UNIVERSIDADE ESTADUAL DE GOIÁS
UNIDADE UNIVERSITÁRIA DE GOIÁS
CURSO DE MATEMÁTICA

UM ESTUDO SOBRE RAÍZES DE POLINÔMIOS CÚBICOS EM ANÉIS COMUTATIVOS

Willian Oliveira Lima de Abreu

Cidade de Goiás
2014

WILLIAN OLIVEIRA LIMA DE ABREU

UM ESTUDO SOBRE RAÍZES DE POLINÔMIOS CÚBICOS EM ANÉIS COMUTATIVOS

Monografia apresentada ao curso de Matemática da Unidade Universitária de Goiás – UEG, como um dos requisitos para obtenção do grau de licenciatura plena em Matemática.

Orientador: Prof°. Ms. Rosemberg Pereira Serrano

Cidade de Goiás
2014

Willian Oliveira Lima de Abreu

UM ESTUDO SOBRE RAÍZES DE POLINÔMIOS CÚBICOS EM ANÉIS COMUTATIVOS

Trabalho de Curso apresentado ao Curso de Matemática da Universidade Estadual de Goiás, da Unidade Universitária de Goiás como um dos requisitos para obtenção do título de Licenciado em Matemática.

Aprovado em 20 de novembro de 2014.

Comissão Examinadora

Rosemberg P. Serrano

Prof° Ms. Rosemberg Pereira Serrano – orientador

UEG/ Câmpus Goiás

Rodrigo Bastos Daude

Prof° Ms. Rodrigo Bastos Daúde

UEG/ Câmpus Goiás

Prof° Esp. Rejane Alves de Souza Tiago

UEG/ Câmpus Goiás

Dedico esse trabalho principalmente aos meus pais, que em todos os momentos nunca me negaram apoio, sempre me dizendo que a melhor saída é seguir em frente sem olhar para traz. Aos meus amigos e companheiros de toda uma trajetória de desafios e conquistas no decorrer dos últimos 4 anos.

AGRADECIMENTOS

Primeiramente agradeço a Deus por ter me dado forças para chegar até onde cheguei, pois sem a sua presença, nada disso seria possível.

Aos professores do curso de Matemática pela dedicação e preocupação em oferecer um conhecimento de qualidade para com os seus.

Ao professor orientador pelo seu tempo destinado às orientações e, sobretudo pela sua paciência em esclarecer as dúvidas que foram surgindo durante todo o processo de construção deste trabalho.

Aos meus amigos do curso por ter incentivado a continuar nessa caminhada, por maiores que seriam os obstáculos a enfrentar.

Aos meus pais, tios, avós e irmãos que sempre me apoiaram em todos os momentos neste longo percurso e por terem me feito pensar que desistir não é a solução.

O princípio criador reside na matemática; a sua certeza é absoluta, enquanto se trata de matemática abstrata, mas diminui na razão direta de sua concretização.

ALBERT EINSTEIN

RESUMO

O presente trabalho abordará os principais conceitos e resultados para a determinação de raízes de polinômios sobre um corpo qualquer, em especial de polinômios cúbicos pela dificuldade enfrentada por muitos estudantes, bem como do processo histórico e dos esforços enfrentados pelos principais matemáticos que focaram seus estudos para determinar as raízes de um dado polinômio. Assim, no decorrer dos estudos feitos, o leitor irá perceber que existem várias maneiras desenvolvidas por diferentes matemáticos para a determinação de raízes de polinômios, mais precisamente sobre polinômios cúbicos em anéis comutativos. Os processos que serão apresentados são processos simples e práticos de fácil compreensão, mas eficientes quando se trata de polinômios e a determinação de suas raízes, pois foram desenvolvidos para minimizar as dificuldades encontradas. Dessa forma, garantir a validade dos principais conceitos e resultados apresentados que serão discutidos no decorrer do texto por meio de exemplos práticos que contribuirá de forma significativa para um bom entendimento do leitor. A noção de grupos e anéis tratados aqui nos permitirá realizar estudos mais avançados sobre os processos para identificar as raízes de determinados polinômios e assim permitir o uso de outros mecanismos eficientes que serão tratadas detalhadamente no corpo deste trabalho, tais como a utilização de: algoritmos, definições, teoremas, software computacional e análises gráficas. Contudo, saber reconhecer quando é necessário utilizar os conceitos sobre extensões algébricas, principalmente quando nos deparamos com raízes quadradas de números negativos. E como existem polinômios cúbicos que não apresentam apenas raízes reais, apresentaremos métodos para a determinação de tais raízes.

Palavras-chaves: Extensões Algébricas. Polinômios Cúbicos. Raízes de Polinômios.

RESUMEM

El presente trabajo discutirá los principales conceptos y resultados para la determinación de raíces de polinomios sobre un cuerpo cualquier, en especial de polinomios cúbicos por la dificultad que enfrentan muchos estudiantes, así como todo proceso histórico y los esfuerzos enfrentados por los principales matemáticos que centraron sus estudios para determinar raíces de un polinomio dato. Así, en el transcurrir de los estudios, el lector irá percebe que hay varias maneras desarrollados por diferentes matemáticos para la determinación de raíces cúbicas en anillos de polinomio, más precisamente en polinomios cúbicos en anillos conmutativos. Los procesos que serán presentados son procesos sencillos y prácticos de fácil comprensión, pero eficiente cuando tratase de polinomios y la determinación de sus raíces, ya que fueron desarrollados para las dificultades encontradas. De esa forma garantir la validez de los discutidos en el texto a través de ejemplos prácticos que contribuirá para la comprensión del lector. La noción de grupos y anillos tratados aquí nos permitirá llevar a cabo más estudios sobre los procesos para identificar las raíces de ciertos polinomios y así permitir el uso de otros mecanismos que serán tratados detalladamente en el cuerpo de este trabajo, como el uso: algoritmos, definiciones, teorema, software computacional y análisis gráfica. Sin embargo, saber reconocer cuando se necesita para utilizar los conceptos de extensiones algébricos, principalmente cuando se enfrentan con las raíces cuadradas de los números negativos. Y ya que hay polinomios cúbicos que no sólo tienen raíces reales, presente los métodos de determinación de estas raíces.

Palabras clave: Extensiones Algébricas. Polinomios Cúbicos. Las Raíces de los Polinomios.

LISTA DE SÍMBOLOS E ABREVIATURAS

TFA: Teorema Fundamental da Álgebra.

$\mathbb{N}$: Conjunto dos números naturais.

$\mathbb{Z}$: Conjunto dos números inteiros.

n$\mathbb{Z}$: Inteiros múltiplos de n.

$\mathbb{Z}_m$: Números inteiros módulo m.

$\mathbb{Z}_p$: Números inteiros módulo p, com p primo.

$\mathbb{Z}[x]$: Conjunto de polinômios com coeficientes inteiros na variável x.

$\mathbb{Q}$: Conjunto dos números racionais.

$\mathbb{R}$: Conjunto dos números reais.

$\mathbb{C}$: Conjunto dos números complexos.

K: Um corpo qualquer.

K[x]: Conjunto de polinômios com coeficientes em K na variável x.

∂: Grau de um polinômio.

(x, y): Par ordenado.

(G, +, ·): Grupo G munido das operações de adição e multiplicação.

(A, +, ·): Anel A munido das operações de adição e multiplicação.

S(P): O conjunto de todas as bijeções de P.

$n!$: n fatorial.

SUMÁRIO

INTRODUÇÃO.....**11**

1 TEOREMA FUNDAMENTAL DA ALGÉBRA.....**13**

2 PRINCIPAIS CONCEITOS E RESULTADOS DE GRUPOS E ANÉIS.....**15**

2.1 Noções De Grupos E Anéis.....**15**

2.2 O Anel De Polinômios.....**20**

2.2.1 Anéis Comutativos.....20

2.2.2 Polinômios Em Uma Variável.....21

2.3 Polinômios Irredutíveis Sobre *K*.....**24**

3 SOBRE RAÍZES DE POLINÔMIOS CÚBICOS.....**26**

3.1 Teorema Do Resto.....**26**

3.2 Algoritmo De Briott-Ruffini.....**27**

3.3 Raízes Múltiplas.....**31**

3.4 Raízes Racionais De Polinômios Cúbicos Com Coeficientes Inteiros.....**32**

3.5 Raízes Complexas De Polinômios Cúbicos Com CoeficientesReais.....**33**

CONSIDERAÇÕES FINAIS.....**36**

REFERÊNCIAS BIBLIOGRÁFICAS.....**37**

APÊNDICE A.....**41**

APÊNDICE B.....**44**

APÊNDICE C.....**46**

INTRODUÇÃO

Desde o começo da construção da álgebra, sempre houve uma preocupação com a procura de métodos que poderiam ser aplicados de modo geral e eficientes, principalmente no que se referia a métodos gerais para a resolução de equações polinomiais. Quando houve o desenvolvimento de uma notação mais apropriada aos polinômios com relação a letras representando seus coeficientes e variáveis, foi permitido encontrar fórmulas gerais que facilitasse a resolução de equações polinomiais, embora poucos tivessem acesso a esses procedimentos para a resolução de equações.

Serão apresentados procedimentos de forma clara e objetiva, como alguns matemáticos do passado tiveram que enfrentar muitos desafios, como por exemplo, ter a validade de seus trabalhos reconhecidos, para se chegar ao conhecimento que temos hoje, desafios que a princípio não foram muito bem aceitos por estudiosos da área na época.

Primeiramente se fará uma breve introdução sobre o contexto histórico dos polinômios bem como os obstáculos enfrentados por muitos estudiosos para a determinação de raízes de polinômios, em particular, de polinômios cúbicos, sendo esse um dos problemas mais antigos da matemática enfrentados pelas pessoas que dirigiam suas atenções a esse tipo de situação. A abordagem procedimentos para encontrar as raízes de um polinômio será de forma simples, que facilite a compreensão do leitor.

O tipo de pesquisa feita para a elaboração deste trabalho foi à pesquisa bibliográfica, isto é, pesquisa elaborada por meio de diversas leituras em diferentes fontes de dados que tratam o referido assunto, assim ter condições de fazer uma análise de várias maneiras acerca do tema abordado por essa modalidade de pesquisa.

Severino (1941, p.122) aponta que ‘‘a pesquisa bibliográfica é aquela que se realiza a partir do registro disponível, decorrente de pesquisas anteriores, em documentos impressos, como livros, artigos, teses, etc’’. Dessa forma para a realização de uma pesquisa dessa modalidade faz-se o uso de informações já mencionadas por outros pesquisadores que foram devidamente documentadas, assim os textos ou as informações encontradas e analisadas de forma adequada para se dar procedência na construção de uma pesquisa acabam se tornando fontes indispensáveis dos temas a serem estudados.

