UNIVERSIDADE FEDERAL DE SANTA CATARINA
CENTRO DE CIÊNCIAS FÍSICAS E MATEMÁTICAS
DEPARTAMENTO DE MATEMÁTICA
CURSO DE ESPECIALIZAÇÃO EM MATEMÁTICA – FORMAÇÃO DE PROFESSOR NA MODALIDADE A DISTÂNCIA

Cristiane Costa

SOLUÇÃO DAS EQUAÇÕES POLINOMIAIS DE 3º E 4º GRAU.

Foz do Iguaçu

2011

Cristiane Costa

SOLUÇÃO DAS EQUAÇÕES POLINOMIAIS DE 3º E 4º GRAU.

Monografia submetida ao Programa de Especialização em Matemática – Formação de Professor da Universidade Federal de Santa Catarina para a obtenção do Grau de Especialista em Matemática.
Orientador: Prof. Dr. Celso Melchiades Doria.

Foz do Iguaçu

2011

UNIVERSIDADE FEDERAL DE SANTA CATARINA
CENTRO DE CIÊNCIAS FÍSICAS E MATEMÁTICAS
Departamento de Matemática
Curso de Especialização em Matemática-Formação de Professor na modalidade a distância

"Solução das Equações Polinomiais do 3° e 4° Grau"

Monografia submetida à Comissão de avaliação do Curso de Especialização em Matemática-Formação do professor em cumprimento parcial para a obtenção do título de Especialista em Matemática.

APROVADA PELA COMISSÃO EXAMINADORA em 18/03/2011

Dr. Celso Melchiades Doria (CFM/UFSC - Orientador) ________________________

Drª .Sonia Palomino Bean (CFM/UFSC - Examinadora) ________________________

Dr. Licio Hernanes Bezerra (CFM/UFSC – Examinador) ________________________

Dra. Neri Terezinha Both Carvalho
Coordenadora do Curso de Especialização em Matemática-Formação de Professor

Foz do Iguaçu, Paraná, março de 2011.

A minha filha
Ana Luisa.

AGRADECIMENTOS

Agradeço ao professor Celso, pela orientação no trabalho.

Agradeço aos professores Silvia, Roberto, Eliezer, Oscar e Méricles pelos conhecimentos transmitidos.

Agradeço a coordenação pela oportunidade de aperfeiçoamento através da especialização.

Os sinais + e - modificam a quantidade diante da qual são colocados como o adjetivo modifica o substantivo.

(Cauchy)

RESUMO

O presente trabalho apresenta um estudo sobre as soluções de equações polinomiais de 3° e 4° grau, através das fórmulas de Tartaglia-Cardano e do Método de Ferrari. Abordando também um pouco sobre o desenvolvimento do conjunto dos números complexos, que surgiram a partir da procura de soluções para equações polinomiais.

Palavras-chave: Números Complexos. Fórmulas de Tartaglia-Cardano.Método de Ferrari.

LISTA DE FIGURAS

SUMÁRIO

1 – INTRODUÇÃO

O primeiro conjunto numérico com que temos contato é o conjunto dos números naturais, representado pelo símbolo N, estes números são utilizados para contagem. Começamos a contar antes mesmo de freqüentar a escola. Esta classe numérica é tão fundamental em matemática que o matemático alemão Kronecker (1823-1891) chegou a afirmar: *Deus criou os números naturais, tudo o mais é obra do homem.*

Em seguida, no final das séries iniciais do ensino fundamental, nos são apresentadas as frações positivas, que pertencem ao conjunto dos números racionais. Um pouco depois, por volta do sétimo ano do ensino fundamental conhecemos os números negativos, e aprendemos que estes, juntamente com os números naturais formam o conjunto dos números inteiros, representado pelo símbolo Z, daí vemos as frações negativas completando o estudo dos números racionais. Por fim estudamos o conjunto dos números irracionais, geralmente representado pelo número π (pi) e então temos o conjunto dos números reais: união do conjunto dos números racionais e irracionais. Somente no ensino médio o conjunto dos números complexos é tratado, além destes, vistos no ensino básico, existem ainda outros conjuntos numéricos que não são abordados, como o conjunto dos *quaternios*.

Podemos então questionar: Porque existe esta diversidade de conjuntos numéricos? Quais os problemas motivaram o surgimento de novos conjuntos? Em qual ordem eles surgiram? (Será que foram desenvolvidos na mesma ordem em que são estudados hoje?).

Historicamente, diversos fatores, em diversos lugares, contribuíram para o desenvolvimento dos diferentes conjuntos numéricos. Por exemplo, uma questão que levou a ampliação do conjunto dos números naturais para o conjunto dos números inteiros, foi a idéia de subtração de números naturais ($a-b$), onde $a<b$. (Domingues, 2003).

Neste trabalho abordaremos as questões relativas ao desenvolvimento dos conjuntos numéricos sob uma ótica diferente: vamos observar a necessidade da utilização de novos sistemas numéricos visando à resolução de equações polinomiais.

O estudo das soluções de equações vem de longa data. Já nos papiros egípcios aparecem problemas matemáticos, geralmente ligados ao cotidiano da época, que são solucionados através da resolução de equações simples. (Milies, p.3)

Neste trabalho abordaremos as soluções das equações polinomiais de 3° e 4° grau. Para as equações cúbicas, as fórmulas que serão estudadas, foram desenvolvidas por Tartaglia e divulgadas por Cardano, na obra Ars Magna, em 1545; estas são conhecidas como fórmulas de Tartaglia-Cardano.

Para as equações de 4° grau, veremos um método que as reduzem a equações cúbicas, desenvolvido pelo matemático Ludovico Ferrari, e conhecido como Método de Ferrari. Para este estudo necessitamos de alguns conceitos prévios, os quais passamos a desenvolver no próximo capítulo.

2 – SISTEMAS NUMÉRICOS TRADICIONAIS

2.1 – O CONJUNTO DOS NÚMEROS INTEIROS (Z): OPERAÇÕES E PROPRIEDADES.

No conjunto Z, definimos as operações soma (+) e produto (.):

$$+ : Z \times Z \to Z \qquad \text{e} \qquad \bullet : Z \times Z \to Z$$

$$(x, y) \to x + y \qquad\qquad (x, y) \to x.y.$$

As operações definidas satisfazem as seguintes propriedades: $\forall x, y, z \in Z$,

I. *Comutatividade* da soma: $x + y = y + x$.

II. *Associatividade* da soma: $(x + y) + z = x + (y + z)$.

III. Existência do *elemento neutro*: $\exists\ 0 \in Z$, tal que: $x + 0 = x; \forall x \in Z$.

IV. Existência do *inverso aditivo*: $\forall x \in Z\ \exists\ -x \in Z$, tal que: $x + (-x) = 0$.

V. *Associatividade* do produto: $(x.y).z = x.(y.z)$

VI. *Distributividade* do produto em relação à soma: $x.(y + z) = x.y + x.z$

VII. *Comutatividade* do produto: $x.y = y.x$

VIII. Existência da *unidade*: $\exists\ 1 \in Z$, tal que $1.x = x.1 = x;\ \forall x \in Z$.

IX. Z não possui *divisores de zero*: Se $x.y = 0$, então $x = 0$ ou $y = 0$.

Em uma próxima seção estaremos definindo *anel,* veremos que para determinado conjunto ser anel, ele precisa estar munido de duas operações, que chamamos soma e produto; e estas devem satisfazer as seis primeiras propriedades acima. Sendo assim o conjunto Z, juntamente com as operações e suas propriedades definidas acima é um anel.

Além disso, neste conjunto o produto é comutativo, neste caso dizemos que Z é um *anel comutativo*; por satisfazer ainda a propriedade VIII, Z é chamado de *anel comutativo com unidade;* finalmente a propriedade IX faz deste conjunto um *anel comutativo com unidade e sem divisores de zero.* Isto é o que definiremos mais adiante como sendo um *Domínio de Integridade.*

Neste conjunto existe ainda a noção de "ordem" ($\leq$), ou seja, tomando $x, y \in Z$, escrevemos $x \leq y$, se, e somente se $\exists\ a \in N$, tal que $x + a = y$. Escrevemos $x < y$ se, e somente se $\exists\ a \in N$, $a \neq 0$ tal que $x + a = y$. Aceitamos conhecidas as propriedades básicas de módulo.

O próximo objetivo desta seção é demonstrar o algoritmo da divisão no conjunto dos inteiros, para isso vamos admitir o princípio da boa ordenação, e em seguida enunciar duas proposições que nos auxiliarão na demonstração, além de admitirmos o algoritmo da divisão em *N.* Estes resultados estão baseados em GONÇALVES (2008, cap. II).

Princípio da Boa Ordenação: Se $S \subset Z$; S não vazio e S é limitado inferiormente, então S possui um mínimo.

