual (A) e (B) são as classes constitutivas. O corte constituído pelas duas classes (A) e (B) representa-se por (A,B). Todo ponto P da reta produz nela um corte. Todo corte da reta é produzido por um ponto dela, isto é, qualquer que seja o corte (A,B) existe sempre um ponto P da reta que separa as duas classes (A) e (B). Número real é o elemento de separação das duas classes de um corte qualquer no conjunto dos números racionais. Se existe um número racional a separar as duas classes, o número real coincidirá com esse número racional; se não existe tal número, o número real dir-se-á irracional (Caraça, 1989, p. 62).

pontos se aproximam de tal modo que a distância entre eles vai ficando cada vez menor, aproximando-se de zero, porém, nunca se encontrando.

Se nada houvesse separando essas classes, certamente as mesmas se encontrariam. Existe então algo que as separa. Porém, se isto que as separa fosse um segmento de reta, a distância entre os dois pontos não poderia se tornar tão pequena quanto desejássemos. Este algo que separa os pontos I_n dos pontos C_n não pode ter dimensão positiva. Então deve existir um ponto P que separa os pontos I_n dos pontos C_n, dado por $\lim_{n\to\infty} I_n = \lim_{n\to\infty} C_n = P$.

Essa idéia corresponde ao seguinte fato geométrico: a medida do comprimento da circunferência é o limite dos perímetros dos polígonos regulares inscritos e dos perímetros dos polígonos regulares circunscritos, quando o número de lados desses polígonos tende ao infinito. Ao ponto P, deverá corresponder o número $\frac{C}{2r}$, que é a razão entre o comprimento da circunferência e o seu diâmetro. Esse número $\frac{C}{2r}$ foi, há muito tempo, designado com a letra grega π (lê-se: pi)[10], isto é: $\frac{C}{2r} = \pi$ e portanto $C = 2.\pi.r$ (IMENES, JAKUBOVIC, TROTTA, manual,1979, p. 92).

Da Tabela 1, para $n = 1000$, temos $3{,}14158748 < \pi < 3{,}14160298$.

O método de Arquimedes mostra que é possível se obter aproximações do valor de π tão precisas quanto desejarmos, bastando aumentar continuamente o número de lados dos polígonos.

A primeira aproximação notável de π depois de Arquimedes foi dada por Cláudio Ptolomeu, que viveu em Alexandria no Egito (150 d.C), em sua famosa obra conhecida popularmente por seu título em árabe *Almagesto*, considerado o maior trabalho de astronomia produzido na Grécia antiga. Nela o valor de π é equivalente a 3,1416 (EVES, 2004, p. 142).

---

[10] A letra π é a primeira letra da palavra grega peripheria $(\pi\varepsilon\rho\iota\mu\varepsilon\tau\rho o\zeta)$, cujo significado é circunferência, ou seja, o contorno ou o perímetro de um círculo. Atribui-se a Leonard Euler, no século XVIII, a popularização do uso da letra grega π para representar a razão entre o comprimento de uma circunferência e seu diâmetro.

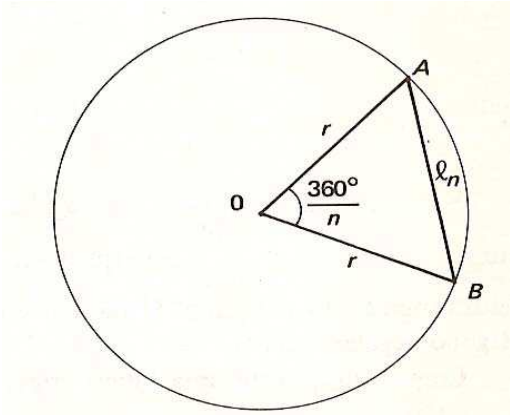
1.4 Área do Círculo

Vamos, agora, calcular a área do círculo, utilizando novamente o método das aproximações sucessivas, e considerar as áreas dos polígonos regulares inscritos e circunscritos em um círculo de raio r.

Para isto vamos, primeiro, calcular a área do polígono regular de n lados inscrito num círculo de raio r. Indicaremos esta área por a_n.

Seja $AB = l_n$ o lado do polígono regular de n lados inscrito num círculo de raio r.

Figura 4

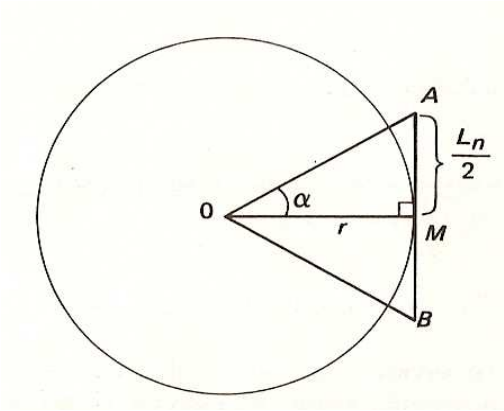


A medida do ângulo central AÔB é igual a $\frac{360^o}{n}$. A área a_n do polígono regular inscrito é igual a n vezes a área do triângulo AOB. A área do triângulo AOB é dada por $\frac{r \cdot r}{2} \cdot sen\left(\frac{360^o}{n}\right)$. Logo $a_n = n \cdot \frac{r \cdot r}{2} \cdot sen\left(\frac{360^o}{n}\right)$ ou $a_n = \left(\frac{n}{2} \cdot sen\left(\frac{360^o}{n}\right)\right) \cdot r^2$.

Podemos notar que a área do polígono regular inscrito ao círculo de raio r é o produto do número $\frac{n}{2} \cdot sen\left(\frac{360^o}{n}\right)$ pelo quadrado do raio. O número $\frac{n}{2} \cdot sen\left(\frac{360^o}{n}\right)$ depende apenas do número de lados do polígono.

Calculemos, agora, a área do polígono regular de n lados circunscrito num círculo de raio r. Indicaremos esta área por A_n. Seja $AB = L_n$.

Figura 5



O ângulo α é a metade do ângulo central AÔB, logo: $\alpha = \dfrac{\dfrac{360^o}{n}}{2} = \dfrac{180\ ^o}{n}$.

No triângulo AOM, temos: $tg\alpha = \dfrac{AM}{r} = \dfrac{\dfrac{L_n}{2}}{r} = \dfrac{L_n}{2r} \quad \therefore \ L_n = 2r \cdot tg\left(\dfrac{180^o}{n}\right)$.

A área A_n do polígono regular circunscrito é igual a n vezes a área do triângulo AOB, portanto: $A_n = n \cdot \dfrac{AB \cdot r}{2} = \dfrac{nr}{2} \cdot 2r \cdot tg\left(\dfrac{180^o}{n}\right) \quad ou \quad A_n = \left(n \cdot tg\left(\dfrac{180^o}{n}\right)\right) \cdot r^2$.

Neste caso, a área do polígono regular circunscrito ao círculo de raio r é o produto do número $n \cdot tg\left(\dfrac{180^o}{n}\right)$ pelo quadrado do raio, e o número $n \cdot tg\left(\dfrac{180^o}{n}\right)$ também depende apenas do número de lados do polígono.

Com o auxílio de uma calculadora científica, podemos obter os valores de $\dfrac{a_n}{r^2} = \dfrac{n}{2} \cdot sen\left(\dfrac{360^o}{n}\right)$ e de $\dfrac{A_n}{r^2} = n \cdot tg\left(\dfrac{360^o}{n}\right)$ para vários polígonos.

Esses valores estão calculados na tabela 2, com aproximação de 8 casas decimais, obtidas por truncamento.

Tabela 2

n	$\frac{a_n}{r^2}$	$\frac{A_n}{r^2}$	$\frac{A_n}{r^2} - \frac{a_n}{r^2}$
3	1,29903810	5,19615242	3,89711432
4	2,00000000	4,00000000	2,00000000
5	2,37764129	3,63271264	1,25507135
6	2,59807621	3,46410161	0,86602540
10	2,93892626	3,24919696	0,31027070
20	3,09016994	3,16768880	0,07751886
60	3,13585389	3,14446675	0,00861286
100	3,13952597	3,14262660	0,00310063
180	3,14095470	3,14191168	0,00095698
360	3,14143315	3,14167240	0,00023925
500	3,14150997	3,14163399	0,00012402

Consideremos agora as duas sequências:

1. A sequência das áreas dos polígonos regulares inscritos em um círculo de raio r, dada por $a_n = \left(\frac{n}{2} \cdot sen\left(\frac{360^o}{n}\right)\right) \cdot r^2$, $n \geq 3$.

2. A sequência das áreas dos polígonos regulares circunscritos em um círculo de raio r, dada por $A_n = \left(n \cdot tg\left(\frac{180^o}{n}\right)\right) \cdot r^2$, $n \geq 3$.

A sequência (a_n) é crescente, ou seja, quando o número de lados do polígono regular inscrito aumenta, a área desse polígono também aumenta. Essa sequência é limitada inferiormente por a_3 e superiormente pela medida da área do círculo, portanto, (a_n) é uma sequência limitada. Podemos concluir que a sequência (a_n) converge.

A sequência (A_n) é decrescente, ou seja, quando o número de lados do polígono regular circunscrito aumenta, a área desse polígono diminui. Essa sequência é limitada superiormente por A_3 e inferiormente pela medida da área do círculo, portanto, (A_n) é uma sequência limitada. Podemos concluir que a sequência (A_n) converge.

Nessa construção, qualquer que seja $n \geq 3$, tem-se $a_n < A_n$.

Além disso, sendo A a área do círculo de raio r, tem-se também que $a_n < A < A_n$, o que nos dá $\frac{a_n}{r^2} < \frac{A}{r^2} < \frac{A_n}{r^2}$, $\forall n \in N,\ n \geq 3$.

A diferença $\frac{A_n}{r^2} - \frac{a_n}{r^2}$ pode tornar-se tão próxima de zero quanto quisermos, desde que se escolha um n adequado, suficientemente grande. A sequência $\left(\frac{A_n}{r^2} - \frac{a_n}{r^2}\right)$, que se aproxima de zero quando n aumenta, mostra que as áreas dos polígonos circunscritos aproximam-se cada vez mais das áreas dos polígonos inscritos (IMENES, JAKUBOVIC, TROTTA, 1979, p. 87-88).

A desigualdade $\frac{a_n}{r^2} < \frac{A}{r^2} < \frac{A_n}{r^2}$ também determina uma sequência de intervalos encaixados, que também se aproxima do ponto π.

Com o mesmo raciocínio feito para o comprimento da circunferência, temos que $\frac{A}{r^2} = \pi$ e, portanto, $A = \pi \cdot r^2$.

Antes de avançarmos, tratemos da seguinte questão:

Como garantir que o número $\frac{C}{2r}$ é igual ao número $\frac{A}{r^2}$, ou seja, como assegurar que os dois processos de aproximações sucessivas empregados no cálculo do comprimento da circunferência e no cálculo da área do círculo convergem para o mesmo número?

Vimos que o número $\frac{C}{2r}$ foi definido como o ponto de separação do corte, cujas classes são $\frac{p_n}{2r} = n \cdot sen\left(\frac{180^o}{n}\right)$ e $\frac{P_n}{2r} = n \cdot tg\left(\frac{180^o}{n}\right)$. Os números $\frac{p_n}{2r}$ são as aproximações por falta do número $\frac{C}{2r}$, enquanto que os números $\frac{P_n}{2r}$ são as aproximações por excesso do número $\frac{C}{2r}$.

Da mesma forma, o número $\frac{A}{r^2}$ foi definido como o ponto de separação do corte cujas classes são $\frac{a_n}{r^2} = \frac{n}{2} \cdot sen\left(\frac{360^o}{n}\right)$ e $\frac{A_n}{r^2} = n \cdot tg\left(\frac{180^o}{n}\right)$. Os números $\frac{a_n}{r^2}$ são as aproximações por falta do número $\frac{A}{r^2}$, enquanto que os números $\frac{A_n}{r^2}$ são as aproximações por excesso do número $\frac{A}{r^2}$.

Como $\frac{P_n}{2r} = n \cdot tg\left(\frac{180^o}{n}\right)$ e $\frac{A_n}{r^2} = n \cdot tg\left(\frac{180^o}{n}\right)$, temos $\frac{P_n}{2r} = \frac{A_n}{r^2}$, ou seja, os números $\frac{C}{2r}$ e $\frac{A}{r^2}$ têm as mesmas aproximações por excesso. Isto é suficiente para concluirmos que $\frac{C}{2r} = \frac{A}{r^2}$, sendo que esse número é único e indicado por π (IMENES, JAKUBOVIC, TROTTA, manual, 1979, p. 44).

O advento do cálculo infinitesimal com Newton e Leibniz, redundou no abandono do método grego, dando lugar aos métodos puramente algébricos das frações contínuas, dos produtos infinitos e das séries (KASNER e NEWMAN, 1968, p. 81).

1.5 A expressão de Viète para o número π

Em 1579, o matemático francês François Viète calculou as nove primeiras casas decimais do número π pelo método clássico, usando polígonos de 393216 lados. Demonstrou que

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

Enquanto Arquimedes utilizou os perímetros dos polígonos regulares com 3, 6, 12, 24, 48 e 96 lados para sua estimativa do π, Viète considerou na sua expressão o cálculo das áreas dos polígonos regulares com 4, 8, 16, 32, ... lados inscritos num círculo de raio $r = 1$. Neste caso, a área do círculo é igual a π.

Geralmente essa expressão aparece nos livros sem uma demonstração. Achamos necessário justificá-la, sem a pretensão de demonstrá-la. Para isso, vamos utilizar a

fórmula que nos dá a área de um polígono regular de *n* lados inscrito em um círculo de raio r. Já vimos que esta fórmula é dada por $a_n = \left(\frac{n}{2}\cdot sen\left(\frac{360^o}{n}\right)\right)\cdot r^2$. Para $r=1$, temos $a_n = \frac{n}{2}\cdot sen\left(\frac{360^o}{n}\right)$.

No cálculo a seguir, iremos, então, considerar uma subsequência[11] da sequência $a_n = \frac{n}{2}\cdot sen\left(\frac{360^o}{n}\right)$, que já sabemos ser convergente para o número π.

Vamos, então, utilizar essa fórmula para $n=4,\ n=8,\ n=16,\ n=32$.

- $n=4$

  $a_4 = \frac{4}{2}\cdot sen\left(\frac{360^o}{4}\right) = 2\cdot sen(90^o) = 2\cdot 1 = 2$. Para $n=4$, temos $a_4 = 2$.

- $n=8$

  $a_8 = \frac{8}{2}\cdot sen\left(\frac{360^o}{8}\right) = 4\cdot sen(45^o) = 4\cdot\frac{\sqrt{2}}{2} = 2\cdot\sqrt{2} = 2\cdot\sqrt{2}\cdot\frac{\sqrt{2}}{\sqrt{2}} = 2\cdot\frac{2}{\sqrt{2}}$

  Para $n=8$, temos $a_8 = 2\cdot\frac{2}{\sqrt{2}}$

- $n=16$

  $a_{16} = \frac{16}{2}\cdot sen\left(\frac{360^o}{16}\right) = 8\cdot sen(22{,}5^o)$

  Para o cálculo de $sen(22{,}5^o)$, utilizaremos a fórmula $senx = \sqrt{\frac{1-\cos(2x)}{2}}$.

Esta fórmula pode ser deduzida da igualdade $\cos(2x) = \cos^2 x - sen^2 x$ e da relação fundamental da trigonometria $sen^2 x + \cos^2 x = 1$.

---

[11] Uma subsequência de uma dada sequência (a_n) é uma restrição desta sequência a um subconjunto infinito N' do conjunto N dos números naturais, ou seja, uma subsequência de (a_n) é uma sequência do tipo $(b_j) = (a_{n_j})$, em que (n_j) é uma sequência crescente de inteiros positivos, isto é, $n_1 < n_2 < \ldots$. Se uma subsequência (a_n) converge para um limite *L*, então, toda subsequência (a_{n_j}) também converge para *L*.

$$sen(22{,}5^{\circ}) = \sqrt{\frac{1-\cos 45^{\circ}}{2}} = \sqrt{\frac{1-\frac{\sqrt{2}}{2}}{2}} = \sqrt{\frac{\frac{2-\sqrt{2}}{2}}{2}} = \sqrt{\frac{2-\sqrt{2}}{4}} = \frac{\sqrt{2-\sqrt{2}}}{2}$$

Então,

$$a_{16} = \frac{16}{2} \cdot sen\left(\frac{360^{\circ}}{16}\right) = 8 \cdot sen(22{,}5^{\circ}) = 8 \cdot \frac{\sqrt{2-\sqrt{2}}}{2} = 4 \cdot \sqrt{2-\sqrt{2}} = 4 \cdot \sqrt{2-\sqrt{2}} \cdot \frac{\sqrt{2+\sqrt{2}}}{\sqrt{2+\sqrt{2}}} =$$

$$= 4 \cdot \frac{\sqrt{2}}{\sqrt{2+\sqrt{2}}} = 4 \cdot \sqrt{2} \cdot \frac{\sqrt{2}}{\sqrt{2}} \cdot \frac{1}{\sqrt{2+\sqrt{2}}} = 2 \cdot \frac{2}{\sqrt{2}} \cdot \frac{2}{\sqrt{2+\sqrt{2}}}$$

Para $n = 16$, temos $a_{16} = 2 \cdot \frac{2}{\sqrt{2}} \cdot \frac{2}{\sqrt{2+\sqrt{2}}}$

- $n = 32$

$$a_{32} = \frac{32}{2} \cdot sen\left(\frac{360^{\circ}}{32}\right) = 16 \cdot sen(11{,}25^{\circ})$$

$$sen(11{,}25^{\circ}) = \sqrt{\frac{1-\cos(22{,}5^{\circ})}{2}}\ .$$

Para o cálculo de $\cos(22{,}5^{\circ})$, utilizamos a fórmula $\cos x = \sqrt{\frac{\cos(2x)+1}{2}}$.

Da mesma maneira, essa fórmula também pode ser deduzida da igualdade $\cos(2x) = \cos^2 x - sen^2 x$ e da relação fundamental da trigonometria $sen^2 x + \cos^2 x = 1$.

$$\cos(22{,}5^{\circ}) = \sqrt{\frac{\cos 45^{\circ}+1}{2}} = \sqrt{\frac{\frac{\sqrt{2}}{2}+1}{2}} = \sqrt{\frac{\frac{\sqrt{2}+2}{2}}{2}} = \frac{\sqrt{\sqrt{2}+2}}{2}$$

Então,

$$sen(11{,}25^{\circ}) = \sqrt{\frac{1-\cos(22{,}5^{\circ})}{2}} = \sqrt{\frac{1-\frac{\sqrt{\sqrt{2}+2}}{2}}{2}} = \frac{\sqrt{2-\sqrt{2+\sqrt{2}}}}{2}$$

Dessa maneira,

$$a_{32} = 16 \cdot \frac{\sqrt{2-\sqrt{2+\sqrt{2}}}}{2} = 8 \cdot \sqrt{2-\sqrt{2+\sqrt{2}}} \cdot \frac{\sqrt{2+\sqrt{2+\sqrt{2}}}}{\sqrt{2+\sqrt{2+\sqrt{2}}}} = 8 \cdot \frac{\sqrt{2-\sqrt{2}}}{\sqrt{2+\sqrt{2+\sqrt{2}}}} =$$

$$= 8 \cdot \sqrt{2-\sqrt{2}} \cdot \frac{\sqrt{2+\sqrt{2}}}{\sqrt{2+\sqrt{2}}} \cdot \frac{1}{\sqrt{2+\sqrt{2+\sqrt{2}}}} = 8 \cdot \frac{\sqrt{2}}{\sqrt{2+\sqrt{2}}} \cdot \frac{1}{\sqrt{2+\sqrt{2+\sqrt{2}}}} =$$

$$= 8 \cdot \sqrt{2} \cdot \frac{\sqrt{2}}{\sqrt{2}} \cdot \frac{1}{\sqrt{2+\sqrt{2}}} \cdot \frac{1}{\sqrt{2+\sqrt{2+\sqrt{2}}}} = 2 \cdot \frac{2}{\sqrt{2}} \cdot \frac{2}{\sqrt{2+\sqrt{2}}} \cdot \frac{2}{\sqrt{2+\sqrt{2+\sqrt{2}}}}$$

Para $n = 32$, temos $a_{32} = 2 \cdot \frac{2}{\sqrt{2}} \cdot \frac{2}{\sqrt{2+\sqrt{2}}} \cdot \frac{2}{\sqrt{2+\sqrt{2+\sqrt{2}}}}$

Neste ponto, já é possível perceber a lei de formação do produto de Viète. Temos, então:

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

1.6 A expressão de John Wallis para o número π

Em 1650, o inglês John Wallis (1616-1703) estabeleceu para π a seguinte igualdade:

$$\frac{\pi}{2} = \frac{2}{1} \cdot \frac{2}{3} \cdot \frac{4}{3} \cdot \frac{4}{5} \cdot \frac{6}{5} \cdot \frac{6}{7} \cdot \frac{8}{7} \cdot \frac{8}{9} \cdot \cdots$$

Uma demonstração bem resumida dessa igualdade é dada em Courant (2000, p. 608-609). Em seguida, vamos desenvolver esta demonstração, explicitando as etapas envolvidas.

Vamos iniciar calculando a integral $\int sen^k x dx$. O método da integração por partes dessa integral irá nos conduzir à demonstração da expressão acima.

Para isso, escrevemos a função $f(x) = sen^k x = sen^{k-1} x \cdot senx$ e a integramos no intervalo delimitado por 0 e $\frac{\pi}{2}$, isto é, vamos calcular $\int_0^{\frac{\pi}{2}} sen^k x dx = \int_0^{\frac{\pi}{2}} sen^{k-1} x \cdot senx dx$, aplicando a fórmula de integração por partes $\int udv = uv - \int vdu$.

Vamos escolher para $u = sen^{k-1} x$ e para $dv = senxdx$. Dessa forma: $du = (k-1) \cdot sen^{k-2} x \cdot \cos x dx$ e $v = -\cos x$. Então,

$$\int_0^{\frac{\pi}{2}} sen^k x dx = \left[sen^{k-1} x \cdot (-\cos x) \right]_0^{\frac{\pi}{2}} - \int_0^{\frac{\pi}{2}} -\cos x \cdot (k-1) \cdot sen^{k-2} x \cdot \cos x dx$$

$$\int_0^{\frac{\pi}{2}} sen^k x dx = sen^{k-1} \frac{\pi}{2} \cdot (-\cos \frac{\pi}{2}) - sen^{k-1} 0 \cdot (-\cos 0) + (k-1) \int_0^{\frac{\pi}{2}} sen^{k-2} x \cdot \cos^2 x dx$$

Como $\cos \frac{\pi}{2} = 0$, $sen0 = 0$ e $\cos^2 x = 1 - sen^2 x$, temos:

$$\int_0^{\frac{\pi}{2}} sen^k x dx = 0 - 0 + (k-1) \int_0^{\frac{\pi}{2}} sen^{k-2} x.(1 - sen^2 x) dx$$

$$\int_0^{\frac{\pi}{2}} sen^k x dx = (k-1) \int_0^{\frac{\pi}{2}} (sen^{k-2} x - sen^k x) dx$$

$$\int_0^{\frac{\pi}{2}} sen^k x dx = (k-1) \int_0^{\frac{\pi}{2}} (sen^{k-2} x) dx - (k-1) \int_0^{\frac{\pi}{2}} sen^k x dx$$

$$\int_0^{\frac{\pi}{2}} sen^k x dx + (k-1) \int_0^{\frac{\pi}{2}} sen^k x dx = (k-1) \int_0^{\frac{\pi}{2}} (sen^{k-2} x) dx$$

$$k \int_0^{\frac{\pi}{2}} sen^k x dx = (k-1) \int_0^{\frac{\pi}{2}} (sen^{k-2} x) dx$$

O que nos dá uma fórmula de recorrência $\int_0^{\frac{\pi}{2}} sen^k x dx = \frac{(k-1)}{k} \int_0^{\frac{\pi}{2}} (sen^{k-2} x) dx$

Considerando para k valores pares e ímpares separadamente, vamos agora determinar duas expressões para $I_k = \int_0^{\frac{\pi}{2}} sen^k x dx$, ou seja, I_{2n} e I_{2n+1}, $n \in N$, $n \geq 1$.

Para $k = 2n$, $n \in N$, $n \geq 1$, $I_{2n} = \int_0^{\frac{\pi}{2}} sen^{2n} x dx$.

Utilizando a fórmula de recorrência $\int_0^{\frac{\pi}{2}} sen^k x dx = \frac{(k-1)}{k} \int_0^{\frac{\pi}{2}} (sen^{k-2} x) dx$, teremos:

$$I_{2n} = \int_0^{\frac{\pi}{2}} sen^{2n} x dx = \frac{2n-1}{2n} \int_0^{\frac{\pi}{2}} sen^{2n-2} x dx .$$

Mas, $\int_0^{\frac{\pi}{2}} sen^{2n-2} x dx = \frac{2n-2-1}{2n-2} \int_0^{\frac{\pi}{2}} sen^{2n-2-2} x dx = \frac{2n-3}{2n-2} \int_0^{\frac{\pi}{2}} sen^{2n-4} x dx .$

Então, $I_{2n} = \frac{2n-1}{2n} \cdot \frac{2n-3}{2n-2} \int_0^{\frac{\pi}{2}} sen^{2n-4} x dx .$

Utilizando novamente a fórmula de recorrência, temos que

$$\int_0^{\frac{\pi}{2}} sen^{2n-4} x dx = \frac{2n-4-1}{2n-4} \int_0^{\frac{\pi}{2}} sen^{2n-4-2} x dx = \frac{2n-5}{2n-4} \int_0^{\frac{\pi}{2}} sen^{2n-6} x dx .$$

Então, $I_{2n} = \frac{2n-1}{2n} \cdot \frac{2n-3}{2n-2} \cdot \frac{2n-5}{2n-4} \int_0^{\frac{\pi}{2}} sen^{2n-6} x dx .$

Utilizando a fórmula de recorrência sucessivas vezes, teremos:

$$I_{2n} = \frac{2n-1}{2n} \cdot \frac{2n-3}{2n-2} \cdot \frac{2n-5}{2n-4} \cdot \cdots \cdot \int_0^{\frac{\pi}{2}} sen^4 x dx =$$

$$= \frac{2n-1}{2n} \cdot \frac{2n-3}{2n-2} \cdot \frac{2n-5}{2n-4} \cdot \cdots \cdot \frac{3}{4} \int_0^{\frac{\pi}{2}} sen^2 x dx =$$

$$= \frac{2n-1}{2n} \cdot \frac{2n-3}{2n-2} \cdot \frac{2n-5}{2n-4} \cdot \cdots \cdot \frac{3}{4} \cdot \frac{1}{2} \int_0^{\frac{\pi}{2}} sen^0 x dx = \frac{2n-1}{2n} \cdot \frac{2n-3}{2n-2} \cdot \frac{2n-5}{2n-4} \cdot \cdots \cdot \frac{3}{4} \cdot \frac{1}{2} \cdot \frac{\pi}{2}$$

Portanto, $I_{2n} = \frac{2n-1}{2n} \cdot \frac{2n-3}{2n-2} \cdot \frac{2n-5}{2n-4} \cdot \cdots \cdot \frac{9}{10} \cdot \frac{7}{8} \cdot \frac{5}{6} \cdot \frac{3}{4} \cdot \frac{1}{2} \cdot \frac{\pi}{2}$

Para $k = 2.n+1,\ n \in N, n \geq 1,\ I_{2n+1} = \int_0^{\frac{\pi}{2}} sen^{2n+1} x dx$.

Analogamente, pela fórmula de recorrência $\int_0^{\frac{\pi}{2}} sen^k x dx = \frac{(k-1)}{k} \int_0^{\frac{\pi}{2}} (sen^{k-2} x) dx$, teremos:

$$I_{2n+1} = \int_0^{\frac{\pi}{2}} sen^{2n+1} x dx = \frac{2n+1-1}{2n+1} \int_0^{\frac{\pi}{2}} sen^{2n+1-2} x dx = \frac{2n}{2n+1} \int_0^{\frac{\pi}{2}} sen^{2n-1} x dx$$

Mas, $\int_0^{\frac{\pi}{2}} sen^{2n-1} x dx = \frac{2n-1-1}{2n-1} \int_0^{\frac{\pi}{2}} sen^{2n-1-2} x dx = \frac{2n-2}{2n-1} \int_0^{\frac{\pi}{2}} sen^{2n-3} x dx$

Então, $I_{2n+1} = \frac{2n}{2n+1} \cdot \frac{2n-2}{2n-1} \int_0^{\frac{\pi}{2}} sen^{2n-3} x dx$.

Utilizando novamente a fórmula de recorrência temos que:

$$\int_0^{\frac{\pi}{2}} sen^{2n-3} x dx = \frac{2n-3-1}{2n-3} \int_0^{\frac{\pi}{2}} sen^{2n-3-2} x dx = \frac{2n-4}{2n-3} \int_0^{\frac{\pi}{2}} sen^{2n-5} x dx$$

Então, $I_{2n+1} = \frac{2n}{2n+1} \cdot \frac{2n-2}{2n-1} \cdot \frac{2n-4}{2n-3} \int_0^{\frac{\pi}{2}} sen^{2n-5} x dx$

Utilizando a fórmula de recorrência sucessivas vezes, teremos:

$$I_{2n+1} = \frac{2n}{2n+1} \cdot \frac{2n-2}{2n-1} \cdot \frac{2n-4}{2n-3} \cdot \cdots \cdot \int_0^{\frac{\pi}{2}} sen^5 x dx =$$
$$= \frac{2n}{2n+1} \cdot \frac{2n-2}{2n-1} \cdot \frac{2n-4}{2n-3} \cdot \cdots \cdot \frac{4}{5} \cdot \int_0^{\frac{\pi}{2}} sen^3 x dx =$$
$$= \frac{2n}{2n+1} \cdot \frac{2n-2}{2n-1} \cdot \frac{2n-4}{2n-3} \cdot \cdots \cdot \frac{4}{5} \cdot \frac{2}{3} \int_0^{\frac{\pi}{2}} senx dx = \frac{2n}{2n+1} \cdot \frac{2n-2}{2n-1} \cdot \frac{2n-4}{2n-3} \cdot \cdots \cdot \frac{4}{5} \cdot \frac{2}{3} \cdot 1$$

Portanto, $I_{2n+1} = \frac{2n}{2n+1} \cdot \frac{2n-2}{2n-1} \cdot \frac{2n-4}{2n-3} \cdot \cdots \cdot \frac{10}{11} \cdot \frac{8}{9} \cdot \frac{6}{7} \cdot \frac{4}{5} \cdot \frac{2}{3} \cdot 1$

Para $0 < x < \frac{\pi}{2}$, temos $0 < senx < 1$. Então, $sen^{2n-1} x > sen^{2n} x > sen^{2n+1} x$, de modo que $I_{2n-1} > I_{2n} > I_{2n+1}$.

Dividindo a desigualdade $I_{2n-1} > I_{2n} > I_{2n+1}$ por I_{2n+1}, temos: $\frac{I_{2n-1}}{I_{2n+1}} > \frac{I_{2n}}{I_{2n+1}} > 1$.

Como $I_{2n-1} = \frac{2n-2}{2n-1} \cdot \frac{2n-4}{2n-3} \cdot \frac{2n-6}{2n-5} \cdot \cdots \cdot \frac{10}{11} \cdot \frac{8}{9} \cdot \frac{6}{7} \cdot \frac{4}{5} \cdot \frac{2}{3} \cdot 1$, então:

$$\frac{I_{2n-1}}{I_{2n+1}} = \frac{\frac{2n-2}{2n-1} \cdot \frac{2n-4}{2n-3} \cdot \cdots \cdot \frac{10}{11} \cdot \frac{8}{9} \cdot \frac{6}{7} \cdot \frac{4}{5} \cdot \frac{2}{3} \cdot 1}{\frac{2n}{2n+1} \cdot \frac{2n-2}{2n-1} \cdot \frac{2n-4}{2n-3} \cdot \cdots \cdot \frac{10}{11} \cdot \frac{8}{9} \cdot \frac{6}{7} \cdot \frac{4}{5} \cdot \frac{2}{3} \cdot 1} = \frac{1}{\frac{2n}{2n+1}} = \frac{2n+1}{2n}$$

Calculando $\frac{I_{2n}}{I_{2n+1}}$, temos:

$$\frac{I_{2n}}{I_{2n+1}} = \frac{\frac{2n-1}{2n}\cdot\frac{2n-3}{2n-2}\cdot\frac{2n-5}{2n-4}\cdot\ldots\cdot\frac{9}{10}\cdot\frac{7}{8}\cdot\frac{5}{6}\cdot\frac{3}{4}\cdot\frac{1}{2}\cdot\frac{\pi}{2}}{\frac{2n}{2n+1}\cdot\frac{2n-2}{2n-1}\cdot\frac{2n-4}{2n-3}\cdot\ldots\cdot\frac{10}{11}\cdot\frac{8}{9}\cdot\frac{6}{7}\cdot\frac{4}{5}\cdot\frac{2}{3}\cdot 1} =$$

$$= \frac{2n-1}{2n}\cdot\frac{2n-3}{2n-2}\cdot\frac{2n-5}{2n-4}\cdot\ldots\cdot\frac{9}{10}\cdot\frac{7}{8}\cdot\frac{5}{6}\cdot\frac{3}{4}\cdot\frac{1}{2}\cdot\frac{\pi}{2}\cdot\frac{2n+1}{2n}\cdot\frac{2n-1}{2n-2}\cdot\frac{2n-3}{2n-4}\cdot\ldots\cdot\frac{11}{10}\cdot\frac{9}{8}\cdot\frac{7}{6}\cdot\frac{5}{4}\cdot\frac{3}{2}\cdot 1 =$$

$$= \frac{(2n+1)\cdot(2n-1)\cdot(2n-1)\cdot(2n-3)\cdot(2n-3)\cdot\cdots\cdot 9\cdot 9\cdot 7\cdot 7\cdot 5\cdot 5\cdot 3\cdot 3\cdot 1}{2n\cdot 2n\cdot(2n-2)\cdot(2n-2)\cdot\cdots\cdot 10\cdot 10\cdot 8\cdot 8\cdot 6\cdot 6\cdot 4\cdot 4\cdot 2\cdot 2}\cdot\frac{\pi}{2}$$

Então,

$$\frac{2n+1}{2n} > \frac{(2n+1)\cdot(2n-1)\cdot(2n-1)\cdot(2n-3)\cdot(2n-3)\cdot\cdots\cdot 9\cdot 9\cdot 7\cdot 7\cdot 5\cdot 5\cdot 3\cdot 3\cdot 1}{2n\cdot 2n\cdot(2n-2)\cdot(2n-2)\cdot\cdots\cdot 10\cdot 10\cdot 8\cdot 8\cdot 6\cdot 6\cdot 4\cdot 4\cdot 2\cdot 2}\cdot\frac{\pi}{2} > 1.$$

Mas, $\lim_{n\to\infty}\frac{2n+1}{2n} = 1$.