O trabalho dividiu-se em 3 capítulos direcionados aos estudos sobre raízes de polinômios cúbicos, apresentando os principais conceitos e resultados para encontrá-las.

O primeiro capítulo apresenta o contexto histórico de um dos conceitos principais da Álgebra relacionados a raízes de polinômios, o Teorema Fundamental da Álgebra (TFA), e o processo enfrentado por alguns matemáticos em tentar chegar a um conceito definitivo para o TFA.

O segundo capítulo aborda os principais conceitos e resultados para o desenvolvimento deste trabalho, tais como: grupos e anéis bem como as propriedades relacionadas.

O terceiro capítulo trata dos métodos para determinação das raízes de polinômios cúbicos podendo ser reais ou complexas com utilização de alguns teoremas, algoritmos e definições.

E por fim, as considerações finais que trará informações acerca de todo o processo de construção deste trabalho, desde as dificuldades encontradas até os objetivos alcançados.

Dessa forma o leitor terá melhores condições de compreender os pontos que serão tratados no corpo de todo o trabalho propriamente dito produzido.

1 O TEOREMA FUNDAMENTAL DA ÁLGEBRA

Entre as preocupações que muitos estudiosos de matemática enfrentavam, como D'Alembert (1717-1783), Karl F. Gauss (1777-1855), Niels H. Abel (1802-1829) era descobrir qual seria a quantidade de raízes que um determinado polinômio apresenta. Assim, em consequências dos estudos de D'Alembert, Karl F. Gauss, Niels H. Abel, entre outros estudiosos, podemos identificar o número de raízes de polinômios por meio do Teorema Fundamental da Álgebra.

Os processos para obter a resolução de equações polinomiais foi uma das principais e mais difíceis preocupações de muitos que focavam seus estudos à álgebra abstrata (ver apêndice A). Matemáticos reconhecidos realizavam várias pesquisas para mostrar a validade de seus trabalhos escritos, e em virtude dessas pesquisas o matemático francês D'Alembert no ano de 1746, imaginou ter chegado à conclusão de que tinha conseguido demonstrar a seguinte situação: toda equação algébrica escrita na forma

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

de grau n[1], para todo n maior ou igual a 1, possuí no mínimo uma raiz imaginária ou complexa.[2]

Essa situação apontada pelo francês ficou conhecida como um teorema que leva o seu nome, ou de maneira mais conhecida hoje, Teorema Fundamental da Álgebra (TFA). De acordo com Oliveira (2011, p. 6) "Em 1799 o alemão K. F. Gauss (1777-1855) em sua tese de doutorado apresenta uma demonstração para o TFA que veio a ser considerada a 1° prova correta do TFA". Gauss em sua tese de doutorado já desconfiava que fosse pouco provável de se obter a solução de equações polinomiais de grau maior que 4 por meio de expressões matemáticas que envolveria seus coeficientes. Essa ideia colocada por Gauss (1777-1855) só foi aceita através de pesquisas e trabalhos realizados pelo norueguês Niels H. Abel (1802-1829) e pelo francês conhecido como Évariste Galois (1811-1832). À álgebra abstrata ou moderna, teve um grande avanço por meio dos trabalhos e pesquisas desenvolvidas sobre os processos de resolução de equações algébricas, que teve início com os trabalhos de Abel e Galois.

---

[1] Expressões que envolvem expoentes menores que zero ou fracionários não são polinômios.

[2] Números imaginários ou complexos são todos aqueles que podem ser escritos de forma $\alpha + \beta i$, para α e $\beta \in \mathbb{R}$.

Neste período, matemáticos consideravam a álgebra como parte fundamental para a teoria dos polinômios, no qual poderia considerar seus coeficientes reais ou complexos. A mesma consideração poderia ser feita para as equações algébricas, onde o Teorema Fundamental da Álgebra passou a ser incontestável. O TFA também teve uma elevada importância para a história e desenvolvimento dos números complexos em toda sua extensão.

Houve muitas tentativas para se demonstrar o TFA por procedimentos variados, em alguns casos obtendo êxito, e em outros não. A demonstração mais convincente em termos de simplicidade é colocada pelo matemático Jean Robert Argand (1768-1822) no ano de 1814, mesmo assim a prova do teorema apresentava um problema. Observe o que Oswaldo Rio Branco Oliveira diz à respeito da demonstração de Argand:

> O problema com a demonstração de Argand é que ela utiliza a extração da raiz n-ésima arbitrária de um número complexo arbitrário e via de regra tal extração é feita usando a Fórmula de Moivre, a qual requer as funções transcendentais senθ e cosθ. Ainda assim, a prova de Argand, ainda que classificada como "fácil", não é elementar. (OLIVEIRA, 2011, p. 9)

Em todas as maneiras[3] de se demonstrar o TFA colocadas até o momento, pode se verificar a existência de um fator relativamente comum entre eles, em todas as demonstrações foram aplicadas teorias relacionadas de forma analiticamente, embora pelo enunciado do teorema se possa perceber uma forma explicitamente algébrica. Assim o teorema nos diz que toda equação algébrica possui raiz em um determinado corpo, Fogliarino Brolesi aponta que:

> Em matemática, o teorema fundamental da Álgebra afirma que qualquer polinômio p(z) com coeficiente complexo 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). (BROLESI, 2006, p. 2)

Com o descobrimento do TFA, pôde-se determinar com precisão qual seria a quantidade exata de raízes de um dado polinômio e dessa forma o teorema passou a ser considerado de grande importância para o estudo de raízes de polinômios de grau *n*, assim considerado um dos principais resultados dessa teoria.

[3] 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. (BROLESI, 2006, p. 6)

2 PRINCIPAIS CONCEITOS E RESULTADOS DE GRUPOS E ANÉIS

Neste capítulo serão apresentados principalmente os conceitos sobre a teoria de grupos e anéis, que serão úteis para o estudo de raízes de polinômios cúbicos em anéis comutativos, assim de forma bastante simples discutiremos as propriedades básicas de grupos e anéis, objetivo principal deste capítulo.

2.1 Noções De Grupos E Anéis

A teoria de grupos nos fornece uma ferramenta muito útil para trabalhar com equações polinomiais de grau *n*, para todo $n \geq 1$. Como estamos nos referindo a grupos que possui um conjunto de elementos quaisquer (como exemplo podemos citar o conjunto dos números inteiros representados por $\mathbb{Z}$), que nada mais é uma estrutura algébrica composta por operações de adição ou multiplicação que satisfazem os principais axiomas ou propriedades operatórias, ou seja, associatividade, a existência do elemento neutro e a existência do elemento simétrico. Se ainda pudermos mostrar a validade da propriedade comutativa, o grupo em estudo recebe um nome diferenciado, de grupo comutativo. As operações mencionadas simplesmente combinam dois elementos de um grupo *G* a um único elemento também de *G*. Observe que:

> Sejam x e y dois quaisquer elementos de um conjunto G. Diz-se que φ é uma operação binária definida em G, ou lei de composição interna em G, sse[4] ao par ordenado (x, y) de G X G corresponde, pela operação φ, um único elemento de G, que se designa por x φ y.
> φ: G X G → G
> (x, y) → z = x φ y (PINTO, 2009, p. 5)

[4] Lê-se: se, e somente se.

Dessa forma Pinto (2009) deixa claramente explícito que as operações realizadas por φ no conjunto G relaciona seus elementos dentro do próprio conjunto G, sob um único elemento.

Considere p um número primo positivo e o conjunto $\mathbb{Q}(\sqrt{p}) = \{a + b\sqrt{p} / a, b \in \mathbb{Q}\}$ munido da operação usual de adição. Mostraremos que $\mathbb{Q}(\sqrt{p})$ com essa operação é grupo, para tanto devemos verificar a validade de algumas propriedades operatórias, são elas: associatividade, existência do elemento neutro e a existência do elemento simétrico.

Observemos que vale a propriedade associatividade. De fato, sejam $x = a_1 + b_1\sqrt{p}$, $y = a_2 + b_2\sqrt{p}$ e $z = a_3 + b_3\sqrt{p}$. Verificaremos que $x + (y + z) = (x + y) + z$

$x + (y + z) = (a_1 + b_1\sqrt{p}) + [(a_2 + b_2\sqrt{p}) + (a_3 + b_3\sqrt{p})]$

$x + (y + z) = (a_1 + b_1\sqrt{p}) + [(a_2 + a_3) + (b_2 + b_3)\sqrt{p}]$

$x + (y + z) = (a_1 + (a_2 + a_3)) + (b_1 + (b_2 + b_3))\sqrt{p}$

Como $\mathbb{Q}$ é grupo associativo, então

$x + (y + z) = ((a_1 + a_2) + a_3) + ((b_1 + b_2) + b_3)\sqrt{p}$

por definição de adição temos que

$x + (y + z) = [(a_1 + a_2) + (b_1 + b_2)\sqrt{p}] + (a_3 + b_3\sqrt{p})$

$x + (y + z) = [(a_1 + b_1\sqrt{p}) + (a_2 + b_2\sqrt{p})] + (a_3 + b_3\sqrt{p})$

$x + (y + z) = (x + y) + z.$

Agora verificaremos a existência do elemento neutro. Consideremos $x = a_1 + b_1\sqrt{p}$, $x \in \mathbb{Q}(\sqrt{p})$ e $\alpha = m_1 + n_1\sqrt{p}$, $m_1, n_1 \in \mathbb{Q}$.

$x + \alpha = x$

$(a_1 + b_1\sqrt{p}) + (m_1 + n_1\sqrt{p}) = a_1 + b_1\sqrt{p}$

$(a_1 + m_1) + (b_1 + n_1)\sqrt{p} = a_1 + b_1\sqrt{p}$

$\begin{cases} a_1 + m_1 = a_1 \\ b_1 + n_1 = b_1 \end{cases}$ daí, segue que $\begin{cases} m_1 = a_1 + (-a_1) = 0 \\ n_1 = b_1 + (-b_1) = 0 \end{cases}$ e portanto $\alpha = 0 + 0\sqrt{p}$ (elemento neutro), logo

$x + \alpha = x$

Finalizaremos mostrando a existência do elemento simétrico. Dado $x = a_1 + b_1\sqrt{p}$, $x \in \mathbb{Q}(\sqrt{p})$, existe um elemento $w = c_1 + d_1\sqrt{p} \in \mathbb{Q}(\sqrt{p})$ tal que $x + w = \alpha$.