Proposição 1 – (*Primeiro Princípio de Indução*) Suponha que $P(n)$ é uma afirmação que depende de $n \in Z$ e satisfaz:

i. $P(a)$ é verdadeira; $a \in Z$

ii. Se $P(k)$ é verdadeira então $P(k+1)$ é verdadeira; $k \geq a$.

Nestas condições $P(n)$ é verdadeira para todo $n \geq a$.

Proposição 2- (*Segundo Princípio de Indução*) Sejam $a \in Z$ e $P(n)$ uma afirmação que depende de $n \in Z$ tais que:

i. $P(a)$ é verdadeira.

ii. Se $m > a$ e $P(k)$ é verdadeira para todo $a \leq k < m$, então $P(m)$ é verdadeira.

Nestas condições $P(n)$ é verdadeira para todo $n \geq a$.

Teorema 1- (*Algoritmo da Divisão em N*) Sejam $n, d \in N$ e $d > 0$. Então existem únicos $q, r \in N$, tais que $n = qd + r$ e $0 \leq r < d$.

Teorema 2- (*Algoritmo da Divisão em Z*) Sejam a e $b \in Z$, $b \neq 0$. Então existem únicos $q, r \in Z$ tais que $a = bq + r$, com $0 \leq r < |b|$.

Demonstração: Inicialmente mostraremos a existência de q, r inteiros satisfazendo as condições e em seguida provaremos à unicidade. Para mostrar a existência analisamos dois casos:

1º caso: $b > 0$;

Se tivermos $a \geq 0$, o resultado segue do algoritmo da divisão em N;

Se $a < 0$, então $-a > 0$, assim, utilizando o algoritmo da divisão em N, podemos escrever: $-a = bq' + r'$, com $0 \leq r' < b$ e $q', r' \in N$.

$a = b(-q') - r'$ (1)

Se $r' = 0$, tome $q = -q'$ e $r = 0$, então $a = bq + r$, com $0 \leq r < b = |b|$.

Se $r' > 0$, temos que $r' < b$, então $0 < b - r' < b = |b|$;

Usando a equação (1) obtemos: $a = b(-q' - 1) + (b - r')$.

Tome $q = -q' - 1$ e $r = b - r'$. Então $a = bq + r$, com $0 \leq r < |b|$.

2º caso: $b < 0$.

Vamos aplicar o 1º caso para $-b > 0$.

Temos que $a=(-b)q'+r'$, com $q',r'\in Z$ e $0\le r'<|b|$.

$a=b(-q')+r'$. Assim basta fazermos $q=-q'$ e $r=r'$.

Para a unicidade, suponha que existam q_1,r_1 e q_2,r_2 inteiros tais que:

$a=bq_1+r_1$; com $0\le r_1<|b|$ (1)

$a=bq_2+r_2$; com $0\le r_2<|b|$. (2)

Vamos supor que $r_1\ne r_2$. Digamos $r_2>r_1$. Usando as expressões (1) e (2) podemos escrever a igualdade:

$bq_1+r_1=bq_2+r_2$

$b(q_1-q_2)=r_2-r_1>0$ (3)

Se $b>0$ temos:

$q_1-q_2>0$, assim $q_1-q_2\ge 1$, multiplicando por b, obtemos: $b(q_1-q_2)\ge b$.

Como $r_1\ge 0$, temos: $r_1+b(q_1-q_2)\ge b(q_1-q_2)\ge b=|b|$. Mas $r_1+b(q_1-q_2)=r_2$, portanto concluímos que $r_2\ge b=|b|$, o que é um absurdo, pois por hipótese $r_2<b$.

Se $b<0$, segue de (3) que $q_1-q_2<0$. Assim: $q_2-q_1>0\Rightarrow q_2-q_1\ge 1$, multiplicando por b, temos:

$b(q_2-q_1)\le b$, ou seja, $b(q_1-q_2)\ge -b=|b|$

Como $r_1\ge 0$, temos: $r_1+b(q_1-q_2)\ge b(q_1-q_2)\ge |b|$. Absurdo, pois $r_2<b$. Com isto verificamos que $r_1=r_2$ e $q_1=q_2$, provando a unicidade. ■

Dando continuidade ao estudo do conjunto dos números inteiros, provaremos que todo número inteiro não nulo pode ser escrito como uma combinação de fatores primos de maneira única. Este resultado é conhecido como Teorema Fundamental da Aritmética.

Definição 1: Um número $p\in Z$ é *primo* quando $p\ne\pm 1$ e os únicos divisores de p são ± 1 e $\pm p$.

Teorema 3: (Teorema Fundamental da Aritmética) Todo número inteiro $n\ne 0$, pode ser escrito como $n=u.p_1.p_2.....p_k$, onde $u\in\{-1,1\}$ e $0<p_1\le p_2\le\ldots\le p_k$ são números primos. Além disso, esta decomposição é única.

Demonstração:

É suficiente provarmos o teorema para $n\in N$, nesse caso $u=1$ e a expressão se reduz a $n=p_1.p_2...p_k$, com $0<p_1\le p_2\le\ldots\le p_k$ primos.

Usaremos indução sobre n.

Se $n=1$ temos que $n=u.p_1.p_2...p_k$; $u=1$ e $k=0$.

Vamos supor que todo número inteiro m, $1\leq m<n$ pode ser escrito como produto de primos. (hipótese de Indução). Provaremos que n também pode ser escrito como produto de primos.

Suponhamos, por absurdo, que n não pode ser escrito como produto de primos. Então n não é um número primo, e assim existem divisores d e d' de n tais que: $n=d.d'$; com $1<d$ e $d'<n$. Pela hipótese de indução temos: $d=q_1,q_2,...,q_r$; $q_1\leq...\leq q_r$ são primos positivos e $d'=q'_1,q'_2,...,q'_s$; $q_1\leq...\leq q_s$ são primos positivos. Seguindo que $n=d.d'=(q_1...q_r).(q'_1...q'_s)$; rearranjando os números primos podemos escrever: $n=p_1.p_2...p_k$, onde $k=r+s$ e $p_1\leq p_2\leq...\leq p_k$ como queríamos mostrar.

Unicidade: Seja $n=u.p_1.p_2...p_k$; $0<p_1\leq p_2\leq...\leq p_k$ primos e $n=u'.p'_1.p'_2...p'_s$; $0<p'_1\leq p'_2\leq...\leq p'_s$ primos. Assim $u.p_1.p_2...p_k = u'.p'_1.p'_2...p'_s \Rightarrow u=u'$ e $p_1.p_2...p_k = p'_1.p'_2...p'_s$. Provaremos que isto implica em $k=s$ e $p_i=p'_i$; $i=1,2,...,k$ usando indução sobre k.

Se $k=1$, temos $p_1=p'_1...p'_s$, assim p'_i/p_1 e como são primos positivos segue que $p_1=p'_1$ e, portanto $s=1=k$ e $p_1=p'_1$.

Suponhamos agora que a unicidade seja verdadeira toda vez que tivermos um produto de r fatores primos positivos, onde $1\leq r<k$ e vamos provar a unicidade para k fatores primos positivos.

Temos, $p_1.p_2...p_k = p'_1.p'_2...p'_s$, $k\geq 2$. Pelo Lema de Euclides $\exists j$, $1\leq j\leq s$ tal que p_1/p'_j e como são primos positivos temos que $p_1=p'_j$ para algum j, $1\leq j\leq s$. De modo análogo $p'_1=p_i$, para algum i, $1\leq i\leq k$. Agora como $p_1\leq p_2\leq...\leq p_k$ e $p'_1\leq p'_2\leq...\leq p'_s$ segue que $p_1=p'_1$. Assim teremos $p_2...p_k=p'_2...p'_s$ e pela hipótese de indução $(r=k-1)$ temos $k-1=s-1$ e $p_2=p'_2...p_k=p'_k$, donde concluímos que $k=s$ e $p_i=p'_i$, $i=1,2,...,k$, como queríamos mostrar.

■

Como mostramos nesta seção, o conjunto dos números inteiros possui muitas propriedades. Poderíamos então nos questionar porque surgiram tantos outros conjuntos numéricos? "*Um dos motivos que historicamente motivaram o aparecimento de outros conjuntos numéricos está relacionado à solubilidade de equações*". (Andrade, 2001). Sendo assim, antes de analisarmos outros conjuntos numéricos, vamos definir o que é equação e o que significa solucioná-la.

Definição 2: Uma *equação polinomial* é uma expressão da forma:

$a_n x^n + a_{n-1}x^{n-1} + ... + a_2 x^2 + a_1 x + a_0 = 0$; onde os $a_{i's}$ são os '*coeficientes*', e $n\in N$ é o *grau* da equação.

