

Teorema Fundamental da Álgebra.

Fogliarino Brolesi

Campinas, Primavera de 2006

Resumo

Esta é uma monografia que faz referência ao Teorema Fundamental da Álgebra.

Em matemática, o teorema fundamental da Álgebra afirma que qualquer polinómio $p(z)$ com coeficientes complexos de uma variável e de grau $n \geq 1$ tem alguma raiz complexa. Por outras palavras, o corpo dos números complexos é algebricamente fechado e, portanto, tal como com qualquer outro corpo algebricamente fechado, a equação $p(z) = 0$ tem n soluções (não necessariamente distintas).

O nome do teorema é hoje em dia considerado inadequado por muitos matemáticos, por não ser fundamental para a Álgebra contemporânea.

Sumário

1 História	4
1.1 Enunciado do teorema	5
2 Demonstrações	6
2.1 Demonstrações analíticas	6
2.2 Demonstrações topológicas	7
2.3 Demonstração algébrica	7
3 Interpretações	8
3.1 Interpretação gráfica	8
3.1.1 Um polinômio de grau 4	9
3.1.2 Um polinômio com raízes múltiplas	9
3.2 Interpretação física de Gauss	9
3.2.1 Exemplo 1:	11
3.2.2 Exemplo 2:	12

Lista de Figuras

1 \mathbb{C}	9
2 $f(z) = z^4 - 1$	10
3 $f(z) = z^8 - 2z^7 + 2z^6 - 4z^5 + 2z^4 - 2z^3 - 5z^2 + 4z - 4$	10

1 História

O problema de perceber o tipo de soluções de uma equação polinomial surgiu desde cedo na história da matemática. Os gregos, com os seus problemas de áreas e volumes depararam-se com equações do tipo

$$x^2 - 2 = 0 \text{ e } x^3 + 9 = 0$$

para os quais não tinham resposta. São conhecidos muitos estudos nesta área que nos chegam dos povos Hindus, Gregos, Árabes, Chineses, etc.

No ano de 800 d.c. já havia notícia de estudos de equações de segundo grau. Al-Khwarizmi, que foi considerado por alguns o pai da álgebra, fez esse estudo, mas nessa altura ainda não se colocava o problema das soluções não reais.

O médico Girolamo Cardano foi o primeiro matemático a compreender que se podia trabalhar com quantidades mais gerais que os números reais. Em 1545 Cardano, publicou no seu livro *Ars Magna* os estudos efectuados, pelo Professor Scipione Del Ferro em 1520, sobre equações do tipo $x^3 + px = q$, $x^3 = px + q$ e $x^3 + q = px$ que Tartaglia havia descoberto em 1535. Nos estudos do Professor Scipione Del Ferro, encontravam-se as soluções das equações quadráticas e cúbicas:

$$x = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}$$

$$x = \sqrt[3]{\sqrt{\frac{p^3}{27} + \frac{q^2}{4}} + \frac{q}{2}} - \sqrt[3]{\sqrt{\frac{p^3}{27} + \frac{q^2}{4}} - \frac{q}{2}}$$

Ao estudar a equação $x^3 = 15x + 4$ Del Ferro encontrou a solução real $x=4$ e também as soluções "fictícias" $x = \pm\sqrt{-121}$ que conseguiu manipular mas que ele próprio não entendia muito bem, usando a notação

$$p + \sqrt{-q}$$

Só em 1572, Bombelli publica no seu livro *Algebra* um conjunto de regras para operar os números complexos.

Peter Rothe, no seu livro *Arithmetica Philosophica* (publicado in 1608), escreveu que uma equação polinomial de grau n (com coeficientes reais) pode ter n soluções. Albert Girard, no seu livro *L'invention nouvelle en l'Algèbre* (publicado in 1629), afirmou que uma equação polinomial de grau n tem n soluções, mas não disse que tais soluções eram necessariamente números complexos. Além disso, ele disse que a sua afirmação era válida «a menos que a equação seja incompleta», querendo dizer com isto que nenhum coeficiente é igual a 0. No entanto, quando ele explica em detalhe o que quer dizer, torna-se claro que, de fato, ele acredita que a afirmação dele é válida em todos os casos; por exemplo, ele mostra que a equação $x^4 = 4x - 3$, embora incompleta, tem quatro soluções: 1, 1, $-1 + i\sqrt{2}$ e $-1 - i\sqrt{2}$.