Verificamos, então, que à medida que *n* aumenta, o termo

$$\frac{(2n+1)\cdot(2n-1)\cdot(2n-1)\cdot(2n-3)\cdot(2n-3)\cdot\cdots\cdot 9\cdot 9\cdot 7\cdot 7\cdot 5\cdot 5\cdot 3\cdot 3\cdot 1}{2n\cdot 2n\cdot(2n-2)\cdot(2n-2)\cdot\cdots\cdot 10\cdot 10\cdot 8\cdot 8\cdot 6\cdot 6\cdot 4\cdot 4\cdot 2\cdot 2}\cdot\frac{\pi}{2}$$

tende para 1, ou seja, a expressão

$$\frac{(2n+1)\cdot(2n-1)\cdot(2n-1)\cdot(2n-3)\cdot(2n-3)\cdot\cdots\cdot 9\cdot 9\cdot 7\cdot 7\cdot 5\cdot 5\cdot 3\cdot 3\cdot 1}{2n\cdot 2n\cdot(2n-2)\cdot(2n-2)\cdot\cdots\cdot 10\cdot 10\cdot 8\cdot 8\cdot 6\cdot 6\cdot 4\cdot 4\cdot 2\cdot 2}$$

tende para $\frac{2}{\pi}$, o que nos dá que

$$\frac{2\cdot 2\cdot 4\cdot 4\cdot 6\cdot 6\cdot 8\cdot 8\cdot 10\cdot 10\cdot\cdots\cdot(2n-2)\cdot(2n-2)\cdot 2n\cdot 2n}{1\cdot 3\cdot 3\cdot 5\cdot 5\cdot 7\cdot 7\cdot 9\cdot 9\cdot\cdots\cdot(2n-3)\cdot(2n-3)\cdot(2n-1)\cdot(2n-1)\cdot(2n+1)}$$

tende para $\frac{\pi}{2}$.

Observemos que:

$$\frac{2\cdot 2\cdot 4\cdot 4\cdot 6\cdot 6\cdot \cdots \cdot 2n\cdot 2n}{1\cdot 3\cdot 3\cdot 5\cdot 5\cdot 7\cdot 7\cdot \cdots \cdot (2n-1)\cdot (2n-1)\cdot (2n+1)} = \frac{(2\cdot 4\cdot 6\cdot \cdots \cdot 2n)\cdot (2\cdot 4\cdot 6\cdot \cdots \cdot 2n)}{1\cdot 3^2\cdot 5^2\cdot 7^2\cdot \cdots \cdot (2n-1)^2\cdot (2n+1)} =$$

$$= \frac{(2\cdot 1\cdot 2\cdot 2\cdot 2\cdot 3\cdot \cdots \cdot 2\cdot n)\cdot (2\cdot 1\cdot 2\cdot 2\cdot 2\cdot 3\cdot \cdots \cdot 2\cdot n)}{1\cdot 3^2\cdot 5^2\cdot 7^2\cdot \cdots \cdot (2n-1)^2\cdot (2n+1)} = \frac{2^n\cdot (1\cdot 2\cdot 3\cdot \cdots \cdot n)\cdot 2^n\cdot (1\cdot 2\cdot 3\cdot \cdots \cdot n)}{1\cdot 3^2\cdot 5^2\cdot 7^2\cdot \cdots \cdot (2n-1)^2\cdot (2n+1)} =$$

$$= \frac{2^{2n}\cdot n!\cdot n!}{1\cdot 3^2\cdot 5^2\cdot 7^2\cdot \cdots \cdot (2n-1)^2\cdot (2n+1)} = \frac{2^{2n}\cdot (n!)^2\cdot 2^2\cdot 4^2\cdot 6^2\cdot 8^2\cdot \cdots \cdot (2n)^2}{1\cdot 2^2\cdot 3^2\cdot 4^2\cdot 5^2\cdot 6^2\cdot 7^2\cdot 8^2\cdot \cdots \cdot (2n-1)^2\cdot (2n)^2\cdot (2n+1)} =$$

$$= \frac{2^{2n}\cdot (n!)^2\cdot 2^{2n}\cdot (n!)^2}{[1\cdot 2\cdot 3\cdot 4\cdot 5\cdot 6\cdot 7\cdot 8\cdot \cdots \cdot (2n-1)\cdot (2n)]^2\cdot (2n+1)} = \frac{2^{4n}\cdot (n!)^4}{[(2n)!]^2\cdot (2n+1)}$$

Para $n \to \infty$, obtemos a representação de Wallis para $\frac{\pi}{2}$.

$$\frac{\pi}{2} = \frac{2\cdot 2\cdot 4\cdot 4\cdot 6\cdot 6\cdot \cdots \cdot 2n\cdot 2n\cdot \cdots}{1\cdot 3\cdot 3\cdot 5\cdot 5\cdot 7\cdot 7\cdot \cdots \cdot (2n-1)\cdot (2n-1)\cdot (2n+1)\cdot \cdots} = \lim_{n\to\infty} \frac{2^{4n}\cdot (n!)^4}{[(2n)!]^2\cdot (2n+1)}$$

1.7 Outras maneiras de se obter uma estimativa para o π

Lord Brouncker (1620-1684), o primeiro presidente da Royal Society, converteu o resultado de Wallis na fração contínua

$$\pi = \cfrac{4}{1 + \cfrac{1^2}{2 + \cfrac{3^2}{2 + \cfrac{5^2}{2 + \cfrac{7^2}{2 + \ddots}}}}}$$

Em 1671, o matemático escocês James Gregory obteve a série $arctgx = x - \frac{x^3}{3} + \frac{x^5}{5} - \frac{x^7}{7} + \frac{x^9}{9} - \frac{x^{11}}{11} + \ldots$, que para $|x| \leq 1$ é convergente.

Talvez tenha passado desapercebido a Gregory que, para $x = 1$, tem-se $\frac{\pi}{4} = 1 - \frac{1}{3} + \frac{1}{5} - \frac{1}{7} + \frac{1}{9} - \frac{1}{11} + \ldots$. Essa série, que converge, era conhecida de Leibniz desde

1674. Gregory tentava provar que é impossível uma solução euclidiana[12] do problema da quadratura (EVES, 2004, p. 144).

Em 1777, o conde de Buffon concebeu seu famoso *problema da agulha*, pelo qual pode-se aproximar π por métodos probabilísticos. O problema consiste no seguinte: suponhamos que se trace num plano horizontal um grande número de retas paralelas equidistantes entre si. Representando por d a distância entre duas retas vizinhas quaisquer, Buffon mostrou que a probabilidade de que uma agulha de comprimento $l < d$ caia cortando uma das retas, quando lançada ao acaso sobre o plano, é dada por $p = \frac{2 \cdot l}{\pi \cdot d}$.

Fazendo uma série de lançamentos de agulhas e contando quantas caem sobre as retas e quantas caem entre os espaços, ou seja, sem tocar as retas, podemos calcular um valor para p experimentalmente.

Realizando esse experimento um grande número de vezes, obtém-se um valor empírico de p que podemos usar para calcular uma aproximação de π. (EVES, 2004, p. 145).

De fato, essa estratégia, quando aplicada em um grande número de lançamentos, resulta numa aproximação bastante aceitável para o valor de π. Alguns pesquisadores se dedicaram a esses experimentos e obtiveram resultados surpreendentes: Lazzerini obteve uma aproximação de 3,1415929 para π após 3408 lançamentos (MACHADO e outros, 2008, p. 43).

Muitos matemáticos, ao longo da História, trataram o π como racional, ou seja, passível de ser transformado em uma fração. Para os egípcios, o valor de π era equivalente a $\frac{256}{81}$, que, na forma decimal, equivale a 3,16. Na Mesopotâmia, esse valor era $\frac{25}{8}$, ou 3,125. Ptolomeu, que viveu em Alexandria, no Egito, por volta do século III d.C., conseguiu calcular o valor de π como $\frac{377}{120}$, que é aproximadamente igual a 3,1416, uma aproximação muito boa para a época.

[12] Solução euclidiana é aquela obtida por meio de construções fundamentadas nos três primeiros postulados de Euclides utilizando apenas uma régua sem escala e um compasso um número finito de vezes.

Em 1768, Johann Heinrich Lambert (1728-1777), um matemático suíço-alemão, provou a irracionalidade do número π, ou seja, provou que não existem números inteiros a e $b \neq 0$, tais que $\frac{a}{b} = \pi$ (MAOR, 2006, p. 247). Sua representação decimal é, então, infinita e não periódica. Em nosso trabalho não apresentaremos a demonstração da irracionalidade do π, uma vez que a prova de sua irracionalidade não está diretamente relacionada com o problema da quadratura do círculo. Uma prova da irracionalidade do número π pode ser vista em Figueiredo (1985, p. 15) ou em Spivak (v. 2, p. 415).

Segundo Eves (2004, p. 148), no cálculo do π com muitas casas decimais, há outras questões além do desafio envolvido. Antes de 1768, quando se provou que π é irracional, uma das razões era verificar se os dígitos de π começavam a se repetir e, se esse fosse o caso, obtê-lo como um número racional, talvez com um denominador muito grande.

O cálculo do π com o maior número possível de algarismos tem sido um desafio para os matemáticos. A evolução desse cálculo foi surpreendente com a introdução do uso de computadores e algoritmos computacionais, possibilitando determinar um número cada vez maior de casas decimais da representação decimal do número π. Um dos últimos recordes foi obtido pelos pesquisadores japoneses Kanada e Takahashi que, em 2002, conseguiram obter o valor aproximado de π com mais de um trilhão de casas decimais.

Atualmente a busca por novos métodos de cálculo de valores aproximados de π também é outro campo de pesquisas. Quanto mais eficiente for o método, mais rapidamente será possível calcular determinada quantidade de dígitos.

Outra linha de pesquisa consiste em estudar a estatística da distribuição dos dígitos de π, de modo a verificar se eles aparecem aleatoriamente ou se há algum tipo de padrão. Os cálculos já realizados tendem a confirmar a aleatoriedade dos dígitos de π. Examinando os 200 bilhões de dígitos iniciais do π, Kanada e Takahashi obtiveram a seguinte distribuição:

Tabela 3

Algarismo	Freqüência	Porcentagem
0	20.000.030.841	10,00002%
1	19.999.914.711	9,99996%
2	20.000.136.978	10,00007%
3	20.000.069.393	10,00003%
4	19.999.921.691	9,99996%
5	19.999.917.053	9,99996%
6	19.999.881.515	9,99994%
7	19.999.967.594	9,99998%
8	20.000.291.044	10,00015%
9	19.999.869.180	9,99993%
Total	**200.000.000.000**	**100%**

Observando a Tabela 3, é possível notar que a freqüência relativa dos algarismos se aproxima muito de 10%, o que evidencia um equilíbrio entre os algarismos, e indica a aleatoriedade dos dígitos de π (MACHADO e outros, 2008, p. 18).

Além do desafio intelectual relacionado a essas pesquisas, o cálculo do π é usado para testar a eficiência dos novos computadores. Por exigir uma computação intensa e precisa, o cálculo de milhões de casas decimais do π pode servir de parâmetro para verificar a velocidade e a confiabilidade dos novos computadores.

Na prática, não é necessário conhecer o valor de π com tantas casas decimais. Na maioria das aplicações, uma aproximação do valor de π com quatro casas decimais, ou seja, $\pi \approx 3{,}1416$, é suficiente para os cálculos envolvendo projetos de construções, desenhos, cálculo de comprimentos, áreas e volumes.

As tentativas de resolver o problema da quadratura do círculo geraram a produção de muitas teorias em diversas áreas da matemática, várias delas envolvendo o número π.

Com o objetivo de apresentar a impossibilidade de se construir um quadrado cuja área seja igual à de um círculo dado, veremos no próximo capítulo a definição de número algébrico e as demonstrações de importantes resultados sobre esses números, que serão utilizados na demonstração da transcendência do número π.

CAPÍTULO 2

Neste capítulo, apresentamos alguns resultados sobre números algébricos que serão utilizados na demonstração da transcendência do número π. Veremos que o conjunto dos números algébricos é enumerável[13] e estudaremos a idéia de traduzir o problema geométrico das construções com régua e compasso para a linguagem algébrica, o que possibilitou concluir que todo número construtível é algébrico.

2.1 Os números algébricos

Em primeiro lugar, *um número se diz* ***algébrico*** *se for solução de uma equação polinomial da forma* $a_n \cdot x^n + a_{n-1} \cdot x^{n-1} + ... + a_1 \cdot x + a_0 = 0$, *em que os coeficientes* $a_n, a_{n-1}, ..., a_1, a_0$ *são números inteiros.*

Podemos escrever esta definição de outra maneira, ou seja, *um número* α *é algébrico se for possível construir uma equação polinomial com coeficientes inteiros, da qual* α *seja raiz* (FIGUEIREDO, 1985, p. 21).

Assim, qualquer número racional $\alpha = \frac{a}{b}$, ($a, b \in$ Z, e $b \neq 0$) é algébrico, porque α é raiz da equação $ax - b = 0$.

No entanto, nem todos os números algébricos são racionais. Existem infinitos números algébricos que não são racionais.

---

[13] Um conjunto *X* diz-se enumerável quando é finito ou quando existe uma bijeção $f : N \to X$, sendo *N* o conjunto dos números naturais.

Por exemplo $\sqrt[n]{2}$, $n \in N$, $n \geq 2$, é algébrico, pois é solução da equação $x^n - 2 = 0$, e $\sqrt[n]{2}$ não é racional.

Para a prova da irracionalidade de $\sqrt[n]{2}$, vamos supor que $\sqrt[n]{2}$ seja um número racional, isto é $\sqrt[n]{2} = \frac{a}{b}$, onde *a* e *b* são inteiros. Suponhamos, ainda, e isto é essencial para a demonstração, que $\frac{a}{b}$ seja uma fração irredutível, isto é, que *a* e *b* sejam primos entre si. Admitimos, especificamente, o fato de que *a* e *b* não são ambos pares porque, se o fossem, $\frac{a}{b}$ não seria irredutível. Elevando a *n* a equação $\sqrt[n]{2} = \frac{a}{b}$, ou seja, $\left(\sqrt[n]{2}\right)^n = \left(\frac{a}{b}\right)^n$, obtemos $2 = \frac{a^n}{b^n}$. Portanto, $a^n = 2b^n$. O termo $2b^n$ representa um inteiro par, de modo que a^n é um inteiro par e, portanto, *a* é um inteiro par, digamos $a = 2c$, onde *c* também é um inteiro. Substituindo *a* por *2c* na equação $a^n = 2b^n$, obtemos $(2c)^n = 2b^n$, ou seja, $2^n c^n = 2b^n$. Dividindo ambos os lados dessa última igualdade por 2 obtemos $2^{n-1} c^n = b^n$, ou, ainda, $2 \cdot (2^{n-2} c^n) = b^n$. O termo $2 \cdot (2^{n-2} c^n)$ representa um inteiro par, de modo que b^n é um inteiro par e, portanto, *b* é um inteiro par. Mas agora chegamos à conclusão de que *a* e *b* são ambos inteiros pares, enquanto que *a* e *b* foram, inicialmente, supostos primos entre si. Esta contradição nos leva à conclusão de que não é possível escrever $\sqrt[n]{2}$ na forma $\frac{a}{b}$ com *a* e *b* inteiros e, portanto, $\sqrt[n]{2}$ é irracional.

Nessa demonstração, afirmamos que "*se* a^n *é um inteiro par, então a é um inteiro par*". Antes de prosseguirmos, vamos demonstrar esse resultado.

Vamos supor por absurdo que *a* seja ímpar, ou seja, $a = 2k + 1$, $k \in Z$. Então, $a^n = (2k+1)^n$. Desenvolvendo a potência $(2k+1)^n$ pelo Binômio de Newton, temos:

$$a^n = (2k+1)^n = \binom{n}{0} \cdot (2k)^0 \cdot 1^n + \binom{n}{1} \cdot (2k)^1 \cdot 1^{n-1} + \binom{n}{2} \cdot (2k)^2 \cdot 1^{n-2} + \binom{n}{3} \cdot (2k)^3 \cdot 1^{n-3} + \ldots +$$
$$+ \binom{n}{n-1} \cdot (2k)^{n-1} \cdot 1^1 + \binom{n}{n} \cdot (2k)^n \cdot 1^0$$

Ou ainda:

$$a^n = (2k+1)^n = 1 + \binom{n}{1} \cdot 2k + \binom{n}{2} \cdot 2^2 k^2 + \binom{n}{3} \cdot 2^3 k^3 + ... + \binom{n}{n-1} \cdot 2^{n-1} k^{n-1} + 2^n k^n$$

$$a^n = (2k+1)^n = 1 + 2 \cdot \left[\binom{n}{1} \cdot k + \binom{n}{2} \cdot 2k^2 + \binom{n}{3} \cdot 2^2 k^3 + ... + \binom{n}{n-1} \cdot 2^{n-2} k^{n-1} + 2^{n-1} k^n \right]$$

Como $\left[\binom{n}{1} \cdot k + \binom{n}{2} \cdot 2k^2 + \binom{n}{3} \cdot 2^2 k^3 + ... + \binom{n}{n-1} \cdot 2^{n-2} k^{n-1} + 2^{n-1} k^n \right]$ é um inteiro, então, podemos escrever $a^n = 2m+1,\ m \in Z$. O termo $2m+1$ representa um inteiro ímpar, de modo que a^n é um inteiro ímpar. Mas, por hipótese, a^n é um inteiro par. Esta contradição nos leva à conclusão de que *a* é par. De forma análoga, mostramos que "*se* b^n *é um inteiro par, então b é um inteiro par*".

Um número que não seja algébrico é chamado de ***transcendente***.

Uma prova da existência dos números transcendentes foi dada pelo matemático francês Joseph Liouville (1809-1882) em 1844. Sua prova permitiu a construção de vários números transcendentes (MAOR, 2006, p. 247), como veremos no capítulo 3.

Uma outra prova da existência de números transcendentes foi dada pelo matemático Georg Cantor, que não só demonstrou a existência de números transcendentes, mas também provou que o conjunto dos números transcendentes é infinito, sem exibir nem mesmo um único número transcendente.

Então, se um número α é transcendente, esse número não é solução de qualquer equação polinomial com coeficientes inteiros, ou seja, dado α, não é possível construir uma equação polinomial com coeficientes inteiros da qual α seja raiz.

Observando os números reais, reparamos, então, que eles podem ser classificados não apenas como racionais ou irracionais, mas também em duas outras categorias. Uma dos números algébricos e outra dos números transcendentes (NIVEN, 1984, p. 79).

Além dessas categorizações dos números reais em racionais ou irracionais, algébricos ou transcendentes, podemos categorizá-los também em números computáveis ou não computáveis.

Um número real é chamado computável se existe um algoritmo que fornece os dígitos de sua representação em uma base qualquer, ou, ainda, podemos aproximá-lo tão precisamente quanto desejarmos por meio de um algoritmo.

Um exemplo é o número π, que, apesar de ser irracional e transcendente, é um número computável. Como já vimos, os pesquisadores japoneses Kanada e Takahashi conseguiram em 2002, com o uso do computador e algoritmos computacionais, obter o valor aproximado de π com mais de um trilhão de casas decimais.

Prova-se que o conjunto dos números computáveis é enumerável. Isso é provado mostrando que, se existe um algoritmo que aproxima o número, então, esse algoritmo pode ser implementado em uma linguagem de programação, mostrado por Turing[14]. Como existem contáveis codificações em uma linguagem finita, então, existem contáveis números computáveis.

Por outro lado, existem números cujas representações não podem ser geradas por meio de algoritmos. Nesse caso, o número é chamado não computável.

Um exemplo de número não computável é a constante Ω de Chaitin, que também é um número transcendente. Resumidamente, podemos construi-la calculando o seguinte somatório: para cada algoritmo existente (cujo natural associado é *n*), se o algoritmo pára, soma-se 2^{-n}, senão, não se soma nada. Como o somatório não pode ser calculado, uma vez que não podemos saber se um algoritmo pára (Problema de Parada), então, a constante de Chaitin é um número não computável. Esse número é perfeitamente definido e é um objeto matemático sem ambigüidade. Contudo ele não pode ser computado. Não conseguimos exibir um algoritmo para gerar a constante Ω de Chaitin, mas podemos descrever como gerá-la, por isso ela é também chamada de um número definível.

A Lógica Matemática e a Teoria da Computação são duas áreas nas quais podemos fazer um estudo sobre os números computáveis e não computáveis descritos apenas como informação.

Voltemos à categorização dos números reais em algébricos e transcendentes.

---

[14] Alan Mathison Turing (1912-1954), analisa o ato de computar e fornece argumentos mediante os quais todas as computações podem ser efetuadas por suas máquinas, que vieram a ser chamadas “máquinas de Turing”. Essas máquinas são importantes porque propiciam um meio físico de raciocinar sobre a lógica. Todo processo efetivo, isto é, para o qual existe um algoritmo, ou um processo mecânico de computação, pode ser efetuado por meio de uma máquina de Turing.

Como já vimos, todo número racional é algébrico. Segue-se então que "*todo número que não é algébrico não é racional*". Seja α um número não algébrico. Vamos supor que α seja racional. Mas se α é racional, então, α é algébrico, como já foi provado. Esta contradição nos leva à conclusão de que α não é racional. Podemos, então, escrever que "*todo número transcendente é irracional*".

No entanto, nem todo número irracional é transcendente. Um número irracional pode ser algébrico. Um exemplo desse caso é o número $\sqrt{2}$, que é solução da equação $x^2 - 2 = 0$, como já foi dito anteriormente.

Esquematicamente, temos:

$$NÚMEROS\ REAIS \begin{cases} RACIONAIS\ \ (todos\ estes\ são\ números\ algébricos) \\ IRRACIONAIS \begin{cases} ALGÉBRICOS\ \ (por\ ex: \sqrt[3]{7}\ ,\ \sqrt{p}\ \ com\ \ p\ \ primo\ ) \\ TRANSCENDENTES\ \ (por\ ex: \pi,\ e,\ 2^{\sqrt{2}}, \ln 2) \end{cases} \end{cases}$$

$$NÚMEROS\ REAIS \begin{cases} ALGÉBRICOS \begin{cases} RACIONAIS \\ IRRACIONAIS \end{cases} \\ TRANSCENDENTES\ (todos\ estes\ são\ números\ irracionais) \end{cases}$$

$$NÚMEROS\ REAIS \begin{cases} COMPUTÁVEIS \\ NÃO\ COMPUTÁVEIS \end{cases}$$

Em seguida, iremos apresentar as demonstrações de que:

i. O conjunto dos números algébricos é enumerável.

ii. Todo número construtível é algébrico.

iii. A aritmética dos números algébricos

- A soma de dois números algébricos é algébrico.
- O produto de dois números algébricos é algébrico.
- O simétrico de um número algébrico é algébrico.
- O inverso α^{-1} de um número algébrico $\alpha \neq 0$ é algébrico.

2.2 O conjunto dos números algébricos é enumerável

A demonstração desse teorema tem como referência Niven (1984, p. 199).

Já vimos que um número algébrico é aquele que satisfaz uma equação do tipo $a_n \cdot x^n + a_{n-1} \cdot x^{n-1} + ... + a_1 \cdot x + a_0 = 0$, em que os coeficientes $a_n, a_{n-1}, ..., a_1, a_0$ são números inteiros.

Vamos supor $a_n > 0$. Se tivermos $a_n < 0$, podemos multiplicar a equação por (-1), sem que isso altere as raízes.

Utilizaremos sem demonstração o seguinte teorema: "*Qualquer equação da forma* $a_n \cdot x^n + a_{n-1} \cdot x^{n-1} + ... + a_1 \cdot x + a_0 = 0$ *com coeficientes inteiros tem no máximo n raízes distintas*". (NIVEN, 1984, p. 198). Como conseqüência desse resultado, temos de imediato que o número de raízes de qualquer equação do tipo $a_n \cdot x^n + a_{n-1} \cdot x^{n-1} + ... + a_1 \cdot x + a_0 = 0$ com coeficientes inteiros é finito.

Em seguida, temos a definição de *altura* de uma equação polinomial com coeficientes inteiros.

Dada a equação $a_n \cdot x^n + a_{n-1} \cdot x^{n-1} + ... + a_1 \cdot x + a_0 = 0$, sua *altura* é definida como o número inteiro e positivo $h = n + a_n + | a_{n-1} | + ... + | a_2 | + | a_1 | + | a_0 |$.

Vejamos alguns exemplos:

Não existe equação de altura igual a 1.

Com altura igual a 2, existe somente a equação $x = 0$.

Com altura igual a 3, temos quatro equações:

- 3 delas de grau um, ou seja, $2x = 0$, $x + 1 = 0$ e $x - 1 = 0$;
- 1 equação de grau 2, ou seja, $x^2 = 0$.

Com altura igual a 4, há onze equações:

- 5 equações de grau 1, ou seja, $3x = 0$, $2x + 1 = 0$, $2x - 1 = 0$, $x + 2 = 0$ e $x - 2 = 0$.
- 5 equações de grau 2, ou seja; $2x^2 = 0$, $x^2 + 1 = 0$, $x^2 - 1 = 0$, $x^2 + x = 0$ e $x^2 - x = 0$.
- 1 equação de grau 3, ou seja, $x^3 = 0$.

E, sucessivamente, para cada valor inteiro e positivo de *h* fixo temos um número finito de equações *(ver Anexo I)*. Isso é justificado pelo fato do grau *n* e os coeficientes $a_n, a_{n-1}, \ldots, a_1, a_0$ estarem restritos a um conjunto finito de inteiros, tais que $h = n + a_n + |a_{n-1}| + \ldots + |a_2| + |a_1| + |a_0|$. À medida que o valor de *h* aumenta, também aumenta o número de equações com essa altura *h*, assim como a quantidade de raízes de todas essas equações. No entanto, por maior que seja o valor de *h*, temos sempre uma quantidade finita de equações com essa altura *h.*

Pelo teorema anterior, para cada uma dessas equações com altura igual a *h* fixa há um número finito de raízes. Seja C_h o conjunto finito constituído pelas raízes de todas as equações com altura *h* (*h* fixo).

Então, temos que a reunião de todos os C_h, h = 1,2,3,4,..., é um conjunto enumerável, pois a união de um conjunto enumerável de conjuntos finitos é enumerável.

Como nesta união aparecem todos os números algébricos, segue-se que o conjunto dos números algébricos é enumerável.

Como R não é enumerável, segue-se que o conjunto dos números transcendentes não é enumerável, o que será provado no capítulo 3.

2.3 Todo número construtível é algébrico

No último capítulo deste trabalho, apresentamos uma demonstração da transcendência do número π, da qual decorre a impossibilidade da quadratura do círculo com régua e compasso, levando em consideração que todo número construtível é algébrico.

Vamos, então, analisar agora esta última afirmação: *todo número construtível é algébrico*.

Em geometria plana, o termo "construção" significava, para os gregos, utilizar em suas construções geométricas apenas uma régua sem escala numerada e um compasso. Em todas essas construções geométricas, a régua é utilizada como instrumento para traçar uma reta e não para medir ou demarcar distância (COURANT, 2000, p. 141).

Construir com régua e compasso, significa efetuar as seguintes construções:

i) traçar uma reta, conhecendo dois de seus pontos;

ii) traçar uma circunferência, conhecendo o seu centro e um ponto da circunferência, que determina o seu raio;

iii) determinar as intersecções: de retas com retas, de circunferências com circunferências e de retas com circunferências (WAGNER, 1993, p. 92).

O que significa então um número ser construtível?

Se α é um número real, dizemos que "construir o número α" significa "construir com régua e compasso, a partir de um segmento tomado para unidade, um segmento de comprimento igual a α". Em termos numéricos, 1 é dado e procura-se determinar quais números se podem construir a partir de 1, usando-se a régua e o compasso um número finito de vezes. Esses números são chamados de **construtíveis** (KAPLANSKY, 1958, p. 57).

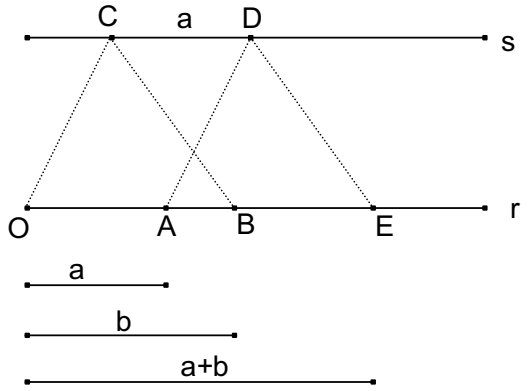
Veremos, em seguida, que dados dois números *a* e *b* construtíveis, então, $a + b$, $-a$, $a.b$, $\frac{1}{a}, \ (a \neq 0)$, e $\sqrt{a}$ também são construtíveis.

Para essas construções, vamos considerar a reta real, a origem e uma unidade.

Construção de $a + b$

1. Sobre uma reta *r*, marcar o ponto *O* correspondente ao número 0. Construir os pontos *A* e *B*, tal que $med(OA) = a$ e $med(OB) = b$.
2. Construir uma reta $s \,//\, r$.
3. Escolher um ponto $C \in s$ e traçar o segmento de reta *OC*. Em seguida, traçar o segmento *CB*.
4. Traçar um segmento de reta passando por *A* e paralelo a *OC*, determinando o ponto $D \in s$.
5. Traçar um segmento de reta passando por *D* e paralelo a *CB*, determinando o ponto $E \in r$.

Figura 6



Dessa forma, temos: *med*(OA) = *med*(CD) = *med*(BE) = *a.*

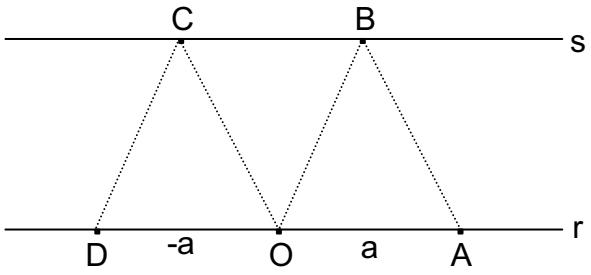
Então, *med*(OE) = *med*(OB) + *med*(BE) = *b*+*a* = *a*+*b*.

O ponto $E \in r$ corresponde ao número ***a*** **+** ***b***.

Construção de –*a*

1. Sobre uma reta *r*, marcar o ponto *O* correspondente ao número 0. Construir o ponto *A*, tal que *med*(*OA*) = *a*.
2. Construir uma reta *s*//*r*
3. Escolher um ponto $B \in s$ e traçar o segmento de reta *AB*. Em seguida, traçar o segmento *BO*.
4. Traçar um segmento de reta passando por *O* e paralelo a *AB*, determinando o ponto $C \in s$.
5. Traçar um segmento de reta passando por *C* e paralelo a *BO*, determinando o ponto $D \in r$.

Figura 7



Dessa forma, temos: *med*(OA) = *med*(CB) = *med*(DO) = *a*.

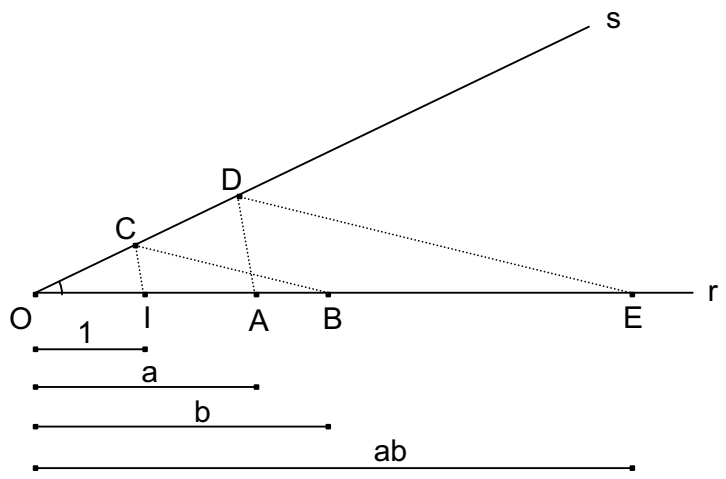
O ponto D corresponde ao número ***–a***.

Construção de a.b

Nessa construção, iremos considerar $a > 1$ e $b > 1$.

1. Sobre uma reta r, marcar o ponto *O* correspondente ao número 0 e o ponto *I* correspondente ao número 1. Construir os pontos $A \in r$ e $B \in r$ tal que *med*(*OA*) = *a* e *med*(*OB*) = *b*.
2. Construir uma reta *s*, passando por *O*, formando com *r* um ângulo agudo.
3. Escolher um ponto $C \in s$ e traçar o segmento *IC*. Em seguida, traçar o segmento *CB*.
4. Traçar um segmento de reta passando por *A* e paralelo ao segmento *IC*, determinando $D \in s$.
5. Traçar o segmento de reta passando por *D* e paralelo ao segmento *CB*, determinando o ponto $E \in r$.

Figura 8



Dessa forma, temos que $\Delta OBC \sim \Delta OED$.

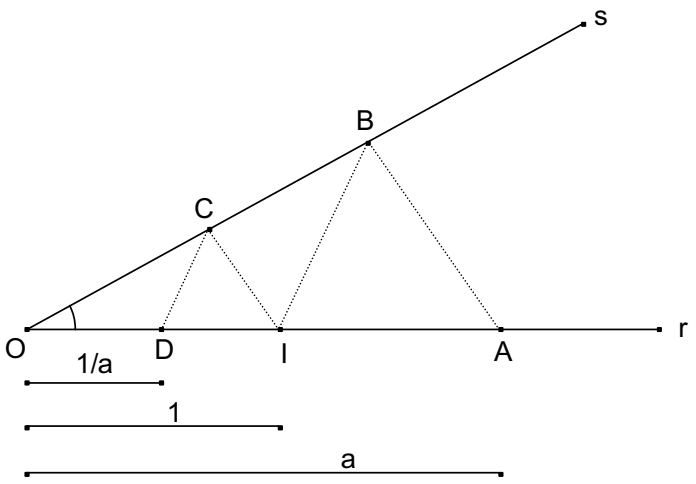
Então, $\frac{OI}{OA} = \frac{OB}{OE}$, ou seja, $\frac{1}{a} = \frac{b}{med(OE)}$, o que nos dá *med*(*OE*) = a.b.

O ponto $E \in$ r, corresponde ao número **a.b** .

Construção de $\frac{1}{a},\ (a>1)$

1. Sobre uma reta *r*, marcar o ponto O correspondente ao número 0 e o ponto I correspondente ao número 1. Construir o ponto $A \in r$ tal que $med(OA) = a$.
2. Construir uma reta *s*, passando por *O*, formando com *r* um ângulo agudo.
3. Escolher um ponto $B \in s$ e traçar o segmento *AB*. Em seguida, traçar o segmento *BI*.
4. Traçar o segmento de reta passando por *I* e paralelo ao segmento *AB*, determinando em *s* o ponto *C*.
5. Traçar o segmento de reta passando por *C* e paralelo ao segmento *BI*, determinado o ponto $D \in r$.

Figura 9



Dessa forma, temos que $\Delta OIC \sim \Delta OAB$.

Então, $\frac{OA}{OI} = \frac{OI}{OD}$, ou seja, $\frac{a}{1} = \frac{1}{med(OD)}$, o que nos dá $med(OD) = \frac{1}{a}$.

O ponto $D \in$ r corresponde ao número $\frac{1}{a}$.

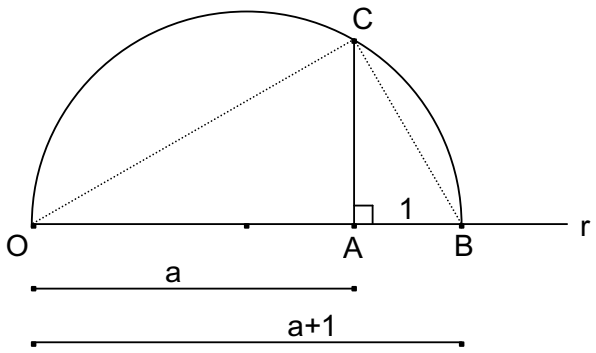
A construção para $0 < a < 1$ é análoga.

As construções de $(a+b)$, $-a$, ab e $1/a$ $(a \neq 0)$ são válidas para quaisquer que sejam os sinais de *a* e *b*.

Construção de $\sqrt{a}$, $a > 0$

1. Sobre uma reta *r*, marcar o ponto *O* correspondente ao número 0. Construir o ponto *A* tal que *med*(*OA*) = *a*. Em seguida, a partir de *A*, construir o ponto *B*, tal que *med*(*OB*) = *a* + 1.
2. Traçar uma semi-circunferência com centro no ponto médio de *OB*, passando por *O*.
3. Traçar por *A* um segmento de reta perpendicular a *OB*, determinando na semi-circunferência o ponto *C*.