Os coeficientes de uma equação podem ser naturais, inteiros, racionais, irracionais, reais ou complexos. Resolver uma equação polinomial significa encontrar um valor α para o qual a igualdade $a_n\alpha^n + a_{n-1}\alpha^{n-1} + ... + a_2\alpha^2 + a_1\alpha + a_0 = 0$ é verdadeira.

Ocorre muitas vezes que α não pertence ao mesmo conjunto dos coeficientes da equação: se considerarmos, por exemplo, a equação $nx = m$, onde m e n são inteiros, nem sempre existe $x \in Z$ que a satisfaz; com isso somos levados a introduzir um novo conjunto numérico: O conjunto dos números Racionais (Q), onde a equação acima sempre admite solução para $n \neq 0$. Este conjunto é o tema de nossa próxima seção.

2.2 – O CONJUNTO DOS NÚMEROS RACIONAIS (Q)

Definição 3: Um número racional é um número que pode ser colocado na forma $\frac{a}{b}$, $a,b \in Z$ e $b \neq 0$.

Diremos que um número racional $\frac{a}{b}$, $b \neq 0$, está na forma irredutível se $MDC(a,b) = 1$, isto é, se não é possível simplificar este número.

No conjunto Q, definimos as operações soma (+) e produto (.):

$$+ : Q \times Q \to Q \qquad \text{e} \qquad \bullet : Q \times Q \to Q$$

$$(\frac{a}{b}, \frac{c}{d}) \to \frac{ad+bc}{b.d} \qquad\qquad (\frac{a}{b}, \frac{c}{d}) \to \frac{a.c}{b.d}$$

Estas operações satisfazem as propriedades definidas na seção 2.1 (I – IX); além de uma outra: no conjunto dos números racionais existe o elemento inverso para a multiplicação, exceto para o zero, isto é, seja $x = \frac{a}{b} \in Q$; $x \neq 0$; existe $y \in Q$; $y = \frac{b}{a}$ tal que $x.y = 1$. Sendo assim, como afirmamos acima, se tomarmos a equação $nx = m$, com $n, m \in Q$, $n \neq 0$ teremos que $x = \frac{m}{n}$ a satisfaz.

Consideremos agora a seguinte equação: $x^2 - 2 = 0$. Uma solução é $\sqrt{2}$, mas $\sqrt{2}$ não pode ser expressa como razão de inteiros, ou seja, $\sqrt{2}$ não é racional. Assim precisamos considerar um conjunto numérico mais abrangente, onde esta solução seja concebível, o conjunto dos números reais, tema da próxima seção.

2.3 – O CONJUNTO DOS NÚMEROS REAIS (R)

Em R, também estão definidas as operações de adição (+) e multiplicação ($\bullet$):

$$+ : R \times R \to R \qquad \text{e} \qquad \bullet : R \times R \to R$$

$$(x,y) \to x+y \qquad\qquad (x,y) \to x.y.$$

Estas duas operações definidas em R satisfazem as propriedades de (I – IX) descritas na seção 2.1, além de neste conjunto também existir o elemento inverso para a multiplicação.

Consideremos agora a seguinte equação: $x^2+1=0$, a qual possui coeficientes reais, que pode ser escrita como $x^2=-1$, mas esta expressão não possui solução em R, já que sendo $x \in R$, o quadrado de x sempre é maior ou igual a zero. Neste caso, ou admitimos que a equação não tem solução ou então consideramos um outro conjunto numérico: o conjunto dos números complexos.

Segundo Milies, os matemáticos europeus ainda não tinham clareza da utilização de números negativos ou dos irracionais, quando surgiram os números hoje denominados *complexos.* Neste conjunto numérico podemos extrair a raiz quadrada de números negativos, o que resolve o problema da equação considerada acima e muitos outros que angustiaram os matemáticos no decorrer da história.

Na publicação denominada *l'Algebra,* 1572, de autoria de Raphael Bombelli, em um dos capítulos, estuda-se a resolução de equações de grau até quatro. Ao considerar a equação $x^3=15x+4$, ele obtém, utilizando a fórmula de Cardano, que será estudada adiante, a seguinte raiz: $x=\sqrt[3]{2+\sqrt{-121}}+\sqrt[3]{2-\sqrt{-121}}$, porém ele percebe que $x=4$ é uma raiz da equação. "*Eis uma situação em que apesar de termos radicais de números negativos, sabemos que existe uma solução para a equação proposta, então precisamos entender o que está acontecendo.*" (MILIES, p. 16).

Na próxima seção definiremos os números complexos e apresentaremos algumas de suas propriedades que serão relevantes durante o estudo das soluções de equações de 3° e 4° graus, tema principal deste trabalho. Não poderíamos falar das soluções de equações cúbicas sem antes estudar detalhadamente os números complexos, já que a necessidade de se trabalhar com estes números surge durante o estudo de soluções para equações de terceiro grau. Os resultados seguintes estão baseados em JANESCH e TANEJA, (2008, cap.6).

2.4 – O CONJUNTO DOS NÚMEROS COMPLEXOS (C)

Definição 4: Um número *complexo,* z é uma expressão da forma $a+bi$, onde $a,b \in R$, e o símbolo *i*, usado para indicar $\sqrt{-1}$, é tal que $i^2=-1$.

No número complexo $z=a+bi$, chamamos $a=\mathrm{Re}(z)$ de parte real de z e $b=\mathrm{Im}(z)$ é o coeficiente da parte imaginária bi. Temos $a+bi=c+di \Leftrightarrow a=c$ e $b=d$.

Definimos as operações de adição (+) e multiplicação (•) pelas seguintes regras:

$$+ : C \times C \to C \qquad\qquad \bullet : C \times C \to C$$

$$(a+bi, c+di) \to (a+c)+(b+d)i \qquad (a+bi, c+di) \to (ac-bd)+(ad+bc)i.$$

Para estas operações continuam válidas as propriedades de (I – IX , seção 2.1) e também existe o elemento inverso para a multiplicação. Neste conjunto, o simétrico de $a+bi$ é $-a-bi$, a unidade é $1+0i$ e o inverso multiplicativo de $a+bi \neq 0$ é $\left(\left(\dfrac{a}{a^2+b^2}\right)-\left(\dfrac{b}{a^2+b^2}\right)i\right)$.

Segue ainda da regra da multiplicação definida acima que $(a+bi).(a-bi)=(a^2+b^2)+(-ab+ba)i=a^2+b^2$. A expressão $a-bi$ é chamada de *conjugado* de z, e denotada por $\bar{z}$.

Chamamos de *norma* de um número complexo $z=a+bi$, a expressão $\sqrt{a^2+b^2}$, e denotamos por $|z|$. Também pode ser chamada de módulo ou valor absoluto. Se considerarmos $z=a+bi$ representado pelo par ordenado (a,b), a norma $|z|$ é a distância deste ponto à origem (0,0). (figura 1)

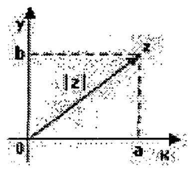

Figura1: representação geométrica da norma de z.

Destacamos as principais propriedades de *norma*:

1) $|z|\geq 0$;

2) $|z|=0 \Leftrightarrow z=0$;

3) $|z.w|=|z|.|w|$ e

4) $|z+w|\leq|z|+|w|$

Além da representação algébrica $z=a+bi$, existe uma outra, chamada de *trigonométrica* ou *polar*, muito útil no cálculo de potências e raízes de um número complexo: Seja $z=a+bi\in C$, $z\neq 0$, consideramos este número representado no plano cartesiano. Sabemos que a distância de z até a origem é $|z|$. Sendo t o ângulo entre este segmento e o eixo positivo OX, conforme representado na figura 2, temos

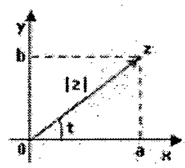

Figura2: Representação geométrica do argumento de z.

$\cos t=\dfrac{a}{|z|}\Rightarrow a=|z|\cos t$

$sen\, t=\dfrac{b}{|z|}\Rightarrow b=|z| sen\, t$, o que nos dá:

$z=|z|(\cos t+i\, sen\, t)$; $0\leq t<2k\pi$.

Esta é a representação polar de z, o ângulo t é chamado de argumento de z e denotado por $\arg(z)$, podemos calculá-lo fazendo $\arg(z) = arctg\left(\frac{b}{a}\right)$. Tomamos $z \neq 0$, para que a representação polar fosse única, no caso $z = 0$, podemos representá-lo de vários modos, por exemplo, $0 = |0|.\left(\cos\frac{\pi}{2} + i\, sen\frac{\pi}{2}\right)$ ou $0 = |0|(\cos\pi + i\, sen\,\pi)$.

Agora veremos uma proposição, devida a Abraham de Moivre (1667 – 1754), a qual nos mostra uma fórmula útil no cálculo de potências de números complexos escritos na forma trigonométrica.