Em 1637, Descartes escreve em *La géométrie* o que anos antes Harriot havia descoberto – se a é raiz de um polinômio, então $x - a$ divide o polinômio. Descartes afirmou também que para todas as equações de grau n , podemos imaginar n raízes, mas estas podem não corresponder a quantidades reais.

Uma consequência do teorema fundamental da Álgebra é que qualquer polinômio com coeficientes reais e grau superior a 0 pode ser escrito como produto de

polinômios com coeficientes reais de graus 1 ou 2. No entanto, em 1702 Leibniz afirmou que nenhum polinômio do tipo $x^4 + a^4$ (com a real e não nulo) pode ser obtido sob aquela forma. Anos mais tarde, Nikolaus Bernoulli afirmou o mesmo relativamente ao polinômio $x^4 - 4x^3 + 2x^2 + 4x + 4$, mas recebeu uma carta de Euler em 1742 na qual lhe foi explicado que o seu polinômio era de facto igual a:

$$(x^2 - (2 + \alpha)x + 1 + \sqrt{7} + \alpha)(x^2 - (2 - \alpha)x + 1 + \sqrt{7} - \alpha)$$

sendo α a raiz quadrada de $4 + 2\sqrt{7}$, enquanto que

$$x^4 + a^4 = (x^2 + a\sqrt{2}x + a^2)(x^2 - a\sqrt{2}x + a^2)$$

Uma primeira tentativa de demonstrar o teorema foi levada a cabo por d'Alembert em 1746, mas na altura a demonstração foi considerada incorrecta. Entre outros problemas, usava implicitamente um teorema (actualmente designado por teorema de Puiseux) que só viria a ser demonstrado um século mais tarde e cuja demonstração se pensava depender do teorema fundamental da álgebra. No entanto, hoje em dia há quem defenda que a demonstração de D'Alembert foi mal compreendida, e que de facto não depende do teorema fundamental da álgebra ou seja, não é circular. Outras tentativas foram levadas a cabo por Euler (1749), de Foncenex (1759), Lagrange (1772) e Laplace (1795). Estas últimas quatro tentativas recorreram à tese de Argand; mais precisamente, a existência de raízes era dada como certa e o que faltava provar era que eram da forma $a + bi$ para números reais a e b . Em terminologia moderna, Euler, de Foncenex, Lagrange e Laplace estavam a supor a existência de um corpo de decomposição do polinômio $p(z)$.

No fim do século XVIII foram publicadas duas novas demonstrações que não supunham a existência de raízes. Uma delas, da autoria de James Wood e sobretudo algébrica, foi publicada em 1798 e completamente ignorada. A demonstração de Wood tinha uma falha de natureza algébrica. A outra demonstração foi publicada por Gauss em 1799 e era sobretudo geométrica, mas tinha uma falha topológica. Uma demonstração rigorosa foi publicada por Argand em 1806; foi aqui que, pela primeira vez, o teorema fundamental da Álgebra foi enunciado para polinômios com coeficientes complexos e não apenas para polinômios com coeficientes reais. Gauss publicou mais duas demonstrações em 1816 e uma nova versão da primeira demonstração em 1849.

O primeiro manual universitário a conter uma demonstração do teorema foi o *Cours d'analyse de l'École Royale Polytechnique*, de Cauchy (1821). A demonstração em questão é a de Argand, embora este não seja mencionado.

Nenhuma das demonstrações até agora mencionadas é construtiva. Foi Weierstrass quem levantou pela primeira vez, em 1891, o problema de encontrar uma demonstração construtiva do teorema. Tal demonstração foi obtida por Hellmuth Kneser em 1940 e simplificada pelo seu filho Martin Kneser em 1981.

1.1 Enunciado do teorema

O enunciado mais conhecido do teorema fundamental da álgebra diz que

Todo o polinômio não constante, de grau n com coeficientes complexos, tem n raízes complexas

no entanto, existem outras formas equivalentes de o enunciar que merecem a nossa atenção.

Outro enunciado do mesmo teorema, diz que

Todo o polinômio não constante, de grau n , com coeficientes complexos, tem pelo menos uma raiz complexa.

O enunciado diz-nos que um polinômio p de grau n , tem uma raiz α . Assim podemos decompô-lo em dois polinômios, $p(x) = (x - \alpha)q(x)$ com q um polinômio de grau $n - 1$. Mas então, sabemos também que q tem uma raiz, logo também pode ser decomposto no produto de um polinômio de grau um com um polinômio de grau $n - 2$. Repetindo este processo até à exaustão, concluímos que p pode ser decomposto em n fatores de grau um ou seja, p tem n raízes.