$(a_1 + b_1\sqrt{p}) + (c_1 + d_1\sqrt{p}) = 0 + 0\sqrt{p}$

$(a_1 + c_1) + (b_1 + d_1)\sqrt{p} = 0 + 0\sqrt{p}$

$\begin{cases} a_1 + c_1 = 0 \\ b_1 + d_1 = 0 \end{cases}$ segue que $\begin{cases} c_1 = 0 + (-a_1) = 0 \\ d_1 = 0 + (-b_1) = 0 \end{cases}$ portanto $w = -a_1 - b_1\sqrt{p} = -x$

Dessa forma, $x + w = \alpha$

Assim concluímos que o conjunto $\mathbb{Q}(\sqrt{p}) = \{a + b\sqrt{p} / a, b, \in \mathbb{Q}\}$ munido da operação de adição é um exemplo de grupo. E se $\mathbb{Q}(\sqrt{p})$ verificar também a propriedade comutativa, dizemos então que $\mathbb{Q}(\sqrt{p})$ é grupo comutativo. Ou seja, considere $x = a_1 + b_1\sqrt{p}$ $x \in \mathbb{Q}(\sqrt{p})$ e $y = a_2 + b_2\sqrt{p}$ $y \in \mathbb{Q}(\sqrt{p})$. Verificaremos que $x + y = y + x$ *(propriedade comutativa)*

$x + y = (a_1 + b_1\sqrt{p}) + (a_2 + b_2\sqrt{p})$

$x + y = (a_1 + a_2) + (b_1 + b_2)\sqrt{p}$, como a propriedade é comutativa em $\mathbb{Q}$, logo temos

$x + y = (a_2 + a_1) + (b_2 + b_1)\sqrt{p}$, e portanto

$x + y = (a_2 + b_2\sqrt{p}) + (a_1 + b_1\sqrt{p})$, isto é, $x + y = y + x$. Assim concluímos que $\mathbb{Q}(\sqrt{p})$ é grupo comutativo.

As operações aqui mencionadas referem-se aos elementos que compõem o grupo, isto é, as propriedades operatórias devem ser válidas para quaisquer que sejam os elementos, caso contrário, se pelo menos uma propriedade não é válida, logo o conjunto mencionado não será dito um grupo. Se um determinado grupo satisfaz a operação de adição, ele será chamado de grupo aditivo, se satisfaz a operação de multiplicação será chamado de grupo multiplicativo, quando a operação não for definida, adotaremos a operação multiplicativa. No que se referem às operações que compõem as estruturas algébricas aqui trabalhadas, principalmente as propriedades operatórias que mencionam a existência dos elementos simétricos da adição e multiplicação, devemos observar que o elemento simétrico da adição é também chamado de oposto, ou seja, dado um elemento qualquer α de um grupo aditivo, o oposto de α será simbolizado por $-\alpha$, e de um grupo multiplicativo o elemento simétrico poderá ser chamado de inverso, isto é, tomemos um elemento qualquer β, o inverso será simbolizado por β^{-1}.

Como estamos focalizando o estudo em raízes de polinômios, a construção a seguir enfatiza que a permutação das raízes munido da operação composição é um grupo denominado por grupo das Permutações de um conjunto finito *P* qualquer, denotados por *S(P)*. Seja $P = \{1, 2, 3, \cdots, r\}$, para entendimento de nossa escrita *S(P)*, que segundo Domingues (1982, p. 83) descreve simplesmente "o conjunto de todas as bijeções de *P*".

De acordo com Domingues (1982, p. 83) "se $E = \{1, 2, \dots, n\}$, $n \geq 1$, tem-se um caso particular importante. S(E) passa a ser indicado por S_n e denominado grupo simétrico de grau n. A análise combinatória nos mostra que S_n é um grupo de ordem n!".

Portanto, considerando a ordem de *S(P)* dos polinômios cúbicos é dado por S_3, ou seja, por 3! [5].

Compreendida a noção básica de grupos, podemos agora introduzir a noção de Anel. Segundo Hygino H. Domingues e Gelson Iezzi (2003, p.211) anel é "Um sistema matemático constituído de um conjunto não vazio A e um par de operações sobre A, respectivamente uma adição $(x, y) \rightarrow x + y$ e uma multiplicação $(x, y) \rightarrow xy$ (ou $x \cdot y$)".

Contudo para que um conjunto não vazio $(A, +, \cdot)$ [6] seja denominado de anel é necessário que este conjunto seja um grupo comutativo[7] com relação à primeira operação, para quaisquer que sejam os elementos contidos em A. Para o caso de anéis, segue as seguintes observações:

> Observações: 1) Observe que a multiplicação não necessita ser comutativa. Quando isto ocorrer, dizemos que A é um anel comutativo.
> 2) Um anel não necessita ter elemento neutro da multiplicação (isto é, um elemento y tal que $xy = yx = x$ para todo $x \in A$). Este elemento é chamado de unidade do anel e denotado por 1. Quando um anel A possui o elemento neutro da multiplicação dizemos que A é um anel com unidade.
> 3) Os elementos não nulos de um anel não necessitam ter inversos multiplicativos (isto é, y é inverso multiplicativo de x se e somente se $xy = yx = 1$). Os elementos de um anel A que possuem inverso multiplicativo são chamados de invertiveis de A ou unidades de A. (MARQUES, 1999, p.10 e 11)

E ainda,

> Se um anel $A, +, \cdot$ satisfaz a propriedade:
> $x, y \in A$, $x \cdot y = 0 \Rightarrow x = 0$ ou $y = 0$, dizemos que $A, +, \cdot$ é um anel sem divisores de zero.
> Se $A, +, \cdot$ é um anel comutativo, com unidade e sem divisores de zero, dizemos que $A, +, \cdot$ é um domínio de integridade.
> E finalmente, se um domínio de Integridade $A, +, \cdot$ satisfaz a propriedade:
> $x \in A$, $x \neq 0$, existe $y \in A$ tal que $x \cdot y = y \cdot x = 1$, dizemos que $A, +, \cdot$ é um corpo. (GONÇALVES, 1979, p. 34 e 35)

---

[5] 3! simplesmente descreve o produto de fatores consecutivos, ou seja, $3 \cdot 2 \cdot 1$. Para n! (n fatorial), temos $n! = n(n-1)(n-2)(n-3)\cdots(3)(2)(1)$

[6] Anel A munido das operações de soma e produto.

[7] Grupo para a qual é válida a propriedade comutativa, isto é, dados quaisquer elementos x e y de um grupo G com a operação de composição interna * têm-se que $x * y = y * x$. O grupo poderá ser identificado também como grupo abeliano, graças ao matemático Niels H. Abel.

A partir dos apontamentos feitos por Gonçalves (1979) e Marques (1999) acima, podemos perceber que existem vários tipos de anéis no que se refere a multiplicação, há anéis que possuem elemento neutro e outros não, há anéis comutativos e outros não, há anéis com unidade e outros não, há anéis que são domínio de integridade e outros não e finalizando há anéis que são corpos e outros não.

Como o foco de nosso trabalho é fazer um estudo sobre raízes de polinômios cúbicos, assim tomemos um conjunto qualquer representado por L[8], com duas operações bem definidas. Construiremos a seguir o anel de polinômios *L* que identificaremos por *K[x]* um conjunto formado por todos os polinômios escritos na variável *x*, com coeficientes no corpo *K*. Observe que *K* é um anel comutativo.

R_1: A operação da adição é associativa, ou seja, dados quaisquer $P(x) = \sum_{i=0}^{n} a_i x^i$, $Q(x) = \sum_{i=0}^{n} b_i x^i$ e $R(x) = \sum_{i=0}^{n} c_i x^i$ elementos de *K*.

Por definição temos que:

$P(x) + (Q(x) + R(x)) = \sum_{i=0}^{n} a_i x^i + (\sum_{i=0}^{n} b_i x^i + \sum_{i=0}^{n} c_i x^i)$

$P(x) + (Q(x) + R(x)) = \sum_{i=0}^{n} a_i x^i + (\sum_{i=0}^{n} (b_i + c_i) x^i)$

$P(x) + (Q(x) + R(x)) = \sum_{i=0}^{n} (a_i + (b_i + c_i)) x^i$, como a regra é associativa, logo

$P(x) + (Q(x) + R(x)) = \sum_{i=0}^{n} ((a_i + b_i) + c_i)x^i$, dessa forma chegamos ao seguinte resultado:

$P(x) + (Q(x) + R(x)) = (\sum_{i=0}^{n} a_i x^i + \sum_{i=0}^{n} b_i x^i) + \sum_{i=0}^{n} c_i x^i$, ou seja,

$P(x) + (Q(x) + R(x)) = (P(x) + Q(x)) + R(x)$

Observe que obtemos uma igualdade verdadeira, então a propriedade associativa da adição é satisfeita.

R_2: A propriedade distributiva é válida para quaisquer que sejam os elementos *P(x)*, *Q(x)* e *R(x)* em *L*. De fato, tomemos $P(x) = \sum_{i=0}^{n} a_i x^i$, $Q(x) = \sum_{j=0}^{n} b_j x^j$ e $R(x) = \sum_{k=0}^{n} c_k x^k$, por definição temos que:

$P(x) \cdot [Q(x) + R(x)] = P(x) \cdot Q(x) + P(x) \cdot R(x)$, ou seja,

$P(x) \cdot [Q(x) + R(x)] = \sum_{i=0}^{n} a_i x^i (\sum_{j=0}^{n} b_j x^j + \sum_{k=0}^{n} c_k x^k)$

$P(x) \cdot [Q(x) + R(x)] = \sum_{i=0}^{n} a_i x^i (\sum_{j,k=0}^{n} b_j x^j + c_k x^k)$, por definição de somatório temos

$P(x) \cdot [Q(x) + R(x)] = \sum_{i,j,k=0}^{n} a_i x^i (b_j x^j + c_k x^k)$, aplicando a propriedade distributiva

$P(x) \cdot [Q(x) + R(x)] = \sum_{i,j,k=0}^{n} a_i\, b_j x^{i+j} + a_i c_k x^{i+k}$, novamente aplicando as propriedades de somatório temos que

[8] Representa o conjunto de todos os polinômios escritos em uma variável.

$P(x) \cdot [Q(x) + R(x)] = \sum_{i,j=0}^{n} a_i\, b_j x^{i+j} + \sum_{i,k=0}^{n} a_i\, c_k x^{i+k}$, assim

$P(x) \cdot [Q(x) + R(x)] = \sum_{i=0}^{n} a_i x^i \cdot \sum_{j=0}^{n} b_j x^j + \sum_{i=0}^{n} a_i x^i \cdot \sum_{k=0}^{n} c_k x^k$, portanto

$P(x) \cdot [Q(x) + R(x)] = P(x) \cdot Q(x) + P(x) \cdot R(x)$

Logo a distributividade é verdadeira para quaisquer que sejam os elementos de L.