Proposição 4 : (Primeira Fórmula de Moivre) Se $z = |z|(\cos t + i\, sen\, t)$, e $n \in N$, então $z^n = |z|^n(\cos n.t + i\, sen\, n.t)$.

Demonstração: Usaremos indução sobre n:

Para $n = 0$, a fórmula é válida, temos: $z^0 = 1 = 1.(\cos\ 0 + i\, sen\, 0) = |z|^0(\cos 0.t + i\, sen\, 0.t)$.

Suponhamos, por hipótese de indução, que a fórmula seja valida para $n = k$, isto é: $z^k = |z|^k(\cos k.t + i\, sen\, k.t)$. Mostraremos que a fórmula é valida para $n = k+1$.

$z^{k+1} = z^k.z = |z|^k(\cos k.t + i\, sen\, k.t).|z|.(\cos t + i\, sen\, t) =$

$|z|^{k+1}((\cos kt.\cos t - sen\, kt.\, sen\, t\ ) + (\cos kt.\, sen\, t + sen\, kt.\cos t)i)$, usando fórmulas trigonométricas obtemos: $z^{k+1} = |z|^{k+1}(\cos(k+1).t + i\, sen\,(k+1).t)$, como queríamos. Portanto a fórmula $z^n = |z|^n(\cos n.t + i\, sen\, n.t)$ é valida para todo $n \in N$. ■

No próximo capitulo, onde estaremos tratando da resolução de equações polinomiais de 3° e 4° graus, vamos precisar extrair raízes de números complexos, sendo assim, vamos agora definir o que se entende por raiz de um número complexo e em seguida veremos uma maneira de se calcular estas raízes, conhecida como Segunda Fórmula de Moivre.

Definição 5: Sejam $n \in N^*$ e $z \in C$. Chamamos de *raiz n-ésima complexa de z* os números complexos que são solução da equação $x^n = z$.

Proposição 5: (Segunda Fórmula de Moivre) Sejam $n \in N^*$ e $z = |z|(\cos t + i\, sen\, t) \in C^*$, existem exatamente n raízes complexas de z dadas por $M_k = \sqrt[n]{|z|}\left(\cos\left(\frac{t + 2k\pi}{n}\right) + i\, sen\left(\frac{t + 2k\pi}{n}\right)\right)$, $k = 0, 1, \ldots, n-1$.

Demonstração: Note inicialmente que M_k é raiz n-ésima complexa de z, já que $(M_k)^n = (\sqrt[n]{|z|})^n\left(\cos\left(\frac{n.(t+2k\pi)}{n}\right)+i\,sen\left(\frac{n.(t+2k\pi)}{n}\right)\right) = |z|(\cos(t+2k\pi)+i\,sen(t+2k\pi)) = |z|(\cos t + i\,sen\,t) = z$.

Mostraremos agora que toda raiz n-ésima complexa de z é da forma M_k; $k \in \{0,1,\ldots,n-1\}$.

Seja $\alpha = |\alpha|(\cos x + i\,sen\,x)$ raiz n-ésima complexa de z, então $\alpha^n = z$, ou seja: $|\alpha|^n(\cos nx + i\,sen\,nx) = |z|(\cos t + i\,sen\,t)$. Como a representação na forma trigonométrica é única, segue que $|\alpha|^n = |z|$ e $n.x = t + 2p\pi$, $p \in Z$.

Assim $\alpha = \sqrt[n]{|z|}\left(\cos\left(\frac{t+2p\pi}{n}\right)+i\,sen\left(\frac{t+2p\pi}{n}\right)\right)$; $p \in Z$.

Dividindo p por n, escrevemos $p = nq + k$, $0 \le k < n$, isto é $k \in \{0,1,\ldots,n-1\}$. Assim temos:

$\frac{t+2p\pi}{n} = \frac{t+2nq\pi+2k\pi}{n} = \frac{t+2k\pi}{n} + 2q\pi$; Como

$$\cos\left(\frac{t+2p\pi}{n}\right) = \cos\left(\frac{t+2k\pi}{n}+2q\pi\right) = \cos\left(\frac{t+2k\pi}{n}\right) \text{ e}$$

$$sen\left(\frac{t+2p\pi}{n}\right) = sen\left(\frac{t+2k\pi}{n}+2q\pi\right) = sen\left(\frac{t+2k\pi}{n}\right),$$

concluímos $\alpha = \sqrt[n]{|z|}\left(\cos\left(\frac{t+2k\pi}{n}\right)+i\,sen\left(\frac{t+2k\pi}{n}\right)\right)$; $k \in \{0,1,\ldots,n-1\}$.■

2.5 – ANEL

Seja A um conjunto não vazio onde estejam definidas duas operações, chamadas de *soma* e *produto*, denotadas respectivamente por + e •, da seguinte maneira:

$$+: A \times A \to A \qquad \text{e} \qquad \bullet: A \times A \to A$$
$$(a,b) \to a+b \qquad\qquad (a,b) \to a.b.$$

Definição 6: Dizemos que $(A,+,\bullet)$ é *anel* se para quaisquer x, y e $z \in A$, as seis propriedades seguintes são satisfeitas:

I. *Associatividade* da soma: $(x+y)+z = x+(y+z)$.

II. Existência do *elemento neutro* para soma: $\exists\ 0 \in A$, tal que: $x+0 = x; \forall\, x \in A$.

III. Existência do *inverso aditivo*: $\forall x \in A \quad \exists! \quad y \in A$, denotado por $y = -x$ tal que: $x+y = y+x = 0$.

IV. *Comutatividade* da soma: $x+y = y+x$.

V. *Associatividade* do produto: $(x.y).z = x.(y.z)$

VI. *Distributividade* do produto em relação à soma: $x.(y+z) = x.y + x.z$; $(x+y).z = x.z + y.z$.

Definição 7: Se um anel $(A,+,\bullet)$ satisfaz a seguinte propriedade:

VII. Existência da *unidade*: $\exists\ 1 \in A,\ 0 \neq 1$, tal que $1.x = x.1 = x;\ \forall x \in A$; dizemos que $(A,+,\bullet)$ é *um anel com unidade* 1.

Definição 8: Se um anel $(A,+,\bullet)$ satisfaz a seguinte propriedade:

VIII. *Comutatividade* do produto: $\forall x.y \in A,\ x.y = y.x$; dizemos que $(A,+,\bullet)$ é *anel comutativo.*

Definição 9: Se um anel $(A,+,\bullet)$ satisfaz a seguinte propriedade:

IX. $\forall x, y \in A,$ se $x.y = 0$, então $x = 0$ ou $y = 0$. Dizemos que $(A,+,\bullet)$ é *um anel sem divisores de zero.*

Definição 10: $(A,+,\bullet)$ é chamado *Domínio de Integridade* se é anel comutativo, com unidade e sem divisores de zero.

Os conjuntos numéricos Z, Q, R e C, com as operações usuais são exemplos de domínios de integridade.

2.6 – CORPO

Definição 11: Se um Domínio de Integridade $(A,+,\bullet)$ satisfaz a propriedade:

X. $\forall x \in A, x \neq 0, \exists y \in A$ tal que $x.y = y.x = 1$, dizemos que $(A,+,\bullet)$ é um *corpo*.

Os conjuntos Q, R e C são exemplos de corpos.

2.7 – ANEL DE POLINÔMIOS

Definição 12: Seja A um anel. Um *polinômio* sobre A, na indeterminada x, é uma expressão na forma: $a_0 + a_1x + a_2x^2 + \ldots$; onde $a_i \in A$, $\forall i \in N$, e existe $n \in N$, tal que $a_j = 0$, para $j > n$. **Notação:** $p(x) = a_0 + a_1x + a_2x^2 + \ldots + a_nx^n$. Os $a_i's$ são chamados de coeficientes.

Quando $a_n \neq 0$ dizemos que $p(x)$ tem *grau* n, e denotamos $\partial(p(x)) = n$. Se $a_n = 1$, $p(x) = a_0 + a_1x + a_2x^2 + \ldots + x^n$ é chamado de *polinômio mônico*. Ainda, um polinômio é chamado *nulo*, quando todos os coeficientes são iguais a zero, neste caso o grau não esta definido.

Seja A um anel. O conjunto de todos os polinômios em x, sobre A, é denotado por $A[x]$. $A[x] = \{a_0 + a_1x + a_2x^2 + \ldots a_nx^n; n \in N; a_i \in A\}$. Agora definiremos a igualdade de polinômios.

Definição 13: Sejam $p(x) = a_0 + a_1x + a_2x^2 + \ldots \in A[x]$ e $q(x) = b_0 + b_1x + b_2x^2 + \ldots \in A[x]$. Temos $p(x) = q(x)$ se, e somente se, $a_i = b_i$; $\forall i \in N$.