Outro enunciado equivalente diz que

Todo o polinômio real pode ser escrito como produto de fatores lineares reais, ou fatores reais de grau dois.

Numa abordagem mais algébrica podemos enunciar o teorema fundamental da álgebra dizendo que

o corpo dos números complexos é algébricamente fechado

Dado que um corpo K se diz algébricamente fechado sempre que todos os polinômios de coeficientes em K se podem decompor em K . Concluímos que \mathbb{C} é algébricamente fechado porque todos os polinômios de coeficientes complexos têm as suas raízes em \mathbb{C} , logo decompõem-se em \mathbb{C} .

2 Demonstrações

Todas as demonstrações do teorema envolvem Análise ou, mais precisamente, o conceito de continuidade de uma função real ou complexa. Algumas funções também empregam derivabilidade ou mesmo funções analíticas.

Algumas demonstrações provam somente que qualquer polinômio de uma variável com coeficientes reais tem alguma raiz complexa. Isto basta para demonstrar o teorema no caso geral pois, dado um polinômio $p(z)$ com coeficientes complexos, o polinômio $q(z) = p(z)p(\bar{z})$ tem coeficientes reais e, se z_0 for uma raiz de $q(z)$, então z_0 ou o seu conjugado é uma raiz de $p(z)$.

Um grande número de demonstrações não algébricas usa o fato de $p(z)$ se comportar como z^n quando $|z|$ for suficientemente grande. Mais precisamente, existe algum número real positivo R tal que, se $|z| > R$, então

$$\frac{|z|^n}{2} < |p(z)| < 3\frac{|z|^n}{2}.$$

Seguem-se demonstrações baseadas em Análise, Topologia e Álgebra:

2.1 Demonstrações analíticas

Seja $r > 0$ tal que $|p(z)| > |p(0)|$ quando $|z| \geq r$ e seja D o disco fechado de raio r centrado em 0. Uma vez que D é compacto, a restrição a D de $|p|$ tem um mínimo; seja z_0 um ponto de D onde esse mínimo seja atingido. Então, z_0

não pode estar situado na fronteira de D , pois nos pontos z da fronteira tem-se $|p(z)| > |p(0)| \geq |p(z_0)|$. Logo, z_0 está no interior de D e, portanto, pelo princípio do mínimo, $p(z_0) = 0$. Por outras palavras, z_0 é um zero de $p(z)$.

Outra demonstração analítica pode ser obtida usando o teorema de Liouville. Suponhamos com vista a um absurdo que $p(z) \neq 0$ para todo o z pertencente a \mathbb{C} . Como $p(z)$ é inteira e não tem raízes, então $\frac{1}{p(z)}$ também é inteira. Visto que $|p(z)| \rightarrow \infty$ quando $|z| \rightarrow \infty$, então existem $M, r > 0$ tais que $|p(z)| > M$ se $|z| > r$. Assim, para $|z| > r$, temos que $|\frac{1}{p(z)}| < \frac{1}{M}$. Como $\frac{1}{p(z)}$ é inteira, é contínua em \mathbb{C} portanto é limitada no compacto $|z| = r$. Logo $\frac{1}{p(z)}$ é limitada em \mathbb{C} . Nestas condições, aplicando o Teorema de Liouville, $\frac{1}{p(z)}$ é constante. Donde, $p(z)$ é constante, o que é um absurdo. Logo $p(z)$ tem que ser zero para algum valor de z pertencente a \mathbb{C} .

2.2 Demonstrações topológicas

Em alternativa ao uso do teorema de Liouville na demonstração anterior, pode-se escrever $p(z)$ como um polinómio em $z - z_0$: há algum número natural k e há números complexos c_k, c_{k+1}, \dots, c_n tais que $c_k \neq 0$ e que

$$p(z) = p(z_0) + c_k(z - z_0)^k + c_{k+1}(z - z_0)^{k+1} + \dots + c_n(z - z_0)^n.$$

Deduz-se que se a for uma raiz de ordem k de $\frac{-p(z_0)}{c_k}$ e se t for positivo e suficientemente pequeno, então $|p(z_0 + ta)| < |p(z_0)|$, o que é impossível, uma vez que $|p(z_0)|$ é o mínimo de $|p|$ em D .