Observe que as propriedades acima foram comprovadas para quaisquer que sejam os elementos *P(x)*, *Q(x)* e *R(x)* em *L*. Dessa forma a construção do anel de polinômios *L* está bem definida com as operações utilizadas em *L*.

2.2 O Anel De Polinômios

Um anel de polinômios é um conjunto cujos elementos são próprios polinômios, assim é de fundamental importância destacar algumas propriedades relacionadas a esse conjunto especial. Dessa forma, ter condições de compreender e aplicar os conceitos necessários para se efetuar operações elementares com esse tipo de estrutura algébrica.

2.2.1 Anéis Comutativos

De acordo com Domingues (1982, p. 135) "dizemos que um anel A é comutativo se a sua multiplicação é comutativa, isto é (∀ a, b) (a, b ∈ A ⟹ ab = ba)". Domingues (1982, p. 135) ainda aponta que "são anéis comutativos $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, n\mathbb{Z}, \mathbb{Z}_m$ e A^X (toda vez que A é comutativo). Se A e B são comutativos, então AxB (produto direto de A por B também é comutativo".

Contudo, quando se trata de anéis comutativos, existem aqueles anéis que possuem uma característica a mais, isto é, aqueles que possuem unidade[9]. Para Marques (1999, p. 12)

[9]Para Domingues (1982), um anel com unidade é um anel A que conta com elemento neutro para a multiplicação.

"o conjunto $\mathbb{Z}[x]$ de todos os polinômios na variável *x* com coeficientes inteiros com a multiplicação e adição usuais é um anel comutativo com unidade".

Domingues (1982, p. 135) define anel comutativo com unidade da seguinte maneira: "um anel comutativo com unidade é um anel cuja multiplicação é comutativa e para a qual exista elemento neutro. O elemento neutro da multiplicação de um anel é chamado, quando existe, de unidade do anel". Seguindo o exemplo colocado por Domingues (1982, p. 136) "os anéis $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, e $\mathbb{C}$ possuem unidade".

Observe que, a partir dos dados acima, podemos perceber que existem anéis comutativos com unidade ou sem unidade, uma característica muito importante para o estudo dos anéis comutativos. De acordo com Domingues (1982, p. 140), os anéis comutativos com unidade recebem um nome específico e define da seguinte forma: "um anel A, comutativo com unidade, onde é verdadeira a seguinte frase ($\forall$ a, b $\in$ A) (ab $= 0_A \Longrightarrow$ a 0_A ou b $= 0_A$) recebe o nome de anel de integridade". Domingues (1982, p. 142) ainda aponta que "todo corpo K é um anel de integridade".

Os conceitos aqui apresentados nos darão suporte para os processos de determinação de raízes de polinômios em anéis comutativos.

2.2.2 Polinômios Em Uma Variável

Nesta seção, apresentaremos os conceitos sobre polinômios em uma variável que serão necessários para o desenvolvimento das próximas seções.

Segundo Gonçalves (1979, p. 63) "seja *K* um corpo qualquer. Chamamos de um polinômio sobre *K* em uma indeterminada *x* a uma expressão formal
p(x) = $a_0 + a_1x + \cdots + a_mx^m + \cdots$ onde $a_i \in K$, $\forall\, i \in \mathbb{N}$ e $\exists\, n \in \mathbb{N}$ tal que $a_j = 0\ \forall\, j \geq n$".

Como estamos estudando um conjunto de polinômios em uma variável qualquer, para facilitar nossa escrita denotaremos um conjunto de quaisquer que sejam os polinômios em uma variável *x*, por exemplo, sobre um corpo *K* por *K[x]*.

Em *K[x]*, alguns polinômios por possuírem certas características recebem nomes especiais. Tais expressões podem ser facilmente identificadas por polinômios identicamente

nulos e polinômios constantes. Assim, uma expressão definida como identicamente nula é escrita da forma:

$I(x) = 0 + 0x + \cdots + 0x^n$

ou seja, todos os coeficientes de *I(x)* são nulos, para quaisquer que sejam eles. Observe que *I(x)* também poderá ser identificado de maneira mais simplificada por *I(x) = 0*, onde

$0 = 0 + 0x + \cdots + 0x^n$

Afirmamos que uma expressão da forma

$C(x) = a_0 + a_1x + \cdots + a_nx^n$

é constante se, e somente se é da forma *C(x) = c* para qualquer que seja *c* um elemento de *C*, isto é, o coeficiente $a_0 \neq 0$ e os coeficientes $a_1, \cdots, a_n$, todos iguais a 0 (zero). Dessa forma *C(x)* se reduz à forma

$C(x) = a_0 + 0x + \cdots + 0x^n$

ou também na forma $C(x) = a_0$, onde $a_0 = c$.

Segundo Gonçalves (1979, p. 64) "se identificarmos os elementos $a \in K$ com os polinômios constantes $p(x) = a$ podemos pensar em $K[x]$ contendo o corpo K".

Quando escrevemos determinados polinômios na forma $P(x)=a_0 + a_1x + \cdots + a_nx^n$ estamos utilizando, o que muitos matemáticos denominam de notação usual para quaisquer que sejam as expressões em *K[x]*. Mas para simplificar o nosso entendimento, toda expressão sob a forma de *P(x)* também pode ser escrita ou representada por meio de uma sequência determinada pelos coeficientes de *P(x)*, ou seja, a sequência finita[10] $(a_0, a_1, ..., a_n)$ também denominada de upla, representa exatamente o polinômio *P(x).* Assim, de acordo com Gonçalves (1979, p. 65) "temos uma realização concreta, através de uplas, das noções de indeterminada "*x*" e de polinômios nessa indeterminada".

Segundo Garcia (2005, p. 14) "um polinômio numa variável sobre A é uma sequência $(a_0, a_1, ..., a_n, ...)$, onde $a_i \in A$ para todo índice e onde $a_i \neq 0$ somente para um número finito de índices". Observe que, diferente de Gonçalves (1979, p. 63) Garcia define um polinômio numa variável sobre um anel *A* por meio de uma sequência ou upla. Assim, com a notação de uplas podemos ter uma melhor compreensão da existência de algumas propriedades entre dois polinômios distintos em *K[x]*. Para Garcia (2005, p. 15 e 16):

[10] Conjuntos de objetos de qualquer natureza, organizados ou escritos numa ordem bem determinada. Para representar uma sequência, escrevemos seus elementos, ou termos, entre parênteses. É importante destacar que, ao contrário do que ocorre num conjunto, qualquer alteração na ordem dos elementos de uma sequência altera a própria sequência. Definição disponível em http://www.colegioweb.com.br/trabalhos-escolares/matematica/sucessoes-ou-sequencias/o-que-sao-sucessoes-ou-sequencias.html

> O elemento (a_0, a_1, ..., a_n, 0, ...) é igual à soma $a_0 + a_1X + \cdots + a_nX^n$, onde a_iX^i designa $a_i \cdot X^i$. Vai ser conveniente representar o elemento (a_0, a_1, ..., a_n, 0, ...) pela expressão $a_0 + a_1X + \cdots + a_nX^n$; então $A = \{\sum_{i=0}^{n} a_iX^i;\ n \in \mathbb{N}$ e $a_i \in A\}$ e as operações deste anel são simplesmente as operações com as quais todo mundo está acostumado.

Por exemplo, podemos através de uplas ou sequências definir as operações de adição e multiplicação entre dois polinômios em uma mesma variável sobre *K*. Assim dadas às sequências $(a_n, ..., a_2, a_1, a_0)$ e $(\beta_n, , ..., \beta_2, \beta_1, \beta_0)$ representando dois polinômios *P(x)* e *Q(x)*, a soma é definida da seguinte maneira,

$(a_n, ..., a_2, a_1, a_0) + (\beta_n, ..., \beta_2, \beta_1, \beta_0) = (a_n + \beta_n, ..., a_2 + \beta_2, a_1 + \beta_1, a_0 + \beta_0)$

A regra para a multiplicação exige mais um pouco de atenção, consideremos a sequência definida acima, assim temos que,

$(a_n, ..., a_2, a_1, a_0) \cdot (\beta_n, , ..., \beta_2, \beta_1, \beta_0) = (\mu_n, ..., \mu_2, \mu_1, \mu_0)$

onde definimos $\mu_n = a_0\beta_n + a_1\beta_{n-1} + a_2\beta_{n-2} + ... + a_{n-2}\beta_2 + a_{n-1}\beta_1 + a_n\beta_0$

Quando escrevemos determinados polinômios por meio de uma sequência, estamos de certa forma reduzindo o grau de dificuldade de se trabalhar com esse tipo de expressões, assim em muitos casos o uso de sequências para se efetuar operações entre polinômios se torna indispensável, pois se trabalha apenas com os coeficientes.

Com a possibilidade de se efetuar operações apenas com a utilização dos coeficientes, também é possível encontrar as raízes de certos polinômios por meio dessa ferramenta. Por exemplo, a famosa fórmula de Bháskara para a resolução das equações de 2° grau e a de Cardano para as de 3° grau da forma $x^3 + px = q$ todas envolvem operações apenas com coeficientes. É como foi colocado por Garcia (2005, p. 16) "operações com as quais todo mundo está acostumado".

São vários os procedimentos para a determinação de raízes de polinômios cúbicos, esses procedimentos serão apresentados no próximo capítulo, são simples e ao mesmo tempo eficientes e serão comprovados por meio de teoremas, definições e algoritmos.

2.3 Polinômios Irredutíveis Sobre *K*

De acordo com Gonçalves (1979, p. 76) "[...] os polinômios em *K[x]* que, dentro da analogia de K[x] com $\mathbb{Z}$, fazem o mesmo papel dos números primos em $\mathbb{Z}$. Esses polinômios serão chamados de polinômios irredutíveis sobre *K*". Assim podemos imaginar que polinômios irredutíveis podem ser escritos como um produto de dois polinômios.

> Seja $f(x) \in K[x]$ tal que $\partial^{11} f(x) \geq 1$. Dizemos que é um polinômio $f(x)$ é um polinômio irredutível sobre *K* se toda vez que $f(x) = g(x) \cdot h(x)$, $g(x), h(x) \in K[x]$ então temos $g(x) = a$ constante em *K* ou $h(x) = b$ constante em *K*. Se $f(x)$ for não irredutível sobre *K* dizemos que *f* é redutível sobre *K*. (GONÇALVES, 1979, P. 76)

Observe que, de acordo com Gonçalves (1979), polinômios irredutíveis podem ser de certa maneira, decompostos em produtos de polinômios, para o qual um dos termos do produto é constante sobre o corpo *K*.