Em $A[x]$, definimos as seguintes operações:

+: $p(x) + q(x) = (a_0 + b_0) + (a_1 + b_1)x + \ldots \in A[x]$

$\bullet$: $p(x).q(x) = c_0 + c_1x + c_2x^2 + \ldots \in A[x]$, onde $c_k = \sum_{i+j=k} a_ib_j$

Teorema 4: Seja A um anel. Então:

i) $A[x]$ é anel.

ii) Se A é comutativo, então $A[x]$ é comutativo.

iii) Se A tem unidade 1, então $A[x]$ tem unidade $g(x) = 1$.

iv) Se A é domínio de integridade, então $A[x]$ também o é.

Observação: Mesmo que A seja um corpo, não teremos $A[x]$ sendo corpo, pois o polinômio $p(x) = x$ não é inversível, ou seja, não existe $q(x) \in A$, tal que $p(x).q(x) = 1$. Porém se $A = K$ é corpo, temos que $K[x]$ é um domínio de integridade, onde o polinômio nulo é o elemento neutro da adição e o polinômio constante 1 é a unidade em $K[x]$.

Sendo A um anel, nem todos os polinômios pertencentes a $A[x]$ são inversíveis, o resultado seguinte nos mostra o que ocorre no caso em que A é domínio de integridade.

Proposição 5: Se A é domínio de integridade, então os elementos inversíveis de A e de $A[x]$ coincidem, isto é, $U(A) = U(A[x])$.

Demonstração:

$U(A) \subset U(A[x])$

Seja $a \in U(A)$, então $a \in A$ e existe $b \in A$ tal que $a.b = 1$.

Tome $p(x) = a \in A[x]$ e $q(x) = b \in A[x]$. Assim a igualdade $a.b = 1$ pode ser escrita como $p(x).q(x) = 1$, o que nos mostra que $p(x) = a \in U(A[x])$.

$U(A[x]) \subset U(A)$

Seja $p(x) \in U(A[x])$. Então existe $q(x) \in A[x]$ tal que $p(x).q(x) = 1$. Como A é domínio, temos que $p(x) \neq 0$ e $q(x) \neq 0$. Assim

$\partial(1) = \partial(p(x).q(x)) = \partial(p(x)) + \partial(q(x))$. Mas $\partial(1) = 0$, logo $\partial(p(x)) = 0 = \partial(q(x))$, de onde concluímos que $p(x) = a \in A$ e $q(x) = b \in A$ e $a.b = 1$, ou seja, $a \in U(A)$.■

Lema 3: Sejam K um corpo e $p(x), q(x) \in K[x]^*$:

i) Se $p(x) + q(x) \neq 0$ então $\partial(p(x) + q(x)) \leq \text{máx } \{\partial(p(x)), \partial(q(x))\}$.

ii) $\partial(p(x).q(x)) = \partial(p(x)) + \partial(q(x))$

Demonstração:

i) Seja $p(x) = a_0 + a_1x + a_2x^2 + ... + a_nx^n$; $a_n \neq 0$ e $q(x) = b_0 + b_1x + b_2x^2 + ... + b_mx^m$; $b_m \neq 0$.

Vamos analisar três casos: $m > n$; $m = n$ e $m < n$.

1° caso: $m > n$.

$p(x) + q(x) = a_0 + b_0 + (a_1 + b_1)x + ... + (a_n + b_n)x^n + ... + b_mx^m$. Assim $\partial(p(x) + q(x)) = m = \text{máx}\{\partial(p(x), \partial(q(x))\}$.

2° caso: $m = n$

$p(x) + q(x) = a_0 + b_0 + (a_1 + b_1)x + ... + (a_n + b_n)x^n$. Pode ocorrer $a_n + b_n = 0$, sendo assim temos $\partial(p(x) + q(x)) \leq n = \text{máx}\{\partial(p(x), \partial(q(x))\}$

3° caso: $m < n$

$p(x)+q(x)=a_0+b_0+(a_1+b_1)x+...+(a_m+b_m)x^m+...+a_nx^n$. Assim $\partial(p(x)+q(x))=n=\text{máx}\{\partial(p(x),\partial(q(x))\}$.

ii) Seja $p(x)=a_0+a_1x+a_2x^2+...+a_nx^n$; $a_n\neq 0$ e $q(x)=b_0+b_1x+b_2x^2+...+b_mx^m$; $b_m\neq 0$.

$p(x).q(x)=a_0b_0+(a_0b_1+a_1b_0)x+...+(a_nb_m)x^{n+m}$. Como $a_n\neq 0$ e $b_m\neq 0$, segue que $a_nb_m\neq 0$. Logo $\partial(p(x).q(x))=n+m=\partial(p(x))+\partial(q(x))$.■

Teorema 5: (Algoritmo da divisão para polinômio) Sejam K um corpo, $f(x);g(x)\in K[x]$ e $g(x)\neq 0$. Então existem únicos $q(x);r(x)\in K[x]$, tais que $f(x)=g(x).q(x)+r(x)$ com $r(x)=0$ ou $\partial(r(x))<\partial(g(x))$.

Demonstração: Seja $f(x)=a_0+a_1x+a_2x^2+...+a_nx^n$ e $g(x)=b_0+b_1x+b_2x^2+...+b_mx^m$, ($\partial(g(x))=m$. Provaremos inicialmente a existência.

Se $f(x)=0$ basta tomarmos $q(x)=r(x)=0$. Suponhamos então que $f(x)\neq 0$, assim $\partial(f(x))=n$. Se $n<m$, tomamos $q(x)=0$ e $r(x)=f(x)$.

Veremos agora o caso em que $n\geq m$. Seja $f_1(x)$ o seguinte polinômio: $f(x)=a_nb_m^{-1}x^{n-m}.g(x)+f_1(x)$. $\partial f_1<\partial f$. Usaremos indução sobre o grau de f que sabemos ser n.

Se $n=0; n\geq m\Rightarrow m=0$, logo $f(x)=a_0\neq 0$; $g(x)=b_0\neq 0$ e teremos, $f(x)=a_0b_0^{-1}g(x)$, bastando tomar $q(x)=a_0b_0^{-1}$ e $r(x)=0$.

Como $f_1(x)=f(x)-a_nb_m^{-1}x^{n-m}g(x)$ e $\partial f_1(x)<\partial f(x)=n$, temos pela hipótese de indução que $\exists\ q_1(x),r_1(x)$ tais que $f_1(x)=q_1(x).g(x)+r_1(x)$, onde $r_1(x)=0$ ou $\partial r_1(x)<\partial g(x)$. Seguindo que $f(x)=\left(q_1(x)+a_nb_m^{-1}x^{n-m}\right)g(x)+r_1(x)$, e assim basta tomar $q(x)=q_1(x)+a_nb_m^{-1}x^{n-m}$ e $r(x)=r_1(x)$.

Vamos mostrar agora a unicidade, para isso, sejam: $q_1(x);q_2(x);r_1(x)$ e $r_2(x)$ tais que: $f(x)=g(x).q_1(x)+r_1(x)=g(x).q_2(x)+r_2(x)$, onde $r_i(x)=0$ ou $\partial(r_i(x))<\partial(g(x))$; $i=1,2$.

Daí segue que: $(q_1(x)-q_2(x)).g(x)=r_2(x)-r_1(x)$. Mas se $q_1(x)\neq q_2(x)$ o grau do polinômio à esquerda da igualdade é $\geq\partial(g(x))$ enquanto que $\partial(r_2(x)-r_1(x))<\partial(g(x))$, o que nos dá uma contradição. Logo devemos ter $q_1(x)=q_2(x)$, donde $r_1(x)=f(x)-q_1(x)g(x)=f(x)-q_2(x)g(x)=r_2(x)$ como queríamos. ■

Definição 14: Se $f(x) = a_0 + a_1x + ... + a_nx^n$ é um polinômio não nulo em $K[x]$ e $\alpha \in K$ é tal que $f(\alpha) = a_0 + a_1\alpha + ... + a_n\alpha^n = 0 \in K$, dizemos que α é uma *raiz de f(x)* em *K*.

O resultado a seguir nos mostra que o número de raízes de um polinômio em um corpo não excede o seu grau.

Proposição 6: Seja K um corpo e seja $f(x) = a_0 + a_1x + ... + a_nx^n$ um polinômio não nulo em $K[x]$ de grau *n*. Então o número de raízes de $f(x)$ em *K* é no máximo igual a $\partial(f(x)) = n$.