Figura 10



Dessa forma, o Δ*OBC* é retângulo em *C*.

Pelas relações métricas no triângulo retângulo, temos: $(med(AC))^2 = med(OA).med(AB)$ o que nos dá $(med(AC))^2 = a.1 \Rightarrow med(AC) = \sqrt{a}$.

Dessas construções, segue-se que o conjunto dos números construtíveis constitui um corpo[15] que chamaremos de K (ou um subcorpo do corpo dos números reais). Isso significa que o conjunto dos números construtíveis é um conjunto de números reais que possui 0 e 1 e é fechado em relação à adição, à multiplicação e ao cálculo de simétricos e de inversos de elementos não nulos. (WAGNER, 1993, p. 96)

Além disso, K satisfaz a condição: se $\alpha \in K$, então, $\sqrt{\alpha} \in K$. A recíproca desta afirmação, também é verdadeira ou seja, se $\sqrt{\alpha} \in K$, então, $\alpha \in K$. Como o produto de dois números construtíveis é construtível, se $\sqrt{\alpha} \in K$, então, $\sqrt{\alpha}.\sqrt{\alpha} \in K$, o que nos dá $\alpha \in K$.

Essa construção de $\sqrt{\alpha}$ será decisiva na demonstração de que todo número construtível é algébrico. Ela será utilizada na construção das extensões do corpo dos racionais.

Dizemos que uma *extensão de um corpo* F é um corpo M, se M contém F, ou seja, $F \subset M$. Por exemplo, R é uma extensão de Q, e R é uma extensão de K.

Do fato de o conjunto dos números construtíveis formarem um corpo, temos como conseqüência imediata que **todo número racional é construtível**, pois qualquer que seja $\frac{a}{b} \in Q$, *a, b* ∈ Z, $b \neq 0$, *a* e *b* são construtíveis a partir de 0 e 1, $\frac{1}{b}$ é construtível a partir de *b,* e $a.\frac{1}{b} = \frac{a}{b}$ é construtível a partir de *a* e $\frac{1}{b}$.

---

[15] Um corpo é um conjunto *X*, munido de duas operações chamadas adição e multiplicação, que satisfazem a certas condições chamadas os axiomas de corpo. A adição faz corresponder a cada par de elementos $x, y \in X$, sua soma $x + y \in X$, enquanto a multiplicação associa a esses elementos o seu produto $x.y \in X$.

Os axiomas de corpo são os seguintes:

A. Axiomas da adição:

A_1. Associatividade: $\forall x, y, z \in X$, tem-se $(x + y) + z = x + (y + z)$

A_2. Comutatividade: $\forall x, y \in X$, tem-se $x + y = y + x$

A_3. Elemento Neutro: $\exists 0 \in X \mid x + 0 = x, \ \forall x \in X$

A_4. Simétrico: $\forall x \in X, \exists (-x) \in X \mid x + (-x) = 0$

B. Axiomas da multiplicação:

M_1. Associatividade: $\forall x, y, z \in X$, tem-se $(x.y).z = x.(y.z)$

M_2. Comutatividade: $\forall x, y \in X$, tem-se $x.y = y.x$

M_3. Elemento Neutro: $\exists 1 \in X \mid 1 \neq 0 \ e \ x.1 = x, \ \forall x \in X$

M_4. Inverso Multiplicativo: $\forall x \in X, x \neq 0, \exists x^{-1} \in X \mid x.x^{-1} = 1$

D_1. Axioma da distributividade:

$\forall x, y, z \in X$, tem-se $x.(y + z) = x.y + x.z$. Pela comutatividade, tem-se também $(x + y).z = x.z + y.z$.

Como todo número racional é algébrico, segue-se que *todos os números construtíveis racionais são algébricos.*

No entanto, *nem todo número construtível é racional*. Um exemplo clássico é o número $\sqrt{2}$ que, embora sendo construtível, não é racional.

Podemos perguntar: além dos números racionais, quais outros números também são construtíveis?

Como já vimos, sendo K o conjunto dos números construtíveis, se $\alpha \in K$, então, $\sqrt{\alpha} \in K$. Temos de imediato que além dos racionais, todos os números da forma $\sqrt{r} \notin Q$, $r \in Q$ são construtíveis.

Consideremos agora $r \in Q$ (r fixo). Se $\sqrt{r} \in Q$, é imediato que os números da forma $a + b.\sqrt{r}$ com $a, b \in$ Q são construtíveis. Analisemos o caso em que $\sqrt{r} \notin Q$. Como o conjunto dos números construtíveis é um corpo, podemos construir todos os números da forma $a + b.\sqrt{r}$, com $a, b \in$ Q.

Podemos também construir os números:

$$(a + b \cdot \sqrt{r}) + (c + d \cdot \sqrt{r}) = (a + c) + (b + d) \cdot \sqrt{r}$$
$$(a + b \cdot \sqrt{r}) \cdot (c + d.\sqrt{r}) = (ac + bdr) + (ad + bc)\sqrt{r}$$
$$-(a + b \cdot \sqrt{r}) = -a + (-b)\sqrt{r}$$
$$\frac{1}{a + b.\sqrt{r}} = \frac{1}{a + b.\sqrt{r}} \cdot \frac{a - b \cdot \sqrt{r}}{a - b \cdot \sqrt{r}} = \frac{a}{a^2 - rb^2} - \frac{b}{a^2 - rb^2} \cdot \sqrt{r}$$

com a, b, c, d racionais, que também são da forma $p + q.\sqrt{r}$, com p, q racionais.

O denominador $a^2 - r \cdot b^2$ não pode ser zero, pois, se $a^2 - r \cdot b^2 = 0$, então, $\sqrt{r} = \frac{a}{b}$, contrariando o fato de $\sqrt{r} \notin Q$.

Logo, o conjunto $\{a + b\sqrt{r},\ a, b \in Q\}$ é um corpo que denotaremos por $Q[\sqrt{r}]$.

Todos os números desse corpo são raízes de equações quadráticas. Seja $x = a + b.\sqrt{r}$. Então, $x - a = b.\sqrt{r}$. Elevando ambos os lados da igualdade ao quadrado, temos: $x^2 - 2ax + a^2 = b^2 \cdot r$, ou seja, $x^2 - 2ax + a^2 - b^2 \cdot r = 0$. Então, todo número

construtível da forma $a+b.\sqrt{r}$ é raiz de uma equação algébrica do 2º grau com coeficientes racionais. Segue-se, então, que esses números são algébricos.

Esse corpo $Q[\sqrt{r}]=\{a+b\sqrt{r},\ a,b\in Q\}$ contém o corpo dos racionais. Basta considerar $b=0$. No entanto, nem todo número real é dessa forma, por exemplo $\sqrt[3]{2}\in R$ e $\sqrt[3]{2}\notin Q[\sqrt{r}]$.

Para facilitar as notações, chamaremos o corpo Q dos racionais de F_0 e corpo $Q[\sqrt{r}]$ de F_1. A construtibilidade de cada número no corpo de extensão[16] F_1 foi estabelecida. Como $F_0\subset F_1$, então, F_1 é uma extensão de F_0.

Podemos agora ampliar nossas construções, considerando um número construtível $\varpi=a+b.\sqrt{r}$ (fixo) de F_1 e extrair sua raiz quadrada, obtendo, assim, o número construtível $\sqrt{a+b.\sqrt{r}}=\sqrt{\omega}$.

Analogamente, podemos construir o corpo de todos os números $u+v.\sqrt{\omega}$, onde $u,v\in F_1$, isto é, são números da forma $a+b.\sqrt{r}$, com $a,b,r\in Q$. Chamemos de F_2 o corpo dos números da forma $u+v.\sqrt{\omega}$. O corpo F_2 contém o corpo F_1, ou seja, $F_1\subset F_2$. Basta fazer $v=0$ em $u+v.\sqrt{\omega}$. Então, F_2 é uma extensão de F_1, que por sua vez é uma extensão de F_0. Temos até agora $F_0\subset F_1\subset F_2$.

Qualquer número de F_2 tem a forma $x=u+v.\sqrt{\omega}$, onde u,v,ω estão no corpo F_1, e, portanto, tem a forma $\omega=a+b\sqrt{r}$, $u=c+d\sqrt{r}$, $v=e+f\sqrt{r}$, onde $a,b,c,d,e,f\in Q$. Mostraremos que os números desse corpo F_2 são raízes de uma equação algébrica de quarto grau.

Como $x=u+v\cdot\sqrt{\omega}$, podemos escrever $x-u=v\cdot\sqrt{\omega}$. Elevando ambos os lados dessa igualdade ao quadrado temos $(x-u)^2=(v.\sqrt{\omega})^2$. Calculando as potências, obtemos $x^2-2ux+u^2=v^2.\omega$, com coeficientes no corpo F_1, gerado por $\sqrt{r}$.

---

[16] Dizemos que um corpo $A\subset R$ é uma extensão de um corpo $B\subset R$ se $A\supset B$. Dado $\alpha\in B$ tal que $\sqrt{\alpha}\notin B$, o conjunto $B[\sqrt{\alpha}]=\{a+b\sqrt{\alpha}\mid a,b\in B\}$ é um exemplo de subcorpo de *R*, ou seja, um subconjunto com as mesmas condições do corpo é também um corpo. Esse é denominado corpo de adjunção de $\sqrt{\alpha}$ a B. Dizemos que $B[\sqrt{\alpha}]$ é uma extensão quadrática de B.

Consideremos agora essa equação $x^2 - 2ux + u^2 = v^2.\omega$, em que $\omega = a + b\sqrt{r}$, $u = c + d\sqrt{r}$, $v = e + f\sqrt{r}$ com $a,b,c,d,e,f \in Q$.

Então,

$$x^2 - 2ux + u^2 = v^2 \cdot \omega \Leftrightarrow x^2 - 2(c + d\sqrt{r})x + (c + d\sqrt{r})^2 = (e + f\sqrt{r})^2 \cdot (a + b\sqrt{r}).$$

Desenvolvendo as operações indicadas, obtemos:

$$x^2 - 2cx - 2d\sqrt{r}x + c^2 + 2cd\sqrt{r} + d^2r = (e^2 + 2ef\sqrt{r} + f^2r)(a + b\sqrt{r}) \Leftrightarrow$$
$$x^2 - 2cx - 2d\sqrt{r}x + c^2 + 2cd\sqrt{r} + d^2r = ae^2 + e^2b\sqrt{r} + 2aef\sqrt{r} + 2efbr + af^2r + f^2rb\sqrt{r} \Leftrightarrow$$
$$x^2 - 2cx + c^2 + d^2r - ae^2 - 2efbr - af^2r = \sqrt{r}(2dx - 2cd + e^2b + 2aef + f^2rb)$$

Fazendo $\begin{cases} -2c = p \\ c^2 + d^2r - ae^2 - 2efbr - af^2r = q \\ 2d = l \\ -2cd + e^2b + 2aef + f^2rb = t \end{cases}$

obtemos $x^2 + px + q = \sqrt{r}.(lx + t)$, onde *p, q, r, l* e *t* são racionais. Elevando novamente ambos os lados dessa equação ao quadrado, obtemos uma equação de quarto grau $(x^2 + px + q)^2 = r.(lx + t)^2$, com coeficientes racionais. Portanto, os números $x = u + v.\sqrt{\omega}$, onde u, v, ω estão no corpo F_1, são raízes de uma equação algébrica de quarto grau.

Segue-se, então, que os números de F_2 também são algébricos.

Repetindo este processo um número finito de vezes a partir do corpo $F_0 = Q$ dos racionais, ou seja, a partir do número 1, chegamos a conclusão de que todo número construtível α pertence a um corpo M da forma F_n tal que existe uma cadeia $Q = F_0 \subset F_1 \subset F_2 \subset ... \subset F_{n-1} \subset F_n = M$ (KAPLANSKY, 1958, p. 59).

Portanto, um número será construtível se e somente se puder ser escrito em termos de número racionais, usando somente adições, multiplicações, simétricos, inversos e raízes quadradas (WAGNER, 1993, p. 98).

Em outras palavras, números construtíveis são aqueles que podem ser alcançados por uma seqüência de corpos de extensão a partir de Q. O número *n* de extensões

necessárias não importa. De certa forma, ele indica o grau de complexidade do problema (COURANT, 2000, p. 160).

Em geral, os números de F_n são raízes de equações algébricas de grau 2^n, com coeficientes racionais.

Começando com um segmento de comprimento unitário, qualquer comprimento que possa ser construído com régua e compasso é um número algébrico de grau 1, ou 2, ou 4, ou 8,..., isto é, um número algébrico de grau igual a uma potência de 2 (NIVEN, 1984, p. 121).

Sempre que um número algébrico for raiz de uma equação de grau **n** com coeficientes inteiros, mas não for raiz de nenhuma equação de grau menor com coeficientes inteiros, dizemos que é um **número algébrico de grau *n***.

Portanto, todo número construtível é algébrico (sobre os racionais) e seu grau é uma potência de 2. Além disso, um número só será construtível se for algébrico de grau igual a uma potência de 2 (WAGNER, 1993, p. 101).

Segundo Courant (2000, p. 144), "a chave para uma compreensão mais profunda consiste em traduzir os problemas geométricos para a linguagem algébrica". Desse modo, o problema de resolver uma construção geométrica equivale a resolver um problema algébrico.

O que irá fornecer os fundamentos de toda essa teoria é o princípio da Geometria Analítica, ou seja, a caracterização quantitativa de objetos geométricos por números reais (COURANT, 2000, p. 145)

Introduzindo coordenadas cartesianas no plano, os pontos passam a ser representados por pares (a, b) de números reais. Um ponto do plano P(a, b) será construtível se e somente se a e b forem construtíveis. Um ponto A do plano cartesiano é construtível a partir de P se é possível determinar A utilizando régua e compasso por meio de um número finito das construções já descritas no início deste item.

Um número real α é construtível se o ponto P(α, 0) é construtível.

Analiticamente, traçar uma reta, determinada por dois pontos construtíveis do plano, significa que podemos considerar retas $y = ax + b$, sendo a e b números construtíveis.

Da mesma forma, traçar uma circunferência, conhecendo o seu centro e um ponto da circunferência, que determina o seu raio, significa que podemos considerar circunferências $(x - a)^2 + (y - b)^2 = r^2$, sendo a, b e r números construtíveis.

Como já vimos, um ponto nas construções com régua e compasso só pode ser determinado por meio de repetição de um número finito das seguintes operações:

[A] determinar a intersecção de duas retas construtíveis

[B] determinar a intersecção de duas circunferências construtíveis

[C] determinar a intersecção de uma reta e uma circunferência construtíveis.

Analiticamente, isso significa que um número construtível α pode ser obtido a partir dos números racionais por meio de uma seqüência finita dos seguintes processos:

[A'] Resolver o sistema $\begin{cases} y = ax + b \\ y = a'x + b' \end{cases}$

[B'] Resolver o sistema $\begin{cases} (x-a)^2 + (y-b)^2 = r^2 \\ (x-a')^2 + (y-b')^2 = r'^2 \end{cases}$

[C'] Resolver o sistema $\begin{cases} y = ax + b \\ (x-a')^2 + (y-b')^2 = r^2 \end{cases}$

Os processos [A'] e [B'], aplicados com coeficientes num corpo L, produzem resultados em L. O processo [C'], em geral, nos faz passar de L a $L[\sqrt{c}] = \{a + b\sqrt{c} \mid a, b \in L\}$, $c \in L$ e $\sqrt{c} \notin L$ (KAPLANSKY, 1958, p. 58-59).

2.4 A aritmética dos números algébricos

As demonstrações a seguir tem como referência Figueiredo (1985, p. 29-34). Novamente, mais uma vez nossa preocupação foi detalhar os raciocínios utilizados nas demonstrações. Com essa intenção, explicamos todas as etapas envolvidas, descrevendo as idéias subentendidas no texto de referência.

2.4.1 A soma de dois números algébricos é algébrico

Se α e β são dois números algébricos, então, a soma $\alpha + \beta$ é um número algébrico.

Para $\alpha = 0$ ou $\beta = 0$ a demonstração é imediata.

Se $\alpha \neq 0$ é um número algébrico, então existe uma equação polinomial $d_n.x^n + d_{n-1}.x^{n-1} + ... + d_1 x + d_0 = 0,\ (d_n \neq 0)$, com coeficientes inteiros tal que

$$d_n \cdot \alpha^n + d_{n-1} \cdot \alpha^{n-1} + ... + d_1 \cdot \alpha + d_0 = 0.$$

Multiplicando essa última igualdade por $\frac{1}{d_n}$, obtemos:

$\alpha^n + \frac{d_{n-1}}{d_n} \cdot \alpha^{n-1} + ... + \frac{d_1}{d_n} \cdot \alpha + \frac{d_0}{d_n} = 0$. Segue-se, então, que α é raiz da equação $x^n + \frac{d_{n-1}}{d_n} \cdot x^{n-1} + ... + \frac{d_1}{d_n} \cdot x + \frac{d_0}{d_n} = 0$ com coeficientes racionais.

Para facilitar a notação, vamos escrever esta equação na seguinte forma:

$$x^n + a_{n-1} \cdot x^{n-1} + ... + a_1 \cdot x + a_0 = 0,\ (a_{n-1}\ ,\ ...\ ,\ a_1, a_0 \in Q).$$

Analogamente, se $\beta \neq 0$ é algébrico, existe uma equação polinomial

$x^m + b_{m-1} \cdot x^{m-1} + ... + b_1 \cdot x + b_0 = 0,\ (b_{m-1}, ...\ ,\ b_1, b_0 \in Q)$, tal que β seja raiz.

Como α é raiz da equação $x^n + a_{n-1} \cdot x^{n-1} + ... + a_1 \cdot x + a_0 = 0$, então, $\alpha^n + a_{n-1} \cdot \alpha^{n-1} + ... + a_1 \cdot \alpha + a_0 = 0$.

Dessa igualdade, podemos escrever α^n como uma combinação linear de

$1, \alpha, ..., \alpha^{n-1}$, ou seja: $\alpha^n = -a_{n-1} \cdot \alpha^{n-1} - ... - a_1 \cdot \alpha - a_0$.

Multiplicando $\alpha^n = -a_{n-1} \cdot \alpha^{n-1} - ... - a_1 \cdot \alpha - a_0$ por α, temos:

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

Substituindo $\alpha^n = -a_{n-1} \cdot \alpha^{n-1} - ... - a_1 \cdot \alpha - a_0$ nesta igualdade, tem-se:

$$\alpha^{n+1} = -a_{n-1} \cdot (-a_{n-1} \cdot \alpha^{n-1} - ... - a_1 \cdot \alpha - a_0) - ... - a_1 \alpha^2 - a_0 \alpha$$

$$\alpha^{n+1} = a_{n-1}^2 \cdot \alpha^{n-1} + ... + a_{n-1} \cdot a_1 \cdot \alpha + a_{n-1} \cdot a_0 - ... - a_1 \cdot \alpha^2 - a_0 \cdot \alpha\ ,$$

o que nos dá:

$$\alpha^{n+1} = a_{n-1}^2 \cdot \alpha^{n-1} + ... + (-a_1) \cdot \alpha^2 + (a_{n-1} \cdot a_1 - a_0) \cdot \alpha + a_{n-1} \cdot a_0$$

Dessa forma, obtemos α^{n+1} também expresso como uma combinação linear de 1, α, ... , α^{n-1} com coeficientes racionais. Esses coeficientes são racionais, pois o conjunto dos números racionais é fechado em relação às operações de adição, subtração, multiplicação e divisão.

Analogamente, multiplicando α^{n+1} por α, obtemos α^{n+2} expresso como combinação linear de 1, α, ... , α^{n-1} com coeficientes racionais, e, assim sucessivamente, podemos obter todas as potências de α^j para $j \geq n$, como combinações lineares de 1, α, ... , α^{n-1}, usando-se coeficientes racionais.

Da mesma forma, podemos exprimir as potências β^k para $k \geq m$, como combinações lineares de 1, β, ... , β^{m-1} usando-se coeficientes racionais.

Para provarmos que $(\alpha + \beta)$ também é um número algébrico, devemos mostrar que $(\alpha + \beta)$ satisfaz uma equação polinomial com coeficientes inteiros.

Para isto, mostraremos que $(\alpha + \beta)$ satisfaz uma equação polinomial de grau *m.n* com coeficientes racionais. Multiplicando-se essa equação por um número que seja um múltiplo comum dos denominadores de todos os seus coeficientes, obteremos uma equação polinomial com coeficientes inteiros, implicando então que $(\alpha + \beta)$ seja algébrico.

Para a construção dessa equação, vamos considerar os $(mn + 1)$ números:

$$(\alpha + \beta)^0, (\alpha + \beta)^1, (\alpha + \beta)^2, (\alpha + \beta)^3, ... , (\alpha + \beta)^{m.n}.$$

Desenvolvendo essas potências, temos:

- $(\alpha + \beta)^0 = 1$
- $(\alpha + \beta)^1 = \alpha + \beta$
- $(\alpha + \beta)^2 = \alpha^2 + 2\alpha\beta + \beta^2$
- $(\alpha + \beta)^3 = \alpha^3 + 3\alpha^2\beta + 3\alpha\beta^2 + \beta^3$

- $(\alpha + \beta)^{m.n} = \alpha^{m.n} + ... + \beta^{m.n}$

Usando o resultado sobre a representação das potências α^j, para $j \geq n$ e β^k, para $k \geq m$, obtemos que os números $(\alpha+\beta)^0, (\alpha+\beta)^1, (\alpha+\beta)^2, (\alpha+\beta)^3, \ldots, (\alpha+\beta)^{m.n}$ podem ser expressos como combinações lineares dos $m.n$ números $\alpha^j\beta^k$, $0 \leq j \leq n-1$, $0 \leq k \leq m-1$, usando-se coeficientes racionais.

Ou seja:

- $(\alpha+\beta)^0 = 1.\ \alpha^0\beta^0 +$ (somatório das outras $m.n$ -1 potências de $\alpha^j\beta^k$, todas com coeficientes iguais a zero).
- $(\alpha+\beta)^1 = 1.\ \alpha^1\beta^0 + 1.\ \alpha^0\beta^1 +$ (somatório das outras $m.n$ -2 potências de $\alpha^j\beta^k$, todas com coeficientes iguais a zero).
- $(\alpha+\beta)^2 = 1.\ \alpha^2\beta^0 + 2.\ \alpha^1\beta^1 + 1.\ \alpha^0\beta^2 +$ (somatório das outras $m.n$ -3 potências de $\alpha^j\beta^k$, todas com coeficientes iguais a zero).

e assim sucessivamente, observando que nos termos em que $\alpha^j\beta^k$ tiverem $j \geq n$ ou $k \geq m$, devemos escrever α^j como combinação linear de $1, \alpha, \ldots, \alpha^{n-1}$ usando-se coeficientes racionais e β^k como combinação linear de $1, \beta, \ldots, \beta^{m-1}$ usando-se coeficientes racionais.

No desenvolvimento das potências $(\alpha+\beta)^i$, $0 \leq i \leq m.n$, existem termos $\alpha^j\beta^k$ com $j \geq n$ ou $k \geq m$, quando ocorrer $i \geq n$ ou $i \geq m$, uma vez que $m.n \geq n$ e $m.n \geq m$.

Podemos escrever:

$$\begin{cases} (\alpha+\beta)^0 = q_{11}\alpha^0\beta^0 + q_{12}\alpha^0\beta^1 + \ldots + q_{1,mn}\alpha^{n-1}\beta^{m-1} \\ (\alpha+\beta)^1 = q_{21}\alpha^0\beta^0 + q_{22}\alpha^0\beta^1 + \ldots + q_{2,mn}\alpha^{n-1}\beta^{m-1} \\ (\alpha+\beta)^2 = q_{31}\alpha^0\beta^0 + q_{32}\alpha^0\beta^1 + \ldots + q_{3,mn}\alpha^{n-1}\beta^{m-1} \\ \text{- -} \\ (\alpha+\beta)^{mn} = q_{mn+1,1}\alpha^0\beta^0 + q_{mn+1,2}\alpha^0\beta^1 + \ldots + q_{mn+1,mn}\alpha^{n-1}\beta^{m-1} \end{cases}$$

Vamos mostrar que essas $(n.m+1)$ potências são linearmente dependentes sobre os racionais, isto é, existem $r_1, r_2, \ldots, r_{mn+1} \in Q$, com alguns (ou todos) diferentes de zero, tais que

$$r_1(\alpha+\beta)^0 + r_2(\alpha+\beta)^1 + r_3(\alpha+\beta)^2 + \ldots + r_{mn+1}(\alpha+\beta)^{mn} = 0$$

Substituindo $(\alpha+\beta)^0, (\alpha+\beta)^1, (\alpha+\beta)^2, (\alpha+\beta)^3, \ldots, (\alpha+\beta)^{m.n}$ pelas expressões acima, temos:

$$
\begin{aligned}
& r_1.(q_{11}\alpha^0\beta^0 + q_{12}\alpha^0\beta^1 + ... + q_{1,mn}\alpha^{n-1}\beta^{m-1}) + \\
& + r_2.(q_{21}\alpha^0\beta^0 + q_{22}\alpha^0\beta^1 + ... + q_{2,mn}\alpha^{n-1}\beta^{m-1}) + \\
& + r_3.(q_{31}\alpha^0\beta^0 + q_{32}\alpha^0\beta^1 + ... + q_{3,mn}\alpha^{n-1}\beta^{m-1}) + ... + \\
& + r_{mn+1}.(q_{mn+1,1}\alpha^0\beta^0 + q_{mn+1,2}\alpha^0\beta^1 + ... + q_{mn+1,mn}\alpha^{n-1}\beta^{m-1}) = 0
\end{aligned}
$$

Efetuando as multiplicações e reagrupando os termos, temos:

$$
\begin{aligned}
& (q_{11}r_1 + q_{21}r_2 + q_{31}r_3 + ... + q_{mn+1,1}r_{mn+1}).\alpha^0\beta^0 + \\
& + (q_{12}r_1 + q_{22}r_2 + q_{32}r_3 + ... + q_{mn+1,2}r_{mn+1}).\alpha^0\beta^1 + ... + \\
& + (q_{1,mn}r_1 + q_{2,mn}r_2 + q_{3,mn}r_3 + ... + q_{mn+1,mn}r_{mn+1}).\alpha^{n-1}\beta^{m-1} = 0
\end{aligned}
$$

Levando em consideração que $\alpha \neq 0$ e $\beta \neq 0$, temos $\alpha^j\beta^k \neq 0$, para $0 \leq j \leq n-1$, $0 \leq k \leq m-1$.

Vemos, então, que $r_1(\alpha+\beta)^0 + r_2(\alpha+\beta)^1 + r_3(\alpha+\beta)^2 + ... + r_{mn+1}(\alpha+\beta)^{mn} = 0$ estará satisfeita se $r_1, r_2, ..., r_{mn+1} \in Q$ forem soluções do sistema de equações lineares

$$
\begin{cases}
q_{11}r_1 + q_{21}r_2 + q_{31}r_3 + ... + q_{mn+1,1}r_{mn+1} = 0 \\
q_{12}r_1 + q_{22}r_2 + q_{32}r_3 + ... + q_{mn+1,2}r_{mn+1} = 0 \\
- \\
q_{1,mn}r_1 + q_{2,mn}r_2 + q_{3,mn}r_3 + ... + q_{mn+1,mn}r_{mn+1} = 0
\end{cases}
$$

Temos, então, um sistema linear homogêneo com *m.n* equações e (*mn*+1) incógnitas. Como um sistema homogêneo de equações lineares com mais incógnitas do que equações tem uma solução não-nula, podemos concluir que existem racionais $r_1, r_2, ..., r_{mn+1} \in Q$ não todos nulos tais que

$$r_1(\alpha+\beta)^0 + r_2(\alpha+\beta)^1 + r_3(\alpha+\beta)^2 + ... + r_{mn+1}(\alpha+\beta)^{mn} = 0,$$

mostrando que $(\alpha+\beta)$ satisfaz uma equação polinomial $r_1x^0 + r_2x^1 + r_3x^2 + ... + r_{mn+1}x^{mn} = 0$, com coeficientes racionais.

Como já foi dito, multiplicando-se essa equação por um número que seja um múltiplo comum dos denominadores de todos os seus coeficientes, obtemos uma equação polinomial com coeficientes inteiros, implicando, então que $(\alpha+\beta)$ seja algébrico.

Portanto, soma de algébricos é algébrica.

2.4.2 O produto de dois números algébricos é algébrico

Se α e β são dois números algébricos, então o produto $\alpha.\beta$ é um número algébrico.

A demonstração desse resultado segue as mesmas linhas da demonstração anterior. Sejam $\alpha \neq 0$ e $\beta \neq 0$ dois números algébricos.

Consideremos, agora, os $mn+1$ números $(\alpha\beta)^0$, $(\alpha\beta)^1$, $(\alpha\beta)^2$,..., $(\alpha\beta)^{mn}$, todos diferentes de zero.

Esses números podem ser expressos como combinações lineares dos *mn* números $\alpha^j\beta^k$, $0 \le j \le n-1$, $0 \le k \le m-1$, usando coeficientes racionais.

Podemos mostrar que essas potências $(\alpha\beta)^0$, $(\alpha\beta)^1$, $(\alpha\beta)^2$,..., $(\alpha\beta)^{mn}$ podem ser expressas como combinações lineares dos *mn* números $\alpha^j\beta^k$, $0 \le j \le n-1$, $0 \le k \le m-1$, usando coeficientes racionais. Além disso, elas são linearmente dependentes sobre os racionais, isto é, existem $r_1, r_2, \ldots, r_{mn+1} \in Q$, não todos nulos, tais que:

$$r_1(\alpha\beta)^0 + r_2(\alpha\beta)^1 + r_3(\alpha\beta)^2 + \ldots + r_{mn+1}(\alpha\beta)^{mn} = 0$$

Segue-se, então, que $\alpha\beta$ satisfaz uma equação polinomial da forma $r_1x^0 + r_2x^1 + r_3x^2 + \ldots + r_{mn+1}x^{mn} = 0$, com coeficientes racionais. Como conseqüência, temos que $\alpha\beta$ é algébrico.

Portanto, o produto de algébricos é algébrico.

2.4.3 O simétrico de um número algébrico é algébrico

Se α é um número algébrico, então, - α é algébrico.

Se α é algébrico, então, α é raiz de uma equação polinomial da forma $a_n \cdot x^n + a_{n-1} \cdot x^{n-1} + \ldots + a_1 \cdot x + a_0 = 0$, onde os coeficientes $a_n, a_{n-1}, \ldots, a_1, a_0$ são números inteiros. Então, $a_n \cdot \alpha^n + a_{n-1} \cdot \alpha^{n-1} + \ldots + a_1 \cdot \alpha + a_0 = 0$.

Para provar que $(-\alpha)$ também é algébrico, é necessário mostrar que $(-\alpha)$ é raiz de uma equação polinomial com coeficientes inteiros.

Vamos, então, à construção dessa equação.

Para isso, utilizaremos os seguintes resultados:

- $a_n \cdot \alpha^n + a_{n-1} \cdot \alpha^{n-1} + ... + a_1 \cdot \alpha + a_0 = 0$
- $\forall \alpha \in \mathrm{R},\ 1.\alpha = \alpha$
- $(-1).\alpha = -\alpha$
- $(-1).(-1) = 1$
- $\forall a, b, c \in \mathrm{R},\ (a.b).c = a.(b.c)$
- $(a.b)^n = a^n.b^n$

Partindo de $a_n \cdot \alpha^n + a_{n-1} \cdot \alpha^{n-1} + ... + a_1 \cdot \alpha + a_0 = 0$, temos:

$$
\begin{aligned}
&a_n.\alpha^n + a_{n-1}.\alpha^{n-1} + ... + a_1\alpha + a_0 = a_n(1.\alpha)^n + a_{n-1}(1.\alpha)^{n-1} + ... + a_1(1.\alpha) + a_0 = \\
&= a_n(((-1).(-1)).\alpha)^n + a_{n-1}(((-1).(-1)).\alpha)^{n-1} + ... + a_1(((-1).(-1)).\alpha) + a_0 = \\
&= a_n((-1).((-1).\alpha)))^n + a_{n-1}((-1).((-1).\alpha)))^{n-1} + ... + a_1((-1).((-1).\alpha))) + a_0 = \\
&= a_n(-1)^n.((-1).\alpha))^n + a_{n-1}(-1)^{n-1}.((-1).\alpha))^{n-1} + ... + a_1(-1).((-1).\alpha)) + a_0 = \\
&= (-1)^n a_n.((-1).\alpha))^n + (-1)^{n-1} a_{n-1}.((-1).\alpha))^{n-1} + ... + (-1)a_1.((-1).\alpha)) + a_0 = \\
&= (-1)^n a_n.(-\alpha)^n + (-1)^{n-1} a_{n-1}.(-\alpha)^{n-1} + ... + (-1)a_1.(-\alpha) + a_0 = 0
\end{aligned}
$$

Portanto, $(-\alpha)$ é raiz da equação

$$(-1)^n a_n \cdot x^n + (-1)^{n-1} a_{n-1} \cdot x^{n-1} + ... + (-1)a_1 \cdot x + a_0 = 0, \quad (a_n, a_{n-1}, ..., a_1, a_0 \in Z).$$

Logo, $(-\alpha)$ é algébrico.

2.4.4 O inverso de um número algébrico $\alpha \neq 0$ é algébrico

Se $\alpha \neq 0$ é um número algébrico, então, α^{-1} é algébrico.

Se $\alpha \neq 0$ é algébrico, então, α é raiz de uma equação polinomial da forma $a_n \cdot x^n + a_{n-1} \cdot x^{n-1} + ... + a_1 \cdot x + a_0 = 0$, onde os coeficientes $a_n, a_{n-1}, ..., a_1, a_0$ são números inteiros. Então, $a_n \cdot \alpha^n + a_{n-1} \cdot \alpha^{n-1} + ... + a_1 \cdot \alpha + a_0 = 0$.

Novamente, para provar que α^{-1} também é algébrico, é necessário mostrar que α^{-1} é raiz de uma equação polinomial com coeficientes inteiros.

Essa equação, da qual α^{-1} é raiz, pode ser construída da seguinte maneira.

Como $\alpha \neq 0$, então, $\alpha^{-n} \neq 0$. Vamos, então, multiplicar os dois lados da igualdade $a_n \cdot \alpha^n + a_{n-1} \cdot \alpha^{n-1} + ... + a_1 \cdot \alpha + a_0 = 0$ por α^{-n}.

Então:

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

Da última igualdade, tem-se que α^{-1} é raiz da equação $a_n + a_{n-1} \cdot x + ... + a_1 \cdot x^{n-1} + a_0 \cdot x^n = 0$ ou $a_0 \cdot x^n + a_1 \cdot x^{n-1} + ... + a_{n-1} \cdot x + a_n = 0$ com coeficientes inteiros.

Com isso, provamos que o conjunto dos números algébricos é um subcorpo do corpo R dos reais.

Em seguida, estudaremos alguns resultados sobre os números transcendentes. Esses resultados não serão utilizados na prova da transcendência do π, porém irão fornecer elementos para entendermos um pouco mais da natureza desses números.

CAPÍTULO 3

Nesta parte do trabalho, trataremos da prova da existência dos números transcendentes de duas maneiras distintas. A primeira delas, realizada em 1844, é a do matemático francês Joseph Liouville (1809-1882), que foi o primeiro a demonstrar a existência de tais números. Sua prova, como veremos mais adiante, permite a construção de exemplos desses números.

A segunda prova é a do matemático Georg Cantor (1845-1918), que provou a existência de números transcendentes sem exibir nenhum deles. Sua prova garante a existência de números reais que não são algébricos, levando em consideração que o conjunto dos números algébricos é enumerável. Veremos também que o conjunto dos números transcendentes é não enumerável. Além dos números de Liouville, apresentamos neste capítulo, outros exemplos de números transcendentes.