Por exemplo, segundo Domingues (1982, p. 206), "o polinômio $p = 1 + X^2 \in \mathbb{R}[X]$ é irredutível sobre $\mathbb{R}$". De fato, basta observar que o polinômio p não pode ser decomposto como um produto de dois polinômios em $\mathbb{R}$.

> Claramente temos que todo polinômio de grau 1 sobre um corpo *M* é irredutível sobre *M*. Observe também que o polinômio $f(x) = x^2 + 1$ é irredutível sobre o corpo $\mathbb{R}$ porém é redutível sobre $\mathbb{C}$. Assim um polinômio $f(x) \in K[x]$ pode ser irredutível sobre *K* e redutível em uma extensão $L \supset K$. (GONÇALVES, 1979, P. 76)

Observe o exemplo colocado por Domingues (1982, p. 206):

> O polinômio $f = 1 - X^3 \in \mathbb{R}[X]$ é redutível. De fato, além de não ser um polinômio constante ($\partial(f) = 3$), o polinômio $g = 1 - X$ é divisor de f, pois $1 - X^3 = (1 - X)(1 + X + X^2)$, e g não é um polinômio constante e nem pode ser decomposto da maneira $g = c(1 - X^3)$, com $c \in \mathbb{R}^*$.

Contudo, para verificar a irredutibilidade de polinômios em um corpo *K*, existe um critério bem simples para este fim. Gonçalves (1979, p. 82) aponta que "a verificação da

[11] Descreve o grau do polinômio *f*.

irredutibilidade de um polinômio sobre um corpo é, em geral, um problema difícil". Por esse motivo utilizaremos o Critério de Eisenstein. Considerando o corpo $\mathbb{Q}$. Observe que:

> (Critério de Eisenstein). Seja $f(x) = a_0 + a_1x + \cdots + a_nx^n$ um polinômio em $\mathbb{Z}[x]$. Suponhamos que exista um inteiro primo p tal que:
> (a) $p\nmid a_n$
> (b) $p\setminus a_0, a_1, \ldots, a_{n-1}$
> (c) $p^2 \nmid a_0$.
> Então $f(x)$ é irredutível sobre $\mathbb{Q}$. (GONÇALVES, 1979, p. 83)

Observe o exemplo colocado por Gonçalves (1979, p.84), "seja $f(x) = x^3 + 2x + 10$. O critério de Einsenstein se aplica para o primo $p = 2$, portanto $f(x)$ é irredutível sobre $\mathbb{Q}$".

Ainda de acordo com Gonçalves (1979, p. 84) "[...] seja p um número primo qualquer e seja $p(x) = x^n - p$ um polinômio de grau $n \geq 1$sobre $\mathbb{Q}$. Claramente, o próprio primo p se aplica no critério de Einsenstein e, portanto $p(x)$ é irredutível sobre $\mathbb{Q}$".

Todos os conceitos estudos até aqui, serão de alta relevância para a determinação de raízes de polinômios cúbicos por meio de alguns procedimentos que serão apresentados no próximo capítulo. Assim teremos maior facilidade para compreender os conceitos apresentados de forma simples e prática.

3 SOBRE RAÍZES DE POLINÔMIOS CÚBICOS

Neste capítulo apresentaremos alguns métodos para a determinação de raízes de polinômios. Em particular para polinômios cúbicos. De acordo com Bordeaux (2005, p. 284) "toda equação algébrica, de grau > 0, tem raízes". Dessa forma exibiremos procedimentos dos métodos para se determinarem tais raízes de forma clara e objetiva.

3.1 Teorema do Resto

Inicialmente para definirmos o teorema do resto podemos utilizar a mesma ideia de divisibilidade tratada em teoria dos números para inteiros, e a partir desse pressusposto, conceituar divisão de polinômios em um anel *A[x]*, já definido no capítulo anterior, para tanto utilizaremos um algoritmo simples para solucionar nosso problema, o Algoritmo de Euclides[12].

Segundo Domingues (1982, p. 190), o algoritmo se reduz da seguinte maneira:

> Dados $f = a_0 + a_1X + \cdots + a_nX^n$ e $g = b_0 + b_1X + \cdots + b_mX^m$ em A[X], suponhamos $g \neq 0$ e o coeficiente dominante de g é inversível. Nessas condições existem q, r ∈ A[X] de modo que $f = gq + r$, onde $r = 0$ ou $\partial(r) < \partial(g)$".

Com essas informações podemos garantir a existência do teorema do resto. De acordo com Facco (2008, p. 12) o teorema se deduz da seguinte forma "dado um polinômio *f*, o resto da divisão deste polinômio *f* por *x – a* é igual ao valor numérico de *f* em *a*". Isto significa que ao dividirmos um polinômio *P(x)* por um polinômio da forma *G(x)*, encontraremos um resto *R(x)* de tal forma que o valor de *R(x)* será dado por *P(μ)*, onde μ é raiz de *P(x)*.

Eliezer Facco (2008) aponta que para mostrar ao teorema apresentado podemos utilizar a definição do algoritmo de Euclides da seguinte maneira:

[12] A demonstração do algoritmo se encontra no livro de álgebra moderna de Hygino H. Domingues, página 190.

> q(x)(x – a) + r(x) = *f*(x), onde q e r formam o quociente e o resto. Como o grau de x – a é 1, logo, o resto r é nulo ou tem grau zero, portanto, é um polinômio constante, ou seja, r = k. Utilizando x – a, para calcular os valores dos polinômios da igualdade acima temos:
> q(a)(a – a) + r(a) = *f*(a). Portanto r = *f*(a). (FACCO, 2008, p. 12).

E dessa forma o teorema do resto está demonstrado.

Considere o polinômio $P(x) = x^3 + 2x^2 - x - 2$, com uma de suas raízes igual a 1. Pelo teorema do resto temos que $P(x) = Q(x) \cdot (x - \mu) + R(x)$, onde $\mu = 1$ raiz de $P(x)$. Assim temos que $P(x) = (x^2 + x - 2) \cdot (x - 1) + R(x)$. Como 1 é raiz, logo $P(1) = 0 \cdot 0 + R(x)$, então $P(1) = R(x) = 0$. Portanto $P(\mu) = R(x)$.

Basta observar que, quando efetuamos a divisão de $x^3 + 2x^2 - x - 2$ por $x - 1$, obtemos como resto da divisão $R(x) = 0$, que é justamente $P(1)$.

Apresentaremos, a seguir, um método muito utilizado para encontrar raízes de polinômios. Para apresentar esse método vamos recorrer aos apontamentos realizados por Facco, em seu trabalho intitulado Polinômios Algébricos.

3.2 O Algoritmo De Briotti-Ruffini

De acordo com Facco (2008, p. 13) "o dispositivo de Briott-Ruffini, como veremos, torna a divisão por polinômio do tipo x – a fácil e rápida uma vez que a forma é diferente do método da chave, mas chega ao mesmo resultado [...]". Para Giovanni (2005, p. 175) devemos seguir alguns passos para efetuar a divisão de polinômios pelo método da chave na seguinte ordem:

> 1. Escrever os polinômios (dividendo e divisor) em ordem decrescente dos seus expoentes e completá-los, quando necessário, com termos de coeficientes zero.
> 2. Dividir o termo de maior grau do dividendo pelo maior grau do divisor, o resultado será um termo do quociente.
> 3. Multiplicar o termo obtido no passo 2 pelo divisor e subtrair esse produto do dividendo.
>
> - Se o grau da diferença for menor do que o grau do divisor, a diferença será o resto da divisão e a divisão termina aqui.
> - Caso contrário, retoma-se o passo 2, considerando a diferença como um novo dividendo.

Assim pelo método da chave pode-se de forma simples e prática efetuar-se a divisão de um polinômio por um monômio sem complicações.

Tomemos como ilustração do método da chave, o exemplo colocado por Giovanni (2008, p. 175):

Determinar o quociente de A(x) = $x^3 + 4x^2 + x - 6$ por B(x) = $x + 2$.
Sendo Q(x) o quociente de A(x) por B(x) e R(x) o resto:
gr(Q) = gr(A) – gr(B) = 2
Como gr(R) < gr(B) = 1, então gr(R) = 0 ou R(x) = 0.

$$
\begin{array}{r|l}
x^3 + 4x^2 + x - 6 & x + 2 \\
\cline{2-2}
-x^3 - 2x^2 & x^2 + 2x - 3 \rightarrow \text{quociente: Q(x)} \\
\cline{1-1}
\quad x^2 + 2x - 6 & \\
-2x^2 - 4x & \\
\cline{1-1}
\quad -3x - 6 & \\
+3x + 6 & \\
\cline{1-1}
\quad 0 & \rightarrow \text{Resto: R(x)}
\end{array}
$$

Verificamos, facilmente, que:
$x^3 + 4x^2 + x - 6 \equiv (x + 2)(x^2 + 2x - 3)$.

Há vários procedimentos para a determinação de raízes de polinômios, e dependendo do grau de certos polinômios os cálculos se tornam muito desgastantes, por esse motivo matemáticos[13] acabaram por desenvolverem processos menos cansativos e eficazes para resolver esses problemas, principalmente quando se refere ao estudo de raízes de polinômios cúbicos.

Descreveremos, a seguir, um procedimento que facilitará a nossa procura por raízes de polinômios. Para tanto, considere o polinômio

H(x) = $a_n x^n + a_{n-1}x^{n-1} + a_{n-2}x^{n-2} + \cdots + a_2 x^2 + x a_1 + a_0$

em *K[x]*, onde o grau de *H(x)* é *n*, para todo n maior ou igual a 1(um). Se α é raiz de *H(x)*, então podemos determinar todas as outras por meio de um algoritmo bastante simples e prático, desenvolvido pelo matemático Briott-Ruffini, tal algoritmo é conhecido por "Algoritmo de Briott-Ruffini[14]".