Demonstração: Se $f(x)$ não possui raízes em *K*, a proposição está provada. Suponhamos então que $\alpha \in K$ seja uma raiz de $f(x)$. Como $g(x) = x - \alpha \in K[x]$, podemos usar o algoritmo da divisão. Assim $\exists q(x), r(x) \in K[x]$ tais que $f(x) = q(x).(x-\alpha) + r(x)$ onde $r(x) = 0$ ou $\partial(r(x)) < \partial(g(x)) = 1$. Assim $r(x) = b_0$ é um polinômio constante, e temos $f(x) = q(x).(x-\alpha) + b_0$ e como α é uma raiz temos também que $f(\alpha) = 0 = 0 + b_0$ ou seja, $r(x) = 0$ e $f(x) = q(x).(x-\alpha)$ onde $\partial q(x) = n-1$. Agora como não existem divisores de zero em um corpo, temos que se $\beta \in K$ é uma raiz qualquer de f então, $f(\beta) = (\beta - \alpha).q(\beta) = 0 \Rightarrow \beta = \alpha$ ou β é uma raiz de $q(x) \in K[x]$. Assim as raízes de f são α e as raízes de $q(x)$. Usaremos indução sobre $\partial f = n$. Se $n = 0$ f não possui raízes em K e a proposição é valida. Agora por indução, $\partial q(x) < \partial f(x) = n$, $q(x)$ possuí no máximo $\partial q(x) = n - 1$ raízes em k e, portanto $f(x)$ possuí no máximo n raízes em K, como queríamos mostrar. ■

Definição 15: Se $L \supset K$ é um corpo dizemos que L é uma *extensão* de K .

Corolário 1: Seja $f(x) = a_0 + a_1x + ... + a_nx^n$ um polinômio não nulo de grau n em $K[x]$. Então, $f(x)$ possui no máximo n raízes em qualquer extensão L de K.

Demonstração: Segue do fato de que se $f(x) \in K[x]$ e $K \subset L$, $f(x) \in L[x]$, assim basta aplicar a proposição 7 para o corpo L. ■

Considere o polinômio $x^3 - 2 = 0$. Observe que no corpo Q ele não possuí raízes, no corpo R possui uma raiz e em C possui três raízes, isto é, ao estendermos o corpo, podemos conhecer mais raízes de um determinado polinômio, porém o número de raízes é limitado pelo grau do polinômio. Esta é uma maneira mais sofisticada de tratarmos aquilo que viemos fazendo no decorrer deste capítulo, quando passamos a definir novos conjuntos numéricos para que pudéssemos encontrar raízes para determinadas equações polinomiais.

No próximo capítulo, estaremos analisando uma maneira de encontrar as raízes de equações polinomiais de terceiro e quarto graus, com coeficientes reais; veremos que para determinar as raízes, necessitamos dos números complexos.

3 – RESOLUÇÃO DE EQUAÇÕES DE 3° E 4° GRAUS.

Atualmente, ao ouvirmos falar em "equação do 2° grau" logo nos vem à mente a expressão $ax^2+bx+c=0$, e rapidamente lembramos a famosa fórmula de Bhaskara para encontrar suas raízes, que são dadas por $x=\dfrac{-b\pm\sqrt{b^2-4ac}}{2a}$; porém ao longo da história as coisas não aconteceram da maneira simples que estamos acostumados a ver nos livros.

Primeiramente as tentativas de resolução de equações demonstraram a necessidade de se ter uma notação mais sofisticada. O uso da letra para representação da incógnita, aparece na *Aritmética* de **Diophanto**, no século IV d.C.. Somente em 1585, na obra *"L' Arithmetique"*, **Simon Stevin** introduz uma notação exponencial para denotar as diferentes potências de uma incógnita. Nesta época já se sabia que os métodos para resolução de equações não dependem dos coeficientes numéricos, mas sim do grau da equação. Mais tarde, em 1591, **François Viète,** utilizou letras para representar também os coeficientes, ele sabia que assim poderia trabalhar com *classes de equações*, ao passo que com o emprego dos números trabalhava com um exemplo por vez. (MILIES, cap. 1)

Apesar de existirem diferentes métodos para a resolução de equações, como por exemplo as Construções Geométricas, que resolvem alguns tipos de equações de grau dois, destacaremos aqui o método aritmético, onde as soluções são expressas por radicais.

3.1 – Fórmula de Cardano-Tartaglia para resolução de equações de 3° grau.

Consideramos a equação

(1) $z^3+az^2+bz+c=0$, onde a,b e c são números reais.

Primeiramente vamos reduzir a solução da equação (1) a solução da equação $x^3+px+q=0$, a qual não contém o termo quadrático. Para isto procuramos uma substituição para a variável z. Façamos

$z=x+t$,

$(x+t)^3+a(x+t)^2+b(x+t)+c=0$,

$x^3+3x^2t+3t^2x+t^3+ax^2+2axt+at^2+bx+bt+c=0$

$x^3+(3t+a)x^2+(3t^2+2at+b)x+(t^3+at^2+bt+c)=0$; queremos anular o coeficiente do termo quadrático, então:

$3t+a=0$; o que implica $t=-\dfrac{a}{3}$.

Logo a substituição procurada é $z=x-\dfrac{a}{3}$. Assim temos:

$\left(x-\dfrac{a}{3}\right)^3+a\left(x-\dfrac{a}{3}\right)^2+b\left(x-\dfrac{a}{3}\right)+c=$

$$x^3 - ax^2 + \frac{a^2}{3}x - \frac{a^3}{27} + ax^2 - \frac{2a^2x}{3} + \frac{a^3}{9} + bx - \frac{ab}{3} + c =$$

$x^3 + \left(b - \frac{a^2}{3}\right)x + \left(\frac{2a^3}{27} - \frac{ab}{3} + c\right) = 0$. Fazendo $p = b - \frac{a^2}{3}$ e $q = \left(\frac{2a^3}{27} - \frac{ab}{3} + c\right)$, obtemos a equação pretendida:

(2) $x^3 + px + q = 0$

Agora passamos a resolver a equação (2); para isto façamos $x = u + v$; assim temos:

(3) $(u+v)^3 + p(u+v) + q = 0$, desenvolvendo o termo cúbico vêm:

$$u^3 + v^3 + 3u^2v + 3uv^2 + p(u+v) + q = 0$$
$$u^3 + v^3 + 3uv(u+v) + p(u+v) + q = 0$$

(4) $(u^3 + v^3 + q) + [(3uv + p)(u+v)] = 0$

Para solucionar a equação (4) basta encontrarmos u e v tais que:

$\begin{cases} u^3 + v^3 + q = 0 \\ 3uv + p = 0 \end{cases}$; ou ainda $\begin{cases} u^3 + v^3 = -q & (5) \\ u^3.v^3 = -\frac{p^3}{27} & (6) \end{cases}$

Isolando v^3 na equação (6), temos $v^3 = -\frac{p^3}{27}.\frac{1}{u^3}$. Agora substituindo v^3 na equação (5), e realizando alguns cálculos, obtemos:

(7) $$(u^3)^2 + q.u^3 - \frac{p^3}{27} = 0;$$

A equação acima é quadrática, sendo assim podemos aplicar a fórmula de Bhaskara para resolvê-la, seguindo que:

$u^3 = \left[-q \pm \sqrt{q^2 - 4.\left(\frac{-p^3}{27}\right)}\right].\frac{1}{2} \Rightarrow u^3 = \frac{-q}{2} \pm \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}$; escolhemos $u^3 = \frac{-q}{2} + \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}$ e substituímos na equação (5), temos então que: $v^3 = \frac{-q}{2} - \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}$.

Finalmente, como $x = u + v$, concluímos

$x = \sqrt[3]{\frac{-q}{2} + \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}} + \sqrt[3]{\frac{-q}{2} - \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}}$, que é a fórmula de Tartaglia-Cardano.■

Para obtermos as três raízes de uma equação cúbica utilizando esta fórmula, será preciso considerar as raízes cúbicas da unidade, como veremos na próxima seção.

3.2 - Discussão da fórmula de Tartaglia-Cardano para alguns casos particulares.

Inicialmente, considere a equação $x^3 - 1 = 0$.

Note que $x = 1$ é uma raiz, assim temos que: $x^3 - 1 = (x-1)(x^2 + x + 1)$, calculemos as raízes da equação $x^2 + x + 1 = 0$. Por Bhaskara, obtemos:

$$x = \left(-1 \pm \sqrt{1^2 - 4.1.1}\right)\frac{1}{2} = \frac{-1}{2} \pm \frac{\sqrt{-3}}{2} = -\frac{1}{2} \pm \frac{i\sqrt{3}}{2};$$

Logo as soluções de $x^3 - 1 = 0$, são:

$x_1 = -1$; $x_2 = -\frac{1}{2} + \frac{i\sqrt{3}}{2}$ e $x_3 = -\frac{1}{2} - \frac{i\sqrt{3}}{2}$. Observe que x_3 é o conjugado de x_2, assim fazendo

$\alpha = -\frac{1}{2} + \frac{i\sqrt{3}}{2}$, podemos reescrever as soluções como:

$x_1 = -1$; $x_2 = \alpha$ e $x_3 = \overline{\alpha}$.