Para outra demonstração topológica, suponha-se que $p(z)$ não tem zeros. Seja R um número real positivo tal que, quando $|z| = R$, o termo dominante z^n de $p(z)$ domine todos os outros; posto de outro modo, tal que $|z|^n > |a_{n-1}z^{n-1} + \dots + a_0|$. À medida que z percorre o círculo $|z| = R$ uma vez no sentido directo, $p(z)$, tal como z^n , dá n voltas em torno de 0 no sentido directo. Por outras palavras, o índice relativamente a 0 do lacete percorrido por $p(z)$ é n . No extremo oposto, quando $|z| = 0$, o lacete $p(z)$ consiste somente no ponto $p(0)$, cujo índice relativamente a 0 é obviamente 0. Se o lacete percorrido por z é deformado continuamente entre estes dois extremos, o caminho percorrido por $p(z)$ também é continuamente deformado. Como $p(z)$ não tem zeros, este caminho nunca passa por 0 à medida que vai sendo deformado, pelo que o seu índice relativamente a 0 não pode mudar. No entanto, como o índice passa de n para 0, isto é absurdo. Logo, $p(z)$ tem necessariamente algum zero.

2.3 Demonstração algébrica

Esta demonstração usa somente dois factos cuja demonstração requer Análise ou, mais precisamente, o teorema dos valores intermédios, nomeadamente:

- qualquer polinómio de grau ímpar com coeficientes reais tem pelo menos um zero real;
- qualquer número real não negativo tem alguma raiz quadrada.

Resulta da segunda afirmação que, se a e b forem números reais, então há números complexos z_1 e z_2 tais que o polinómio $z^2 + az + b$ é igual a $(z - z_1)(z - z_2)$.

Como já foi observado, basta demonstrar que o teorema é válido para polinómios $p(z)$ com coeficientes reais. O teorema pode ser demonstrado por indução relativamente ao menor inteiro não negativo k tal que 2^k divide o grau n de $p(z)$. Seja F um corpo de decomposição de $p(z)$ (visto como um polinómio com coeficientes complexos); por outras palavras, o corpo F contém \mathbb{C} e há elementos z_1, z_2, \dots, z_n de F tais que

$$p(z) = (z - z_1)(z - z_2) \cdots (z - z_n).$$

Se $k = 0$, então n é ímpar e, portanto, $p(z)$ tem alguma raiz real. Suponha-se agora que $n = 2^k m$ (com m ímpar e $k > 0$) e que o teorema já se encontra demonstrado no caso em que o grau do polinómio é da forma $2^{k-1} m'$ com m' ímpar. Para um número real t , seja:

$$q_t(z) = \prod_{1 \leq i < j \leq n} (z - z_i - z_j - tz_i z_j)$$

Então os coeficientes de $q_t(z)$ são polinómios simétricos nos z_i com coeficientes reais. Logo, podem ser expressos como polinómios com coeficientes reais nos polinómios simétricos elementares, ou seja, em $-a_1, a_2, \dots, (-1)^n a_n$, pelo que q_t tem, de facto, coeficientes reais. Além disso, o grau de q_t é igual a $\frac{n(n-1)}{2} = 2^{k-1} m(n-1)$, e $m(n-1)$ é ímpar. Logo, pela hipótese de indução, q_t tem alguma raiz real; por outras palavras, $z_i + z_j + tz_i z_j$ é real para dois elementos distintos i e j de $\{1, \dots, n\}$. Como há mais números reais do que pares (i, j) , é possível encontrar números reais distintos t e s tais que $z_i + z_j + tz_i z_j$ e $z_i + z_j + sz_i z_j$ sejam reais (para os mesmos i e j). Consequentemente, tanto $z_i + z_j$ como $z_i z_j$ são números reais e, portanto, z_i e z_j são números complexos, pois são raízes do polinómio $z^2 - (z_i + z_j)z + z_i z_j$.