Com esse processo, não apenas podemos encontrar todas as raízes de um dado polinômio *P(x)*, como também efetuar de forma simples e rápida a divisão de *P(x)* por outro polinômio *Q(x)*, pois o algoritmo se aplica apenas nos coeficientes de um dado polinômio, por

[13] Podemos fazer referências a Tartaglia, Joseh-Louis Lagrange, Evariste Galois, Karl F. Gauss e Niels H. Abel.
[14] Também muito utilizado para se efetuar divisões de um polinômio por um monômio, e alguns livros didáticos o algoritmo também é conhecido por dispositivo de Briott- Ruffini.

esse motivo é mais simples de se trabalhar. O método de determinação de raízes consiste em aplicar sucessivamente o algoritmo no resto da divisão de *P(x)* por *Q(x).*

Considere o polinômio *P(x)* = $x^3 + 2x^2 - 3x$, com uma de suas raízes igual a 0. Pelo algoritmo temos que:

1	2	-3	0	0
1	2	-3	0	

Aplicando sucessivamente o processo no quociente da divisão temos:

1	2	-3	0	0
1	2	-3	0	-3
1	-1	0		1
1	0			

Observe que os termos {1, 2, -3} representam os coeficientes do polinômio *P(x)* = $x^2 + 2x - 3$ com raiz -3 e os termos {1, -1} o polinômio *P(x)* = *x* – 1 com raiz 1. Portanto as raízes de *P(x)* = $x^3 + 2x^2 - 3x$ são 0, -3 e 1 respectivamente.

De forma geral, dado o polinômio *P(x)* = $a_0 + a_1x + \cdots + a_nx^n$, onde o elemento μ é uma de suas raízes, utilizando o algoritmo podemos encontrar sua segunda raiz da seguinte forma:

Coeficientes de *P(x)*	Raiz de *P(x)*

ou seja,

a_0	a_1	...	a_n	μ
α_0	$\mu a_0 + a_1$	...	$\mu(\mu a_0 + a_1) + a_n$	

Considere o quociente da divisão *Q(x)* = $a_0 + (\mu a_0 + a_1)$ e o resto *R(x)* = $\mu(\mu a_0 + a_1) + \alpha_n$.

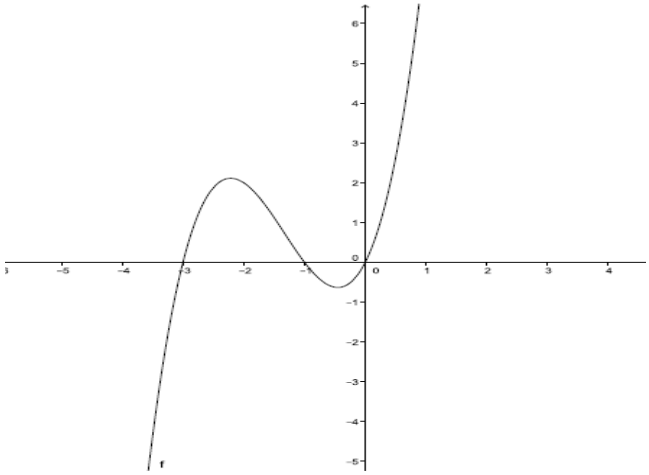
Entretanto com esse processo podemos encontrar raízes apenas de alguns polinômios, cujas raízes são todas inteiras. Contudo podemos utilizar outras ferramentas que são úteis para a determinação das raízes ou para se chegar a uma aproximação conveniente. Para efeito, podemos estar utilizando o software computacional Geogebra[15], para fazer uma análise do

[15] Software computacional utilizado para se fazer cálculos de álgebra, geometria e construção de gráficos. Disponível para download em http://www.baixaki.com.br/download/geogebra.htm.
O leitor que não encontrar afinidade com o Geogebra pode estar utilizando também o software Winplot para analisar o comportamento dos gráficos de alguns polinômios.

comportamento do gráfico de um determinado polinômio e assim ter condições de identificar o modelo de suas raízes.

Como queremos fazer nosso estudo sobre polinômios cúbicos. Considere o polinômio cúbico $P(x) = ax^3 + bx^2 + cx + d$, dados os seguintes coeficientes $a = 1$, $b = 2$, $c = 3$ e $d = 0$, através do algoritmo apresentado podemos determinar suas raízes, que são respectivamente – 3, - 1 e 0, o gráfico deste polinômio *P(x)* foi ilustrado na figura 1:

Figura 1 – Gráfico do polinômio $P(x) = x^3 + 2x^2 + 3x$



Fonte: Criada pelo autor

Observe que as raízes de *P(x)* são todas distintas entre si, ou seja, nenhuma delas se repetem, então dizemos que neste caso todas as raízes são simples, ou seja, nenhuma delas possuem multiplicidade. Segundo Dante (2004, p. 296) "o número de vezes que uma mesma raiz aparece indica a multiplicidade da raiz". Os conceitos sobre multiplicidade serão estudados na seção a seguir, com fundamentação nos trabalhos realizados por Domingues (1982) e Facco (2008).

3.3 Raízes Múltiplas

Raízes múltiplas são raízes de certos polinômios que possuem multiplicidade, isto é, observe o polinômio cúbico *P(x)* = $x^3 - 8$, temos que *P(x) = 0* se, e somente se, $x^3 - 8 = 0$, portanto *x = 2*, e pelo teorema fundamental da álgebra tem-se que *P(x)* possui no máximo 3 raízes, então nesse caso *x = 2* possui multiplicidade 3.

Segundo Domingues (1982, p. 208), define raízes múltiplas da seguinte maneira:

> Seja K um corpo. Se f ∈ K[X] e se u ∈ K já vimos que vale o seguinte resultado: "u é raiz de f ⇔ (X – u) | f".
> Nessas condições, se q_1 é o quociente na divisão de f por (X – u), então f = (X – u)q_1.
> Se q_1 (u) ≠ 0 dizemos que u é uma raiz simples de f.
> Se q_1 (u) = 0, então q_1 também é divisível por (X – u) e, portanto existe q_2 ∈ K[X] tal que q_1 = (X – u)q_2. Donde f = $(X - u)^2 q_2$.
> Se q_2 (u) ≠ 0 dizemos que u é raiz dupla de f.
> Generalizando, se existe um número natural r ≥ 1 de maneira que f = $(X - u)^r q_r$. e q_r (u) ≠ 0 dizemos que u é raiz de multiplicidade r de f.
> Uma raiz múltipla de f é uma raiz de f cuja multiplicidade é r > 1.

Por exemplo, considere a seguinte situação colocada por Facco (2008, p. 19).

> Na decomposição de um polinômio p(x) em um produto de fatores do 1° grau, pode ser que existam dois ou mais fatores iguais. Por exemplo, no polinômio:
> P(x) = 7(x – 4) (x – 4) (x – 4) (x + 2)(x + 1)(x + 1), há três fatores iguais a x – 4, um igual a x + 2, e dois iguais a x + 1. Neste caso, diremos que: 4 é raiz tripla (de multiplicidade 3), -2 é raiz simples (de multiplicidade 1) e -1 é raiz dupla (de multiplicidade 2).

Dessa forma podemos dizer que multiplicidade de uma raiz é a quantidade de vezes que ela aparece. Segundo Facco (2008) "definimos que α é uma raiz ou elemento algébrico de multiplicidade $\mathcal{M}$ de um polinômio *p(x)*, quando surgem, ao se decompor um polinômio em apenas fatores de grau 1, somente fatores iguais a $x - \alpha$". Observe que o exemplo citado acima apresenta todas as raízes de *P(x)* inteiras, mas nem sempre conseguimos determinar apenas raízes inteiras, em alguns casos podem haver polinômios com coeficientes inteiros, cujas suas raízes são racionais.

Apresentaremos agora um processo para se determinares raízes desse modelo, ou seja, raízes racionais escritas da forma $\frac{p}{q}$ com p e q ambos primos e $q \neq 0$.

3.4 Raízes Racionais de Polinômios Cúbicos Com Coeficientes Inteiros

Inicialmente dizemos que uma raiz é racional quando esta é escrita da forma $\frac{p}{q}$ com p e q ambos primos e $q \neq 0$. Segundo Facco (2008, p. 15), vale o seguinte teorema[16] "se o número racional p/q com p e q primos entre si e $q \neq 0$, é uma raiz da equação polinomial com coeficientes inteiros: $a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 = 0$, então p é divisor de a_0, além disso q é divisor de a_n".

Consequentemente, a partir da afirmação de Facco (2008), para se determinar as raízes racionais de um polinômio cúbico, basta encontrar inicialmente os divisores de a_o. Em seguida encontrar os divisores de a_n. As possíveis raízes são as frações do tipo p/q onde p e q são divisores de a_o e a_n, respectivamente. Assim temos o primeiro passo para se determinar tais raízes. O exemplo, a seguir, ilustrará a afirmação de Facco.

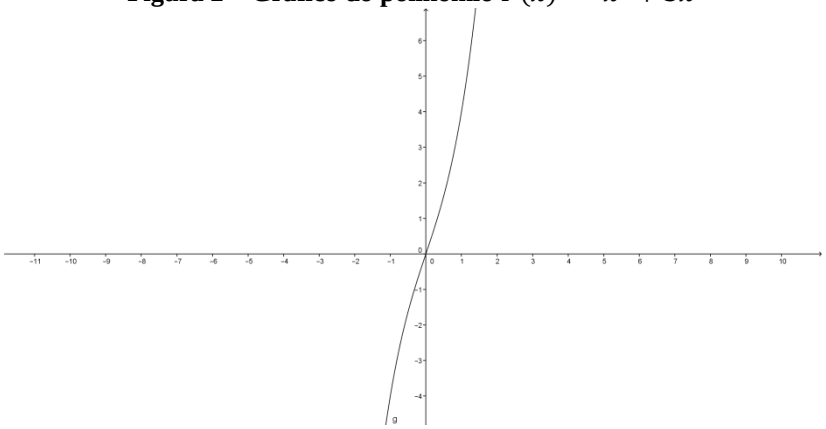
Por exemplo:

> Determinar as raízes racionais de $3x^3 + x^2 + x - 2 = 0$.
> Pelo teorema anterior sabe-se que se $\frac{p}{q}$ é uma raiz racional da equação, então p é divisor de -2 (± 1, ± 2); q é divisor de 3 (± 1, ± 3), logo, ± 1, $\pm {}^{1}/_{3}$, ± 2 e $\pm \frac{2}{3}$. Fazendo uma verificação, vê-se que $\frac{2}{3}$ é raiz. (FACCO, 2008, p. 16).