Considere a equação $x^3 - h = 0$, onde h é um número real. As soluções desta equação são dadas por:

$x = \sqrt[3]{h} = \sqrt[3]{h.1} = \sqrt[3]{h}.\sqrt[3]{1} = \sqrt[3]{h}.1$; $\sqrt[3]{h}.\alpha$ e $\sqrt[3]{h}.\overline{\alpha}$.

Na fórmula de Tartaglia-Cardano, façamos $\frac{q^2}{4} + \frac{p^3}{27} = \Delta$, podemos então reescrevê-la como:

$$x = \sqrt[3]{-\frac{q}{2} + \sqrt{\Delta}} + \sqrt[3]{-\frac{q}{2} - \sqrt{\Delta}}.$$

Passaremos agora a analisar os seguintes casos: $\Delta > 0$, $\Delta = 0$ e $\Delta < 0$.

1° caso) $\Delta > 0$: Assim temos que $\sqrt{\Delta}$ é real e cada raiz cúbica é obtida multiplicando-se as raízes cúbicas reais u e v, pelas raízes cúbicas da unidade. Seguindo que:

$\sqrt[3]{-\frac{q}{2} + \sqrt{\Delta}} = u.1,\ u.\alpha,\ u.\overline{\alpha}$ e

$\sqrt[3]{-\frac{q}{2} - \sqrt{\Delta}} = v.1,\ v.\alpha,\ v.\overline{\alpha}$,

Então $\sqrt[3]{-\frac{q}{2} + \sqrt{\Delta}} + \sqrt[3]{-\frac{q}{2} - \sqrt{\Delta}}$ pode ser formado de nove maneiras:

$u + v$; $u + v.\alpha$; $u + v.\overline{\alpha}$; $u.\alpha + v$; $(u+v)\alpha$; $u.\alpha + v.\overline{\alpha}$; $u.\overline{\alpha} + v$; $u.\overline{\alpha} + v.\alpha$; $(u+v)\overline{\alpha}$

No entanto temos que $u.v = -\frac{p}{3} \in R$. assim, satisfazendo esta condição as três soluções para a equação dada são: $x_1 = u + v = \sqrt[3]{\frac{-q}{2} + \sqrt{\Delta}} + \sqrt[3]{\frac{-q}{2} - \sqrt{\Delta}}$;

$$x_2 = u.\alpha + v\overline{\alpha} = \sqrt[3]{\frac{-q}{2} + \sqrt{\Delta}}.\ \alpha + \sqrt[3]{\frac{-q}{2} - \sqrt{\Delta}}.\ \overline{\alpha};$$

$$x_3 = u.\overline{\alpha} + v.\alpha = \sqrt[3]{\frac{-q}{2} + \sqrt{\Delta}}.\ \overline{\alpha} + \sqrt[3]{\frac{-q}{2} - \sqrt{\Delta}}.\ \alpha.$$

Isto significa que quando $\Delta > 0$ a equação dada possui uma raiz real e duas raízes complexas, as quais são conjugadas uma da outra.

2° caso) $\Delta = 0$: Logo $\sqrt{\Delta}$ é nula; $u = \sqrt[3]{\frac{-q}{2}}$ e $v = \sqrt[3]{\frac{-q}{2}}$. Então

$$x_1 = u + v = \sqrt[3]{\frac{-q}{2}} + \sqrt[3]{\frac{-q}{2}} = 2\sqrt[3]{\frac{-q}{2}};$$

$x_2 = u.\alpha + v\overline{\alpha}$; como $u = v$, temos: $x_2 = x_3 = u.(\alpha + \overline{\alpha}) = u.(-1) = \sqrt[3]{\frac{q}{2}}$.

Assim, quando $\Delta = 0$, a equação possui três raízes reais, sendo que duas são iguais.

3° caso) $\Delta < 0$: Neste caso $\sqrt{\Delta}$ é um número complexo e temos que:

$u^3 = \frac{-q}{2} + i\sqrt{-\Delta}$ e $v^3 = \frac{-q}{2} - i\sqrt{-\Delta}$, que são complexos conjugados.

Para calcularmos u e v, precisamos extrair as raízes complexas, sendo assim escreveremos u^3 e v^3 na forma trigonométrica, como definimos na seção 2.4:

$u^3 = |z|(\cos(t) + i\,sen(t))$ e $v^3 = |z|(\cos(t) - i\,sen(t))$.

Lembrando que:

$|z| = \sqrt{a^2 + b^2} = \sqrt{\left(\frac{-q}{2}\right)^2 + \left(\sqrt{-\Delta}\right)^2} = \sqrt{\frac{q^2}{4} - \left(\frac{q^2}{4} + \frac{p^3}{27}\right)} = \sqrt{\frac{-p^3}{27}}$ e o argumento

$$t = arctg\left(\frac{b}{a}\right) = arctg\left(\frac{\sqrt{-\Delta}}{\frac{-q}{2}}\right) = arctg\left(-\frac{2\sqrt{-\Delta}}{q}\right).$$

Utilizando a segunda fórmula de Moivre, encontramos três pares de raízes: u_0, v_0 ; u_1, v_1 e u_2, v_2 que são duas a duas conjugadas:

$u_0 = \sqrt[3]{|z|}.\left[\cos\left(\frac{t}{3}\right) + i\,sen\left(\frac{t}{3}\right)\right]$; $u_1 = \sqrt[3]{|z|}.\left[\cos\left(\frac{t+2\pi}{3}\right) + i\,sen\left(\frac{t+2\pi}{3}\right)\right]$ e

$$u_2=\sqrt[3]{|z|}.\left[\cos\left(\frac{t+4\pi}{3}\right)+i\,sen\left(\frac{t+4\pi}{3}\right)\right];$$

$$v_0=\sqrt[3]{|z|}.\left[\cos\left(\frac{t}{3}\right)-i\,sen\left(\frac{t}{3}\right)\right];\ v_1=\sqrt[3]{|z|}.\left[\cos\left(\frac{t+2\pi}{3}\right)-i\,sen\left(\frac{t+2\pi}{3}\right)\right]\text{ e}$$

$$v_2=\sqrt[3]{|z|}.\left[\cos\left(\frac{t+4\pi}{3}\right)-i\,sen\left(\frac{t+4\pi}{3}\right)\right].$$

Como devemos ter $u.v=-\frac{p}{3}\in R$, as soluções $x=u+v$ são dadas por:

$$x_1=u_0+v_0=\sqrt[3]{|z|}.\left[\cos\left(\frac{t}{3}\right)+i\,sen\left(\frac{t}{3}\right)\right]+$$

$$\sqrt[3]{|z|}.\left[\cos\left(\frac{t}{3}\right)-i\,sen\left(\frac{t}{3}\right)\right]=2\sqrt[3]{|z|}\cos\left(\frac{t}{3}\right);$$

$$x_2=u_1+v_1=2\sqrt[3]{|z|}\cos\left(\frac{t+2\pi}{3}\right)\text{ e}$$

$$x_3=u_2+v_2=2\sqrt[3]{|z|}\cos\left(\frac{t+4\pi}{3}\right).$$

Assim, quando $\Delta<0$, a equação possui três raízes reais e distintas.

Exemplo 1: Determine as raízes da equação $z^3-15z-4=0$

Neste caso temos $a=0$; $b=-15$ e $c=-4$, o que nos dá: $p=-15$ e $q=-4$. Assim encontramos $\Delta=-121$. Como $\Delta<0$, teremos três raízes reais e distintas.

$u^3=|z|(\cos(t)+i\,sen(t))$ e $v^3=|z|(\cos(t)-i\,sen(t))$.

$|z|=\sqrt{\frac{-p^3}{27}}=\sqrt{125}=5\sqrt{5}$ e o argumento $t=arctg\left(-\frac{2\sqrt{-\Delta}}{q}\right)=arctg\left(\frac{11}{2}\right)$. Logo

$$x_1=2\sqrt[3]{|z|}\cos\left(\frac{t}{3}\right)=2\sqrt[3]{5\sqrt{5}}\cos\left(\frac{t}{3}\right)\Rightarrow x_1=4.$$

$$x_2 = 2\sqrt[3]{|z|}\cos\left(\frac{t+2\pi}{3}\right) = 2\sqrt[3]{5\sqrt{5}}\cos\left(\frac{t+2\pi}{3}\right) \cong -3{,}72 \text{ e}$$

$$x_3 = 2\sqrt[3]{|z|}\cos\left(\frac{t+4\pi}{3}\right) = 2\sqrt[3]{5\sqrt{5}}\cos\left(\frac{t+4\pi}{3}\right) \cong -0{,}27.$$

3.3 – Método de Ferrari para solução de equações quarto grau.