3.1 Os números transcendentes: considerações iniciais

Liouville demonstrou que os números algébricos irracionais são aqueles que não podem ser aproximados por números racionais com um grau muito elevado de precisão, a menos que os denominadores das frações sejam bastante grandes (COURANT, 2000, p. 125).

O que significa dizer que um número irracional α pode ser aproximado com qualquer grau desejado de precisão por um número racional?

Isso significa que podemos encontrar uma sequência $\alpha_m = \frac{p_m}{q_m} \in Q,\ p_m, q_m \in Z,\ q_m \neq 0$, ou seja, $(\frac{p_1}{q_1}, \frac{p_2}{q_2}, \cdots)$ de números racionais com denominadores cada vez maiores tais que $\alpha_m = \frac{p_m}{q_m} \to \alpha$.

Uma maneira de se obter valores aproximados de um número irracional, como $\sqrt{2}$, é usar a forma decimal $\sqrt{2} = 1{,}41421356 \ldots$. Os números 1; 1,4; 1,41; 1,414; 1,4142; 1,41421; 1,414213; 1,4142135; 1,41421356; ..., formam uma sequência de aproximações, cada vez mais precisas, de $\sqrt{2}$.

Os números da sequência são todos racionais e temos, desse modo, uma sequência de aproximações racionais de $\sqrt{2}$:

$$\left(\frac{1}{1}, \frac{14}{10}, \frac{141}{100}, \frac{1414}{1000}, \frac{14142}{10000}, \frac{141421}{100000}, \frac{1414213}{1000000}, \frac{14142135}{10000000}, \ldots\right).$$

À medida que avançamos na sequência, esses números se aproximam cada vez mais de $\sqrt{2}$.

Consideremos o número $\pi = 3{,}14159265 \ldots$.

A sequência para π é

$$\left(\frac{3}{1}, \frac{31}{10}, \frac{314}{100}, \frac{3141}{1000}, \frac{31415}{10000}, \frac{314159}{100000}, \frac{3141592}{1000000}, \frac{31415926}{10000000}, \ldots\right).$$

Nos dois exemplos anteriores, utilizamos nas sequências de aproximações racionais denominadores $10, 10^2, 10^3, \ldots$. No entanto, demonstra-se que todo número irracional pode ser aproximado por um número racional de denominador arbitrário (NIVEN, 1984, p. 140).

Já vimos que 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 nenhuma outra equação desse tipo, de grau menor que* n*, da qual* α *seja raiz* (FIGUEIREDO, 1985, p. 36).

Por exemplo, os números racionais coincidem com os números algébricos de grau 1, pois qualquer número racional $\alpha = \frac{p}{q}$ é raiz da equação $q.x - p = 0$, com $p, q \neq 0$

inteiros. Uma consequência desse resultado é que um número algébrico de grau $n>1$ não pode ser racional.

3.2 O Teorema de Liouville

Se α *é um número algébrico de grau* $n>1$ *e se* $\alpha_m = \frac{p_m}{q_m} \in Q,\ \ p_m, q_m \in Z,\ q_m \neq 0$ *e* $\alpha_m \to \alpha$, *então* $\left|\alpha - \frac{p_m}{q_m}\right| > \frac{1}{q_m^{n+1}}$ *para* m *suficientemente grande.*

Em seguida, iremos apresentar a demonstração desse teorema, justificando e explicando as etapas envolvidas, tendo como referência Courant (2000, p. 127).

Seja α um número algébrico de grau $n>1$.

Então, α satisfaz uma equação algébrica com coeficientes inteiros $f(x) = a_n \cdot x^n + a_{n-1} \cdot x^{n-1} + ... + a_2 \cdot x^2 + a_1 \cdot x^1 + a_0 = 0$, com $(a_n \neq 0)$, porém nenhuma outra equação deste tipo de grau inferior a n.

Consideremos uma sequência de números racionais $\beta_m = \frac{a_m}{b_m}$ tal que $\beta_m \to \alpha$.

Para garantir a existência de uma sequência de números racionais escritos na forma $\frac{p}{q} \in Q,\ \ p, q \in Z,\ q \neq 0$, com denominadores cada vez maiores e que convirja para α, basta observar que se $\beta_m = \frac{a_m}{b_m} \in Q$ e $\beta_m \to \alpha$, então, a seqüência $\alpha_m = \left(\frac{a_m}{b_m} + \frac{1}{10^m}\right)$ também converge para α, uma vez que $\lim_{m\to\infty}\left(\frac{a_m}{b_m} + \frac{1}{10^m}\right) = \lim_{m\to\infty}\frac{a_m}{b_m} + \lim_{m\to\infty}\frac{1}{10^m} = \alpha + 0 = \alpha$.

Dessa maneira, os denominadores de α_m são cada vez maiores, pois

$$\alpha_m = \frac{a_m}{b_m} + \frac{1}{10^m} = \frac{a_m}{b_m} \cdot \frac{10^m}{10^m} + \frac{1}{10^m} \cdot \frac{b_m}{b_m} = \frac{a_m . 10^m + b_m}{b_m . 10^m} \in Q,$$

$$(a_m . 10^m + b_m) \in Z \ \ e \ \ b_m . 10^m \in Z - \{0\}.$$

É imediato que $\lim_{m\to\infty} b_m.10^m = \infty$.

Fazendo $\frac{a_m.10^m + b_m}{b_m.10^m} = \frac{p_m}{q_m}$, temos $\alpha_m = \frac{p_m}{q_m} \in Q$, $p_m, q_m \in Z$, $q_m \neq 0$ e $\alpha_m \to \alpha$ de tal forma que, qualquer que seja $M > 0$, existe um valor de $m \in N$ tal que $q_m > M$.

Como $f(\alpha) = 0$, então

$$f(\alpha_m) = f(\alpha_m) - f(\alpha) = (a_n\alpha_m^n + a_{n-1}\alpha_m^{n-1} + ... + a_3\alpha_m^3 + a_2\alpha_m^2 + a_1\alpha_m^1 + a_0) + \\ -(a_n\alpha^n + a_{n-1}\alpha^{n-1} + ... + a_3\alpha^3 + a_2\alpha^2 + a_1\alpha^1 + a_0)$$

Agrupando os termos semelhantes, podemos escrever

$$f(\alpha_m) = a_1.(\alpha_m - \alpha) + a_2.(\alpha_m^2 - \alpha^2) + a_3.(\alpha_m^3 - \alpha^3) + ... + a_{n-1}.(\alpha_m^{n-1} - \alpha^{n-1}) + a_n.(\alpha_m^n - \alpha^n)$$

Dividindo ambos os lados desta equação por $(\alpha_m - \alpha)$, obtemos:

$$\frac{f(\alpha_m)}{\alpha_m - \alpha} = \frac{a_1.(\alpha_m - \alpha)}{\alpha_m - \alpha} + \frac{a_2.(\alpha_m^2 - \alpha^2)}{\alpha_m - \alpha} + ... + \frac{a_{n-1}.(\alpha_m^{n-1} - \alpha^{n-1})}{\alpha_m - \alpha} + \frac{a_n.(\alpha_m^n - \alpha^n)}{\alpha_m - \alpha}$$

Para continuar o desenvolvimento da demonstração, vamos precisar agora da fatoração de $\alpha_m^n - \alpha^n$.

Essa fatoração é dada por:

$$\alpha_m^n - \alpha^n = (\alpha_m - \alpha).(\alpha_m^{n-1} + \alpha_m^{n-2}\cdot\alpha^1 + \alpha_m^{n-3}\cdot\alpha^2 + ... + \alpha_m^2\cdot\alpha^{n-3} + \alpha_m^1\cdot\alpha^{n-2} + \alpha^{n-1}).$$

Portanto,

$$\frac{\alpha_m^n - \alpha^n}{\alpha_m - \alpha} = \alpha_m^{n-1} + \alpha_m^{n-2}\cdot\alpha^1 + \alpha_m^{n-3}\cdot\alpha^2 + ... + \alpha_m^2\cdot\alpha^{n-3} + \alpha_m^1\cdot\alpha^{n-2} + \alpha^{n-1}$$

Utilizando o resultado dessa última igualdade, temos:

$$\frac{(\alpha_m - \alpha)}{\alpha_m - \alpha} = 1$$

$$\frac{(\alpha_m^2 - \alpha^2)}{\alpha_m - \alpha} = \frac{(\alpha_m - \alpha).(\alpha_m + \alpha)}{\alpha_m - \alpha} = (\alpha_m + \alpha)$$

$$\frac{(\alpha_m^3 - \alpha^3)}{\alpha_m - \alpha} = \frac{(\alpha_m - \alpha).(\alpha_m^2 + \alpha_m\alpha + \alpha^2)}{\alpha_m - \alpha} = (\alpha_m^2 + \alpha_m\alpha + \alpha^2)$$

$$---------- \ldots ----------$$

$$\frac{(\alpha_m^{n-1} - \alpha^{n-1})}{\alpha_m - \alpha} = \frac{(\alpha_m - \alpha).(\alpha_m^{n-2} + \alpha_m^{n-3}\alpha + \alpha_m^{n-4}.\alpha^2 + \ldots + \alpha_m\alpha^{n-3} + \alpha^{n-2})}{\alpha_m - \alpha} =$$

$$= (\alpha_m^{n-2} + \alpha_m^{n-3}\alpha + \alpha_m^{n-4}.\alpha^2 + \ldots + \alpha_m\alpha^{n-3} + \alpha^{n-2})$$

Utilizando esses resultados, obtemos para

$$\frac{f(\alpha_m)}{\alpha_m - \alpha} = \frac{a_1.(\alpha_m - \alpha)}{\alpha_m - \alpha} + \frac{a_2.(\alpha_m^2 - \alpha^2)}{\alpha_m - \alpha} + \ldots + \frac{a_{n-1}.(\alpha_m^{n-1} - \alpha^{n-1})}{\alpha_m - \alpha} + \frac{a_n.(\alpha_m^n - \alpha^n)}{\alpha_m - \alpha}$$

a seguinte igualdade:

$$\frac{f(\alpha_m)}{\alpha_m - \alpha} = a_1 + a_2.(\alpha_m + \alpha) + a_3.(\alpha_m^2 + \alpha_m\alpha + \alpha^2) + \ldots + a_n.(\alpha_m^{n-1} + \ldots + \alpha^{n-1})$$

Levando em consideração que $\alpha_m \to \alpha$, temos que para *m* suficientemente grande, α_m difere de α menos que 1, ou seja,$|\alpha_m - \alpha| < 1$.

Este fato será utilizado para fazermos uma estimativa de $\frac{f(\alpha_m)}{\alpha_m - \alpha}$.

Para isto, observemos que$|\alpha_m| - |\alpha| < |\alpha_m - \alpha|$. Como $|\alpha_m - \alpha| < 1$, podemos escrever $|\alpha_m| - |\alpha| < |\alpha_m - \alpha| < 1$, o que nos dá $|\alpha_m| - |\alpha| < 1$ ou ainda $|\alpha_m| < |\alpha| + 1$.

Utilizando $|\alpha_m| < |\alpha| + 1$ e a desigualdade triangular, temos:

$$|\alpha_m + \alpha| \leq |\alpha_m| + |\alpha| < |\alpha| + 1 + |\alpha| + 1 < 2.|\alpha| + 2 = 2.(|\alpha| + 1),$$

ou seja,

$$|\alpha_m + \alpha| < 2.(|\alpha| + 1).$$

Da mesma forma

$$|\alpha_m^2+\alpha_m.\alpha+\alpha^2|\le|\alpha_m|^2+|\alpha_m|.|\alpha|+|\alpha|^2<(|\alpha|+1)^2+(|\alpha|+1).(|\alpha|+1)+(|\alpha|+1)^2=$$
$$=3.(|\alpha|+1)^2$$

ou seja; $|\alpha_m^2+\alpha_m.\alpha+\alpha^2|<3.(|\alpha|+1)^2$.

Analogamente

$$|\alpha_m^3+\alpha_m^2\cdot\alpha+\alpha_m\cdot\alpha^2+\alpha^3|<|\alpha_m|^3+|\alpha_m|^2.|\alpha|+|\alpha_m|.|\alpha|^2+|\alpha|^3<$$

$$<(|\alpha|+1)^3+(|\alpha|+1)^2.(|\alpha|+1)+(|\alpha|+1).(|\alpha|+1)^2+(|\alpha|+1)^3=4.(|\alpha|+1)^3$$

ou seja; $|\alpha_m^3+\alpha_m^2\cdot\alpha+\alpha_m\cdot\alpha^2+\alpha^3|<4\cdot(|\alpha|+1)^3$.

Utilizando o mesmo raciocínio, podemos escrever

$$|\alpha_m^{n-1}+\ldots+\alpha^{n-1}|\le|\alpha_m|^{n-1}+\ldots+|\alpha|^{n-1}<(|\alpha|+1)^{n-1}+\ldots+(|\alpha|+1)^{n-1}=n.(|\alpha|+1)^{n-1}$$

Voltando à expressão

$$\frac{f(\alpha_m)}{\alpha_m-\alpha}=a_1+a_2.(\alpha_m+\alpha)+a_3.(\alpha_m^2+\alpha_m\alpha+\alpha^2)+\ldots+a_n.(\alpha_m^{n-1}+\ldots+\alpha^{n-1}),$$

temos que:

$$\left|\frac{f(\alpha_m)}{\alpha_m-\alpha}\right|=\left|a_1+a_2.(\alpha_m+\alpha)+a_3.(\alpha_m^2+\alpha_m\alpha+\alpha^2)+\ldots+a_n.(\alpha_m^{n-1}+\ldots+\alpha^{n-1})\right|$$

Aplicando a desigualdade triangular e os resultados acima, temos:

$$\left|\frac{f(\alpha_m)}{\alpha_m-\alpha}\right|<|a_1|+2.|a_2|.(|\alpha|+1)+3.|a_3|.(|\alpha|+1)^2+4.|a_4|.(|\alpha|+1)^3+\ldots+n.|a_n|.(|\alpha|+1)^{n-1}$$

Como α é fixo em nosso raciocínio, podemos concluir que o lado direito desta desigualdade também é um número fixo, que representaremos por M.

Vamos, então, escrever $\left|\frac{f(\alpha_m)}{\alpha_m-\alpha}\right|<M$, M fixo. De $\left|\frac{f(\alpha_m)}{\alpha_m-\alpha}\right|<M$ temos:

$$\frac{|f(\alpha_m)|}{|\alpha_m - \alpha|} < M$$

$$|f(\alpha_m)| < M.|\alpha_m - \alpha|$$

$$|\alpha_m - \alpha| > \frac{|f(\alpha_m)|}{M}$$

Escolhamos agora um valor para *m* (*m* fixo) suficientemente grande tal que em $\alpha_m = \frac{p_m}{q_m}$ o denominador q_m seja maior do que *M*.

Como $q_m > M$ então $|\alpha_m - \alpha| > \frac{|f(\alpha_m)|}{M} > \frac{|f(\alpha_m)|}{q_m}$.

Da igualdade $|\alpha_m - \alpha| = |\alpha - \alpha_m|$ temos $|\alpha - \alpha_m| > \frac{|f(\alpha_m)|}{q_m}$.

Como $f(x) = a_n \cdot x^n + a_{n-1} \cdot x^{n-1} + ... + a_2 \cdot x^2 + a_1 \cdot x^1 + a_0$, então

$$|f(\alpha_m)| = |a_n \cdot \alpha_m^n + a_{n-1} \cdot \alpha_m^{n-1} + ... + a_2 \cdot \alpha_m^2 + a_1 \cdot \alpha_m + a_0|.$$

Tomando $\alpha_m = \frac{p_m}{q_m}$, temos:

$$|f(\alpha_m)| = |a_n \cdot (\frac{p_m}{q_m})^n + a_{n-1} \cdot (\frac{p_m}{q_m})^{n-1} + ... + a_2 \cdot (\frac{p_m}{q_m})^2 + a_1 \cdot (\frac{p_m}{q_m})^1 + a_0|$$

$$|f(\alpha_m)| = |a_n \cdot \frac{p_m^n}{q_m^n} + a_{n-1} \cdot \frac{p_m^{n-1}}{q_m^{n-1}} + ... + a_2 \cdot \frac{p_m^2}{q_m^2} + a_1 \cdot \frac{p_m^1}{q_m^1} + a_0|$$

$$|f(\alpha_m)| = |\frac{a_n p_m^n + a_{n-1} q_m p_m^{n-1} + ... + a_2 q_m^{n-2} p_m^2 + a_1 q_m^{n-1} p_m + a_0 q_m^n}{q_m^n}|$$

O número racional $\alpha_m = \frac{p_m}{q_m}$ não pode ser raiz de $f(x) = 0$, pois se α_m fosse raiz de $f(x) = 0$, poderíamos fatorar (x - α_m) de $f(x)$ e neste caso α (que é um número algébrico de grau *n*) satisfaria uma equação de grau menor do que *n*. Portanto, $f(\alpha_m) \neq 0$.

Analisando, agora, o numerador do lado direito da igualdade

$$| f(\alpha_m) | = | \frac{a_n p_m^n + a_{n-1} q_m p_m^{n-1} + ... + a_2 q_m^{n-2} p_m^2 + a_1 q_m^{n-1} p_m + a_0 q_m^n}{q_m^n} |$$

$$| f(\alpha_m) | = \frac{| a_n p_m^n + a_{n-1} q_m p_m^{n-1} + ... + a_2 q_m^{n-2} p_m^2 + a_1 q_m^{n-1} p_m + a_0 q_m^n |}{q_m^n}$$

temos que ele é um número inteiro, e deve ser maior ou igual a 1.

Dessa consideração temos que $| f(\alpha_m) | \geq \frac{1}{q_m^n}$.

Então, de $| \alpha - \alpha_m | > \frac{| f(\alpha_m) |}{q_m}$ e $| f(\alpha_m) | \geq \frac{1}{q_m^n}$ temos:

$| \alpha - \alpha_m | > \frac{1}{q_m} \cdot | f(\alpha_m) | > \frac{1}{q_m} \cdot \frac{1}{q_m^n} = \frac{1}{q_m^{n+1}}$, ou seja, $| \alpha - \alpha_m | > \frac{1}{q_m^{n+1}} \Rightarrow | \alpha - \frac{p_m}{q_m} | > \frac{1}{q_m^{n+1}}$

o que prova o teorema.

3.3 Os números de Liouville

Mostraremos, agora, como esse teorema possibilita a construção de números transcendentes.

Qualquer número da forma $\alpha = \sum_{k=1}^{\infty} \frac{a_k}{10^{k!}}$, onde a_k é um algarismo qualquer de 1 a 9, é um número de Liouville.

Ou seja:

$$\alpha = a_1 \cdot 10^{-1!} + a_2 \cdot 10^{-2!} + a_3 \cdot 10^{-3!} + a_4 \cdot 10^{-4!} + ... + a_m \cdot 10^{-m!} + a_{m+1} \cdot 10^{-(m+1)!} + ...$$
$$\alpha = 0{,}1 \cdot a_1 + 0{,}01 \cdot a_2 + 0{,}000001 \cdot a_3 + ...$$
$$\alpha = 0, a_1 a_2 000 a_3 00000000000000000 a_4 000...$$

onde os algarismos iguais a a_k ocorrem nas casas decimais 1, 2, 6, 24, 120, 720, ..., ou seja, nas casas decimais 1!, 2!, 3!, 4!, 5!, 6!, ...

Esse número é caracterizado pelo aumento rápido do comprimento dos "grupos de 0" interrompidos por dígitos não nulos isolados.

Vamos, agora, considerar a fração decimal finita tomando-se apenas os termos de α até $a_m.10^{-m!}$, inclusive. Chamemos essa fração de α_m.

Sendo assim, temos: $\alpha_m = a_1.10^{-1!} + a_2.10^{-2!} + a_3.10^{-3!} + a_4.10^{-4!} + ... + a_m.10^{-m!}$.

Então $|\alpha - \alpha_m| = a_{m+1}.10^{-(m+1)!} + a_{m+2}.10^{-(m+2)!} + a_{m+3}.10^{-(m+3)!} + a_{m+4}.10^{-(m+4)!} + ...$

Como $1 \le a_{m+1} \le 9$, podemos concluir que $|\alpha - \alpha_m| < 10.10^{-(m+1)!}$.

Vamos supor, agora, que α seja um número algébrico de grau *n*, qualquer que seja $n > 1$.

Fazendo $\frac{p_m}{q_m} = \alpha_m = \frac{p_m}{10^{m!}}$, como $\alpha_m \to \alpha$, pelo Teorema de Liouville, existe um $m \in N$, tal que $|\alpha - \frac{p_m}{q_m}| > \frac{1}{q_m^{n+1}}$. Obtemos, então, que $|\alpha - \alpha_m| > \frac{1}{(10^{m!})^{n+1}}$, ou seja $|\alpha - \alpha_m| > \frac{1}{10^{(n+1).m!}}$, para *m* suficientemente grande.

De $|\alpha - \alpha_m| < 10.10^{-(m+1)!}$ e $\frac{1}{10^{(n+1).m!}} < |\alpha - \alpha_m|$ temos

$$\frac{1}{10^{(n+1).m!}} < 10.10^{-(m+1)!} = \frac{10^1}{10^{(m+1)!}} = \frac{1}{10^{(m+1)!-1}} \quad \text{ou seja} \quad \frac{1}{10^{(n+1).m!}} < \frac{1}{10^{(m+1)!-1}}.$$

Essa última desigualdade implica em $(n+1)\cdot m! > (m+1)!-1$, para todos os valores de *m* suficientemente grandes.

Porém, para qualquer valor de *m* maior do que *n,* a desigualdade $(n+1)\cdot m! > (m+1)!-1$ é falsa, o que gera uma contradição. Em seguida, vamos mostrar que essa desigualdade é falsa.

Uma maneira de verificar essa contradição é supondo que essa desigualdade seja verdadeira para qualquer valor de *m* maior que *n*. No caso de $(n+1)\cdot m! > (m+1)!-1$ ser verdadeira, teríamos:

$$n.m!+m! > (m+1).m!-1 \Leftrightarrow$$
$$n.m!+m! > m.m!+m!-1 \Leftrightarrow$$
$$n.m! > m.m!-1 \Leftrightarrow$$
$$n.m!-m.m! > -1 \Leftrightarrow$$
$$m.m!-n.m! < 1 \Leftrightarrow$$
$$(m-n).m! < 1$$

Para qualquer $m = n+k$, $k \in \mathrm{N}$, $k \geq 1$,temos:

$$(m-n).m! = (n+k-n).(n+k)! = k.(n+k)!.$$

Como $n > 1$ e $k \geq 1$, então $k.(n+k)! \geq 1.2 > 1$. Portanto, a suposição de que a desigualdade $(n+1).m! > (m+1)!-1$ é verdadeira é falsa. Ou seja, para qualquer valor de *m* maior que *n*, essa desigualdade sempre será falsa. Essa contradição foi gerada pela suposição de que α é um número algébrico de grau *n.*

Então, essa suposição de que α é um número algébrico de grau *n*, qualquer que seja *n*, é falsa. Logo, α é transcendente.

Pelo método da "Diagonal de Cantor", utilizado para demonstrar que o conjunto dos números reais não é enumerável, podemos demonstrar que o conjunto dos números de Liouville também é um conjunto não enumerável.

3.4 Prova de Cantor para a existência de números transcendentes

A demonstração apresentada nesta seção tem como referência Niven (1984, p. 201-202).

Já vimos que o conjunto dos números algébricos é enumerável.

Como um subconjunto infinito de um conjunto enumerável é enumerável, então, o conjunto dos números reais algébricos entre 0 e 1 é enumerável.

Por outro lado, o conjunto dos números reais não é enumerável. Na demonstração desse resultado é utilizado o famoso método da diagonal de Cantor, que veremos agora.

Suponha que o conjunto dos números reais x entre 0 e 1 ($0 < x \leq 1$) seja enumerável. Listando esses números teríamos: $r_1, r_2, r_3, r_4, ..., r_n, ...$.

Escrevendo todos esses números em forma decimal infinita, temos:

$$r_1 = 0, a_{11}a_{12}a_{13}a_{14}a_{15}...$$
$$r_2 = 0, a_{21}a_{22}a_{23}a_{24}a_{25}...$$
$$r_3 = 0, a_{31}a_{32}a_{33}a_{34}a_{35}...$$
$$r_4 = 0, a_{41}a_{42}a_{43}a_{44}a_{45}...$$
$$- - - - - - - - - - - - - - - -$$

e assim sucessivamente.

Construiremos, agora, um número $\beta = 0, b_1 b_2 b_3 b_4 ... b_n ...$ tal que:

- b_1 é qualquer algarismo entre 1 e 9, porém $b_1 \neq a_{11}$
- b_2 é qualquer algarismo entre 1 e 9, porém $b_2 \neq a_{22}$
- b_3 é qualquer algarismo entre 1 e 9, porém $b_3 \neq a_{33}$

E, assim sucessivamente, temos em geral b_n qualquer algarismo entre 1 e 9, porém $b_n \neq a_{nn}$.

Por exemplo, podemos considerar $b_n = \begin{cases} a_{nn} + 1 \text{ , } se\ a_{nn} \neq 9 \\ 1 \text{ , } se\ a_{nn} = 9 \end{cases}$

Por meio deste critério de construção temos que:

- $\beta \neq r_1$, pois eles diferem pelo menos na primeira casa decimal;
- $\beta \neq r_2$, pois eles diferem pelo menos na segunda casa decimal;
- $\beta \neq r_3$, pois eles diferem pelo menos na terceira casa decimal;

E assim sucessivamente, temos $\beta \neq r_n$, pois eles diferem pelo menos na n-ésima casa decimal.

Dessa maneira, construímos um número β que é diferente de cada um dos r_i, $i = 1,2,3,4, \ldots$.

Mas β é um número real entre 0 e 1. Obtemos, então, uma contradição, pois supomos que todos os números compreendidos entre 0 e 1 são os números $r_1, r_2, r_3, r_4, ..., r_n, ...$.

Essa contradição é conseqüência do fato de se supor que o conjunto dos números reais entre 0 e 1 seja enumerável. Portanto, essa suposição é falsa.

Podemos, então, concluir que o conjunto dos reais entre 0 e 1 é um conjunto não enumerável.

Consideremos, agora, os dois resultados:

i) o conjunto dos números algébricos entre 0 e 1 é enumerável
ii) o conjunto dos números reais entre 0 e 1 não é enumerável.

Então, devem existir números reais entre 0 e 1 que não sejam algébricos. Esses são os números transcendentes, cuja existência fica demonstrada (NIVEN, 1984, p. 203).

3.5 O conjunto dos números transcendentes não é enumerável

Além disso, Cantor demonstrou que o conjunto dos números reais transcendentes não é enumerável.

Para a demonstração desse resultado, vamos supor que o conjunto dos números reais transcendentes seja enumerável.

Já vimos que os números reais podem ser classificados em algébricos ou transcendentes, ou seja, o conjunto dos números reais pode ser obtido pela união do conjunto dos números algébricos com o conjunto dos números transcendentes.

Dessa forma, o conjunto dos números reais seria enumerável, pois a união de dois conjuntos enumeráveis é enumerável, o que é uma contradição, pois já sabemos que o conjunto dos números reais não é enumerável.

Essa contradição é conseqüência da suposição de que o conjunto dos números reais transcendentes seja enumerável. Portanto, essa suposição é falsa e vale a sua negação, ou seja, o conjunto dos números reais transcendentes não é enumerável. (NIVEN, 1984, p. 203).

3.6 Outros exemplos de números transcendentes

Tomando como referência Boyer (1974, p. 443),

> No Congresso de Paris de 1900, David Hilbert, renomado professor de Göttingen, apresentou uma exposição em que tentou, com base nas tendências da pesquisa matemática no fim do glorioso século dezenove, predizer a direção de progressos futuros. Isso ele fez propondo vinte e três problemas que ele acreditava estariam ou deveriam estar entre os que ocupariam a atenção dos matemáticos no século vinte. "Se quisermos ter uma idéia do desenvolvimento provável do conhecimento matemático no futuro imediato", ele disse, "devemos fazer passar por nossas mentes as questões não resolvidas e olhar os problemas que a ciência de hoje coloca e cujas soluções esperamos do futuro".

Especificamente, o sétimo problema de Hilbert consistia em estabelecer se certos números eram transcendentes, no qual perguntava-se se o número α^{β}, em que α é algébrico $(\alpha \neq 0 \ e \ \alpha \neq 1)$ e β é irracional e algébrico, é transcendente.

Essa questão foi resolvida em 1934 por Aleksander Osipovich Gelfond que provou que a conjectura de Hilbert, agora conhecida como Teorema de Gelfond, era correta: *Sejam α e β números algébricos (reais ou complexos). Se $\alpha \neq 0$, $\alpha \neq 1$ e β não for um número racional (real), então α^{β} é transcendente* (FIGUEIREDO, 1985, p. 96) . Em 1935, Schneider também provou esse teorema, independentemente dos trabalhos de Gelfond.

A transcendência de $2^{\sqrt{2}}$ é um caso específico desse resultado geral.

Uma outra conseqüência específica é a transcendência de $\log_{10} 2$.

Fazendo $\beta = \log_{10} 2$ e $\alpha = 10$, pela definição de logaritmo decimal $\alpha^{\beta} = 10^{\log_{10} 2} = 2$. Se $\beta = \log_{10} 2$ fosse algébrico e irracional, pelo Teorema de Gelfond, 2 seria transcendente. Mas 2 não é transcendente, portanto, $\beta = \log_{10} 2$ é racional ou transcendente. Mas $\log_{10} 2$ não é racional (NIVEN, 1984, p.110) . Portanto, $\log_{10} 2$ é transcendente.

Generalizando, o Teorema de Gelfond estabelece a transcendência de $\log_{10} r$, desde que r seja racional e $\log_{10} r$ irracional. Então, $\log_{10} r$ é transcendente, desde que r seja um número racional positivo diferente de 10^n, $n \in Z$. Por exemplo, para $1 \leq m \leq 1000$, m

inteiro, $m \neq 1,\ m \neq 10,\ m \neq 100,\ m \neq 1000$, os números $\log_{10} m$ são transcendentes (NIVEN, 1984, p. 115).

e^{π} é transcendente, pois $e^{\pi} = \dfrac{1}{e^{-\pi}} = \dfrac{1}{i^{2i}}$, e i^{2i} é transcendente pelo Teorema de Gelfond (BOYER, 1974, p. 445).

Um outro exemplo de número transcendente é o número de Champernowne 0,123456789101112131415..., obtido escrevendo-se a seqüência de números inteiros na base 10.

Em seguida, provaremos dois resultados que permitirão escrever outros infinitos exemplos de números transcendentes a partir de um número transcendente conhecido.

[A] Sejam $\alpha, \beta \in R$, sendo α algébrico e β transcendente. Então, $(\alpha + \beta)$ é transcendente.

Vamos supor que $(\alpha + \beta)$ seja algébrico. Por hipótese, α é algébrico. Então, $(-\alpha)$ também é algébrico. Como a soma de dois números algébricos é um número algébrico, então $(-\alpha) + (\alpha + \beta) = (-\alpha + \alpha) + \beta = 0 + \beta = \beta$ é algébrico. Mas, por hipótese, β é transcendente. Essa contradição nos leva à conclusão de que $(\alpha + \beta)$ não é algébrico. Portanto, $(\alpha + \beta)$ é transcendente.

Por exemplo, seja $\alpha \in Q$ e β um número de Liouville. Então, $(\alpha + \beta)$ é transcendente.

[B] Sejam $\alpha, \beta \in R$, sendo $\alpha \neq 0$ algébrico e β transcendente. Então, $\alpha.\beta$ é transcendente.

Vamos supor que $\alpha.\beta$ seja algébrico. Por hipótese, $\alpha \neq 0$ é algébrico. Então, α^{-1} também é algébrico. Como o produto de dois números algébricos é um número algébrico, então, $\alpha^{-1} \cdot (\alpha \cdot \beta) = (\alpha^{-1} \cdot \alpha) \cdot \beta = 1 \cdot \beta = \beta$ é algébrico. Mas, por hipótese, β é transcendente. Essa contradição nos leva à conclusão de que $\alpha.\beta$ não é algébrico. Portanto, $\alpha.\beta$ é transcendente.

Por exemplo, seja $\alpha \in Q$ e $\alpha \neq 0$ e o transcendente $\log_{10} 2$. Então, $\alpha.\log_{10} 2$ é transcendente.

No próximo capítulo, iremos fazer uma revisão sobre as relações entre os coeficientes e as raízes de uma equação polinomial. Também estudaremos os polinômios simétricos e suas propriedades. Esses resultados serão utilizados na demonstração da transcendência do π.

CAPÍTULO 4

Este capítulo será dedicado ao estudo dos polinômios simétricos e de três resultados que serão empregados na demonstração da transcendência do π. O primeiro deles será uma revisão sobre as relações entre os coeficientes e as raízes de uma equação polinomial, geralmente estudado no ensino médio. O segundo e o terceiro resultados se referem a dois teoremas dos polinômios simétricos.

4.1 Relações entre os coeficientes e as raízes de uma equação

Seja $f(x) = a_n \cdot x^n + a_{n-1} \cdot x^{n-1} + ... + a_2 \cdot x^2 + a_1 \cdot x^1 + a_0 = 0$ uma equação polinomial com coeficientes inteiros, $a_n \neq 0$.

De acordo com o Teorema Fundamental da Álgebra, "*toda equação polinomial* $f(x) = 0$ *a coeficientes complexos e grau* $n \geq 1$*, tem pelo menos uma raiz*". Na França, este teorema é conhecido frequentemente como teorema de d'Alembert devido ao grande tempo e esforço que d'Alembert dedicou à sua prova. (BOYER, 1974, p. 330). Por outro lado, em 1799, Gauss em sua tese de doutorado apresenta uma "Nova demonstração que toda função algébrica racional inteira em uma variável pode ser decomposta em fatores de primeiro ou segundo grau". Esse enunciado, a que Gauss mais tarde se referiu como "O Teorema Fundamental da Álgebra" é essencialmente o teorema de d'Alembert. (BOYER, 1974, p. 370).

De qualquer maneira, de acordo com o Teorema Fundamental da Álgebra, existe pelo menos uma raiz t_1 de $f(x) = 0$.

Então, $x - t_1$ é um fator de $f(x)$ e $f(x) = (x - t_1).f_1(x)$.

$f_1(x)$ é um polinômio de grau $n - 1$ cujo coeficiente do termo de maior grau é a_n.

Da mesma forma, existe uma raiz t_2 de $f_1(x) = 0$ e $f_1(x) = (x - t_2).f_2(x)$, onde $f_2(x)$ é um polinômio de grau $n - 2$, cujo coeficiente do termo de maior grau é a_n.

Podemos, então, escrever que $f(x) = (x - t_1).(x - t_2).f_2(x)$.

Prosseguindo com esse raciocínio, obtemos sucessivamente

$$\begin{aligned}
&f_2(x) = (x - t_3).f_3(x)\\
&f_3(x) = (x - t_4).f_4(x)\\
&- - - - - - - - - - - - - - -\\
&f_{n-2}(x) = (x - t_{n-1}).f_{n-1}(x)\\
&f_{n-1}(x) = a_n(x - t_n)
\end{aligned}$$

o que nos dá $f(x) = (x - t_1).(x - t_2).(x - t_3). \ldots .a_n(x - t_n) = 0$ ou

$$f(x) = a_n(x - t_1).(x - t_2).(x - t_3). \ldots .(x - t_{n-1}).(x - t_n) = 0 .$$

Vemos, então, que $t_1, t_2, \ldots, t_n$ são as raízes de $f(x) = 0$.

Como essa decomposição é única, não existem raízes diferentes de $t_1, t_2, \ldots, t_n$. (BEZERRA, 1965, p. 285-286).