Com esse processo citado acima, podemos encontrar raízes racionais da forma $\frac{p}{q}$ de qualquer polinômio cúbico. Facco (2008, p. 16) coloca que "toda equação polinomial de coeficientes inteiros e cujo coeficiente do termo de maior grau é 1, se possuir raízes racionais, elas serão todas inteiras". De fato, basta observar que, quando o coeficiente do maior termo for 1, então os únicos divisores de 1 são ± 1, assim teríamos raízes da forma $\frac{p}{-1}$ ou $\frac{p}{1}$, isto é, - *p* ou *p*.Mas em muitos casos polinômios cúbicos não apresentam somente raízes racionais ou inteiras, dependendo do polinômio dado suas raízes podem ser também complexas, ou seja, raízes da forma $a + bi$ com $a, b \in \mathbb{R}$. Por exemplo, considere o polinômio $P(x) = x^3 + 3x$ com suas respectivas raízes $\{0, i\sqrt{3}, -i\sqrt{3}\}$, uma real e duas complexas. O gráfico de *P(x)* está ilustrado na figura 2.

[16] Para o leitor que se interessar pela demonstração do teorema, procurar em (FACCO, 2008, P. 15).

Figura 2 – Gráfico do polinômio $P(x) = x^3 + 3x$



Fonte: Criada pelo autor

São raízes dessa forma que procuramos tratar na próxima seção.

3.5 Raízes Complexas de Polinômios Cúbicos com Coeficientes Reais

Considere o exemplo $P(x) = x^3 + x^2 + x + 1$, cujas raízes são exatamente -1, $+i$ e $-i$. Repare bem o leitor que nesse momento não estamos trabalhando apenas com o conjunto $\mathbb{R}$, mas também com o conjunto $\mathbb{C}$. Segundo Ripoll (2006, p. 211) "[...] o campo dos números complexos é capaz de dar resposta a questões básicas da teoria dos polinômios e das equações polinomiais", por isso os números complexos tem sua importância para o estudo de raízes de equações cúbicas (ver apêndice C).

Observe que neste exemplo, o coeficiente do termo de maior grau é 1, então podemos utilizar os conceitos aplicados na seção 3.4 para polinômios desse modelo, como colocado por Facco (2008) e assim, encontrar pelo menos uma raiz inteira. Com a informação de pelo menos uma raiz inteira, podemos aplicar os conceitos estudados na seção 3.3, isto é o algoritmo de Briott- Ruffini. Assim, conseguimos determinar as raízes de $P(x) = x^3 + x^2 + x + 1$.

O processo se resume da seguinte forma: observe que os únicos divisores do coeficiente de x^3 são ± 1 e os únicos divisores do coeficiente de x^0 também são ± 1, portanto uma das raízes é -1.

Quando aplicamos o algoritmo de Briott-Ruffini, isto é,

1	1	1	1	-1
1	0	1	0	

os termos 1, 0, 1, 0 representam os coeficientes de um polinômio de grau 2, pois o polinômio original trabalhado é de grau 3, e quando se aplica o algoritmo, os polinômios resultantes ficam decrescidos em 1 grau. Assim temos o polinômio $P(x) = x^2 + 1$, onde suas raízes podem ser encontradas pela fórmula de Bháskara[17]. Portanto as outras raízes são exatamente $+i$ e $-i$.

Mas, se tratando das cúbicas, nem sempre conseguimos determinar suas raízes por meio de uma única fórmula resolutiva.

> Dada uma equação cúbica de coeficientes reais $x^3 + px + q = 0$, é verdade que, sempre que ela tiver raíz(es) real (is), ao menos uma delas é dada pela fórmula $x = \sqrt[3]{-\frac{q}{2} + \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}} + \sqrt[3]{-\frac{q}{2} - \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}}$?
> E se os coeficientes p e q "travam" tal fórmula, será que podemos garantir que a equação dada não tem nenhuma raiz real?
> A resposta para ambas às questões é não. E um exemplo comprobatório é a equação $x^3 - 15x - 4 = 0$. De fato, note que, por um lado, por inspeção direta, vemos que a mesma tem 4, -2 + $\sqrt{3}$, -2 - $\sqrt{3}$ para raízes reais. Por outro lado, fazendo a substituição de $p =$ -15 e $q =$ -4 na candidata fórmula, obtemos $\sqrt[3]{2 + \sqrt{-121}} + \sqrt[3]{2 - \sqrt{-121}}$, expressão absurda no campo numérico dos reais, pois o lado direito envolve a raiz quadrada de um número negativo e, nos reais, não está definida a raiz de um número negativo. (RIPOLL, 2006, p. 219).

Portanto, no campo dos reais, a fórmula acima não é válida para a resolução de cúbicas da forma $x^3 + px + q = 0$. No entanto, quando se trata do campo dos números complexos a fórmula passa a ser incontestável, pois dessa forma conseguimos calcular raízes de números negativos.

Considere o seguinte exemplo colocado por Ripoll (2006).

> Acompanhe o desenvolvimento feito por Bombelli onde é aplicado, conforme o próprio Bombelli mencionou, a "ideia louca" de operar com expressões do tipo $a + b\sqrt{-1}$ como se fossem números reais e, desta forma, "destravar" o cálculo das raízes da cúbica $x^3 - 15x - 4 = 0$:
> $x = \sqrt[3]{2 + \sqrt{-121}} + \sqrt[3]{2 - \sqrt{-121}}$
> $= \sqrt[3]{2 + 11\sqrt{-1}} + \sqrt[3]{2 - 11\sqrt{-1}}$

[17] Para resolver uma equação da forma $ax^2 + bx + c = 0$, utiliza-se a fórmula: $x = \frac{-b \mp \sqrt{b^2 - 4ac}}{2a}$.

$$= \sqrt[3]{(2 + 11\sqrt{-1})^3} + \sqrt[3]{(2 - 11\sqrt{-1})^3}$$
$$= (2 + \sqrt{-1}) + (2 - \sqrt{-1}) = 4 \text{ (RIPOLL, 2006, P. 220).}$$

Portanto, com a introdução dos números complexos na matemática foi possível extrair raízes quadradas de números negativos, assim encontrar soluções de equações cúbicas quando estas apresentavam números negativos em seus radicais, o que era um grande desafio para muitos matemáticos.

CONSIDERAÇÕES FINAIS

Neste trabalho procura-se aplicar técnicas simples, como o teorema do resto, algoritmo de Briott-Ruffimi, entre outros, no entanto eficientes para se determinar raízes de polinômios cúbicos, bem como todo o processo em que matemáticos tiveram que enfrentar para se chegar ao conhecimento que temos hoje sobre o referido tema. Mostramos que o conjunto dos polinômios escritos na variável *x, K[x]*, munido das operações usuais de polinômios possui uma estrutura algébrica, conhecida como anel. As estruturas algébricas tais como: grupos e anéis que aqui foram apresentados contribuíram de forma relevante para o desenvolvimento deste trabalho.

E a partir daí, foram apresentados métodos simples e práticos, excluindo o máximo possível, o grau de dificuldade em determinar raízes de polinômios. Apresentamos também que existem algumas condições para se determinar as raízes de algumas equações.

Apresenta-se alguns métodos de forma clara e objetiva para a determinação de tais raízes, podendo elas serem reais ou complexas.

Assim o estudo feito contribui de forma significativa para resolução de equações cúbicas, bem como a compreensão dos vários processos apresentados para determinar as raízes de polinômios de modo geral.

No início encontramos algumas dificuldades em reunir informações necessárias para a construção deste projeto bem como definir quais seriam os pontos chaves a serem abordados no decorrer do texto. O trabalho proposto buscou principalmente enfatizar maneiras claras e objetivas para a determinação de raízes de polinômios cúbicos, visando trazer aos leitores os processos de forma clara, objetiva e ao mesmo tempo eficientes.

As dificuldades se deram principalmente na determinação de processos eficazes para encontrar raízes de polinômios cúbicos, sabendo que não há uma fórmula resolutiva para polinômios de grau 3 de modo geral.

Contudo, ao final da construção deste trabalho, percebe-se que as dificuldades encontradas podem ser superadas, pois as observações feitas sobre os processos utilizados podem facilmente manuseados, dessa forma conseguimos atingir nosso objetivo principal.

REFERÊNCIAS BIBLIOGRÁFICAS

AZEVEDO, Danielle Santos. *Solubilidade de Equações Polinomiais por Radicais Reais e Cálculo do Grupo de Galois em Q[x]*. Dissertação (Mestrado em Ciência Matemática). Universidade federal do Rio Grande do Sul, 2012. Acesso em 3 de Julho de 2014. Disponível em: http://www.lume.ufrgs.br/bitstream/handle/10183/65427/000870206.pdf?sequence=1

ARAÚJO, Kalasas Vasconcelos. *Estruturas Algébricas II*. UFS: [s. n.], 2009. Acesso em 3 de Agosto de 2014 às 15h28min. Disponível em: https://www.sigaa.ufs.br/sigaa/verProducao?idProducao=163515&key=5189b03bedaae500ebc9fd74785aec90

BORDEAUX, Ana Lúcia; et al; PITOMBEIRA, João Bosco (Coord). *Matemática, terceira série*. Rio de Janeiro: [s. n.], 2005.

BURGUETTI, Renata. *Utilização dos Polinômios.* Campo Mourão: [s. n.], 2010. Acesso em 23 de Setembro de 2014 às 8h39min. Disponível em: http://repositorio.roca.utfpr.edu.br/jspui/bitstream/1/655/1/CM_ESPMAT_I_2011_13.pdf

BROLESI, Fogliarino. *Teorema Fundamental da Álgebra.* Campinas: [s. n.], 2006. Acesso em 16 de Março de 2014 às 9h11min. Disponível em: http://www.profezequias.net/fabio-fogliarini-brolesi.pdf

BRUSAMARELLO, Rosali. *Equações Algébricas*. I Colóquio Regional da Região Centro-Oeste: Universidade Federal de Mato Grosso do Sul, 2009. Acesso em 25 de Junho de 2014 às 5h44min. Disponível em: http://www.coloquiodematematica.ufms.br/conteudo/material/mc02_7.pdf

DANTE, Luis Roberto. *Matemática.* São Paulo: Ática, 2004.

DOMINGUES, Higino H.; IEZZI, Gelson. *Álgebra Moderna*, volume único, 4° edição reform. São Paulo: atual. 2003.

FACCO, Elieser. *Polinômios Algébricos*. Santa Maria/RS: [s. n.], 2008. Acesso em 13 de Março de 2014 às 12h02min. Disponível em: http://www.unifra.br/cursos/matematica/downloads/Elieser%20Facco.pdf.pdf

GARCIA, Arnaldo; et al. *Elementos de Álgebra.* Rio de Janeiro: IMPA, 2005.

GEOGEBRA, *Software Computacional*. Acesso em 17 de Agosto de 2014 às 22h44min. Disponível em: http://www.baixaki.com.br/download/geogebra.htm

GIOVANNI, José Ruy; BONJORNO, José Roberto. *Matemática Completa*. São Paulo: FTD, 2005.