3 Interpretações

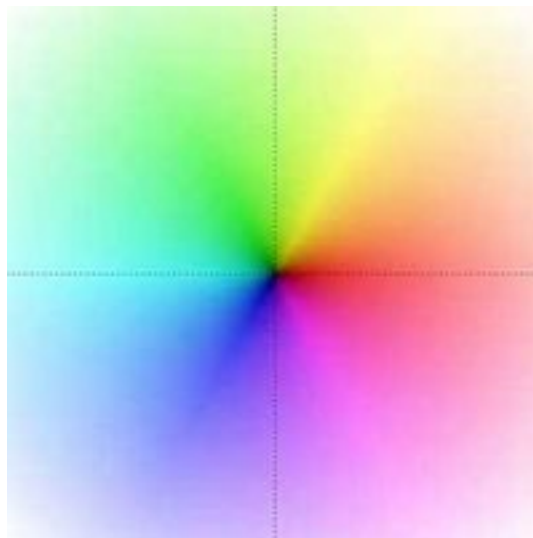
3.1 Interpretação gráfica

As funções complexas são funções de quatro dimensões, mas a nossa visão é limitada, e conseguimos ver no máximo até três dimensões. É impossível desenhá-las?

Se considerarmos que \mathbb{C} se comporta como \mathbb{R}^2 , podemos tratar $f : \mathbb{C} \rightarrow \mathbb{C}$ como se fosse uma função do tipo $f : \mathbb{R}^2 \rightarrow \mathbb{R}^2$. E como é que fazemos os gráficos dessas funções?

O método é muito simples. Começamos por "imaginar" uma circunferência centrada na origem e atribuímos cores a todos os pontos, partindo da reta $y = 0$ quando $x > 0$. Primeiro temos encarnado, amarelo, verde, etc, e andando sempre no sentido contrário aos ponteiros do relógio, como ilustra 3.1, abaixo. Se nos aproximarmos da origem, as cores ficam mais escuras e se nos afastamos as cores esbatem-se e ficam mais claras. Por isso quando z se aproxima de zero, temos preto, e quando $|z|$ se aproxima do infinito, temos branco.

A partir deste esquema de cores, podemos desenhar qualquer função do tipo $f : \mathbb{C} \rightarrow \mathbb{C}$. A cada ponto z do plano atribuímos a cor que corresponde a $f(z)$, usando para isso as cores da 3.1, como se vê nos exemplos que se seguem.

Figura 1: \mathbb{C}

3.1.1 Um polinômio de grau 4

Podemos observar que:

- f tem quatro pontos pintado a preto, ou seja, quatro zeros.
- Entre os zeros da função forma-se um "círculo" azul claro, ou seja, quando $|z| \rightarrow 0$, $f(z) \rightarrow -1$
- As cores diluem-se rapidamente, tendo-se maioritariamente branco quando estamos a uma certa distância do "centro", ou seja, $\lim_{|z| \rightarrow \infty} f(z) = \infty$.

3.1.2 Um polinômio com raízes múltiplas

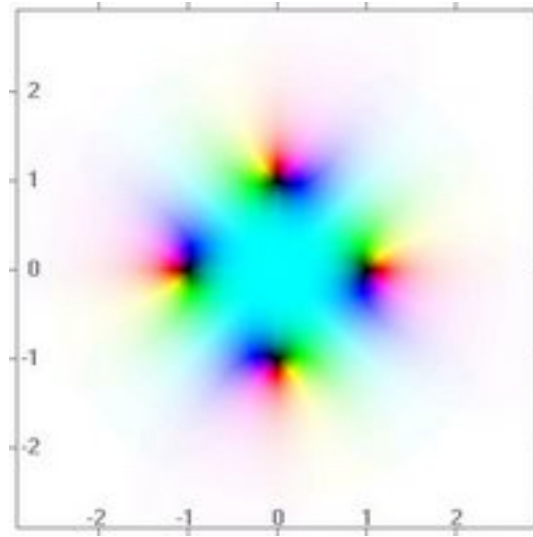
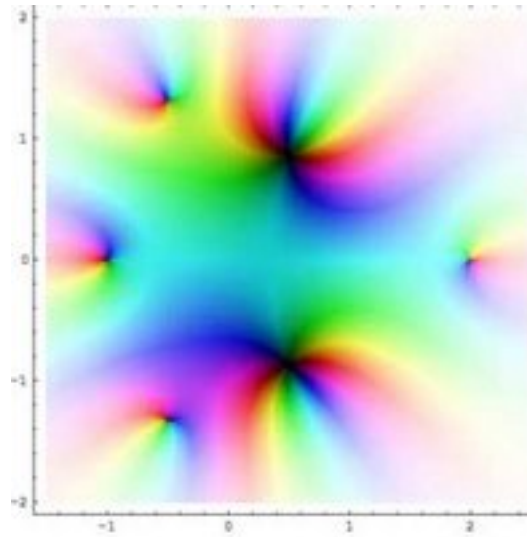
Se fizermos uma observação superficial desta imagem, podemos ser levados a concluir que o gráfico está mal feito ou que o teorema fundamental da álgebra é falso, visto que só encontramos seis manchas pretas e temos um polinômio de grau oito.