Efetuando o produto dos *n* binômios em

$$a_n(x - t_1).(x - t_2).(x - t_3). \ldots .(x - t_{n-1}).(x - t_n) = 0$$

temos:

$$a_n \cdot x^n - a_n(t_1 + t_2 + \ldots + t_n) \cdot x^{n-1} + a_n(t_1t_2 + t_1t_3 + \ldots + t_{n-1}t_n) \cdot x^{n-2} + \ldots + (-1)^n \cdot a_n(t_1t_2 \ldots t_n) = 0$$

Como os primeiros membros da equação

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

e desta última igualdade devem ser idênticos, temos:

$$a_n = a_n$$
$$a_{n-1} = -a_n(t_1 + t_2 + ... + t_n)$$
$$a_{n-2} = a_n(t_1t_2 + t_1t_3 + ... + t_{n-1}t_n)$$
$$----------$$
$$a_0 = (-1)^n \cdot a_n(t_1t_2...t_n)$$

de onde obtemos as relações entre os coeficientes e as raízes da equação $a_n \cdot x^n + a_{n-1} \cdot x^{n-1} + a_{n-2} \cdot x^{n-2} + ... + a_2 \cdot x^2 + a_1 \cdot x^1 + a_0 = 0$

$$t_1 + t_2 + ... + t_n = -\frac{a_{n-1}}{a_n}$$
$$t_1t_2 + t_1t_3 + ... + t_{n-1}t_n = \frac{a_{n-2}}{a_n}$$
$$t_1t_2t_3 + t_1t_2t_4 + ... + t_{n-2}t_{n-1}t_n = -\frac{a_{n-3}}{a_n}$$ (BEZERRA, 1965, p. 291-292)
$$----------$$
$$t_1t_2t_3 \cdot ... \cdot t_n = (-1)^n \cdot \frac{a_0}{a_n}$$

Vejamos dois exemplos que ilustram esse resultado:

1) Seja a equação do segundo grau $a_2 \cdot x^2 + a_1 \cdot x + a_0 = 0$ e t_1, t_2 suas raízes. Fatorando a equação temos $a_2 \cdot (x - t_1) \cdot (x - t_2) = 0$ e efetuando o produto obtemos $a_2 \cdot (x^2 - (t_1 + t_2) \cdot x + t_1t_2) = 0$, ou seja, $a_2 \cdot x^2 - a_2 \cdot (t_1 + t_2) \cdot x + a_2 \cdot t_1t_2 = 0$, de onde temos

$$\begin{cases} t_1 + t_2 = -\dfrac{a_1}{a_2} \\ t_1t_2 = \dfrac{a_0}{a_2} \end{cases}$$

2) Seja a equação do terceiro grau $a_3 \cdot x^3 + a_2 \cdot x^2 + a_1 \cdot x + a_0 = 0$ e t_1, t_2, t_3 suas raízes. Fatorando a equação temos $a_3 \cdot (x - t_1) \cdot (x - t_2) \cdot (x - t_3) = 0$ e efetuando o produto obtemos $a_3 \cdot (x^3 - (t_1 + t_2 + t_3) \cdot x^2 + (t_1t_2 + t_1t_3 + t_2t_3) \cdot x - t_1t_2t_3) = 0$, ou seja, $a_3 \cdot x^3 - a_3 \cdot (t_1 + t_2 + t_3) \cdot x^2 + a_3 \cdot (t_1t_2 + t_1t_3 + t_2t_3) \cdot x - a_3 \cdot t_1t_2t_3 = 0$, de onde temos

$$\begin{cases} t_1 + t_2 + t_3 = -\dfrac{a_2}{a_3} \\ t_1t_2 + t_1t_3 + t_2t_3 = \dfrac{a_1}{a_3} \\ t_1t_2t_3 = -\dfrac{a_0}{a_3} \end{cases}$$

4.2 Polinômios Simétricos

Vamos iniciar nosso estudo tratando dos polinômios simétricos com duas variáveis. Em seguida, daremos a definição dos polinômios simétricos com *n* variáveis.

Um polinômio *P*, a duas variáveis t_1, t_2, é simétrico, se $P(t_1,t_2) = P(t_2,t_1)$ para todos os valores de t_1, t_2.

Vejamos alguns exemplos:

a) $P(t_1,t_2) = t_1^2 + t_2^2 + 6 \cdot t_1t_2$ é um polinômio simétrico, pois

$P(t_2,t_1) = t_2^2 + t_1^2 + 6 \cdot t_2t_1 = t_1^2 + t_2^2 + 6 \cdot t_1t_2 = P(t_1,t_2)$.

b) $P(t_1,t_2) = t_1 + t_2 \quad e \quad P(t_1,t_2) = t_1t_2$ são os polinômios simétricos elementares, que serão representados por $s_1 = t_1 + t_2 \quad e \quad s_2 = t_1t_2$.

c) $P_n(t_1,t_2) = t_1^n + t_2^n$, $n \in N$, também são polinômios simétricos.

Uma propriedade dos polinômios simétricos a duas variáveis é que $P(t_1,t_2)$ pode ser sempre representado por um polinômio $g(s_1,s_2)$ onde $s_1 = t_1 + t_2 \quad e \quad s_2 = t_1t_2$, tal que $P(t_1,t_2) = G(s_1,s_2)$. Veremos mais adiante um resultado análogo a esse para qualquer polinômio simétrico $P(t_1,t_2,...,t_{n-1},t_n)$.

Por exemplo,

a) O polinômio $P(t_1,t_2) = t_1^2 + t_2^2 + 5t_1t_2$ é simétrico e

$P(t_1,t_2) = t_1^2 + t_2^2 + 5t_1t_2 = t_1^2 + 2t_1t_2 + t_2^2 + 3t_1t_2 = (t_1 + t_2)^2 + 3t_1t_2$.

Então, $G(s_1,s_2)$ nesse caso será $G(s_1,s_2) = s_1^2 + 3s_2$

b) O polinômio $P_n(t_1,t_2) = t_1^n + t_2^n$, $n \in N, n \geq 2$ é simétrico e

$$P_n(t_1,t_2) = t_1^n + t_2^n = (t_1 + t_2)\cdot(t_1^{n-1} + t_2^{n-1}) - t_1t_2\cdot(t_1^{n-2} + t_2^{n-2}) = s_1 \cdot P_{n-1}(t_1,t_2) - s_2 \cdot P_{n-2}(t_1,t_2)$$

Para $n = 0$ e $n = 1$ temos, respectivamente, $P_0(t_1,t_2) = t_1^0 + t_2^0 = 1 + 1 = 2$ e

$$P_1(t_1,t_2) = t_1^1 + t_2^1 = t_1 + t_2 = s_1 .$$

Para $n = 2$

$$P_2(t_1,t_2) = t_1^2 + t_2^2 = s_1 \cdot P_1(t_1,t_2) - s_2 \cdot P_0(t_1,t_2) = s_1 \cdot s_1 - s_2 \cdot 2 = s_1^2 - 2s_2$$

Neste caso $G(s_1,s_2) = s_1^2 - 2s_2$

Para n =3

$$P_3(t_1,t_2) = t_1^3 + t_2^3 = s_1 \cdot P_2(t_1,t_2) - s_2 \cdot P_1(t_1,t_2) = s_1 \cdot (s_1^2 - 2s_2) - s_2 \cdot s_1 = s_1^3 - 3 \cdot s_1s_2$$

Neste caso $G(s_1,s_2) = s_1^3 - 3 \cdot s_1s_2$

Usando a lei de recorrência $P_n(t_1,t_2) = t_1^n + t_2^n = s_1 \cdot P_{n-1}(t_1,t_2) - s_2 \cdot P_{n-2}(t_1,t_2)$, sempre é possível determinar $P_n(t_1,t_2) = t_1^n + t_2^n$ em função de s_1 e s_2, para todo $n \geq 2$.

c) Num polinômio simétrico $P_n(t_1,t_2) = a \cdot t_1^n \cdot t_2^n$, temos

$P_n(t_1,t_2) = a \cdot t_1^n \cdot t_2^n = a \cdot (t_1t_2)^n = a \cdot s_2^n$. Neste caso $G(s_1,s_2) = a \cdot s_2^n$

d) Consideremos agora os polinômios simétricos que possuem um termo da forma $b \cdot t_1^l \cdot t_2^m$, com $l < m$. Como $P(t_1,t_2)$ é simétrico, se $b \cdot t_1^l \cdot t_2^m$ com $l < m$, é um termo de $f(t_1,t_2)$, então o termo $b \cdot t_1^m \cdot t_2^l$ também deverá existir em $P(t_1,t_2)$, para que a condição $P(t_1,t_2) = P(t_2,t_1)$ seja satisfeita. Neste caso, podemos escrever: $b \cdot t_1^l \cdot t_2^m + b \cdot t_1^m \cdot t_2^l = b \cdot t_1^l \cdot t_2^l \cdot (t_1^{m-l} + t_2^{m-l}) = b \cdot s_2^l \cdot P_{m-l}(t_1,t_2)$. Como já vimos no exemplo b, $P_{m-l}(t_1,t_2)$ pode ser escrito como um polinômio em s_1 e s_2, pois $(m-l) \in N$, uma vez que $l < m$ (GOMES, 2008).

Veremos, agora, a definição de um polinômio simétrico em $(t_1, t_2, ..., t_{n-1}, t_n)$, com coeficientes em um conjunto A (**A** = Z ou **A** = Q).

Para isso, precisamos da definição de *permutação* dos inteiros 1, 2, ..., *n*.

Uma permutação dos inteiros 1, 2, ..., *n* é uma função bijetora do conjunto {1, 2, ..., *n*} nele próprio.

$$\begin{aligned} \sigma : \{1,2, \dots ,n\} &\to \{1,2, \dots ,n\} \\ j &\mapsto \sigma(j) \end{aligned}$$

Por exemplo, para *n* = 2, há 2! = 2 permutações. São elas:

$$\sigma_1 : \begin{matrix} 1 \to 1 \\ 2 \to 2 \end{matrix} \quad \text{e} \quad \sigma_2 : \begin{matrix} 1 \to 2 \\ 2 \to 1 \end{matrix}$$

Se *n* = 3, temos 3! = 6 permutações. São elas:

$$\sigma_1 : \begin{matrix} 1 \to 1 \\ 2 \to 2 \\ 3 \to 3 \end{matrix} \qquad \sigma_2 : \begin{matrix} 1 \to 1 \\ 2 \to 3 \\ 3 \to 2 \end{matrix} \qquad \sigma_3 : \begin{matrix} 1 \to 2 \\ 2 \to 1 \\ 3 \to 3 \end{matrix}$$

$$\sigma_4 : \begin{matrix} 1 \to 2 \\ 2 \to 3 \\ 3 \to 1 \end{matrix} \qquad \sigma_5 : \begin{matrix} 1 \to 3 \\ 2 \to 1 \\ 3 \to 2 \end{matrix} \qquad \sigma_6 : \begin{matrix} 1 \to 3 \\ 2 \to 2 \\ 3 \to 1 \end{matrix}$$

Em geral, existem *n*! permutações dos inteiros {1, 2, ..., *n*}.

Em seguida, veremos a definição dos polinômios simétricos com *n* variáveis.

Um polinômio $P(t_1, t_2, ..., t_{n-1}, t_n)$ *é chamado simétrico se*

$$P^{\sigma}(t_1, t_2, ..., t_{n-1}, t_n) = P(t_{\sigma(1)}, t_{\sigma(2)}, ..., t_{\sigma(n-1)}, t_{\sigma(n)}) = P(t_1, t_2, ..., t_{n-1}, t_n)$$

para todas as permutações σ *dos inteiros* 1, 2, ..., *n* – 1, *n* .

Já vimos que $P(t_1, t_2)$ é um polinômio simétrico, se $P(t_1, t_2) = P(t_2, t_1)$.

Para *n* = 3, temos que $P(t_1, t_2, t_3)$ é um polinômio simétrico, se

$$P(t_1, t_2, t_3) = P(t_1, t_3, t_2) = P(t_2, t_1, t_3) = P(t_2, t_3, t_1) = P(t_3, t_1, t_2) = P(t_3, t_2, t_1).$$

4.2.1 Polinômios simétricos elementares

Se $t_1, t_2, ..., t_n \in C$ são as raízes de um polinômio *P*(x), então podemos escrever esse polinômio na forma $P(x) = (x - t_1) \cdot (x - t_2) \cdot ... \cdot (x - t_n)$, supondo nesse caso que o coeficiente líder de *P*(x) é igual a 1.

Desenvolvendo esse produto, temos: $P(x) = x^n - s_1 \cdot x^{n-1} + s_2 \cdot x^{n-2} + ... + (-1)^n \cdot s_n$, onde

$$s_1 = \sum_{j=1}^{n} t_j$$

$$s_2 = \sum_{1 \le i < j \le n} t_i t_j$$

$$s_3 = \sum_{1 \le i < j < k \le n} t_i t_j t_k$$

$$- - - - - - - - - - - - -$$

$$s_n = t_1 \cdot t_2 \cdot ... \cdot t_n$$

Os polinômios $s_1, s_2, s_3, ..., s_n$ são chamados de polinômios simétricos elementares em $t_1, t_2, ..., t_{n-1}, t_n$. Esses polinômios terão um papel fundamental no enunciado de dois teoremas sobre os polinômios simétricos que estudaremos agora.

Antes disso, veremos a definição de *grau* e *peso* de um polinômio em $t_1, t_2, ..., t_{n-1}, t_n$.

Uma expressão da forma $a \cdot t_1^{k_1} \cdot t_2^{k_2} \cdot ... \cdot t_n^{k_n}$ é chamada de *monômio.*

O *grau* do monômio $a \cdot t_1^{k_1} \cdot t_2^{k_2} \cdot ... \cdot t_n^{k_n}$ é, por definição, o número inteiro $\sum_{j=1}^{n} k_j = k_1 + k_2 + ... + k_n$.

O *peso* do monômio $a \cdot t_1^{k_1} \cdot t_2^{k_2} \cdot ... \cdot t_n^{k_n}$ é, por definição, o número inteiro $\sum_{j=1}^{n} j \cdot k_j = 1 \cdot k_1 + 2 \cdot k_2 + ... + n \cdot k_n$.

O grau de um polinômio em $t_1, t_2, ..., t_{n-1}, t_n$ é o máximo dos graus dos monômios que o formam. Igualmente, o peso de um polinômio em $t_1, t_2, ..., t_{n-1}, t_n$ é o máximo dos pesos dos monômios que o constituem. (FIGUEIREDO, 1985, p. 77)

4.2.2 Teorema

Seja $P(t_1,t_2,...,t_{n-1},t_n)$ *um polinômio simétrico de grau d, com coeficientes em* ***A*** *(****A*** *= Z ou* ***A*** *= Q). Então, existe um polinômio* $G(s_1,s_2,...,s_{n-1},s_n)$ *de peso menor ou igual a d com coeficientes em* ***A****, onde* $s_1,s_2,...,s_{n-1},s_n$ *são os polinômios simétricos elementares em* $t_1,t_2,...,t_{n-1},t_n$ *tal que* $P(t_1,t_2,...,t_{n-1},t_n)=G(s_1,s_2,...,s_{n-1},s_n)$. (FIGUEIREDO, 1985, p. 80)

A demonstração desse teorema será feita por indução sobre *n* .

Para *n* = 1, o teorema se verifica, pois neste caso $t_1 = s_1$. Se $P(t_1)$ é um polinômio de grau *d,* então existe $G(s_1)$, $G(s_1) \equiv P(t_1)$ também de grau *d*, portanto de peso menor ou igual a *d*, tal que $P(t_1)=G(s_1)$.

Hipótese de Indução (1): Suponhamos que o teorema seja válido para polinômios simétricos em $t_1,t_2,...,t_{n-1}$

Tese: O teorema é válido para polinômios simétricos em $t_1,t_2,...,t_{n-1},t_n$.

Considerando a *Hipótese de Indução* (1)*,* vamos agora escrever os polinômios simétricos elementares em $t_1,t_2,...,t_{n-1}$, que representaremos por $\bar{s}_1,\bar{s}_2,\bar{s}_3$, ... , $\bar{s}_{n-1}$ tomando $t_n = 0$ nas expressões dos polinômios simétricos elementares em $t_1,t_2,...,t_{n-1},t_n$. Desse modo:

$$\bar{s}_1 = \sum_{j=1}^{n-1} t_j = t_1 + t_2 + ... + t_{n-1}$$

$$\bar{s}_2 = \sum_{1\le i<j\le n-1} t_i t_j = t_1t_2 + ... + t_1t_{n-1} + ... + t_{n-2}t_{n-1}$$

$$\bar{s}_3 = \sum_{1\le i<j<k\le n-1} t_i t_j t_k = t_1t_2t_3 + ... + t_{n-3}t_{n-2}t_{n-1}$$

$$- -$$

$$\bar{s}_{n-1} = t_1t_2t_3. \ ... \ .t_{n-1}$$

Para provar que o teorema é válido para polinômios simétricos em $t_1,t_2,...,t_{n-1},t_n$, utilizaremos novamente um prova por indução. Porém, essa indução agora será feita sobre os graus *d* desses polinômios.

Hipótese de Indução (2): Suponhamos que o teorema seja válido para polinômios simétricos em $t_1, t_2, ..., t_{n-1}, t_n$ de grau menor que *d*.

Tese: O teorema é válido para polinômios de grau *d*.

Para $d = 0$, o resultado é válido. Nesse caso, temos apenas os polinômios constantes, ou seja, $P(t_1, t_2, ..., t_{n-1}, t_n) = c = G(s_1, s_2, ..., s_{n-1}, s_n)$.

Consideremos um polinômio simétrico $P(t_1, t_2, ..., t_{n-1}, t_n)$ de grau *d*. Pela *Hipótese de Indução* (1), para $t_n = 0$, existe um polinômio simétrico $G(\bar{s}_1, \bar{s}_2, ..., \bar{s}_{n-1})$ de peso menor ou igual a d, tal que $P(t_1, t_2, ..., t_{n-1}, 0) = G_1(\bar{s}_1, \bar{s}_2, ..., \bar{s}_{n-1})$.

Considerando G_1 aplicado em $s_1, s_2, ..., s_{n-1}$, temos que $G_1(s_1, s_2, ..., s_{n-1})$ é um polinômio simétrico em $t_1, t_2, ..., t_{n-1}, t_n$ com grau menor ou igual a *d*.

Seja agora o polinômio $P_1(t_1, t_2, ..., t_{n-1}, t_n)$ dado por

$P_1(t_1, t_2, ..., t_{n-1}, t_n) = P(t_1, t_2, ..., t_{n-1}, t_n) - G_1(s_1, s_2, ..., s_{n-1})$ o qual também é simétrico em $t_1, t_2, ..., t_{n-1}, t_n$.

Fazendo $t_n = 0$ em $P_1(t_1, t_2, ..., t_{n-1}, t_n) = P(t_1, t_2, ..., t_{n-1}, t_n) - G_1(s_1, s_2, ..., s_{n-1})$, temos $P_1(t_1, t_2, ..., t_{n-1}, 0) = P(t_1, t_2, ..., t_{n-1}, 0) - G_1(\bar{s}_1, \bar{s}_2, ..., \bar{s}_{n-1})$.

Como $P(t_1, t_2, ..., t_{n-1}, 0) = G_1(\bar{s}_1, \bar{s}_2, ..., \bar{s}_{n-1})$, concluímos que $P_1(t_1, t_2, ..., t_{n-1}, 0) = 0$.

Do fato de $P_1(t_1, t_2, ..., t_{n-1}, 0) = 0$, podemos concluir que t_n é um fator comum em $P_1(t_1, t_2, ..., t_{n-1}, t_n)$. Como $P_1(t_1, t_2, ..., t_{n-1}, t_n)$ é um polinômio simétrico em $t_1, t_2, ..., t_{n-1}, t_n$ e t_n é um fator comum em $P_1(t_1, t_2, ..., t_{n-1}, t_n)$, segue-se, então, que $t_1, t_2, ..., t_{n-1}$ também são fatores comuns de $P_1(t_1, t_2, ..., t_{n-1}, t_n)$. Lembrando que $s_n = t_1.t_2. ... .t_n$, segue-se que $P_1(t_1, t_2, ..., t_{n-1}, t_n) = s_n.P_2(t_1, t_2, ..., t_{n-1}, t_n)$, onde o grau de P_2 é menor ou igual $d - n < d$.

Aplicando agora a *Hipótese de Indução* (2), existe um polinômio simétrico $G_2(s_1, s_2, ..., s_{n-1}, s_n)$ de peso menor ou igual a $(d - n)$ tal que

$$P_2(t_1, t_2, ..., t_{n-1}, t_n) = G_2(s_1, s_2, ..., s_{n-1}, s_n).$$

Então, $P_1(t_1,t_2,...,t_{n-1},t_n) = s_n.G_2(s_1,s_2,...,s_{n-1},s_n)$.

Desse modo obtemos de $P_1(t_1,t_2,...,t_{n-1},t_n) = P(t_1,t_2,...,t_{n-1},t_n) - G_1(s_1,s_2,...,s_{n-1})$ que

$$P(t_1,t_2,...,t_{n-1},t_n) = P_1(t_1,t_2,...,t_{n-1},t_n) + G_1(s_1,s_2,...,s_{n-1}).$$

Como $P_1(t_1,t_2,...,t_{n-1},t_n) = s_n.G_2(s_1,s_2,...,s_{n-1},s_n)$, segue-se que

$$P(t_1,t_2,...,t_{n-1},t_n) = s_n G_2(s_1,s_2,...,s_{n-1},s_n) + G_1(s_1,s_2,...,s_{n-1}).$$

Fazendo $G(s_1,s_2,...,s_{n-1},s_n) = s_n G_2(s_1,s_2,...,s_{n-1},s_n) + G_1(s_1,s_2,...,s_{n-1})$ temos $P(t_1,t_2,...,t_{n-1},t_n) = G(s_1,s_2,...,s_{n-1},s_n)$ o que mostra que $P(t_1,t_2,...,t_{n-1},t_n)$ é igual a um polinômio $G(s_1,s_2,...,s_{n-1},s_n)$ simétrico em $s_1,s_2,...,s_{n-1},s_n$ de peso menor ou igual a d, concluindo a demonstração (FIGUEIREDO, 1985, p. 81-84).

4.2.3 Teorema

Sejam $\alpha_1,\alpha_2,...,\alpha_n$ números algébricos, tais que os polinômios simétricos elementares

$$s_1 = \sum_{j=1}^{n} \alpha_j$$
$$s_2 = \sum \alpha_i.\alpha_j \quad 1 \le i < j \le n$$
$$- - - - - - - - - - - - - - - - - -$$
$$s_n = \alpha_1.\alpha_2. \ ... \ .\alpha_n$$

sejam números racionais. Considere agora os $\binom{n}{2}$ números algébricos $\beta_{ij} = \alpha_i + \alpha_j$, $1 \le i < j \le n$. Então, os polinômios simétricos elementares associados aos β_{ij}'s são também números racionais.

Como conseqüência desse teorema, temos o seguinte resultado:

Se $\alpha_1, \alpha_2, ..., \alpha_n$ *são as raízes de um polinômio*

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

de grau n, com coeficientes racionais, então os $\binom{n}{2}$ *números* β_{ij}*'s anteriores são as raízes de um polinômio de grau* $\binom{n}{2}$ *com coeficientes racionais* (FIGUEIREDO, 1985, p. 86).

Neste trabalho, ilustramos esse resultado só para n = 2 e n = 3 a fim de compreender melhor o enunciado do teorema e sua conseqüência.

Para n = 2, temos os números algébricos α_1, α_2. Os polinômios simétricos elementares são $s_1 = \alpha_1 + \alpha_2 \in Q$ *e* $s_2 = \alpha_1 \cdot \alpha_2 \in Q$. Nesse caso, temos apenas um número algébrico $\beta_{12} = \alpha_1 + \alpha_2$. O único polinômio simétrico associado ao β_{12} é o próprio $\beta_{12} = \alpha_1 + \alpha_2$, que imediatamente é racional. Sejam α_1, α_2 raízes do polinômio $P(x) = a_2 \cdot x^2 + a_1 \cdot x + a_0$ com coeficientes racionais. Então, β_{12} é raiz de um polinômio de grau $\binom{2}{2} = 1$ com coeficientes racionais. Esse polinômio é dado por $P(x) = x - \beta_{12}$.

Para n = 3, temos os números algébricos $\alpha_1, \alpha_2, \alpha_3$. Nesse caso, os polinômios simétricos elementares são

$$\begin{aligned} s_1 &= \alpha_1 + \alpha_2 + \alpha_3 \\ s_2 &= \alpha_1\alpha_2 + \alpha_1\alpha_3 + \alpha_2\alpha_3 \qquad \text{com } s_1, s_2, s_3 \in Q \\ s_3 &= \alpha_1\alpha_2\alpha_3 \end{aligned}$$

Consideremos os $\binom{3}{2} = 3$ números algébricos

$$\begin{aligned} \beta_{12} &= \alpha_1 + \alpha_2 \\ \beta_{13} &= \alpha_1 + \alpha_3 \\ \beta_{23} &= \alpha_2 + \alpha_3 \end{aligned}$$

Os polinômios simétricos elementares associados aos $\beta_{ij}'s$ são:

$$S_1 = \beta_{12} + \beta_{13} + \beta_{23}$$
$$S_2 = \beta_{12}\beta_{13} + \beta_{12}\beta_{23} + \beta_{13}\beta_{23}$$
$$S_3 = \beta_{12}\beta_{13}\beta_{23}$$

Para provar que esses polinômios simétricos elementares associados aos $\beta_{ij}'s$ são também números racionais, basta provar que eles são polinômios simétricos em $\alpha_1, \alpha_2, \alpha_3$, pois, como já vimos, dado um polinômio simétrico P em $\alpha_1, \alpha_2, \alpha_3$, existe um polinômio $G(s_1, s_2, s_3)$ tal que $P(\alpha_1, \alpha_2, \alpha_3) = G(s_1, s_2, s_3)$. Desse fato, podemos concluir que os polinômios simétricos elementares associados aos $\beta_{ij}'s$ também são racionais, pois estarão escritos em função de s_1, s_2, s_3, que, por hipótese, são números racionais.

Vejamos:

$$S_1 = \beta_{12} + \beta_{13} + \beta_{23} = \alpha_1 + \alpha_2 + \alpha_1 + \alpha_3 + \alpha_2 + \alpha_3 = 2.(\alpha_1 + \alpha_2 + \alpha_3) = 2s_1 \in Q$$

$$S_2 = \beta_{12}\beta_{13} + \beta_{12}\beta_{23} + \beta_{13}\beta_{23} = (\alpha_1 + \alpha_2).(\alpha_1 + \alpha_3) + (\alpha_1 + \alpha_2).(\alpha_2 + \alpha_3) +$$
$$+ (\alpha_1 + \alpha_3).(\alpha_2 + \alpha_3) = \alpha_1^2 + \alpha_2^2 + \alpha_3^2 + 3.(\alpha_1 \cdot \alpha_2 + \alpha_1\alpha_3 + \alpha_2 \cdot \alpha_3)$$

que é um polinômio simétrico em $\alpha_1, \alpha_2, \alpha_3$. Portanto, $S_2 \in Q$.

$$S_3 = \beta_{12}\beta_{13}\beta_{23} = (\alpha_1 + \alpha_2).(\alpha_1 + \alpha_3).(\alpha_2 + \alpha_3) =$$
$$= \alpha_1^2 \cdot \alpha_2 + \alpha_1 \cdot \alpha_2^2 + \alpha_1^2 \cdot \alpha_3 + \alpha_1 \cdot \alpha_3^2 + \alpha_2^2 \cdot \alpha_3 + \alpha_2 \cdot \alpha_3^2 + 2 \cdot \alpha_1 \cdot \alpha_2 \cdot \alpha_3$$

que é um polinômio simétrico em $\alpha_1, \alpha_2, \alpha_3$. Portanto, $S_3 \in Q$.

Sejam $\alpha_1, \alpha_2, \alpha_3$ raízes do polinômio $P(x) = a_3 \cdot x^3 + a_2 \cdot x^2 + a_1 \cdot x + a_0$ com coeficientes racionais. Então, $\beta_{12}, \beta_{13}, \beta_{23}$ são raízes de um polinômio de grau $\binom{3}{2} = 3$ com coeficientes racionais.

Esse polinômio pode ser obtido da seguinte maneira:

$P(x) = (x - \beta_{12}).(x - \beta_{13}).(x - \beta_{23})$. Desenvolvendo os produtos indicados, temos:

$P(x) = x^3 - (\beta_{12} + \beta_{13} + \beta_{23}) \cdot x^2 + (\beta_{12}\beta_{13} + \beta_{12}\beta_{23} + \beta_{13}\beta_{23}) \cdot x - \beta_{12}\beta_{13}\beta_{23}$, ou seja:

$P(x) = x^3 - S_1 \cdot x^2 + S_2 \cdot x - S_3$, com $S_1, S_2, S_3 \in Q$.

Esse teorema pode ser generalizado da seguinte maneira:

Sejam $\alpha_1,\alpha_2,...,\alpha_n$ *números algébricos, tais que os polinômios simétricos elementares*

$$s_1 = \sum_{j=1}^{n} \alpha_j$$
$$s_2 = \sum \alpha_i \cdot \alpha_j \quad 1 \le i < j \le n$$
$$---------$$
$$s_n = \alpha_1 \cdot \alpha_2 \cdot \ldots \cdot \alpha_n$$

sejam números racionais. Considere agora os $\binom{n}{j}$ *números algébricos* $\beta_{k_1 \ldots k_j} = \alpha_{k_1} + \ldots + \alpha_{k_j}$, $1 \le k_1 < \ldots < k_j \le n$. *Então, os polinômios simétricos elementares associados a esses* $\beta's$ *são também números racionais.*

Como conseqüência, temos que:

Se $\alpha_1,\alpha_2,...,\alpha_n$ *são as raízes de um polinômio de grau n, com coeficientes racionais, então os* $\beta's$ *são raízes de um polinômio de grau* $\binom{n}{j}$ *com coeficientes racionais.* (FIGUEIREDO, 1985, p. 87-88).

Mostramos em seguida outros resultados que serão utilizados na demonstração da transcendência do número π. As demonstrações são dadas nos Anexos II, III e IV.

[A] A fórmula de Euler *(ver Anexo II)*

$e^{iy} = \cos y + i \cdot seny$. Para $y = \pi$, temos a famosa igualdade $e^{i\pi} = -1$.

[B] Cálculo da soma $\sum_{i=1}^{n} \binom{n}{i}$ ***(ver Anexo II)***

$$\sum_{i=1}^{n} \binom{n}{i} = \binom{n}{1} + \binom{n}{2} + \binom{n}{3} + \ldots + \binom{n}{n} = 2^n - 1$$

Esta soma será utilizada para determinar o grau de um polinômio que será construído durante a demonstração.

[C] Seja $Q(x)=\sum_{j=0}^{r} a_j \cdot x^j$ um polinômio com coeficientes inteiros e seja $p<r$ um inteiro positivo. Então:

a) $Q^{(i)}(x)=\sum_{j=i}^{r} \frac{j!}{(j-i)!} \cdot a_j \cdot x^{j-i}$, $i \le r$, onde $Q^{(i)}(x)$ representa a derivada de ordem i de $Q(x)$.

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

O item *a*) será utilizado na demonstração do item *b*). O item *b*) motivou a definição de uma função que dará sequência no plano da demonstração. *(ver anexo III)*

[D] Seja a função $F(x)=P(x)+P'(x)+...+P^{(r-1)}(x)+P^{(r)}(x)$, em que $P(x)$ é um polinômio de grau *r* e $P^{(r)}(x)$ representa a derivada de ordem *r* de $P(x)$.Então:

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

Esse resultado também será utilizado na definição de uma função.

[E] Desigualdade do valor médio para funções de uma variável complexa ***(ver anexo IV)***

Teorema: *Seja* $f : C \to C$ *uma função analítica e sejam* $z_1, z_2 \in C$. *Então:* $|f(z_2)-f(z_1)| \le 2.|z_2-z_1|.\sup\{|f'(z_1+\lambda.(z_2-z_1))| : 0 \le \lambda \le 1\}$, *onde* $|z|$ *representa o módulo do complexo z = x + i.y, isto é;* $|z| = \sqrt{x^2+y^2}$ (FIGUEIREDO, 1985, p. 61).

No próximo capítulo faremos um estudo sobre a demonstração da transcendência do π, aplicando os resultados vistos até agora.

Veremos que todos esses resultados interagem entre si, cada um dando sua contribuição na construção do raciocínio utilizado na demonstração.

CAPÍTULO 5

Neste capítulo, veremos a demonstração da transcendência do número π, tendo como referências (FIGUEIREDO, 1985, p. 65-73), (ALVES, 1999, p. 15-17) e (AUGUSTINI, OLIVEIRA e SILVA, 2005, p. 81-86).

Assim como Alves (1999), Augustini, Oliveira e Silva (2005) também utilizaram a demonstração dada em Figueiredo (1985), como referência em seus trabalhos.

Em nosso trabalho, tivemos o cuidado de apresentá-la de forma mais detalhada, justificando todas as afirmações e etapas envolvidas durante a demonstração.

O método usado por Hermite para demonstrar a transcendência de *e* foi estendido por Lindemann, para demonstrar a transcendência do número π, em 1882.

A demonstração dada em Figueiredo (1985, p. 65), tem como referência a demonstração de R. Moritz, a qual por sua vez foi inspirada na prova de Hurwitz para a trancendência de *e*.

5.1 Demonstração da transcendência do número π

Para demonstrar que π é transcendente, vamos supor exatamente o contrário, isto é, que o número π seja algébrico, obtendo assim, uma contradição.

Suponhamos, então, que π seja um número algébrico.

Como o número complexo $i \in C$ é solução da equação polinomial $x^2 + 1 = 0$, então i é um número algébrico.

Pela aritmética dos números algébricos, o produto de dois números algébricos é algébrico. Logo, $i \cdot \pi$ também é algébrico.

Isso significa que $i \cdot \pi$ é raiz de uma equação polinomial de grau *n* com coeficientes inteiros, que será representada por $P_1(x) = 0$. Neste caso, temos $P_1(i \cdot \pi) = 0$.

Vamos representar as *n* raízes (reais ou complexas) de $P_1(x) = 0$ por

$$\alpha_1 = i \cdot \pi,\ \alpha_2, \alpha_3, \ldots, \alpha_n .$$

Fatorando $P_1(x) = 0$ temos

$$P_1(x) = a_1 \cdot (x - \alpha_1) \cdot (x - \alpha_2) \cdot \ldots \cdot (x - \alpha_n),\ \ a_1 \in Z,\ (a_1 \neq 0),\ P_1(\alpha_i) = 0,\ i = 1,2,3, \ldots, n .$$

Da Fórmula de Euler $e^{ix} = \cos x + isenx$, temos para $x = \pi$, a igualdade $e^{i\pi} = -1$.

Consideremos, agora, o produto $\prod_{j=1}^{n} (1 + e^{\alpha_j})$.