Considere a equação geral de quarto grau:

(1) $z^4 + az^3 + bz^2 + cz + d = 0$

Para encontrar suas soluções transformaremos esta equação em uma outra equivalente com duas incógnitas, para isso iniciamos reescrevendo-a como:

$z^4 + az^3 = -bz^2 - cz - d$

Em seguida, somamos o termo $\frac{a^2z^2}{4}$ a ambos os membros da equação, obtendo:

$$\left(z^2 + \frac{az}{2}\right)^2 = \left(\frac{a^2}{4} - b\right)z^2 - cz - d.$$

Agora adicionamos membro a membro o termo $\left(z^2 + \frac{az}{2}\right)y + \frac{y^2}{4}$, o que nos dá:

(2) $\left(z^2 + \frac{az}{2} + \frac{y}{2}\right)^2 = \left(\frac{a^2}{4} - b + y\right)z^2 + \left(\frac{ay}{2} - c\right)z + \left(\frac{y^2}{4} - d\right)$; que é uma equação com duas incógnitas, z e y. O segundo membro da equação (2) é um trinômio de grau dois na indeterminada z, cujos coeficientes dependem de y. Escolhemos y para que este trinômio seja o quadrado de um binômio do primeiro grau $\alpha z + \beta$. Ou seja, queremos $Az^2 + Bz + C = (\alpha z + \beta)^2$.

Desenvolvendo o segundo membro da equação, obtemos:

$Az^2 + Bz + C = \alpha^2 z^2 + 2\alpha\beta z + \beta^2$, que é equivalente ao seguinte sistema de equações:

$\begin{cases} A = \alpha^2 \\ B = 2\alpha\beta \\ C = \beta^2 \end{cases}$; resolvendo o sistema, temos:

$\alpha = \sqrt{A}$; $\beta = \sqrt{C}$ e $B = 2\sqrt{AC} \Rightarrow B^2 = 4AC \Rightarrow B^2 - 4AC = 0$; onde

$A = \frac{a^2}{4} - b + y$; $B = \frac{ay}{2} - c$ e $C = \frac{y^2}{4} - d$. Substituindo os valores de A, B e C, obtemos a seguinte equação em y:

$\left(\frac{ay}{2} - c\right)^2 - 4\left(\frac{a^2}{4} - b + y\right)\left(\frac{y^2}{4} - d\right) = 0$. Desenvolvendo esta encontramos a equação cúbica

(3) $y^3 - by^2 + (ac - 4d)y - \left[d(a^2 - 4b) + c^2\right] = 0$.

Resolvemos a equação (3) utilizando as fórmulas de Tartaglia-Cardano, obtendo uma solução, digamos y_0, e assim determinamos α e β em função desta solução, ou seja:

(4) $\left(z^2 + \dfrac{az}{2} + \dfrac{y_0}{2}\right)^2 = (\alpha z + \beta)^2$.

Finalmente, a partir das duas equações quadráticas dadas em (4), encontramos as quatro raízes da equação considerada inicialmente. ■

Exemplo 2: Determine as quatro raízes da equação $z^4 - 1 = 0$.

Utilizando o método de Ferrari, obtemos a equação cúbica $y^3 + 4y = 0$. Resolveremos esta equação pela fórmula de Cardano-Tartaglia:

Temos $a = 0$; $b = 4$ e $c = 0$, assim

$p = b - \dfrac{a^2}{3} \Rightarrow p = 4$ e $q = \dfrac{2a^3}{27} - \dfrac{ba}{3} + c \Rightarrow q = 0$.

Calculando Δ obtemos $\Delta = \dfrac{64}{27} > 0$, logo a equação possui uma raiz real e duas raízes complexas que são conjugadas uma da outra:

$u = 2\sqrt[3]{\dfrac{1}{3\sqrt{3}}}$ e $v = -2\sqrt[3]{\dfrac{1}{3\sqrt{3}}}$

$y_1 = 0$

$$y_2 = \left[2\sqrt[3]{\frac{1}{3\sqrt{3}}}\left(\frac{-1}{2} + \frac{\sqrt{3}}{2}i\right)\right] + \left[-2\sqrt[3]{\frac{1}{3\sqrt{3}}}\left(\frac{-1}{2} - \frac{\sqrt{3}}{2}i\right)\right] = 2\sqrt{3}\sqrt[3]{\frac{1}{3\sqrt{3}}} = 2i.$$

$y_3 = -2i$.

Escolhemos uma das soluções para substituir na equação (4) . Seja $y_0 = 2i$. Assim :

$z^2 + i = \pm\sqrt{2i}$. Primeiramente $z^2 + i = +\sqrt{2i}$.

$z^2 + i = \sqrt{2i} \Rightarrow z^2 - \sqrt{2i} + i = 0$, resolvemos a equação quadrática pela fórmula de Bhaskara: $\Delta = 4$, $z = \dfrac{\pm 2}{2}$, ou seja: $z_1 = 1$ e $z_2 = -1$.

Agora façamos $z^2 + i = -\sqrt{2i} \Rightarrow z^2 + \sqrt{2i} + i = 0$, novamente por Bhaskara, obtemos: $\Delta = -4$, $z = \dfrac{\pm\sqrt{-4}}{2}$, ou seja: $z_3 = i$ e $z_4 = -i$.

Portanto as raízes quartas da unidade são $z_1 = 1$; $z_2 = -1$; $z_3 = i$ e $z_4 = -i$.

Exemplo 3: Determinar as quatro raízes da equação $z^4 - 5z^3 + 5z^2 + 5z - 6 = 0$.

Pelo método de Ferrari encontramos a equação cúbica auxiliar $y^3 - 5y^2 - y + 5 = 0$. Assim $a = -5$, $b = -1$ e $c = 5$. Inicialmente façamos a substituição $y = x + \dfrac{5}{3}$, obtendo a equação $x^3 - \dfrac{28}{3}x - \dfrac{160}{27} = 0$, onde $p = \dfrac{-28}{3}$ e $q = \dfrac{-160}{27}$. Calculando Δ obtemos $\Delta = \dfrac{-64}{3}$.

Agora vamos determinar u^3 e v^3, na forma trigonométrica:

$$|z| = \frac{56\sqrt{7}}{27} \text{ e } t = arctg\left(\frac{9\sqrt{3}}{10}\right) \Rightarrow t = 1.$$

$$x_1 = 2\sqrt[3]{\frac{56\sqrt{7}}{27}}.\cos\left(\frac{1}{3}\right) \Rightarrow x_1 \cong 3{,}35$$

Substituindo este valor em $y = x + \dfrac{5}{3}$ encontramos $y_0 = 5$.

Calculamos α e β: $\alpha = \dfrac{5}{2}$ e $\beta = \dfrac{7}{2}$. Assim $z^2 - \dfrac{5}{2}z + \dfrac{5}{2} = \dfrac{5z}{2} \pm \dfrac{7}{2}$. Primeiramente façamos $z^2 - \dfrac{5}{2}z + \dfrac{5}{2} = \dfrac{5z}{2} + \dfrac{7}{2}$, obtendo a equação quadrática $z^2 - 5z + 6 = 0$, cujas soluções são $z_1 = 3$ e $z_2 = 2$.

Agora façamos $z^2 - \dfrac{5}{2}z + \dfrac{5}{2} = \dfrac{5z}{2} - \dfrac{7}{2}$, que é equivalente a equação quadrática $z^2 - 1 = 0$, cujas soluções são $z_3 = 1$ e $z_4 = -1$.

Portanto as quatro raízes da equação $z^4 - 5z^3 + 5z^2 + 5z - 6 = 0$ são $z_1 = 3$; $z_2 = 2$; $z_3 = 1$ e $z_4 = -1$.

CONSIDERAÇÕES FINAIS

Após o surgimento das fórmulas de Tartaglia-Cardano e do Método de Ferrari, muitos matemáticos tentaram encontrar a solução geral para equações de grau maior ou igual a cinco. Como nenhum lograva êxito, começaram a acreditar que não haveria solução para o problema; até que em 1824, Abel provou que a equação geral de grau cinco não é solúvel por radicais. Mais tarde, Galois encontrou uma maneira de decidir quando uma equação é solúvel ou não por meio de radicais, através das propriedades do grupo de automorfismos de um corpo. Este resultado é considerado um dos mais belos da história da matemática e poderá ser abordado em estudos futuros.

REFERÊNCIAS

ANDRADE, Fernando Prado de. **Números Complexos e Multivetores no Plano.** Londrina: Midiograf, 2001.

GONÇALVES, Adilson. **Introdução à Álgebra.** Rio de Janeiro: Impa, 2008.

JANESCH, Oscar Ricardo e TANEJA, I. **Álgebra I**. EAD/UFSC. Florianópolis, 2008.

MILIES, César Polcino. **Breve História da Álgebra Abstrata.** São Paulo.