A verdade é que não há qualquer erro. Se fizermos uma observação mais cuidadosa, verificamos que em torno de cada ponto preto, andando no sentido contrário aos ponteiros do relógio, encontramos as cores da "paleta" inicial. E verificamos ainda que em torno de duas dessas manchas pretas, há repetição de cores, ou seja, esses zeros têm multiplicidade dois. Estão assim encontradas as oito raízes do polinômio.

3.2 Interpretação física de Gauss

Gauss desenvolveu uma explicação física para as raízes quadradas de números negativos. O exemplo da equação $x^2 + 4 = 0$ ajuda a perceber o que Gauss queria dizer.

Se perguntarmos a alguém o significado físico da equação $x^2 = 4$, a resposta é simples: x é o lado de um quadrado de área 4. Mas se perguntarmos a alguém

Figura 2: $f(z) = z^4 - 1$ Figura 3: $f(z) = z^8 - 2z^7 + 2z^6 - 4z^5 + 2z^4 - 2z^3 - 5z^2 + 4z - 4$

o significado físico da equação $x^2 = -4$, o mais natural é obtermos a resposta que Euler e Lagrange deram:

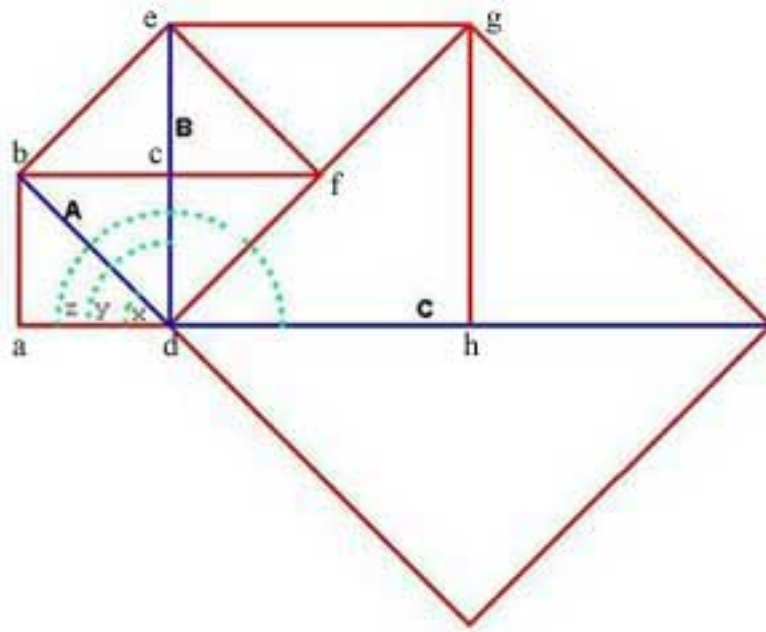
$x^2 = -1$ não tem significado físico, logo $x^2 = -4$ é impossível.

Gauss ridicularizou esta resposta, porque não faz sentido dizer que, uma equação tem solução mas que a solução é impossível.

Gauss demonstrou o significado físico da equação $x^2 = -1$, mas fê-lo num domínio cognitivo e não visível, aplicando o princípio de quadrar ilustrado na 3.2.1.

3.2.1 Exemplo 1:

A solução física da equação $x^2 - 4 = 0$ obtém-se pelo princípio de quadrar do seguinte modo.



Dado um quadrado qualquer de área 1, o Princípio de quadrar é a combinação física de dois processos:

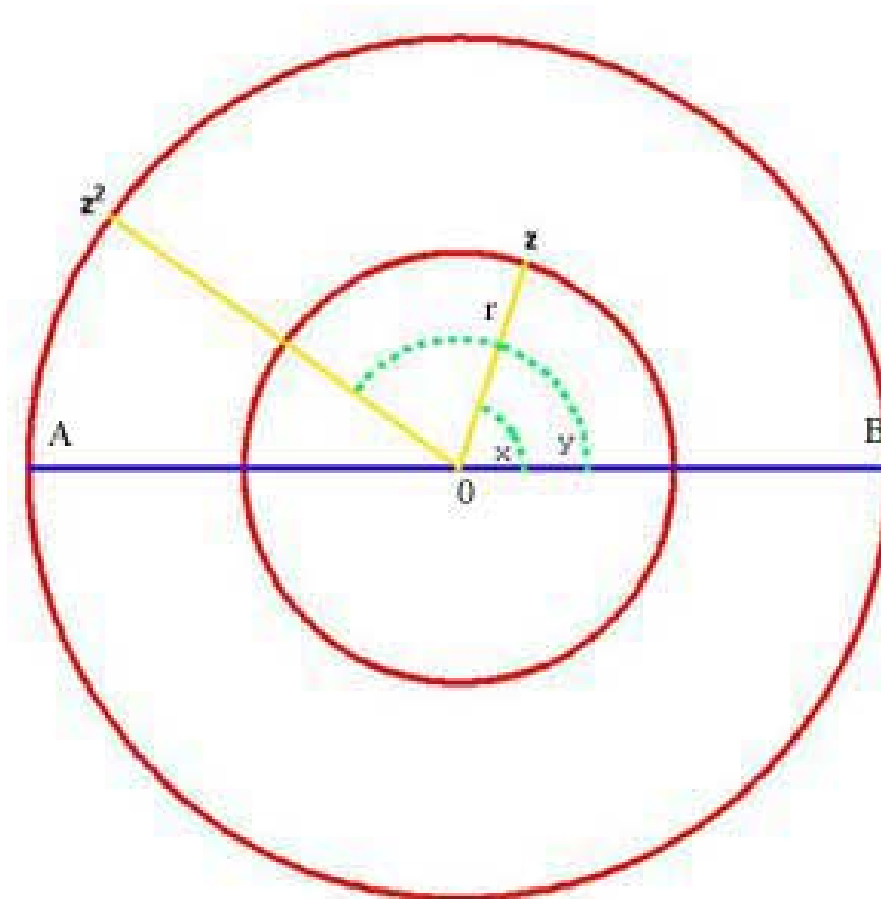
1. Duplicar o ângulo de rotação
2. Quadrar o comprimento da diagonal de um quadrado inicial.

Começamos por desenhar um quadrado [abcd] de área igual a 1 e diagonal $A = \sqrt{2}$. Desenhemos um novo quadrado, usando para lado a diagonal do quadrado inicial. A área deste novo quadrado é 2. Agora, repetimos a ação para gerar um quadrado cuja área é 4. Então o que é o princípio de quadrar aqui ilustrado? A ação que gerou o quadrado cuja área é dois, foi a rotação de 45° e a extensão do comprimento 1 para $\sqrt{2}$. Para produzir o quadrado cuja área é quatro, a rotação de 45° foi duplicada e a extensão foi quadrada.

A raiz quadrada é simplesmente a ação inversa, isto é, dividir por dois o ângulo de rotação e fazer a raiz quadrada do comprimento da diagonal.

3.2.2 Exemplo 2:

A interpretação física da equação $x^2 + 4 = 0$ pode ser obtida aplicando o Princípio de quadrar, agora numa circunferência.



Dada uma circunferência de centro em O e raio r e diâmetro \overline{AB} , e um ponto z sobre a circunferência, traçamos o raio $r = \overline{OZ}$ que faz com o diâmetro um ângulo x . Para obter z^2 aplicamos o princípio da quadratura, desta vez no sentido contrário aos ponteiros do relógio. Vemos assim que para obter z^2 duplicamos o ângulo e o círculo original é projetado num círculo de raio r^2 .

Reconhecemos nestes dois exemplos uma aplicação física feita por Gauss das fórmulas de De Moivre.

Referências

- [1] <http://hemsidor.torget.se/users/m/mauritz/math/alg/dihed.htm>
- [2] <http://pessoal.sercomtel.com.br/matematica/geometria/geom-areas/geom-areas-poli.htm>
- [3] http://en.wikipedia.org/wiki/Dihedral_group_of_order_6
- [4] Elementos de álgebra; A. Garcia e Y. Lequain, Projeto Euclides, IMPA 2002.
- [5] Elementos de Álgebra Abstrata; R.A. Dean, Livros Técnicos Científicos, 1974.
- [6] Estruturas Algébricas; S. Lang, Livro Técnico, 1972.
- [7] A concrete Introduction to Higher Algebra; L. Childs, Springer-Verlag 1995.