Como $e^{i\pi} = -1$, segue-se que $\prod_{j=1}^{n} (1 + e^{\alpha_j}) = 0$, pois

$$\prod_{j=1}^{n} (1 + e^{\alpha_j}) = (1 + e^{\alpha_1}) \cdot (1 + e^{\alpha_2}) \cdot \ldots \cdot (1 + e^{\alpha_n}) = (1 + e^{i\pi}) \cdot (1 + e^{\alpha_2}) \cdot \ldots \cdot (1 + e^{\alpha_n}) =$$
$$= (1 + (-1)) \cdot (1 + e^{\alpha_2}) \cdot \ldots \cdot (1 + e^{\alpha_n}) = 0 \cdot (1 + e^{\alpha_2}) \cdot \ldots \cdot (1 + e^{\alpha_n}) = 0$$

Desenvolvendo o produto do lado esquerdo da igualdade $\prod_{j=1}^{n} (1 + e^{\alpha_j}) = 0$, obtemos uma expressão da forma:

$$1 + e^{\alpha_1} + e^{\alpha_2} + \ldots + e^{\alpha_n} + e^{\alpha_1 + \alpha_2} + \ldots + e^{\alpha_1 + \alpha_n} + \ldots + e^{\alpha_{n-1} + \alpha_n} + e^{\alpha_1 + \alpha_2 + \alpha_3} + \ldots +$$
$$+ e^{\alpha_{n-2} + \alpha_{n-1} + \alpha_n} + \ldots + e^{\alpha_1 + \alpha_2 + \ldots + \alpha_n} = 0$$

ou seja, 1 + somatório de exponenciais, cujos expoentes são:

[1] $\alpha_1, \alpha_2, \alpha_3, \ldots, \alpha_n$, com $\binom{n}{1} = n$ termos

[2] $\alpha_i + \alpha_j$, para todos i < j, com $\binom{n}{2}$ termos

[3] $\alpha_i + \alpha_j + \alpha_k$, para todos i < j < k, com $\binom{n}{3}$ termos

[n] $\alpha_1 + \alpha_2 + \alpha_3 + ... + \alpha_n$, com $\binom{n}{n} = 1$ termo.

onde $\binom{n}{m} = \frac{n!}{m!.(n-m)!}$, para $0 \le m \le n$, são os coeficientes binomiais.

Para exemplificar esse resultado, consideremos os 2 casos abaixo:

$$a) \prod_{j=1}^{2} (1 + e^{\alpha_j}) = (1 + e^{\alpha_1}).(1 + e^{\alpha_2}) = 1 + e^{\alpha_1} + e^{\alpha_2} + e^{\alpha_1 + \alpha_2} = 0$$

$$b) \prod_{j=1}^{3} (1 + e^{\alpha_j}) = (1 + e^{\alpha_1}).(1 + e^{\alpha_2}).(1 + e^{\alpha_3}) = 1 + e^{\alpha_1} + e^{\alpha_2} + e^{\alpha_3} + e^{\alpha_1 + \alpha_2} +$$
$$+ e^{\alpha_1 + \alpha_3} + e^{\alpha_2 + \alpha_3} + e^{\alpha_1 + \alpha_2 + \alpha_3} = 0$$

Somando o número de termos em [1], [2], [3], ..., [n], temos:

$$\binom{n}{1} + \binom{n}{2} + \binom{n}{3} + ... + \binom{n}{n} = 2^n - 1 \text{ termos.}$$

Agora, do fato de que $\alpha_1, \alpha_2, \alpha_3, ..., \alpha_n$ satisfazem uma equação polinomial de grau *n* com coeficientes inteiros, $P_1(x) = 0$, segue-se que:

a) os números $\alpha_i + \alpha_j$, para todos $i < j$, satisfazem uma equação polinomial de grau $\binom{n}{2}$ com coeficientes inteiros que denotaremos por $P_2(x) = 0$. Essa equação pode ser escrita na forma fatorada

$$P_2(x) = a_2 \cdot (x - (\alpha_1 + \alpha_2)) \cdot \ldots \cdot (x - (\alpha_1 + \alpha_n)) \cdot \ldots \cdot (x - (\alpha_{n-1} + \alpha_n)), \ a_2 \neq 0, \ a_2 \in Z$$

b) os números $\alpha_i + \alpha_j + \alpha_k$, para todos $i < j < k$, satisfazem uma equação polinomial de grau $\binom{n}{3}$ com coeficientes inteiros que denotaremos por $P_3(x) = 0$. Essa equação pode ser escrita na forma fatorada

$$P_3(x) = a_3 \cdot (x - (\alpha_1 + \alpha_2 + \alpha_3)) \cdot \ldots \cdot (x - (\alpha_{n-2} + \alpha_{n-1} + \alpha_n)), \ a_3 \neq 0, \ a_3 \in Z.$$

E assim sucessivamente.

Em resumo, os números $\alpha_1,\alpha_2,\alpha_3,\ldots,\alpha_n$; $\alpha_i+\alpha_j$, para todos $i<j$; $\alpha_i+\alpha_j+\alpha_k$, para todos $i<j<k$; ...; $\alpha_1+\alpha_2+\alpha_3+\ldots+\alpha_n$, satisfazem uma equação polinomial $P_1(x).P_2(x).P_3(x).\ldots.P_n(x)=0$, com coeficientes inteiros de grau 2^n-1.

Como alguns dos números $\alpha_1,\alpha_2,\alpha_3,\ldots,\alpha_n$; $\alpha_i+\alpha_j$, $(i<j)$; $\alpha_i+\alpha_j+\alpha_k$,$(i<j<k)$; ... ; $\alpha_1+\alpha_2+\alpha_3+\ldots+\alpha_n$, podem se anular, vamos supor que desses (2^n-1) números, *m* deles sejam diferentes de zero. Esses *m* números diferentes de zero serão representados por $\beta_1, \beta_2, \beta_3, \ldots, \beta_m$.

Se tivermos $m<(2^n-1)$, podemos simplificar em $P_1(x)\cdot P_2(x)\cdot P_3(x)\cdot\ldots\cdot P_n(x)=0$ os fatores da forma x^q ($q > 0$), obtendo uma equação polinomial de grau *m* com coeficientes inteiros cujas raízes são os números $\beta_1,\beta_2,\beta_3,\ldots,\beta_m$.

Essa equação será representada por $R(x)=c\cdot x^m+c_{m-1}\cdot x^{m-1}+\ldots+c_1\cdot x+c_0=0$

Considerando ainda esses *m* números diferentes de zero representados por $\beta_1,\beta_2,\beta_3,\ldots,\beta_m$, vamos efetuar novamente o produto $\prod_{j=1}^{n}(1+e^{\alpha_j})=0$, que já vimos ser uma expressão da forma (1 + somatório de exponenciais).

Agrupando as potências de ***e*** cujos expoentes são iguais a zero (se houver) no início desta soma de exponenciais, obtemos:

$$1+e^0+e^0+\ldots+e^0+e^{\beta_1}+e^{\beta_2}+e^{\beta_3}+\ldots+e^{\beta_m}=0$$

$$k+e^{\beta_1}+e^{\beta_2}+e^{\beta_3}+\ldots+e^{\beta_m}=0$$

$$k=-(e^{\beta_1}+e^{\beta_2}+e^{\beta_3}+\ldots+e^{\beta_m}) \quad ou \quad k=-\sum_{j=1}^{m}e^{\beta_j} \; ; \; \beta_j\neq 0, \; j=1,2,3,\ldots,m$$

Definimos o polinômio $P(x)=\frac{c^s}{(p-1)!}\cdot x^{p-1}\cdot(R(x))^p$, onde c é o coeficiente da potência de x^m em $R(x)=c\cdot x^m+c_{m-1}\cdot x^{m-1}+\ldots+c_1\cdot x+c_0=0$; *p* é um número primo a ser escolhido; $s=mp-1$ e *m* é o grau de $R(x)=0$.

O grau de *P* é igual a $mp + p - 1 = mp - 1 + p = s + p$.

Definimos, agora, a função:

$$F(x) = P(x) + P'(x) + P''(x) + ... + P^{(s+p)}(x)$$

onde $P^{(s+p)}(x)$ representa a derivada de ordem $(s+p)$ *de* $P(x)$.

Multiplicando ambos os lados da igualdade acima por e^{-x}, temos:

$$e^{-x} \cdot F(x) = e^{-x} \cdot (P(x) + P'(x) + P''(x) + ... + P^{(s+p)}(x))$$

Desta forma, $\frac{d}{dx}(e^{-x}.F(x)) = -e^{-x}.P(x)$

Seja $f : C \to C$ uma função analítica e sejam $z_1, z_2 \in C$. Então:

$| f(z_2) - f(z_1) | \leq 2. | z_2 - z_1 | .\sup\{ | f'(z_1 + \lambda.(z_2 - z_1)) | : 0 \leq \lambda \leq 1 \}$, sendo |z| o módulo do número complexo $z = x + i.y$, isto é, $| z | = \sqrt{x^2 + y^2}$.

Aplicando essa desigualdade à função $f(z) = e^{-z}.F(z)$ para $z_1 = 0$ e $z_2 = \beta_j$ (j = 1, 2, ..., *m*), temos:

$$| f(\beta_j) - f(0) | \leq 2. | \beta_j - 0 | .\sup\{| f'(0 + \lambda(\beta_j - 0)) | : 0 \leq \lambda \leq 1\}$$

$$| f(\beta_j) - f(0) | \leq 2. | \beta_j | .\sup\{| f'(\lambda(\beta_j)) | : 0 \leq \lambda \leq 1\}$$

Como $f(z) = e^{-z} \cdot F(z)$, temos

$$f(\beta_j) = e^{-\beta_j} \cdot F(\beta_j) \quad \text{e} \quad f(0) = e^{-0} \cdot F(0) = 1 \cdot F(0) = F(0)$$

Usando $\frac{d}{dz}\left(e^{-z} \cdot F(z)\right) = -e^{-z} \cdot P(z)$, podemos escrever

$$\frac{d}{dz}\left(e^{-z} \cdot F(z)\right) = \frac{d}{dz}\left(f(z)\right) = -e^{-z} \cdot P(z), \text{ ou seja, } f'(z) = -e^{-z} \cdot P(z).$$

Segue-se que $f'(\lambda(\beta_j)) = -e^{-\lambda.(\beta_j)} \cdot P(\lambda(\beta_j))$, $j = 1, 2, 3, ..., m$.

Então, em $| f(\beta_j) - f(0) | \leq 2. | \beta_j | .\sup\{| f'(\lambda(\beta_j)) | : 0 \leq \lambda \leq 1\}$, temos:

$$| e^{-\beta_j} \cdot F(\beta_j) - F(0) | \leq 2 \cdot | \beta_j | .\sup\{| -e^{-\lambda\beta_j}.P(\lambda\beta_j) | : 0 \leq \lambda \leq 1\}$$

Multiplicando essa desigualdade por $\frac{1}{|e^{-\beta_j}|}$, obtemos:

$$|F(\beta_j) - e^{\beta_j} \cdot F(0)| \leq 2 \cdot |\beta_j| \cdot \sup\{|e^{(1-\lambda).\beta_j} \cdot P(\lambda\beta_j)| : 0 \leq \lambda \leq 1\}$$

Fazendo $\varepsilon_j = 2 \cdot |\beta_j| \cdot \sup\{|e^{(1-\lambda).\beta_j} \cdot P(\lambda\beta_j)| : 0 \leq \lambda \leq 1\}$, podemos escrever

$|F(\beta_j) - e^{\beta_j}.F(0)| \leq \varepsilon_j$, $j = 1,2,3, \ldots, m$.

Para *j* de 1 até *m*, obtemos:

$|F(\beta_1) - e^{\beta_1} \cdot F(0)| \leq \varepsilon_1$

$|F(\beta_2) - e^{\beta_2} \cdot F(0)| \leq \varepsilon_2$

$|F(\beta_3) - e^{\beta_3} \cdot F(0)| \leq \varepsilon_3$

$|F(\beta_m) - e^{\beta_m} \cdot F(0)| \leq \varepsilon_m$

Somando essas desigualdades, segue-se que:

$$|F(\beta_1) - e^{\beta_1} \cdot F(0)| + |F(\beta_2) - e^{\beta_2} \cdot F(0)| + \ldots + |F(\beta_m) - e^{\beta_m} \cdot F(0)| \leq \varepsilon_1 + \varepsilon_2 + \ldots + \varepsilon_m$$

Aplicando a desigualdade triangular no lado esquerdo dessa desigualdade, obtemos:

$$|(F(\beta_1) - e^{\beta_1} \cdot F(0)) + (F(\beta_2) - e^{\beta_2} \cdot F(0)) + \ldots + (F(\beta_m) - e^{\beta_m} \cdot F(0))| \leq$$
$$\leq |F(\beta_1) - e^{\beta_1} \cdot F(0)| + |F(\beta_2) - e^{\beta_2} \cdot F(0)| + \ldots + |F(\beta_m) - e^{\beta_m} \cdot F(0)| \leq$$
$$\leq \varepsilon_1 + \varepsilon_2 + \ldots + \varepsilon_m$$

Ou seja,

$$|\sum_{j=1}^{m} F(\beta_j) - \sum_{j=1}^{m} e^{\beta_j}.F(0)| \leq |F(\beta_1) - e^{\beta_1}.F(0)| + |F(\beta_2) - e^{\beta_2}.F(0)| + \ldots +$$
$$+ |F(\beta_m) - e^{\beta_m}.F(0)| \leq \sum_{j=1}^{m} \varepsilon_j$$

Resumindo, $|\sum_{j=1}^{m} F(\beta_j) - \sum_{j=1}^{m} e^{\beta_j}.F(0)| \leq \sum_{j=1}^{m} \varepsilon_j$. Como $k = -\sum_{j=1}^{m} e^{\beta_j}$, obtemos

$$|k.F(0) + \sum_{j=1}^{m} F(\beta_j)| \leq \sum_{j=1}^{m} \varepsilon_j .$$

O objetivo a partir deste momento é mostrar que o lado esquerdo dessa desigualdade é um inteiro não nulo, e que o lado direito, para um número primo conveniente, é menor que 1, gerando uma contradição.

Em primeiro lugar, vamos analisar o lado esquerdo dessa desigualdade. Para isso, devemos calcular $F(0)$ e $F(\beta_j)$, para $j = 1, 2, ..., m$.

Lembrando que $F(x) = P(x) + P'(x) + P''(x) + ... + P^{(s+p)}(x)$, temos:

a) $F(0) = P(0) + P'(0) + P''(0) + ... + P^{(s+p)}(0)$ e

b) $F(\beta_j) = P(\beta_j) + P'(\beta_j) + P''(\beta_j) + ... + P^{(s+p)}(\beta_j)$, para $j = 1, 2, ..., m$.

Vamos, então, calcular $P(0)$, $P(\beta_j)$ e as várias derivadas de $P(x)$ nos pontos

$$0, \beta_1, \beta_2, \beta_3, ..., \beta_m .$$

Como $P(x) = \frac{c^s}{(p-1)!} \cdot x^{p-1} \cdot (R(x))^p$ e $R(x) = c \cdot x^m + c_{m-1} \cdot x^{m-1} + ... + c_1 \cdot x + c_0$,

podemos escrever $P(x)$ na seguinte forma:

$$P(x) = \frac{c^s}{(p-1)!} \cdot x^{p-1} \cdot (cx^m + c_{m-1}x^{m-1} + ... + c_1x + c_0)^p$$

Desenvolvendo as operações indicadas, temos:

$$P(x) = \frac{c^s}{(p-1)!} \cdot (c_0{}^p x^{p-1} + bx^p + ... + c^p x^{mp+p-1}).$$

Como $s = mp - 1$, então:

$$P(x) = \frac{c^s}{(p-1)!} \cdot (c_0{}^p x^{p-1} + bx^p + ... + c^p x^{s+p}).$$

No ponto $\boldsymbol{x = 0}$, temos:

$$P(0) = \frac{c^s}{(p-1)!} \cdot (c_0{}^p .0^{p-1} + b.0^p + ... + c^p .0^{s+p}) = \frac{c^s}{(p-1)!} \cdot 0 = 0$$

Para o cálculo de $P^{(i)}(0)$, onde $P^{(i)}(0)$ representa a derivada de ordem i de $P(x)$ calculada no ponto 0, vamos fazer nossa análise em 3 partes: para $i < p - 1$, $i = p - 1$ e $i \geq p$.

Para $i < p - 1$, em qualquer derivada de ordem i, o polinômio $P(x)$ apresentará potências de x em todos os seus termos. Então, concluímos que para $i < p - 1$ temos $P^{(i)}(0) = 0$.

Para $i = p-1$,

$$P^{(i)}(x) = \frac{c^s}{(p-1)!} \cdot ((p-1)!{c_0}^p + b \cdot p!x + ... + c^p \cdot (s+p) \cdot ... \cdot (s+2) \cdot x^{s+1})$$

Então:

$$P^{(i)}(0) = \frac{c^s}{(p-1)!} \cdot ((p-1)!{c_0}^p + b.p!.0 + ... + c^p.(s+p). ... .(s+2).0^{s+1}) =$$

$$= \frac{c^s}{(p-1)!} \cdot ((p-1)!{c_0}^p + 0 + 0 + ... + 0) = \frac{c^s}{(p-1)!} \cdot (p-1)!{c_0}^p = c^s \cdot {c_0}^p$$

Resumindo: para $i = p - 1$, temos $P^{(i)}(0) = c^s \cdot {c_0}^p$.

Para $i \geq p$, os coeficientes de $P^{(i)}(x)$ são inteiros divisíveis por p. Como esses coeficientes também são divisíveis por c^s, concluímos, então, que os coeficientes de $P^{(i)}(x)$, $i \geq p$, são inteiros divisíveis por $p.c^s$. Disso concluímos que, para $i \geq p$, os coeficientes de $P^{(i)}(0)$ são números inteiros divisíveis por $p.c^s$.

Então:

$$F(0) = P(0) + P'(0) + P''(0) + ... + P^{(p-2)}(0) + P^{(p-1)}(0) + P^{(p)}(0) + ... + P^{(s+p)}(0)$$

$$F(0) = \quad 0 \quad + \quad 0 \quad + \quad 0 \quad + ... + \quad 0 \quad + c^s.{c_0}^p \quad + k_0.\, p.c^s$$

$$F(0) = \; c^s.{c_0}^p + k_0.\, p.c^s, \;\; (k_0 \in Z)$$

Nos pontos $x = \beta_j$, para $j = 1, 2, 3, \ldots, m$, temos:

Como $R(\beta_j) = 0$, para $j = 1, 2, 3, \ldots, m$, então:

$$P(\beta_j) = \frac{c^s}{(p-1)!} \cdot {\beta_j}^{p-1}.(R(\beta_j))^p = \frac{c^s}{(p-1)!} \cdot {\beta_j}^{p-1}.0^p = 0.$$

Para i < p, segue-se diretamente de $P(x) = \frac{c^s}{(p-1)!} \cdot x^{p-1} \cdot (R(x))^p$, que $P^{(i)}(\beta_j) = 0$, pois a expressão $R(x)$ é fator comum nas derivadas $P^{(i)}(x)$, para $i < p$ e $R(\beta_j) = 0$, para $j = 1, 2, 3, \ldots, m$.

Para as derivadas de ordem $i \geq p$, os coeficientes de $P^{(i)}(x)$ são inteiros divisíveis por $p.c^s$. Então, para $i \geq p$, os coeficientes de $P^{(i)}(\beta_j)$ para $j = 1, 2, 3, \ldots, m$, são inteiros divisíveis por $p.c^s$.

Calculando $F(\beta_j)$, temos:

$$F(\beta_j) = P(\beta_j) + P'(\beta_j) + \ldots + P^{(p-1)} + P^{(p)}(\beta_j) + \ldots + P^{(s+p)}(\beta_j)$$

$$F(\beta_j) = \quad 0 \quad + \quad 0 \quad + \ldots + \quad 0 \quad + P^{(p)}(\beta_j) + \ldots + P^{(s+p)}(\beta_j)$$

$$F(\beta_j) = P^{(p)}(\beta_j) + P^{(p+1)}(\beta_j) \ \ldots + P^{(s+p)}(\beta_j), \text{ para } j = 1, 2, 3, \ldots, m.$$

Para j de 1 até m, temos:

$$F(\beta_1) = P^{(p)}(\beta_1) + P^{(p+1)}(\beta_1) \ \ldots + P^{(s+p)}(\beta_1)$$

$$F(\beta_2) = P^{(p)}(\beta_2) + P^{(p+1)}(\beta_2) \ \ldots + P^{(s+p)}(\beta_2)$$

$$F(\beta_m) = P^{(p)}(\beta_m) + P^{(p+1)}(\beta_m) \ \ldots + P^{(s+p)}(\beta_m)$$

Somando termo a termo

$$F(\beta_1) + F(\beta_2) + \ldots + F(\beta_m) = [P^{(p)}(\beta_1) + P^{(p)}(\beta_2) + \ldots + P^{(p)}(\beta_m)] +$$
$$+ [P^{(p+1)}(\beta_1) + P^{(p+1)}(\beta_2) + \ldots + P^{(p+1)}(\beta_m)] + \ldots + [P^{(s+p)}(\beta_1) + P^{(s+p)}(\beta_2) + \ldots +$$
$$+ P^{(s+p)}(\beta_m)]$$

Usando a notação do somatório

$$\sum_{j=1}^{m} F(\beta_j) = \sum_{j=1}^{m} P^{(p)}(\beta_j) + \sum_{j=1}^{m} P^{(p+1)}(\beta_j) + \ldots + \sum_{j=1}^{m} P^{(p+s)}(\beta_j)$$

$$\sum_{j=1}^{m} F(\beta_j) = \sum_{i=p}^{s+p} (\sum_{j=1}^{m} P^{(i)}(\beta_j))$$

Observemos, agora, a expressão

$$\sum_{j=1}^{m} P^{(i)}(\beta_j) = P^{(i)}(\beta_1) + P^{(i)}(\beta_2) + \ldots + P^{(i)}(\beta_m),$$

para cada i fixado, com $p \leq i \leq s+p$.

O polinômio $P^{(i)}$ tem coeficientes inteiros divisíveis por $p.c^s$ e grau $s + p - i \leq s$, pois $p \leq i$.

Para $i = p$, o grau de $P^{(p)}$ será $s + p - p = s \leq s$.

Como o polinômio $P^{(p)}$ tem coeficientes divisíveis por $p.c^s$ e grau s, podemos escrevê-lo da seguinte forma:

$$P^{(p)}(x) = p.c^s.(d_0 + d_1.x + d_2.x^2 + \ldots + d_s.x^s),\ d_i \in Z,\ i = 0, 1, 2, \ldots, s\ \ (d_s \neq 0)$$

Então,

$$\sum_{j=1}^{m} P^{(p)}(\beta_j) = P^{(p)}(\beta_1) + P^{(p)}(\beta_2) + \ldots + P^{(p)}(\beta_m) =$$
$$= p.c^s.(d_0 + d_1.\beta_1 + d_2.\beta_1^{\,2} + \ldots + d_s.\beta_1^{\,s}) + p.c^s.(d_0 + d_1.\beta_2 + d_2.\beta_2^{\,2} + \ldots + d_s.\beta_2^{\,s}) +$$
$$+ \ldots + p.c^s.(d_0 + d_1.\beta_m + d_2.\beta_m^{\,2} + \ldots + d_s.\beta_m^{\,s}) = p.c^s.[m.d_0 + (\beta_1 + \beta_2 + \ldots + \beta_m)d_1 +$$
$$(\beta_1^{\,2} + \beta_2^{\,2} + \ldots + \beta_m^{\,2})d_2 + \ldots + (\beta_1^{\,s} + \beta_2^{\,s} + \ldots + \beta_m^{\,s})d_s = p.c^s.Q_p(\beta_1, \beta_2, \ldots, \beta_m)$$

$\sum_{j=1}^{m} P^{(p)}(\beta_j) = p.c^s.Q_p(\beta_1, \beta_2, \ldots, \beta_m)$, onde $Q_p(\beta_1, \beta_2, \ldots, \beta_m)$ é um polinômio nos $\beta_j's$ de grau s.

Pelo desenvolvimento acima, podemos concluir que $Q_p(\beta_1, \beta_2, \ldots, \beta_m)$ é um polinômio simétrico nos $\beta_j's$, com coeficientes inteiros.

Logo, existe um polinômio $G_p(\sigma_1, \sigma_2, \ldots, \sigma_m)$ de grau menor ou igual a s com coeficientes inteiros, onde $\sigma_1, \sigma_2, \ldots, \sigma_m$ são os polinômios simétricos elementares em $\beta_1, \beta_2, \ldots, \beta_m$, tal que $Q_p(\beta_1, \beta_2, \ldots, \beta_m) = G_p(\sigma_1, \sigma_2, \ldots, \sigma_m)$.

Então, $\sum_{j=1}^{m} P^{(p)}(\beta_j) = p \cdot c^s \cdot G_p(\sigma_1, \sigma_2, \ldots, \sigma_m)$.

Pela definição de polinômios simétricos elementares, temos que:

$$\begin{cases} \sigma_1 = \sum_{j=1}^{m} \beta_j \\ \sigma_2 = \sum_{i<j} \beta_i.\beta_j \\ \sigma_3 = \sum_{i<j<k} \beta_i.\beta_j.\beta_k \\ - - - - - - - - - \\ \sigma_n = \beta_1.\beta_2. \ldots .\beta_m \end{cases}$$

Como $\beta_1, \beta_2, ..., \beta_m$, são raízes de $R(x) = c \cdot x^m + c_{m-1} \cdot x^{m-1} + ... + c_1 \cdot x + c_0$, segue-se que:

$$\begin{cases} \sum_{j=1}^{m} \beta_j = -\frac{c_{m-1}}{c} \\ \sum_{i<j} \beta_i.\beta_j = \frac{c_{m-2}}{c} \\ \sum_{i<j<k} \beta_i.\beta_j.\beta_k = -\frac{c_{m-3}}{c} \\ - - - - - - - - - - - \\ \beta_1.\beta_2. \ ... \ .\beta_m = (-1)^m.\frac{c_0}{c} \end{cases}$$

Igualando esses dois sistemas, temos:

$$\begin{cases} \sigma_1 = -\frac{c_{m-1}}{c} \\ \sigma_2 = \frac{c_{m-2}}{c} \\ \sigma_3 = -\frac{c_{m-3}}{c} \\ - - - - - - - \\ \sigma_m = (-1)^m.\frac{c_0}{c} \end{cases}$$

Como $G_p(\sigma_1, \sigma_2, ..., \sigma_m)$ tem grau menor ou igual a s com coeficientes inteiros, então a expressão $\sum_{j=1}^{m} P^{(p)}(\beta_j) = p \cdot c^s \cdot G_p(\sigma_1, \sigma_2, ..., \sigma_m) = p.k_p$, $k_p \in Z$.

Analogamente, para $i = p + 1$, o grau de $P^{(p+1)}$ será igual a $s + p - (p + 1) = s - 1 \leq s$.

Como o polinômio $P^{(p+1)}$ tem coeficientes divisíveis por $p.c^s$ e grau $s - 1$, podemos escrevê-lo da seguinte forma:

$P^{(p+1)}(x) = p \cdot c^s \cdot (e_0 + e_1 \cdot x + e_2 \cdot x^2 + ... + e_{s-1} \cdot x^{s-1})$, $e_i \in$ Z, $i = 0, 1, 2, \ldots, (s-1)$, $(e_{s-1} \neq 0)$.

Então,

$$\sum_{j=1}^{m} P^{(p+1)}(\beta_j) = P^{(p+1)}(\beta_1) + P^{(p+1)}(\beta_2) + ... + P^{(p+1)}(\beta_m) =$$

$$= p.c^s.(e_0 + e_1.\beta_1 + e_2.\beta_1^{\,2} + ... + e_{s-1}.\beta_1^{\,s-1}) + p.c^s.(e_0 + e_1.\beta_2 + e_2.\beta_2^{\,2} + ... + e_{s-1}.\beta_2^{\,s-1}) +$$

$$+ ... + p.c^s.(e_0 + e_1.\beta_m + e_2.\beta_m^{\,2} + ... + e_{s-1}.\beta_m^{\,s-1}) = p.c^s.[m.e_0 + (\beta_1 + \beta_2 + ... + \beta_m)e_1 +$$

$$(\beta_1^{\,2} + \beta_2^{\,2} + ... + \beta_m^{\,2})e_2 + ... + (\beta_1^{\,s-1} + \beta_2^{\,s-1} + ... + \beta_m^{\,s-1})e_{s-1} = p.c^s.Q_{p+1}(\beta_1, \beta_2, ..., \beta_m)$$

$\sum_{j=1}^{m} P^{(p+1)}(\beta_j) = p.c^s.Q_{p+1}(\beta_1,\beta_2,...,\beta_m)$, onde $Q_{p+1}(\beta_1,\beta_2,...,\beta_m)$ é um polinômio nos β_j's de grau (s – 1). Pelo desenvolvimento acima, podemos ver também que $Q_{p+1}(\beta_1,\beta_2,...,\beta_m)$ é um polinômio simétrico com coeficientes inteiros. Logo, existe um polinômio $G_{p+1}(\sigma_1,\sigma_2,...,\sigma_m)$ de grau menor ou igual a (s – 1) com coeficientes inteiros e onde $\sigma_1,\sigma_2,...,\sigma_m$ são os polinômios simétricos elementares em $\beta_1,\beta_2,...,\beta_m$, tal que $Q_{p+1}(\beta_1,\beta_2,...,\beta_m) = G_{p+1}(\sigma_1,\sigma_2,...,\sigma_m)$.

Então $\sum_{j=1}^{m} P^{(p+1)}(\beta_j) = p \cdot c^s \cdot G_{p+1}(\sigma_1,\sigma_2,...,\sigma_m)$.

Como $G_{p+1}(\sigma_1,\sigma_2,...,\sigma_m)$ tem grau menor ou igual a (s – 1) com coeficientes inteiros, então a expressão $\sum_{j=1}^{m} P^{(p+1)}(\beta_j) = p \cdot c^s \cdot G_{p+1}(\sigma_1,\sigma_2,...,\sigma_m) = p \cdot k_{p+1}$, $k_{p+1} \in Z$.

De forma análoga, como já vimos, para cada i fixado, com $p \le i \le s + p$, o polinômio $P^{(i)}$ têm coeficientes inteiros divisíveis por $p.c^s$. Além disso, como P tem grau $s + p$, segue-se que $P^{(i)}$ tem grau $s + p - i \le s$, pois $p \le i$.

Logo, a expressão $\sum_{j=1}^{m} P^{(i)}(\beta_j) = P^{(i)}(\beta_1) + P^{(i)}(\beta_2) + ... + P^{(i)}(\beta_m)$ pode ser escrita como $\sum_{j=1}^{m} P^{(i)}(\beta_j) = p \cdot c^s \cdot Q_i(\beta_1,\beta_2,...,\beta_m)$, onde $Q_i(\beta_1,\beta_2,...,\beta_m)$ é um polinômio simétrico nos β_j's, de grau menor ou igual a s, com coeficientes inteiros. Logo, existe um polinômio $G_i(\sigma_1,\sigma_2,...,\sigma_m)$ de grau menor ou igual a s com coeficientes inteiros e onde $\sigma_1,\sigma_2,...,\sigma_m$ são os polinômios simétricos elementares em $\beta_1,\beta_2,...,\beta_m$, tal que $Q_i(\beta_1,\beta_2,...,\beta_m) = G_i(\sigma_1,\sigma_2,...,\sigma_m)$.

Segue-se que

$$\sum_{j=1}^{m} P^{(i)}(\beta_j) = p \cdot c^s \cdot G_i(\sigma_1,\sigma_2,...,\sigma_m) = p \cdot k_i, \quad k_i \in Z$$

Então,

$$\sum_{j=1}^{m} F(\beta_j) = \sum_{i=p}^{s+p} (\sum_{j=1}^{m} P^{(i)}(\beta_j)) = \sum_{j=1}^{m} P^{(p)}(\beta_j) + \sum_{j=1}^{m} P^{(p+1)}(\beta_j) + ... +$$

$$+ \sum_{j=1}^{m} P^{(p+s)}(\beta_j) = p \cdot k_p + p \cdot k_{p+1} + ... + p \cdot k_{p+s} = p \cdot (k_p + k_{p+1} + ... + k_{p+s}) = p \cdot K, \;\; K \in Z$$

Retomando as expressões $F(0)$ e $\sum_{j=1}^{m} F(\beta_j)$, temos:

$$F(0) = c^s \cdot c_0^p + k_0 \cdot p \cdot c^s, \; k_0 \in Z \quad \text{e} \quad \sum_{j=1}^{m} F(\beta_j) = p \cdot K, \; K \in Z .$$

Então, na expressão $| k \cdot F(0) + \sum_{j=1}^{m} F(\beta_j) |$, obtemos:

$$| k \cdot F(0) + \sum_{j=1}^{m} F(\beta_j) | = | k \cdot (c^s \cdot c_0^p + k_0 \cdot p \cdot c^s) + p \cdot K | =$$

$$= | k \cdot c^s \cdot c_0^p + k \cdot k_0 \cdot p \cdot c^s + p \cdot K | = | p \cdot (k \cdot k_0 \cdot c^s + K) + k \cdot c^s \cdot c_0^p | = | p \cdot L + k \cdot c^s \cdot c_0^p |$$

sendo $L = k \cdot k_0 \cdot c^s + K$.

Todo esse desenvolvimento foi necessário para mostrar que

$$| k \cdot F(0) + \sum_{j=1}^{m} F(\beta_j) | = | p \cdot L + k \cdot c^s \cdot c_0^p | \in Z, \; s = mp - 1.$$

Agora, devemos escolher um número primo *p*, de modo que ele seja maior que *k*, *c* e c_0. Este *p* existe, pois o conjunto dos números primos é infinito. Desta maneira, o inteiro $k \cdot c^s \cdot c_0^p$ não é divisível por *p*, pois *p* não é fator de *k*, nem de c^s e de c_0^p. Como p divide *p.L* e *p* não divide $k \cdot c^s \cdot c_0^p$, então *p* não divide a soma $(p \cdot L + k \cdot c^s \cdot c_0^p)$. Logo, o número $| p \cdot L + k \cdot c^s \cdot c_0^p |$, para tal valor de *p*, é um inteiro não nulo.

Consequentemente, $| k \cdot F(0) + \sum_{j=1}^{m} F(\beta_j) | \geq 1.$

Para completar a demonstração, necessitamos fazer uma estimativa do termo $\sum_{j=1}^{m} \varepsilon_j$ que aparece no lado direito da expressão $| \sum_{j=1}^{m} F(\beta_j) - \sum_{j=1}^{m} e^{\beta_j} \cdot F(0) | \leq \sum_{j=1}^{m} \varepsilon_j$.

Para isto, devemos recordar que $\varepsilon_j = 2\cdot|\beta_j|\cdot\sup\{|\, e^{(1-\lambda).\beta_j}\cdot P(\lambda\beta_j)\,|: 0\le\lambda\le 1\}$ e $P(x)=\dfrac{c^s}{(p-1)!}\cdot x^{p-1}\cdot(R(x))^p$.

Seja $M = máx\{|\,\beta_1\,|, |\,\beta_2\,|, \ldots, |\,\beta_m\,|\}$.

Então $\varepsilon_j \le 2\cdot M\cdot\sup\{|\, e^{(1-\lambda).M}\cdot P(\lambda\beta_j)\,|: 0\le\lambda\le 1\}$.

Antes de prosseguirmos com a estimativa, justifiquemos a desigualdade acima em relação à expressão $\varepsilon_j = 2\cdot|\beta_j|\cdot\sup\{|\, e^{(1-\lambda).\beta_j}\cdot P(\lambda\beta_j)\,|: 0\le\lambda\le 1\}$.

Como $M = máx\{|\,\beta_1\,|, |\,\beta_2\,|, \ldots, |\,\beta_m\,|\}$, então é imediato que $|\,\beta_j\,|\le M$ para $j = 1,2,3,\ldots,m$.

Veremos, agora, que

$$\sup\{|\, e^{(1-\lambda).\beta_j}\cdot P(\lambda\beta_j)\,|: 0\le\lambda\le 1\} \le \sup\{|\, e^{(1-\lambda).M}\cdot P(\lambda\beta_j)\,|: 0\le\lambda\le 1\}$$

Seja $\beta_j = a_j + b_j.i,\ a_j, b_j \in R$. Então $|\,\beta_j\,| = \sqrt{a_j^2 + b_j^2} \le M$ e

$$e^{(1-\lambda).\beta_j} = e^{(1-\lambda).(a_j+b_j.i)} = e^{(1-\lambda).a_j+(1-\lambda)b_j.i} = e^{(1-\lambda).a_j}.e^{(1-\lambda).b_j.i} =$$
$$= e^{(1-\lambda).a_j}.(\cos[(1-\lambda)b_j] + i.sen[(1-\lambda)b_j]).$$

Utilizamos, no último passo, a Fórmula de Euler $\boldsymbol{e^{ix} = cosx + i.senx}$.

$$|\, e^{(1-\lambda).\beta_j}\,| = |\, e^{(1-\lambda).a_j}.(\cos[(1-\lambda)b_j] + i.sen[(1-\lambda)b_j])\,| =$$
$$= |\, e^{(1-\lambda).a_j}\,|.|\,(\cos[(1-\lambda)b_j] + i.sen[(1-\lambda)b_j])\,| =$$
$$= |\, e^{(1-\lambda).a_j}\,|.\sqrt{(\cos[(1-\lambda)b_j])^2 + (sen[(1-\lambda)b_j])^2} = |\, e^{(1-\lambda).a_j}\,|.1 =$$
$$= |\, e^{(1-\lambda).a_j}\,| = e^{(1-\lambda).a_j} \le e^{(1-\lambda).M}$$

pois $a_j \le \sqrt{a_j^2 + b_j^2} \le M$ e $(1 - \lambda) \ge 0$.

Então $|\, e^{(1-\lambda).\beta_j}\,| \le |\, e^{(1-\lambda).M}\,|$.

Logo, $\sup\{|\, e^{(1-\lambda).\beta_j}\cdot P(\lambda\beta_j)\,|: 0\le\lambda\le 1\} \le \sup\{|\, e^{(1-\lambda).M}\cdot P(\lambda\beta_j)\,|: 0\le\lambda\le 1\}$ o que termina a justificativa da desigualdade.

Continuando com a estimativa.

$$\varepsilon_j \le 2 \cdot M \cdot \sup\{|\, e^{(1-\lambda).M} \cdot P(\lambda\beta_j)\,| : 0 \le \lambda \le 1\}$$

Como $P(x) = \frac{c^s}{(p-1)!} \cdot x^{p-1} \cdot (R(x))^p$ e $e^{(1-\lambda).M} \le e^M$, pois $0 \le \lambda \le 1$, segue-se que:

$$\varepsilon_j \le 2 \cdot M \cdot e^M \cdot \sup\{|\, \frac{c^s}{(p-1)!}(\lambda\beta_j)^{p-1} \cdot (R(\lambda\beta_j))^p\,| : 0 \le \lambda \le 1\}\ .$$

Como $|\lambda\beta_j|^{p-1} = |\lambda|^{p-1}.|\beta_j|^{p-1} \le |\lambda|^{p-1}.|M|^{p-1} = (\lambda)^{p-1}.M^{p-1} = (\lambda.M)^{p-1}$ segue-se que

$$\varepsilon_j \le 2.M.e^M.\sup\{|\, \frac{c^s}{(p-1)!}(\lambda M)^{p-1}.(R(\lambda\beta_j))^p\,| : 0 \le \lambda \le 1\}$$

Como $\frac{c^s}{(p-1)!}$ e M são constantes e que $(\lambda.M)^{p-1} \le M^{p-1}$, podemos escrever

$$\varepsilon_j \le 2.M.e^M \cdot \frac{|c|^s}{(p-1)!} \cdot M^{p-1}.\sup\{|\, (R(\lambda\beta_j))^p\,| : 0 \le \lambda \le 1\}$$

Seja $N = máx\{|R(z)| : |z| < M\}$, o que nos fornece

$\varepsilon_j \le 2.M.e^M \cdot \frac{|c|^s}{(p-1)!}.M^{p-1}.N^p$. Sendo $s = m.p - 1$,

$$\varepsilon_j \le 2 \cdot M \cdot e^M \cdot \frac{|c|^{mp-1}}{(p-1)!} \cdot M^{p-1} \cdot N^p =$$
$$= 2 \cdot M \cdot e^M \cdot \frac{|c|^{mp-1+m-m}}{(p-1)!} \cdot M^{p-1} \cdot N^{p-1} \cdot N^1 =$$
$$= 2 \cdot M \cdot e^M \cdot N \cdot \frac{|c|^{m-1}.|c|^{mp-m}}{(p-1)!} \cdot M^{p-1} \cdot N^{p-1} =$$
$$= 2 \cdot M \cdot e^M \cdot N \cdot |c|^{m-1} \cdot \frac{(|c|^m)^{p-1}}{(p-1)!} \cdot M^{p-1} \cdot N^{p-1} =$$
$$= 2 \cdot M \cdot e^M \cdot N \cdot |c|^{m-1} \cdot \frac{(|c|^m \cdot M \cdot N)^{p-1}}{(p-1)!}$$

Então $\varepsilon_j \le 2 \cdot M \cdot e^M \cdot N \cdot |c|^{m-1} \cdot \frac{(|c|^m \cdot M \cdot N)^{p-1}}{(p-1)!}$

Fazendo $|c|^m \cdot M \cdot N = A$, temos:

$$\varepsilon_j \leq 2 \cdot M \cdot e^M \cdot N \cdot |c|^{m-1} \cdot \frac{A^{p-1}}{(p-1)!}$$

Vamos analisar, agora, qual é o comportamento da expressão $2 \cdot M \cdot e^M \cdot N \cdot |c|^{m-1} \cdot \frac{A^{p-1}}{(p-1)!}$, quando $p \to \infty$.

Como o fatorial domina qualquer exponencial, temos

$$\lim_{p\to\infty} 2 \cdot M \cdot e^M \cdot N \cdot |c|^{m-1} \cdot \frac{A^{p-1}}{(p-1)!} = 2 \cdot M \cdot e^M \cdot N \cdot |c|^{m-1} \cdot \lim_{p\to\infty} \frac{A^{p-1}}{(p-1)!} =$$
$$= 2 \cdot M \cdot e^M \cdot N \cdot |c|^{m-1} \cdot 0 = 0$$

para qualquer A > 0.

Então, para p suficientemente grande, podemos fazer $\varepsilon_j \leq \frac{1}{m+1}$, para j = 1, 2, 3, ..., m, o que nos dá:

$$\sum_{j=1}^{m} \varepsilon_j = \varepsilon_1 + \varepsilon_2 + \ldots + \varepsilon_m \leq \frac{1}{m+1} + \frac{1}{m+1} + \ldots + \frac{1}{m+1} = \frac{m}{m+1} < 1$$

ou seja, $\sum_{j=1}^{m} \varepsilon_j < 1$.

Então, na expressão $|k \cdot F(0) + \sum_{j=1}^{m} F(\beta_j)| \leq \sum_{j=1}^{m} \varepsilon_j$, temos

$$|k \cdot F(0) + \sum_{j=1}^{m} F(\beta_j)| \geq 1 \quad \text{e} \quad \sum_{j=1}^{m} \varepsilon_j < 1,$$

o que nos dá um absurdo.

Portanto, a suposição inicial de que π é um número algébrico é falsa.

Logo, π é transcendente.

CONSIDERAÇÕES FINAIS

As construções com régua e compasso já aparecem no século V a.C., época dos pitagóricos, e tiveram enorme importância no desenvolvimento da Matemática grega. A ciência grega fundamenta-se numa curiosidade altamente intelectual contrastando com o espírito prático do pensamento pré-helênico. "Na Grécia antiga, a palavra *número* era usada só para os inteiros, e uma fração era considerada apenas uma razão entre números. Esses conceitos naturalmente causavam dificuldade nas medidas das grandezas. A noção de número real estava ainda muito longe de ser concebida, mas, na época de Euclides (século III a.C.), uma idéia nova apareceu. As grandezas, no lugar de serem associadas a números, passaram a ser associadas a segmentos de reta. Assim, o conjunto dos números continuava discreto e o das grandezas contínuas passou a ser tratado por métodos geométricos. Nasce, então, nesse período, uma nova álgebra completamente geométrica, onde a palavra *resolver* era sinônimo de *construir"* (WAGNER, 1993, p. 1).

A questão da quadratura do círculo se apresenta como um problema geométrico. No entanto, para demonstrar a impossibilidade de quadrá-lo utilizando apenas régua e compasso, que levou mais de 20 séculos, foi necessário traduzi-lo para a linguagem algébrica e analisá-lo com as ferramentas do Cálculo e da Análise Matemática. Não se trata de uma aplicação prática da matemática, mas de uma questão teórica envolvendo uma distinção entre uma boa aproximação e a exatidão do pensamento.

A solução desse problema consistiu não em exibir a construção do quadrado com área igual à do círculo, mas em afirmar que não é possível efetuar tal construção. Isso não significa que a região quadrada proposta não exista, ao contrário, ela existe, mas não pode ser construída usando apenas régua e compasso. A impossibilidade é própria da construção.

Muitas tentativas foram realizadas sem sucesso e muitos erros foram cometidos na busca de uma solução para esse problema. Isso nos mostra que muitas descobertas e avanços que ocorrem nas Ciências e na Matemática são frutos de muito trabalho, investigação, dúvidas, persistência, erros, impregnados de condição humana, com suas forças e as suas fraquezas (CARAÇA, 1989, XIII).

Liouville, (1809-1882), foi o primeiro matemático a provar a existência de números transcendentes. Sua prova, em 1844, permitiu a construção de tais números, chamados "números de Liouville". Uma outra prova da existência de números transcendentes foi dada pelo matemático Georg Cantor (1845-1918), que não só demonstrou a existência desses números, mas também provou que o conjunto dos transcendentes é infinito, sem exibir um único número transcendente.

Em 1873, Hermite demonstrou que o número *e* (número de Euler) é transcendente. O método usado por Hermite para a demonstração da transcendência de *e* foi estendido por Lindemann, para demonstrar a transcendência do número π, em 1882.

A transcendência de π estabeleceu de uma vez por todas a impossibilidade de quadrar o círculo usando régua e compasso, que pode ser resumida da seguinte forma:

i) Vimos que todo número construtível é algébrico.

ii) Supondo que seja possível quadrar o círculo de raio igual a 1, poderíamos construir, com régua e compasso, um quadrado de área igual a π. Essa afirmação equivale a dizer que poderíamos construir um quadrado de lado igual $\sqrt{\pi}$, ou seja, $\sqrt{\pi}$ seria um número construtível.

iii) Se $\sqrt{\pi}$ é construtível, então, π também é construtível. Como todo número construtível é algébrico, então, π seria algébrico.

iv) Absurdo, pois foi provado que π é transcendente.

v) Esse absurdo é conseqüência da possibilidade de quadrar o círculo com régua e compasso, dada em **ii**. Portanto, essa suposição é falsa. Logo, vale a sua negação, ou seja, não é possível construir, usando régua e compasso, um quadrado com área igual à do círculo.

Se fosse possível quadrar o círculo com régua e compasso, o número π seria construtível e, portanto, algébrico, gerando uma contradição, pois π é transcendente.

No estudo que fizemos sobre a quadratura do círculo, fez-se necessário conhecer um pouco mais sobre a natureza dos números e suas propriedades e, sem dúvida, fazer muita interação matemática entre o contínuo e o discreto, o real e o complexo, o racional e o irracional, o algébrico e o transcendente, a geometria, a álgebra e a análise, o finito e o infinito, o enumerável e o não enumerável, as igualdades e as desigualdades, os números, as funções, os limites, as seqüências, as séries, os polinômios.

Neste trabalho, constatamos que as demonstrações desempenham um papel fundamental no estudo da matemática e que, para efetuá-las, às vezes é necessário o desenvolvimento e a criação de novas teorias.

Esperamos que este trabalho ofereça aos professores e aos alunos de licenciatura em matemática um material a mais de consulta sobre o problema da quadratura do círculo e a natureza dos números, especialmente sobre o número π.

REFERÊNCIAS

ALVES, Alessandro Ferreira. *Algumas importantes constantes em matemática*. 1999. Dissertação (mestrado em matemática) Instituto de Matemática, Estatística e Computação Científica, UNICAMP, Campinas, SP.

AUGUSTINI, Edson; OLIVEIRA, Anselmo A. de A.; SILVA, Uziel P. da. *A transcendência do número π.* FAMAT em revista, Universidade Federal de Uberlândia, MG, abril de 2005, n. 4, p. 69-86.

BEZERRA, Manoel Jairo. *Curso de matemática*. 17.ed. São Paulo: Companhia Editora Nacional, 1965.

BOYER, Carl Benjamin. *História da matemática*. Tradução por Elza F. Gomide. São Paulo: Edgard Blücher, 1974.

CARAÇA, Bento de Jesus. *Conceitos fundamentais da matemática.* 9.ed. Portugal, Lisboa: Livraria Sá da Costa Editora, 1989.

COURANT, Richard; ROBBINS, Herbert. *O que é matemática?*. Tradução por Adalberto da Silva Brito. Rio de Janeiro: Ciência Moderna, 2000.

DANTZIG, Tobias. *Número: a linguagem da ciência*. Tradução por Sérgio Góes de Paula. Rio de Janeiro: Zahar Editores, 1970.

DAVIS, Philip J; HERSH, Reuben. *A experiência matemática*. Tradução por João Bosco Pitombeira. 4.ed. Rio de Janeiro: Francisco Alves, 1989. 481p.

DELAHAYE, Jean-Paul. *Le fascinant nombre π.* France, Paris: Bibliotèque Scientifique, 1997.

EVES, Howard. *Introdução à história da matemática*. Tradução por Higyno H. Domingues. Campinas, SP: Editora da Unicamp, 2004.

FIGUEIREDO, Djairo Guedes de. *Números irracionais e transcendentes*. Brasília: 1985. 101p. Coleção Fundamentos da Matemática Elementar. Sociedade Brasileira de Matemática.

GOMES, Carlos A. *Polinômios Simétricos*. Disponível em <*www.oei.es/oim/revistaoim/numero24/gomes.pdf*>. Acesso em: 12 out. 2008. UFRN, Natal, RN.

HOGBEN, Lancelot. *Maravilhas da Matemática.* Tradução por Paulo Moreira da Silva. 2.ed. Porto Alegre: Editora Globo, 1950. 1v.

IMENES, Luiz Marcio Pereira; JAKUBOVIC, José; TROTTA, Fernando. *Matemática Aplicada.* São Paulo: Moderna Ltda, 1979. 2v.

_____. *Matemática Aplicada: manual do professor.* São Paulo: Moderna Ltda, 1979. 2v.

KAPLANSKY, I. *Introdução à teoria de Galois*. Notas redigidas por Elon Lages Lima. Rio de Janeiro: 1958. 153p. Notas de Matemática n.13. Coleção publicada sob a direção de L.Nachbin. Fascículo publicado pelo Instituto de Matemática Pura e Aplicada do Conselho Nacional de Pesquisas.

KARLSON, Paul. *A magia dos números*. Tradução por Henrique Carlos Pfeifer, Eugênio Brito e Frederico Porta. Porto Alegre: Editora Globo, 1961.

KASNER, Edward; NEWMAN, James. *Matemática e imaginação*. Tradução por Jorge Fortes. Rio de Janeiro: Zahar Editores, 1968.

LARS, Garding. *Encontro com a matemática*. Tradução por Célio W. Manzi Alvarenga e Maria Manuela V. Marques M. Alvarenga. 2.ed. Brasília: Editora Universidade de Brasília, 1997.

LAVILLE, Christian; DIONNE, Jean. *A construção do saber: manual de metodologia da pesquisa em ciências humanas.*Tradução por Heloísa Monteiro e Francisco Settineri. Revisão técnica e adaptação da obra: Lana Mara Siman. Porto Alegre: Editora Artes Médicas Sul Ltda.; Belo Horizonte: Editora UFMG, 1999.

LIMA, Elon Lages. Conceitos e controvérsias. *Revista do Professor de Matemática* – RPM, São Paulo, n. 3, p. 22-23, 2º semestre de 1983. Sociedade Brasileira de Matemática.

MACHADO, Nilson José; GRANJA, Carlos Eduardo de Souza Campos; MELLO, José Luiz Pastore; MOISÉS, Roberto Perides; SPINELLI, Walter. *Caderno do professor: matemática* – 8ª. série, 4º bimestre, Secretaria da Educação; coordenação geral Maria Inês Fini. São Paulo: SEE, 2008.

MAOR, Eli. *e: a história de um número*. Tradução por Jorge Calife. 3.ed. Rio de Janeiro: Record, 2006.

NIVEN, Ivan Morton. *Números: racionais e irracionais*. Tradução por Renate Watanabe. Rio de Janeiro: 1984, 216p. Coleção Fundamentos da Matemática Elementar. Sociedade Brasileira de Matemática.

SINGH, Simon. *O último teorema de Fermat*. Tradução por Jorge Luiz Calife. 4.ed. Rio de Janeiro: Record, 1999.

SPIVAK, Michael. *Cálculo Infinitesimal.* Espanha: Editorial Reverte, S.A. 2v.

STRUIK, Dirk J. *História concisa das matemáticas*. Tradução por João Cosme Santos Guerreiro. 3.ed. Lisboa: Gradiva, 1997.

WAGNER, Eduardo. *Construções geométricas*. 4.ed. Rio de Janeiro: 1993. Coleção Professor de Matemática. Sociedade Brasileira de Matemática.

ANEXOS

Anexo I

Para cada valor inteiro e positivo de $h \geq 2$, existe um número finito de equações $a_n \cdot x^n + a_{n-1} \cdot x^{n-1} + ... + a_1 \cdot x + a_0 = 0$ com coeficientes inteiros, $a_n > 0$, sendo $h = n + a_n + |a_{n-1}| + ... + |a_2| + |a_1| + |a_0|$ sua altura.

Para mostrar esse resultado, utilizaremos as combinações completas $CR_k^p = \binom{k+p-1}{p} = \frac{(k+p-1)!}{p!.(k-1)!}$ para determinar o número de soluções inteiras e não negativas da equação $x_1 + x_2 + ... + x_k = p$, p um inteiro positivo.

Dada a equação $a_n \cdot x^n + a_{n-1} \cdot x^{n-1} + ... + a_1 \cdot x + a_0 = 0$ com coeficientes inteiros, $a_n > 0$, e sua altura $h = n + a_n + |a_{n-1}| + ... + |a_2| + |a_1| + |a_0|$, temos que $a_n + |a_{n-1}| + ... + |a_2| + |a_1| + |a_0| = h - n$.

Como $a_n > 0$, devemos ter $1 \leq n \leq h-1$.

Dado $h \geq 2$ (h fixo), vamos determinar o número de equações com altura h para $n = 1$, $n = 2$, $n = 3$,..., $n = h - 1$, e em seguida somar todas essas quantidades, obtendo o número de equações com essa altura h.

Para ***n* = 1,** temos as equações $a_1 x + a_0 = 0$, $a_1 > 0$ *e* $a_1 + |a_0| = h - 1$.

1º caso: $a_1 > 0,\ a_0 > 0$

Fazendo $a_1 = 1 + b_1$ e $a_0 = 1 + b_0$, temos: $a_1 + a_0 = 1 + b_1 + 1 + b_0 = h - 1$, ou seja: $b_1 + b_0 = h - 3$. Então $CR_2^{h-3} = \binom{2 + h - 3 - 1}{h - 3} = \binom{h-2}{h-3}$.

Considerando $\pm a_0$, temos então $2.\binom{h-2}{h-3}$ equações.

2º caso: $a_1 > 0,\ a_0 = 0$

Fazendo $a_1 = 1 + b_1$ e $a_0 = 0$, temos: $a_1 + a_0 = 1 + b_1 + 0 = h - 1$, ou seja, $b_1 = h - 2$. Então $CR_1^{h-2} = \binom{1 + h - 2 - 1}{h - 2} = \binom{h-2}{h-2} = 1$ equação, dada por $(h-1) \cdot x^1 = 0$.

Portanto, o número de equações do 1º grau com altura *h* (*h* fixo) é igual a $\binom{1}{0} \cdot 2^1 \cdot \binom{h-2}{h-3} + \binom{1}{1} \cdot 2^0 \cdot \binom{h-2}{h-2} = \sum_{j=0}^{1} \binom{1}{j} \cdot 2^{1-j} \cdot \binom{h-2}{h-3+j}$.

Para ***n* = 2,** temos as equações

$$a_2 \cdot x^2 + a_1 \cdot x + a_0 = 0,\ a_2 > 0 \ e\ \ a_2 + |a_1| + |a_0| = h - 2.$$

1º caso: $a_2 > 0,\ a_1 > 0,\ a_0 > 0$

Fazendo $a_2 = 1 + b_2$, $a_1 = 1 + b_1$ e $a_0 = 1 + b_0$, temos:

$a_2 + a_1 + a_0 = 1 + b_2 + 1 + b_1 + 1 + b_0 = h - 2$, ou seja, $b_2 + b_1 + b_0 = h - 5$.

Então $CR_3^{h-5} = \binom{3 + h - 5 - 1}{h - 5} = \binom{h-3}{h-5}$.

Considerando $\pm a_1, \pm a_0$, temos $2^2 \cdot \binom{h-3}{h-5}$ equações.

2º caso: $a_2 > 0,\ a_1 > 0,\ a_0 = 0$

Fazendo $a_2 = 1 + b_2$, $a_1 = 1 + b_1$ e $a_0 = 0$, temos:

$$a_2 + a_1 + a_0 = 1 + b_2 + 1 + b_1 + 0 = h - 2, \text{ ou seja, } b_2 + b_1 = h - 4.$$

Então $CR_2^{h-4} = \binom{2+h-4-1}{h-4} = \binom{h-3}{h-4}$.

Considerando $\pm a_1$, temos $2 \cdot \binom{h-3}{h-4}$ equações.

3º caso: $a_2 > 0,\ a_1 = 0,\ a_0 > 0$

Sendo análogo ao caso anterior, nesse temos também $2 \cdot \binom{h-3}{h-4}$ equações.

4º caso: $a_2 > 0,\ a_1 = a_0 = 0$

Fazendo $a_2 = 1 + b_2$ e $a_1 = a_0 = 0$, temos: $a_2 + a_1 + a_0 = 1 + b_2 + 0 + 0 = h - 2$, ou seja, $b_2 = h - 3$.

Então $CR_1^{h-3} = \binom{1+h-3-1}{h-3} = \binom{h-3}{h-3} = 1$ equação, dada por $(h-2) \cdot x^2 = 0$.

Portanto, o número de equações do 2º grau com altura h (h fixo) é igual a $\binom{2}{0} \cdot 2^2 \cdot \binom{h-3}{h-5} + \binom{2}{1} \cdot 2^1 \cdot \binom{h-3}{h-4} + \binom{2}{2} \cdot 2^0 \cdot \binom{h-3}{h-3} = \sum_{j=0}^{2} \binom{2}{j} \cdot 2^{2-j} \cdot \binom{h-3}{h-5+j}$.

Para ***n* = 3,** temos as equações $a_3 \cdot x^3 + a_2 \cdot x^2 + a_1 \cdot x + a_0 = 0,\ a_3 > 0$ e $a_3 + |a_2| + |a_1| + |a_0| = h - 3$.

1º caso: $a_3 > 0, a_2 > 0,\ a_1 > 0,\ a_0 > 0$

Fazendo $a_3 = 1 + b_3$, $a_2 = 1 + b_2$, $a_1 = 1 + b_1$ e $a_0 = 1 + b_0$, temos:

$a_3 + a_2 + a_1 + a_0 = 1 + b_3 + 1 + b_2 + 1 + b_1 + 1 + b_0 = h - 3$, ou seja, $b_3 + b_2 + b_1 + b_0 = h - 7$.

Então $CR_4^{h-7} = \binom{4+h-7-1}{h-7} = \binom{h-4}{h-7}$.

Considerando $\pm a_2$, $\pm a_1$, $\pm a_0$, temos $2^3 \cdot \binom{h-4}{h-7}$ equações.

2º caso: $a_3 > 0, a_2 > 0,\ a_1 > 0,\ a_0 = 0$

Fazendo $a_3 = 1 + b_3$, $a_2 = 1 + b_2$, $a_1 = 1 + b_1$ e $a_0 = 0$, temos:

$a_3 + a_2 + a_1 + a_0 = 1 + b_3 + 1 + b_2 + 1 + b_1 + 0 = h - 3$, ou seja, $b_3 + b_2 + b_1 = h - 6$.

Então $CR_3^{h-6} = \begin{pmatrix} 3 + h - 6 - 1 \\ h - 6 \end{pmatrix} = \begin{pmatrix} h - 4 \\ h - 6 \end{pmatrix}$.

Considerando $\pm a_2$, $\pm a_1$, temos $2^2 \cdot \begin{pmatrix} h - 4 \\ h - 6 \end{pmatrix}$ equações.

Para cada um dos casos

$$a_3 > 0, a_2 > 0,\ a_1 = 0,\ a_0 > 0 \quad \text{e} \quad a_3 > 0, a_2 = 0,\ a_1 > 0,\ a_0 > 0$$

temos também $2^2 \cdot \begin{pmatrix} h - 4 \\ h - 6 \end{pmatrix}$ equações.

Portanto temos um total de $\begin{pmatrix} 3 \\ 1 \end{pmatrix} \cdot 2^2 \cdot \begin{pmatrix} h - 4 \\ h - 6 \end{pmatrix}$ equações.

3º caso: $a_3 > 0,\ a_2 > 0,\ a_1 = a_0 = 0$

Fazendo $a_3 = 1 + b_3$, $a_2 = 1 + b_2$, $a_1 = a_0 = 0$, temos:

$a_3 + a_2 + a_1 + a_0 = 1 + b_3 + 1 + b_2 + 0 + 0 = h - 3$, ou seja, $b_3 + b_2 = h - 5$.

Então $CR_2^{h-5} = \begin{pmatrix} 2 + h - 5 - 1 \\ h - 5 \end{pmatrix} = \begin{pmatrix} h - 4 \\ h - 5 \end{pmatrix}$.

Considerando $\pm a_2$, temos $2 \cdot \begin{pmatrix} h - 4 \\ h - 5 \end{pmatrix}$ equações.

Para cada um dos casos

$$a_3 > 0,\ a_2 = 0,\ a_1 > 0,\ a_0 = 0 \quad \text{e} \quad a_3 > 0,\ a_2 = 0,\ a_1 = 0,\ a_0 > 0$$

temos também $2 \cdot \begin{pmatrix} h - 4 \\ h - 5 \end{pmatrix}$ equações.

Portanto, temos um total de $\begin{pmatrix} 3 \\ 2 \end{pmatrix} \cdot 2^1 \cdot \begin{pmatrix} h - 4 \\ h - 5 \end{pmatrix}$ equações.

4º caso: $a_3 > 0,\ a_2 = 0,\ a_1 = 0,\ a_0 = 0$

Fazendo $a_3 = 1 + b_3,\ a_2 = a_1 = a_0 = 0$, temos:

$$a_3 + a_2 + a_1 + a_0 = 1 + b_3 + 0 + 0 + 0 = h - 3$$, ou seja, $b_3 = h - 4$.

Então $CR_1^{h-4} = \binom{1 + h - 4 - 1}{h - 4} = \binom{h-4}{h-4} = 1$ equação, dada por $(h-3) \cdot x^3 = 0$.

Portanto, o número de equações do 3º grau com altura *h* (*h* fixo) é igual a

$$\binom{3}{0} \cdot 2^3 \cdot \binom{h-4}{h-7} + \binom{3}{1} \cdot 2^2 \cdot \binom{h-4}{h-6} + \binom{3}{2} \cdot 2^1 \cdot \binom{h-4}{h-5} + \binom{3}{3} \cdot 2^0 \cdot \binom{h-4}{h-4} =$$

.

$$= \sum_{j=0}^{3} \binom{3}{j} \cdot 2^{3-j} \cdot \binom{h-4}{h-7+j}$$

Para ***n* = 4,** temos as equações $a_4 \cdot x^4 + a_3 \cdot x^3 + a_2 \cdot x^2 + a_1 \cdot x + a_0 = 0,\ a_4 > 0$ e $a_4 + |a_3| + |a_2| + |a_1| + |a_0| = h - 4$.

1º caso: $a_4 > 0,\ a_3 > 0, a_2 > 0,\ a_1 > 0,\ a_0 > 0$

Fazendo $a_4 = 1 + b_4\ a_3 = 1 + b_3$, $a_2 = 1 + b_2$, $a_1 = 1 + b_1$ e $a_0 = 1 + b_0$, temos:

$$a_4 + a_3 + a_2 + a_1 + a_0 = 1 + b_4 + 1 + b_3 + 1 + b_2 + 1 + b_1 + 1 + b_0 = h - 4,$$

ou seja,

$$b_4 + b_3 + b_2 + b_1 + b_0 = h - 9.$$

Então $CR_5^{h-9} = \binom{5 + h - 9 - 1}{h - 9} = \binom{h-5}{h-9}$.

Considerando $\pm a_3, \pm a_2, \pm a_1, \pm a_0$, temos $2^4 \cdot \binom{h-5}{h-9}$ equações.

2º caso: $a_4 > 0,\ a_3 > 0, a_2 > 0,\ a_1 > 0,\ a_0 = 0$

Fazendo $a_4 = 1 + b_4$, $a_3 = 1 + b_3$, $a_2 = 1 + b_2$, $a_1 = 1 + b_1$ e $a_0 = 0$, temos:

$$a_4 + a_3 + a_2 + a_1 + a_0 = 1 + b_4 + 1 + b_3 + 1 + b_2 + 1 + b_1 + 0 = h - 4,$$

ou seja,

$$b_4 + b_3 + b_2 + b_1 = h - 8 .$$

Então $CR_4^{h-8} = \binom{4+h-8-1}{h-8} = \binom{h-5}{h-8}$.

Considerando $\pm a_3$, $\pm a_2$, $\pm a_1$, temos $2 \cdot \binom{h-5}{h-8}$ equações.

Para cada um dos outros três casos $a_4 > 0,\ a_3 > 0, a_2 > 0,\ a_1 = 0,\ a_0 > 0$, $a_4 > 0,\ a_3 > 0,\ a_2 = 0,\ a_1 > 0,\ a_0 > 0$, $a_4 > 0,\ a_3 = 0,\ a_2 > 0,\ a_1 > 0,\ a_0 > 0$, temos também $2^3 \cdot \binom{h-5}{h-8}$ equações.

Portanto, temos um total de $\binom{4}{1} \cdot 2^3 \cdot \binom{h-5}{h-8}$ equações.

3º caso: $a_4 > 0,\ a_3 > 0, a_2 > 0,\ a_1 = 0,\ a_0 = 0$

Fazendo $a_4 = 1 + b_4$, $a_3 = 1 + b_3$, $a_2 = 1 + b_2$, $a_1 = 0$ e $a_0 = 0$, temos:

$$a_4 + a_3 + a_2 + a_1 + a_0 = 1 + b_4 + 1 + b_3 + 1 + b_2 + 0 + 0 = h - 4 ,$$

ou seja,

$$b_4 + b_3 + b_2 = h - 7 .$$

Então $CR_3^{h-7} = \binom{3+h-7-1}{h-7} = \binom{h-5}{h-7}$.

Considerando $\pm a_3$, $\pm a_2$, temos $2^2 \cdot \binom{h-5}{h-7}$ equações.

Considerando as outras possibilidades, teremos um total de $\binom{4}{2} \cdot 2^2 \cdot \binom{h-5}{h-7}$ equações.

4º caso: $a_4 > 0,\ a_3 > 0, a_2 = 0,\ a_1 = 0,\ a_0 = 0$

Fazendo $a_4 = 1 + b_4$, $a_3 = 1 + b_3$, $a_2 = 0$, $a_1 = 0$ e $a_0 = 0$, temos:

$$a_4 + a_3 + a_2 + a_1 + a_0 = 1 + b_4 + 1 + b_3 + 0 + 0 + 0 = h - 4,$$

ou seja,

$$b_4 + b_3 = h - 6.$$

Então $CR_2^{h-6} = \binom{2 + h - 6 - 1}{h - 6} = \binom{h-5}{h-6}$.

Considerando $\pm a_3$, temos $2.\binom{h-5}{h-6}$ equações.

Considerando as outras possibilidades, teremos um total de $\binom{4}{3} \cdot 2 \cdot \binom{h-5}{h-6}$ equações.

5º caso: $a_4 > 0,\ a_3 = 0, a_2 = 0,\ a_1 = 0,\ a_0 = 0$

Fazendo $a_4 = 1 + b_4$, $a_3 = 0$, $a_2 = 0$, $a_1 = 0$ e $a_0 = 0$, temos:

$$a_4 + a_3 + a_2 + a_1 + a_0 = 1 + b_4 + 0 + 0 + 0 + 0 = h - 4,$$

ou seja,

$$b_4 = h - 5.$$

Então $CR_1^{h-5} = \binom{1 + h - 5 - 1}{h - 5} = \binom{h-5}{h-5} = 1$ equação, que é dada por $(h-4) \cdot x^4 = 0.$

Portanto, o número de equações do 4º grau com altura *h* (*h* fixo) é igual a

$$\binom{4}{0} \cdot 2^4 \cdot \binom{h-5}{h-9} + \binom{4}{1} \cdot 2^3 \cdot \binom{h-5}{h-8} + \binom{4}{2} \cdot 2^2 \cdot \binom{h-5}{h-7} + \binom{4}{3} \cdot 2^1 \cdot \binom{h-5}{h-6} + \binom{4}{4} \cdot 2^0 \cdot \binom{h-5}{h-5} =$$

$$= \sum_{j=0}^{4} \binom{4}{j} \cdot 2^{4-j} \cdot \binom{h-5}{h-9+j}$$

Para $\boldsymbol{n = 5}$, temos as equações

$$a_5 \cdot x^5 + a_4 \cdot x^4 + a_3 \cdot x^3 + a_2 \cdot x^2 + a_1 \cdot x + a_0 = 0,\ a_5 > 0 \text{ e}$$

$$a_5 + |\, a_4 \,| + |\, a_3 \,| + |\, a_2 \,| + |\, a_1 \,| + |\, a_0 \,| = h - 5 .$$

Analogamente, o número de equações do 5º grau com altura h (h fixo) é igual a

$$\binom{5}{0} \cdot 2^5 \cdot \binom{h-6}{h-11} + \binom{5}{1} \cdot 2^4 \cdot \binom{h-6}{h-10} + \binom{5}{2} \cdot 2^3 \cdot \binom{h-6}{h-9} + \binom{5}{3} \cdot 2^2 \cdot \binom{h-6}{h-8} + \binom{5}{4} \cdot 2^1 \cdot \binom{h-6}{h-7} +$$

$$+ \binom{5}{5} \cdot 2^0 \cdot \binom{h-6}{h-6} = \sum_{j=0}^{5} \binom{5}{j} \cdot 2^{5-j} \cdot \binom{h-6}{h-11+j}$$

Como $1 \le n \le h-1$, este procedimento termina para $n = h-1$. Neste caso, temos a equação $a_{h-1} \cdot x^{h-1} + a_{h-2} \cdot x^{h-2} + \ldots + a_2 \cdot x^2 + a_1 \cdot x + a_0 = 0,\ a_{h-1} > 0$ e $a_{h-1} + |\, a_{h-2} \,| + \ldots + |\, a_2 \,| + |\, a_1 \,| + |\, a_0 \,| = h - (h-1) = 1$. Como $a_{h-1} > 0$, temos apenas o caso em que $a_{h-1} = 1$ e $a_{h-2} = \ldots = a_2 = a_1 = a_0 = 0$, ou seja, temos uma única equação com altura h e $n = h-1$, que é dada por $1 \cdot x^{h-1} = 0$.

Somando o número de equações para cada valor de n, $1 \le n \le h-1$, temos:

$$N = \sum_{j=0}^{1} \binom{1}{j} \cdot 2^{1-j} \cdot \binom{h-2}{h-3+j} + \sum_{j=0}^{2} \binom{2}{j} \cdot 2^{2-j} \cdot \binom{h-3}{h-5+j} + \sum_{j=0}^{3} \binom{3}{j} \cdot 2^{3-j} \cdot \binom{h-4}{h-7+j} +$$

$$+ \sum_{j=0}^{4} \binom{4}{j} \cdot 2^{4-j} \cdot \binom{h-5}{h-9+j} + \ldots + \sum_{j=0}^{h-1} \binom{h-1}{j} \cdot 2^{h-1-j} \cdot \binom{h-(h-1)-1}{h-[2(h-1)+1]+j} =$$

$$= \sum_{n=1}^{h-1} \left[\sum_{j=0}^{n} \binom{n}{j} \cdot 2^{n-j} \cdot \binom{h-n-1}{h-(2n+1)+j} \right]$$

Essa fórmula, desde que sejam satisfeitas as condições de existência no cálculo das combinações, dá o número de equações com altura h (h fixo).

Portanto, o número de equações com altura h é finito.

Vejamos 4 exemplos que ilustram o uso dessa fórmula.

1. Para $h = 2$.

$$N = \sum_{n=1}^{1}\left[\sum_{j=0}^{n}\binom{n}{j}\cdot 2^{n-j}\cdot\binom{1-n}{2-(2n+1)+j}\right] = \sum_{j=0}^{1}\binom{1}{j}\cdot 2^{1-j}\cdot\binom{0}{j-1} =$$

$$= \binom{1}{0}\cdot 2^{1}\cdot\binom{0}{-1} + \binom{1}{1}.2^{0}\cdot\binom{0}{0}$$

Desconsiderando o termo $\binom{1}{0}\cdot 2^{1}\cdot\binom{0}{-1}$, que não satisfaz às condições de existência, temos $N = 1$.

Nesse caso, temos uma única equação com altura $h = 2$, que é dada por $x = 0$.

2. Para $h = 3$.

$$N = \sum_{n=1}^{2}\left[\sum_{j=0}^{n}\binom{n}{j}\cdot 2^{n-j}\cdot\binom{2-n}{3-(2n+1)+j}\right] = \sum_{j=0}^{1}\binom{1}{j}\cdot 2^{1-j}\cdot\binom{1}{j} + \sum_{j=0}^{2}\binom{2}{j}\cdot 2^{2-j}\cdot\binom{0}{j-2} =$$

$$= \binom{1}{0}\cdot 2^{1}\cdot\binom{1}{0} + \binom{1}{1}.2^{0}\cdot\binom{1}{1} + \binom{2}{0}\cdot 2^{2}\cdot\binom{0}{-2} + \binom{2}{1}.2^{1}\cdot\binom{0}{-1} + \binom{2}{2}.2^{0}\cdot\binom{0}{0}$$

Desconsiderando os termos $\binom{2}{0}\cdot 2^{2}\cdot\binom{0}{-2}$ e $\binom{2}{1}.2^{1}\cdot\binom{0}{-1}$ que não satisfazem as condições de existência, temos $N = 3+1 = 4$.

Nesse caso temos:

- 3 equações de grau 1: $2x = 0$, $x + 1 = 0$ e $x - 1 = 0$.
- 1 equação de grau 2: $x^2 = 0$

3. Para $h = 4$.

$$N = \sum_{n=1}^{3}\left[\sum_{j=0}^{n}\binom{n}{j}\cdot 2^{n-j}\cdot\binom{3-n}{4-(2n+1)+j}\right] =$$

$$= \sum_{j=0}^{1}\binom{1}{j}\cdot 2^{1-j}\cdot\binom{2}{1+j} + \sum_{j=0}^{2}\binom{2}{j}\cdot 2^{2-j}\cdot\binom{1}{j-1} + \sum_{j=0}^{3}\binom{3}{j}\cdot 2^{3-j}\cdot\binom{0}{j-3} =$$

$$= \binom{1}{0}\cdot 2^{1}\cdot\binom{2}{1} + \binom{1}{1}.2^{0}\cdot\binom{2}{2} + \binom{2}{0}\cdot 2^{2}\cdot\binom{1}{-1} + \binom{2}{1}.2^{1}\cdot\binom{1}{0} + \binom{2}{2}.2^{0}\cdot\binom{1}{1} +$$

$$+ \binom{3}{0}.2^{3}\cdot\binom{0}{-3} + \binom{3}{1}\cdot 2^{2}\cdot\binom{0}{-2} + \binom{3}{2}.2^{1}\cdot\binom{0}{-1} + \binom{3}{3}.2^{0}\cdot\binom{0}{0}$$

Desconsiderando os termos que não satisfazem as condições de existência, temos $N = 4 + 1 + 4 + 1 + 1 = 11$.

Nesse caso temos:

- 5 equações de grau 1: $3x = 0$, $2x + 1 = 0$, $2x - 1 = 0$, $x + 2 = 0$ e $x - 2 = 0$.
- 5 equações de grau 2: $2x^2 = 0$, $x^2 + 1 = 0$, $x^2 - 1 = 0$, $x^2 + x = 0$, $x^2 - x = 0$.
- 1 equação de grau 3: $x^3 = 0$.

4. Para $h = 5$.

$$N = \sum_{n=1}^{4}\left[\sum_{j=0}^{n}\binom{n}{j}\cdot 2^{n-j}\cdot\binom{4-n}{5-(2n+1)+j}\right] =$$

$$= \sum_{j=0}^{1}\binom{1}{j}\cdot 2^{1-j}\cdot\binom{3}{2+j} + \sum_{j=0}^{2}\binom{2}{j}\cdot 2^{2-j}\cdot\binom{2}{j} + \sum_{j=0}^{3}\binom{3}{j}\cdot 2^{3-j}\cdot\binom{1}{j-2} + \sum_{j=0}^{4}\binom{4}{j}\cdot 2^{4-j}\cdot\binom{0}{j-4} =$$

$$= \binom{1}{0}\cdot 2^{1}\cdot\binom{3}{2} + \binom{1}{1}\cdot 2^{0}\cdot\binom{3}{3} + \binom{2}{0}\cdot 2^{2}\cdot\binom{2}{0} + \binom{2}{1}\cdot 2^{1}\cdot\binom{2}{1} + \binom{2}{2}\cdot 2^{0}\cdot\binom{2}{2} + \binom{3}{0}\cdot 2^{3}\cdot\binom{1}{-2} +$$

$$+ \binom{3}{1}\cdot 2^{2}\cdot\binom{1}{-1} + \binom{3}{2}\cdot 2^{1}\cdot\binom{1}{0} + \binom{3}{3}\cdot 2^{0}\cdot\binom{1}{1} + \binom{4}{0}\cdot 2^{4}\cdot\binom{0}{-4} + \binom{4}{1}\cdot 2^{3}\cdot\binom{0}{-3} + \binom{4}{2}\cdot 2^{2}\cdot\binom{0}{-2} +$$

$$+ \binom{4}{3}\cdot 2^{1}\cdot\binom{0}{-1} + \binom{4}{4}\cdot 2^{0}\cdot\binom{0}{0}$$

Desconsiderando os termos que não satisfazem as condições de existência, temos $N = 6 + 1 + 4 + 8 + 1 + 6 + 1 + 1 = 28$.

Nesse caso temos:

- 7 equações de grau 1: $x + 3 = 0$, $x - 3 = 0$, $2x + 2 = 0$, $2x - 2 = 0$, $3x + 1 = 0$, $3x - 1 = 0$, $4x = 0$.
- 13 equações de grau 2: $x^2 + x + 1 = 0$, $x^2 + x - 1 = 0$, $x^2 - x + 1 = 0$, $x^2 - x - 1 = 0$, $x^2 + 2x = 0$, $x^2 - 2x = 0$, $x^2 + 2 = 0$, $x^2 - 2 = 0$, $2x^2 + x = 0$, $2x^2 - x = 0$, $2x^2 + 1 = 0$, $2x^2 + 1 = 0$ e $3x^2 = 0$.
- 7 equações de grau 3: $x^3 + x^2 = 0$, $x^3 - x^2 = 0$, $x^3 + x = 0$, $x^3 - x = 0$, $x^3 + 1 = 0$, $x^3 - 1 = 0$, $2x^3 = 0$.
- 1 equação de grau 4: $1x^4 = 0$.

Anexo II

A Fórmula de Euler

Euler adotou como base de suas exponenciais e seus logaritmos o número $e = 2{,}718281... = \lim_{n\to\infty}\left(1+\frac{1}{n}\right)^n$.

O número *e*, assim como o número π, além de serem irracionais, são transcendentes.

A teoria da exponencial e do logaritmo tem como ponto de partida, segundo Euler, a definição da potência e^z, onde o expoente $z = x + iy$ é um número complexo.

Do Cálculo, temos que para todo número real x,

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

Da mesma forma, a definição da exponencial e^z, onde $z = x + iy$ é um número complexo, é dada por:

$$e^z = 1 + z + \frac{z^2}{2!} + \frac{z^3}{3!} + ... + \frac{z^n}{n!} + ...$$

Desenvolvendo *senx* e *cosx* em série, temos:

$$senx = x - \frac{x^3}{3!} + \frac{x^5}{5!} - \frac{x^7}{7!} + \frac{x^9}{9!} - ... + (-1)^n.\frac{x^{2n+1}}{(2n+1)!} + ...$$

$$\cos x = 1 - \frac{x^2}{2!} + \frac{x^4}{4!} - \frac{x^6}{6!} + \frac{x^8}{8!} - ... + (-1)^n.\frac{x^{2n}}{(2n)!} + ...$$

Para $z = iy$, temos:

$$e^{iy} = 1 + iy + \frac{(iy)^2}{2!} + \frac{(iy)^3}{3!} + \frac{(iy)^4}{4!} + \frac{(iy)^5}{5!} + \frac{(iy)^6}{6!} + \frac{(iy)^7}{7!} + \frac{(iy)^8}{8!} + \frac{(iy)^9}{9!} + ...$$

Calculando as potência de *i*, que pertencem ao conjunto { *i,* -1*, -i ,* 1}, temos

$$e^{iy} = 1 + iy - \frac{y^2}{2!} - i\cdot\frac{y^3}{3!} + \frac{y^4}{4!} + i\cdot\frac{y^5}{5!} - \frac{y^6}{6!} - i\cdot\frac{y^7}{7!} + \frac{y^8}{8!} + i\cdot\frac{y^9}{9!} + ...$$

Agrupando as partes reais e imaginárias temos:

$$e^{iy} = \left(1 - \frac{y^2}{2!} + \frac{y^4}{4!} - \frac{y^6}{6!} + \frac{y^8}{8!} - \ldots\right) + i.\left(y - \frac{y^3}{3!} + \frac{y^5}{5!} - \frac{y^7}{7!} + \frac{y^9}{9!} - \ldots\right)$$

ou seja, $e^{iy} = \cos y + i.seny$, que é a Fórmula de Euler.

Para $y = \pi$, temos a seguinte igualdade:

$$e^{i\pi} = \cos\pi + isen\pi$$
$$e^{i\pi} = -1 + i.0 \qquad \text{(LIMA, 1983, p. 22)}$$
$$e^{i\pi} = -1$$

Cálculo da soma $\sum_{i=1}^{n}\binom{n}{i}$

Desenvolvendo $(a + b)^n$ pelo binômio de Newton temos:

$$(a+b)^n = \binom{n}{0}.a^n + \binom{n}{1}.a^{n-1}.b^1 + \binom{n}{2}.a^{n-2}.b^2 + \ldots + \binom{n}{n}.b^n$$

Fazendo a=1 e b=1 na igualdade acima, segue-se:

$$(1+1)^n = \binom{n}{0}.1^n + \binom{n}{1}.1^{n-1}.1^1 + \binom{n}{2}.1^{n-2}.1^2 + \ldots + \binom{n}{n}.1^n$$

$$(2)^n = \binom{n}{0} + \binom{n}{1} + \binom{n}{2} + \binom{n}{3}\ldots + \binom{n}{n}$$

$$2^n - \binom{n}{0} = \binom{n}{1} + \binom{n}{2} + \binom{n}{3}\ldots + \binom{n}{n},$$

o que nos dá: $\binom{n}{1} + \binom{n}{2} + \binom{n}{3}\ldots + \binom{n}{n} = 2^n - 1$

Anexo III

[C] Seja a função $F(x) = P(x) + P'(x) + ... + P^{(r-1)}(x) + P^{(r)}(x)$, em que $P(x)$ é um polinômio de grau *r* e $P^{(r)}(x)$ representa a derivada de ordem *r* de $P(x)$. Então:

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

Demonstração:

$$e^{-x}.F(x) = e^{-x}.(P(x) + P'(x) + ... + P^{(r-1)}(x) + P^{(r)}(x))$$

Então:

$$\frac{d}{dx}(e^{-x}.F(x)) = -e^{-x}.(P(x) + P'(x) + ... + P^{(r-1)}(x) + P^{(r)}(x)) +$$
$$+ e^{-x}.(P'(x) + P''(x) + ... + P^{(r)}(x) + P^{(r+1)}(x))$$

Pela propriedade distributiva da multiplicação em relação à adição, temos:

$$\frac{d}{dx}(e^{-x}.F(x)) = -e^{-x}.P(x) - e^{-x}P'(x) - e^{-x}P''(x) - ... - e^{-x}P^{(r-1)}(x) - e^{-x}P^{(r)}(x) +$$
$$+ e^{-x}.P'(x) + e^{-x}P''(x) + ... + e^{-x}P^{(r-1)}(x) + e^{-x}P^{(r)}(x) + e^{-x}P^{(r+1)}(x))$$

Como o grau de $P(x)$ é igual a *r*, temos $P^{(r+1)}(x) = 0$.

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

[D] Seja $Q(x) = \sum_{j=0}^{r} a_j.x^j$ um polinômio com coeficientes inteiros e seja $p < r$ um inteiro positivo. Então:

a) $Q^{(i)}(x) = \sum_{j=i}^{r} \frac{j!}{(j-i)!}.a_j.x^{j-i}$, $i \le r$, onde $Q^{(i)}(x)$ representa a derivada de ordem *i* de $Q(x)$.

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

Demonstração:

$$a)\ Q(x) = \sum_{j=0}^{r} a_j.x^j = a_0 + a_1x^1 + a_2x^2 + a_3x^3 + a_4x^4 + ... + a_rx^r$$

Calculando as sucessivas derivadas de $Q^{(i)}(x)$, vamos perceber a regularidade que ocorre e concluir a demonstração.

$$Q^{(1)}(x) = 1.a_1 + 2.a_2.x + 3.a_3.x^2 + 4.a_4.x^3 + ... + r.a_r.x^{(r-1)}$$
$$Q^{(1)}(x) = \frac{1!}{0!}.a_1 + \frac{2!}{1!}.a_2.x + \frac{3!}{2!}.a_3.x^2 + \frac{4!}{3!}.a_4.x^3 + ... + \frac{r!}{(r-1)!}.a_r.x^{(r-1)}$$

$$Q^{(2)}(x) = 2.1.a_2 + 3.2.a_3.x^1 + 4.3.a_4.x^2 + ... + r.(r-1).a_r.x^{(r-2)}$$
$$Q^{(2)}(x) = \frac{2!}{0!}.a_2 + \frac{3!}{1!}.a_3.x^1 + \frac{4!}{2!}.a_4.x^2 + ... + \frac{r!}{(r-2)!}.a_r.x^{(r-2)}$$

$$Q^{(3)}(x) = 3.2.1.a_3 + 4.3.2.a_4.x^1 + ... + r.(r-1)(r-2).a_r.x^{(r-3)}$$
$$Q^{(3)}(x) = \frac{3!}{0!}.a_3 + \frac{4!}{1!}.a_4.x^1 + ... + \frac{r!}{(r-3)!}.a_r.x^{(r-3)}$$

Então:

$$Q^{(i)}(x) = \frac{i!}{0!}.a_i + \frac{(i+1)!}{1!}.a_{i+1}.x^1 + \frac{(i+2)!}{2!}.a_{i+2}.x^2 + \frac{(i+3)!}{3!}.a_{i+3}.x^3 + ... + \frac{r!}{(r-i)!}.a_r.x^{(r-i)}$$

Utilizando o somatório, temos:

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

Observação: para $i > r$, temos $Q^{(i)}(x) = 0$.

b) Usando o resultado anterior, podemos escrever

$$\frac{1}{(p-1)!}.Q^{(i)}(x) = \frac{1}{(p-1)!}.\sum_{j=i}^{r} \frac{j!}{(j-i)!}.a_j.x^{j-i}\ .$$

Os coeficientes de $\frac{1}{(p-1)!}.Q^{(i)}(x)$ são da forma $\frac{1}{(p-1)!}.\frac{j!}{(j-i)!}.a_j,\ \ a_j \in Z$, com $p \le i \le r$, p fixo.

Para $j = i + k,\ k \in N$, temos:

$$\frac{1}{(p-1)!}.\frac{j!}{(j-i)!}.a_j = \frac{1}{(p-1)!}.\frac{(i+k)!}{(i+k-i)!}.a_{i+k} = \frac{(i+k)!}{k!.(p-1)!}.a_{i+k}$$

Como $p \le i$, temos $i + k \ge p$. Então:

$$\frac{(i+k)!}{k!.(p-1)!}.a_{i+k} = \frac{(i+k).(i+k-1). \ldots .p.(p-1)!}{k!.(p-1)!}.a_{i+k} = \frac{(i+k).(i+k-1). \ldots .p}{k!}.a_{i+k}$$

Esse numerador possui $i + k - (p-1) = i + k - p + 1$ fatores. Como $p \le i$, podemos concluir que ele terá pelo menos $k+1$ fatores.

Então:

$$\frac{(i+k)!}{k!.(p-1)!}.a_{i+k} = \frac{(i+k).(i+k-1). \ldots .(i+1).i.(i-1). \ldots .p}{k!}.a_{i+k} =$$

$$= \frac{(i+k).(i+k-1). \ldots .(i+1)}{k!}.\frac{i!}{i!}.i.(i-1). \ldots .p.a_{i+k} = \binom{i+k}{k}.i.(i-1). \ldots .p.a_{i+k}$$

Mas $\binom{i+k}{k}$ é um número binomial, portanto, natural.

Então $\binom{i+k}{k}.i.(i-1). \ldots .p.a_{i+k} \in Z$.

Portanto, $\frac{1}{(p-1)!}.\frac{j!}{(j-i)!}.a_j = \frac{(i+k)!}{k!.(p-1)!}.a_{i+k} = \binom{i+k}{k}.i.(i-1). \ldots .p.a_{i+k} \in Z.$

Como p aparece na decomposição desse número em fatores, concluímos que $\frac{1}{(p-1)!}.\frac{j!}{(j-i)!}.a_j$, é divisível por p.

Anexo IV

Desigualdade do valor médio para funções de uma variável complexa

Uma função de uma variável complexa $f : C \to C$ tem derivada no ponto z, se existir o limite $f'(z) = \lim_{z_0 \to 0} \frac{f(z + z_0) - f(z)}{z_0}$, onde $z_0 \in C$.

$f'(z)$ é chamada a derivada de f em z.

Diz-se que *a função $f : C \to C$ é analítica em C, se f é derivável em todos os pontos de C, ou seja, existe $f'(z)$ qualquer que seja $z \in C$.*

Seja $z = x + i.y$, com $x, y \in$ R. Podemos escrever $f(x + i.y) = u(x,y) + i.v(x,y)$ onde $u(x,y)$ é a parte real de $f(z)$ e $v(x,y)$ é a parte imaginária de $f(z)$.

Por exemplo, se $f(z) = z^2$, então $f(x+iy) = (x+iy)^2 = x^2 - y^2 + 2.i.xy$. Neste caso, temos $u(x,y) = x^2 - y^2$ e $v(x,y) = 2.xy$.

Considerando $z_0 = h + ik$, podemos também escrever

$$f'(z) = \lim_{\substack{h \to 0 \\ k \to 0}} \frac{f((x+h) + i.(y+k)) - f(x+iy)}{h+ik} =$$

$$= \lim_{\substack{h \to 0 \\ k \to 0}} \frac{u(x+h, y+k) + i.v(x+h, y+k) - u(x,y) - i.v(x,y)}{h+ik}$$

independente da maneira como $z_0 \to 0$ ou $h \to 0$ e $k \to 0$.

Supondo que $f(z) = u(x,y) + i.v(x,y)$, $z = x + i.y$, seja analítica em C, vamos calcular $f'(z) = \lim_{z_0 \to 0} \frac{f(z + z_0) - f(z)}{z_0}$ usando valores reais para $z_0 = h + i.k$, ou seja, vamos considerar $z_0 = h \neq 0$ e $k = 0$.

Neste caso, $z + z_0 = x + i.y + h = (x+h) + i.y$ e

$f(z + z_0) = f((x+h) + i.y) = u(x+h, y) + i.v(x+h, y)$.

Portanto,

$$f'(z) = \lim_{z_0 \to 0} \frac{f(z+z_0) - f(z)}{z_0} = \lim_{h \to 0} \frac{u(x+h,y) + i.v(x+h,y) - u(x,y) - i.v(x,y)}{h} =$$

$$= \lim_{h \to 0} \frac{u(x+h,y) - u(x,y)}{h} + i.\lim_{h \to 0} \frac{v(x+h,y) - v(x,y)}{h} = \frac{\partial u}{\partial x}(x,y) + i.\frac{\partial v}{\partial x}(x,y)$$

Ou seja $f'(z) = \frac{\partial u}{\partial x}(x,y) + i.\frac{\partial v}{\partial x}(x,y)$ (I)

Agora vamos calcular $f'(z)$ usando valores imaginários puros para $z_0 = h + i.k$, ou seja, $z_0 = i.k$ ($h = 0$ e $k \neq 0$).

Então $z + z_0 = x + i.y + i.k = x + i.(y+k)$

$f(z + z_0) = f(x + i.(y+k)) = u(x, y+k) + i.v(x, y+k)$

Portanto,

$$f'(z) = \lim_{z_0 \to 0} \frac{f(z+z_0) - f(z)}{z_0} = \lim_{k \to 0} \frac{u(x,y+k) + i.v(x,y+k) - u(x,y) - i.v(x,y)}{i.k} =$$

$$= \lim_{k \to 0} \frac{u(x,y+k) - u(x,y)}{i.k} + i.\lim_{k \to 0} \frac{v(x,y+k) - v(x,y)}{i.k} =$$

$$= \frac{1}{i}\lim_{k \to 0} \frac{u(x,y+k) - u(x,y)}{k} + \frac{i}{i}.\lim_{k \to 0} \frac{v(x,y+k) - v(x,y)}{k} = \frac{1}{i}.\frac{\partial u}{\partial y}(x,y) + \frac{\partial v}{\partial y}(x,y) =$$

$$= -i.\frac{\partial u}{\partial y}(x,y) + \frac{\partial v}{\partial y}(x,y)$$

Ou seja, $f'(z) = -i.\frac{\partial u}{\partial y}(x,y) + \frac{\partial v}{\partial y}(x,y)$ (II)

Identificando (I) e (II), obtemos: $\frac{\partial u}{\partial x}(x,y) + i.\frac{\partial v}{\partial x}(x,y) = -i.\frac{\partial u}{\partial y}(x,y) + \frac{\partial v}{\partial y}(x,y)$, ou seja,

$$\boxed{\frac{\partial u}{\partial x}(x,y) = \frac{\partial v}{\partial y}(x,y)} \text{ e } \boxed{\frac{\partial u}{\partial y}(x,y) = -\frac{\partial v}{\partial x}(x,y)}$$

Estas duas equações são chamadas de Equações de *Cauchy-Riemman*.

Se *f* for analítica em C, então as equações de *Cauchy-Riemman* valem em qualquer ponto de C.

Desigualdade do valor médio para funções de uma variável complexa

Teorema: *Seja* $f : C \to C$ *uma função analítica e sejam* $z_1, z_2 \in C$ *. Então:* $| f(z_2) - f(z_1) | \leq 2.| z_2 - z_1 |.\sup\{| f'(z_1 + \lambda.(z_2 - z_1)) | : 0 \leq \lambda \leq 1\}$*, onde* $| z |$ *representa o módulo do complexo z = x + i.y, isto é;* $| z | = \sqrt{x^2 + y^2}$ (FIGUEIREDO, 1985, p. 61).

Esta demonstração tem como referências (FIGUEIREDO, 1985, p. 59-65) e (AUGUSTINI, OLIVEIRA e SILVA, 2005, p. 72-75).

Demonstração:

Seja $f : C \to C$ uma função analítica dada por *f(z) = u(x,y) + i.v(x,y).*

Primeiramente vamos mostrar que o teorema é válido para $z_2 = z_0$ e $z_1 = 0$, ou seja, que $| f(z_0) - f(0) | \leq 2.| z_0 |.\sup\{| f'(\lambda.(z_0)) | : 0 \leq \lambda \leq 1\}$.

De $z_2 = z_0 = x_0 + i.y_0$ e $z_1 = 0 = 0 + i.0$, temos:

$$f(z_0) = u(x_0, y_0) + i.v(x_0, y_0)$$
$$f(0) = u(0,0) + i.v(0,0)$$

Então

$$\boxed{f(z_0) - f(0) = u(x_0, y_0) - u(0,0) + i.(v(x_0, y_0) - v(0,0))}$$

Dado $z_0 = x_0 + i.y_0$, vamos definir agora duas funções reais:

$$\phi : R \to R \qquad \text{e} \qquad \psi : R \to R$$
$$\lambda \mapsto \phi(\lambda) = u(\lambda x_0, \lambda y_0) \qquad\qquad \lambda \mapsto \psi(\lambda) = v(\lambda x_0, \lambda y_0)$$

Aplicando o Teorema do Valor Médio[17] às funções reais ϕ e ψ no intervalo [0,1], obtemos:

$$\phi(1) - \phi(0) = \phi'(\lambda_1).(1 - 0), \quad 0 < \lambda_1 < 1$$
$$\psi(1) - \psi(0) = \psi'(\lambda_2).(1 - 0), \quad 0 < \lambda_2 < 1$$

[17] Seja $f : [a,b] \to R$ uma função contínua no intervalo fechado $[a,b]$ e derivável no intervalo aberto (a,b). Então existe $c \in (a,b)$ tal que $f(b) - f(a) = f'(c)(b - a)$.

Então

$$\phi(1)-\phi(0)=\phi'(\lambda_1),\ \ 0<\lambda_1<1$$
$$\psi(1)-\psi(0)=\psi'(\lambda_2),\ \ 0<\lambda_2<1$$

Vamos agora calcular as derivadas $\phi'(\lambda_1)$ e $\psi'(\lambda_2)$. Para isso utilizamos o Teorema de Derivação de Funções Compostas[18].

- Calculando $\phi'(\lambda)$ temos: $\phi'(\lambda)=\frac{\partial u}{\partial x}(\lambda x_0,\lambda y_0).x_0+\frac{\partial u}{\partial y}(\lambda x_0,\lambda y_0).y_0$.

Então, $\phi'(\lambda_1)=\frac{\partial u}{\partial x}(\lambda_1 x_0,\lambda_1 y_0).x_0+\frac{\partial u}{\partial y}(\lambda_1 x_0,\lambda_1 y_0).y_0$

- Calculando $\varphi'(\lambda)$ temos: $\varphi'(\lambda)=\frac{\partial v}{\partial x}(\lambda x_0,\lambda y_0).x_0+\frac{\partial v}{\partial y}(\lambda x_0,\lambda y_0).y_0$.

Então, $\varphi'(\lambda_2)=\frac{\partial v}{\partial x}(\lambda_2 x_0,\lambda_2 y_0).x_0+\frac{\partial v}{\partial y}(\lambda_2 x_0,\lambda_2 y_0).y_0$

De $\phi(\lambda)=u(\lambda x_0,\lambda y_0)$ e $\psi(\lambda)=v(\lambda x_0,\lambda y_0)$, temos:

- para $\lambda=1$, $\phi(1)=u(x_0,y_0)$ e $\psi(1)=v(x_0,y_0)$
- para $\lambda=0$, $\phi(0)=u(0,0)$ e $\psi(0)=v(0,0)$

Então,

$$u(x_0,y_0)-u(0,0)=\phi(1)-\phi(0)=\phi'(\lambda_1)=\frac{\partial u}{\partial x}(\lambda_1 x_0,\lambda_1 y_0).x_0+\frac{\partial u}{\partial y}(\lambda_1 x_0,\lambda_1 y_0).y_0$$
$$v(x_0,y_0)-v(0,0)=\psi(1)-\psi(0)=\psi'(\lambda_2)=\frac{\partial v}{\partial x}(\lambda_2 x_0,\lambda_2 y_0).x_0+\frac{\partial v}{\partial y}(\lambda_2 x_0,\lambda_2 y_0).y_0$$

Substituindo estas duas igualdades em

$$f(z_0)-f(0)=u(x_0,y_0)-u(0,0)+i.(v(x_0,y_0)-v(0,0)),$$

[18] Sejam $u=h(x,y)$ e $x=p(\lambda)$ e $y=q(\lambda)$ em que h,p e q são diferenciáveis por hipótese. Então $\frac{du}{d\lambda}=\frac{\partial u}{\partial x}.\frac{dx}{d\lambda}+\frac{\partial u}{\partial y}.\frac{dy}{d\lambda}$

temos:

$$f(z_0) - f(0) = \frac{\partial u}{\partial x}(\lambda_1 x_0, \lambda_1 y_0).x_0 + \frac{\partial u}{\partial y}(\lambda_1 x_0, \lambda_1 y_0).y_0 +$$
$$+ i.\left[\frac{\partial v}{\partial x}(\lambda_2 x_0, \lambda_2 y_0).x_0 + \frac{\partial v}{\partial y}(\lambda_2 x_0, \lambda_2 y_0).y_0\right]$$

Aplicando nesta última igualdade a desigualdade $|z| \leq |x| + |y|$ que diz que o módulo de um número complexo $z = x + i.y$ é menor ou igual que a soma dos valores absolutos de sua parte real e imaginária, temos:

$$|f(z_0) - f(0)| \leq \left|\frac{\partial u}{\partial x}(\lambda_1 x_0, \lambda_1 y_0).x_0 + \frac{\partial u}{\partial y}(\lambda_1 x_0, \lambda_1 y_0).y_0\right| +$$
$$+ \left|\frac{\partial v}{\partial x}(\lambda_2 x_0, \lambda_2 y_0).x_0 + \frac{\partial v}{\partial y}(\lambda_2 x_0, \lambda_2 y_0).y_0\right|$$

Aplicando agora a desigualdade de Cauchy-Schwars[19], temos:

$$|f(z_0) - f(0)| \leq \sqrt{\left(\frac{\partial u}{\partial x}(\lambda_1 x_0, \lambda_1 y_0)\right)^2 + \left(\frac{\partial u}{\partial y}(\lambda_1 x_0, \lambda_1 y_0)\right)^2}.\sqrt{x_0^2 + y_0^2} +$$
$$+ \sqrt{\left(\frac{\partial v}{\partial x}(\lambda_2 x_0, \lambda_2 y_0)\right)^2 + \left(\frac{\partial v}{\partial y}(\lambda_2 x_0, \lambda_2 y_0)\right)^2}.\sqrt{x_0^2 + y_0^2}$$

De $f'(z) = \frac{\partial u}{\partial x}(x, y) + i.\frac{\partial v}{\partial x}(x, y)$ e das equações de *Cauchy-Riemman*

$$\frac{\partial u}{\partial x}(x, y) = \frac{\partial v}{\partial y}(x, y) \text{ e } \frac{\partial u}{\partial y}(x, y) = -\frac{\partial v}{\partial x}(x, y),$$

temos:

1) $\boxed{f'(z) = \frac{\partial u}{\partial x}(x, y) - i.\frac{\partial u}{\partial y}(x, y)}$

2) $\boxed{f'(z) = \frac{\partial v}{\partial y}(x, y) + i.\frac{\partial v}{\partial x}(x, y)}$

---

[19] Dados $a_1, a_2, b_1, b_2 \in R$, tem-se que $|a_1 b_1 + a_2 b_2| \leq \sqrt{a_1^2 + a_2^2}.\sqrt{b_1^2 + b_2^2}$

Calculando $f'(\lambda_1 z_0)$ na primeira equação e $f'(\lambda_2 z_0)$ na segunda equação, obtemos:

$$f'(\lambda_1 z_0) = \frac{\partial u}{\partial x}(\lambda_1 x_0, \lambda_1 y_0) - i.\frac{\partial u}{\partial y}(\lambda_1 x_0, \lambda_1 y_0)$$

$$f'(\lambda_2 z_0) = \frac{\partial v}{\partial y}(\lambda_2 x_0, \lambda_2 y_0) + i.\frac{\partial v}{\partial x}(\lambda_2 x_0, \lambda_2 y_0)$$

Vamos agora calcular o módulo dessas expressões:

$$|f'(\lambda_1 z_0)| = \sqrt{\left(\frac{\partial u}{\partial x}(\lambda_1 x_0, \lambda_1 y_0)\right)^2 + \left(\frac{\partial u}{\partial y}(\lambda_1 x_0, \lambda_1 y_0)\right)^2}$$

$$|f'(\lambda_2 z_0)| = \sqrt{\left(\frac{\partial v}{\partial y}(\lambda_2 x_0, \lambda_2 y_0)\right)^2 + \left(\frac{\partial v}{\partial x}(\lambda_2 x_0, \lambda_2 y_0)\right)^2}$$

Como $|z_0| = \sqrt{x_0^2 + y_0^2}$, voltando em

$$|f(z_0) - f(0)| \le \sqrt{\left(\frac{\partial u}{\partial x}(\lambda_1 x_0, \lambda_1 y_0)\right)^2 + \left(\frac{\partial u}{\partial y}(\lambda_1 x_0, \lambda_1 y_0)\right)^2}.\sqrt{x_0^2 + y_0^2} +$$
$$+ \sqrt{\left(\frac{\partial v}{\partial x}(\lambda_2 x_0, \lambda_2 y_0)\right)^2 + \left(\frac{\partial v}{\partial y}(\lambda_2 x_0, \lambda_2 y_0)\right)^2}.\sqrt{x_0^2 + y_0^2}$$

temos:

$$|f(z_0) - f(0)| \le |f'(\lambda_1 z_0)|.|z_0| + |f'(\lambda_2 z_0)|.|z_0| = |z_0|.(|f'(\lambda_1 z_0)| + |f'(\lambda_2 z_0)|)$$

Como $0 < \lambda_1 < 1$ e $0 < \lambda_2 < 1$, então:

$$|f'(\lambda_1 z_0)| \le \sup\{|f'(\lambda z_0)| : 0 \le \lambda \le 1\} \quad \text{e} \quad |f'(\lambda_2 z_0)| \le \sup\{|f'(\lambda z_0)| : 0 \le \lambda \le 1\}.$$

Portanto, $|f(z_0) - f(0)| \le |z_0|.2\sup\{|f'(\lambda.(z_0))| : 0 \le \lambda \le 1\}$, ou seja

$$|f(z_0) - f(0)| \le 2.|z_0|.\sup\{|f'(\lambda.(z_0))| : 0 \le \lambda \le 1\}.$$

Considerando a função $g(z) = f(z + z_1)$ e ao ponto $z_0 = z_2 - z_1$, segue-se que:

$$| g(z_0) - g(0) | \leq 2. | z_0 | . \sup \{ | g'(\lambda.(z_0)) | : 0 \leq \lambda \leq 1 \} .$$

Como

$$g(0) = f(0 + z_1) = f(z_1)$$
$$g(z_0) = g(z_2 - z_1) = f(z_2 - z_1 + z_1) = f(z_2)$$
$$g'(\lambda z_0) = g'(\lambda(z_2 - z_1)) = f''(z_1 + \lambda(z_2 - z_1))$$

Concluímos que

$$| f(z_2) - f(z_1) | \leq 2. | z_2 - z_1 | . \sup \{ | f'(z_1 + \lambda.(z_2 - z_1)) | : 0 \leq \lambda \leq 1 \} ,$$

o que conclui a demonstração.