GONÇALVES, Adilson. *Introdução à Álgebra*. Rio de Janeiro: Instituto de Matemática Pura e Aplicada, 1979.

LISBOA, Viviane de Jesus. *Polinômios com coeficientes da sequência de Fibonacci*. Colégio de Matemática da UEFS: [s. n.], 2013. Acesso em 23 de Julho às 14h55min. Disponível em: http://www2.uefs.br/sigma/arquivos/COP/COP02-2008_Viviane_Lisboa.pdf

MARQUES, Cristina Maria. *Introdução à Teoria de Anéis*. UFMG: [s. n.], 1999. Acesso em 8 de Agosto de 2014 às 13h21min. Disponível em: http://www.mat.ufmg.br/~marques/Apostila-Aneis.pdf

OLIVEIRA, Oswaldo Rio Branco. *Teorema Fundamental da Álgebra (TFA).* [s. n.], 2011. Acesso em 15 de Março de 2014 às 17h06min. Disponível em: http://www.ime.usp.br/~oliveira/TFACOLEGIAL5.pdf

PINTO, Maria Manuela Pereira. *Grupos e Simetrias*. Tese (Mestrado em Matemática). Universidade Portucalense Infante D. Henrique, 2009. Acesso em 25 de Junho de 2014 às 15h53min. Disponível em: http://repositorio.uportu.pt/jspui/bitstream/11328/537/2/TMMAT%20112.pdf

QUEIROZ, Cleber da Costa. *Funções e Equações Polinomiais, Comportamento da Função do 3° Grau.* Tese (Mestrado Profissional em matemática em Rede Nacional). Universidade Federal de Goiás, 2013. Acesso em 11 de Maio de 2014 às 21h54min. Disponível em: http://bit.profmat-sbm.org.br/xmlui/bitstream/handle/123456789/453/2011_00342_CLEBER_DA_COSTA_QUEIROZ.pdf?sequence=1

RIPOLL, Jaime Bruck. *Números racionais, reais e complexos.* Porto Alegre: Editora da UFRGS, 2006.

SEVERINO, Antônio Joaquim. *Metodologia do Trabalho Científico*; 23 ed. Ver. e atual. – São Paulo: Cortez, 2007.

SILVA, Pedro V. *Álgebra*. Tese (Mestrado em matemática). Faculdade de Ciências do Porto: [s. n.], 2004. Acesso em 16 de Abril de 2014 às 10h43min. Disponível em: http://cmup.fc.up.pt/cmup/pvsilva/pubs/Algebra.pdf

Susseções ou Sequências. Acesso em 3 de Setembro de 2014 às 12h32min. Disponível em: www.colegioweb.com.br/trabalhos-escolares/matematica/sucessoes-ou-sequencias/o-que-sao-sucessoes-ou-sequencias.html

ZANOELLO, Simone Fátima. *Raízes Polinomiais em Corpos Finitos*. Dissertação (Mestrado em Matemática Aplicada). Universidade Federal do Rio Grande do Sul, 2004. Acesso em 21 de Setembro de 2014às 16h12min. Disponível em: https://www.lume.ufrgs.br/bitstream/handle/10183/3554/000401876.pdf?sequence=1

APÊNDICES

APÊNDICE A – CONTEXTO HISTÓRICO DOS POLINÔMIOS

O contexto histórico dos polinômios caminha lado a lado com a história da matemática, não se sabe ao certo onde e quando surgiu. O que sabemos é que desde a época primitiva o ser humano busca novas maneiras para se adaptarem à suas necessidades. Viviane de Jesus Lisboa diz claramente que:

> O pensamento matemático é desenvolvido pelo ser humano desde a época primitiva. Pode-se pensar nele presente há 50.000 anos, quando o homem dava forma aos barcos que o levaram à Austrália e planejava as quantidades de recursos a serem transportados durante a viagem. Ou mesmo há 2.000.000 de anos quando o homo-hábilis quebrava pedras para dar-lhe formas úteis. (LISBOA, 2007, p.1)

Nas proximidades do ano 2000 a.C. a civilização babilônica já havia dado um grande salto para a evolução da aritmética para a álgebra retórica[18]. A partir de então os babilônicos não apenas encontravam a solução de equações quadráticas como também havia uma grande e intensa discussão sobre as equações cúbicas. São apresentados diversos problemas que tratam as equações polinomiais cúbicas escritas da forma

$\alpha^3 + \alpha^2 = c$

no qual esses problemas poderiam encontrar sua solução utilizando uma tábua com a característica $n^3 + n^2$, que é justamente uma sequência de números inteiros dentro do intervalo fechado [1, 30].

As equações do terceiro grau ou equações cúbicas surgiram de forma muito interessante, pois eram situações que intrigava muitos matemáticos, principalmente pelas dificuldades encontradas em trabalhar com esse tipo de expressão. Para Moro (2000/2, p. 4) "temos notícia de que Arquimedes (225 a. C.) manipulou uma cúbica vinda de um problema geométrico".

Segundo Lisboa (2007, p. 2) "vários problemas envolvendo polinômios (equações polinomiais) instigaram a curiosidade de matemáticos como Nicoló Fontana (Tartáglia),

[18]A álgebra pode ser subdividida em três classificações: álgebra retórica, anterior a Diofanto; álgebra sincopada, criada por Diofanto, consiste basicamente em diminuir operações que se repetem várias vezes por meio de abreviações; álgebra simbólica, composta por símbolos e teve um grande salto a partir do século XVII.

Ludovico Ferrari, Isaac Newton dentre muitos outros". O estudo e os processos de desenvolvimento dos métodos utilizados para efetuar a resolução de equações polinomiais, principalmente para as cúbicas tiveram um grande avanço a partir dos séculos XV e XVI com um grupo de matemáticos italianos[19], também era muito comum as grandes mentes matemáticas se reunirem para estudar um determinado assunto.

Os polinômios cúbicos conhecidos por polinômios de terceiro grau ou de grau 3, são todos aqueles que podem ser colocados ou escrito da maneira

$P(x) = ax^3 + bx^2 + cx + d$

onde se exige que o coeficiente de x^3 tem que ser não nulo, caso contrário teríamos um polinômio quadrado.

Segundo Brusamarello (2009, p. 4) "a descoberta de uma solução para estas equações ocorreu na Itália, no século XVI, e gerou uma disputa histórica entre alguns matemáticos italianos".

O primeiro matemático a encontrar um processo para resolver uma equação de 3° grau colocada da forma $x^3 + px = q$ onde p e q ambos números positivos, foi um professor da Universidade de Bolonha, Scipione del Ferro (1456-1526), no entanto, ele manteve segredo sobre sua ilustre descoberta, até próximo a sua morte, quando decidiu revelar a um aluno da Universidade, Antônio Fior. A descoberta de Scipione se reduz na seguinte fórmula:

Fórmula de Scipione del Ferro para cúbicas da forma $x^3 + px = q$

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

Fonte: Ripoll (2006, p. 219)

Girolamo Cardano (1501-1576) também acabou desenvolvendo um processo para resolver as cúbicas, ou seja, determinar suas raízes. O método utilizado por Cardano reduzia a cúbica da forma

$ax^3 + bx^2 + cx + d = 0$ para uma escrita de maneira $x^3 + \alpha x + \beta = 0$, ou seja, fazendo mudanças de variáveis, e assim conseguia extrair suas raízes. Com essas informações, Cardano contribuiu de forma significativa para a resolução das equações cúbicas.

[19] Leonardo de Pisa (1180-1250); Scipione del Ferro (1465-1562); Chistoff Rudolff (1500-1545); Ludovico Ferrari (Tartaglia); Girolamo Cardano entre outros matemáticos.

$x^3 + \alpha x + \beta = 0$, ou seja, fazendo mudanças de variáveis, e assim conseguia extrair suas raízes. Com essas informações, Cardano contribuiu de forma significativa para a resolução das equações cúbicas. Muitos matemáticos contribuiu de forma bastante significativa para os processos de resolução de equações, por exemplo:

> Outro matemático bem conhecido daquela época era Nicolo Fontana (conhecido como Tartaglia) [...]. Querendo ganhar fama às custas de seu mestre, Antônio Maria Fior escolheu Tartaglia para um desafio matemático. Fior planejava propor problemas que resolvessem a resolução da equação cúbica, mas Tartaglia ficou sabendo disso e se empenhou na busca das soluções das mesmas. (BRUSAMARELLO, 2009, P. 4 e 5)

Portanto, para se chegar ao conhecimento que temos hoje, matemáticos tiveram que passar por diversas situações e desafios para ter seus trabalhos reconhecidos e aceitos, assim desde as primeiras equações resolvidas pelos babilônicos até as mais sofisticadas técnicas para a resolução de equações principalmente em caso de equações cúbicas tiveram um longo processo de desenvolvimento, há relatos de que matemáticos levaram mais de 20 anos para concluir suas pesquisas e assim ter seus trabalhos reconhecidos.

APÊNDICE B – EXTENSÕES ALGÉBRICAS SOBRE UM CORPO *K*

Quando se trata de raízes de polinômios ou equações polinomiais o que se procura determinar é sob quais condições um polinômio *P(x)* seja igual a *0*. Isto é, se existe um elemento α no corpo *K* tal que *P(α) = 0*, então neste caso dizemos que α é raiz do polinomio *P(x)*. Segundo Facco (2008, p. 14) "Numa equação polinomial de coeficientes inteiros, pode-se obter suas eventuais raízes inteiras [...]".

De acordo com Facco (2008, p. 14) "denomina-se raiz da equação $a_n x^n + a_{n-1}x^{n-1} + \cdots + a_2 x^2 + a_1 x + a_0 = 0$ o valor r de x que satisfaz a igualdade, ou seja, o valor tal que: $a_n r^n + a_{n-1}r^{n-1} + \cdots + a_2 r^2 + a_1 r + a_0 = 0$", isto significa que o valor encontrado para *x* tornará a igualdade igual à zero. Mas nem sempre é possível determinar raízes de certos polinômios em determinados conjuntos, isto é, os conjuntos $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ ou $\mathbb{C}$ e por esse motivo há a necessidade de estudar extensões algébricas.

O estudo sobre as extensões algébricas sobre um corpo qualquer nos fornece uma ferramenta muito importante para o estudo de raízes de determinados polinômios, pois é por meio dessa ferramenta que em muitos casos é possível encontrá-las. Observe que os corpos $\mathbb{Q}$, $\mathbb{R}$ e $\mathbb{C}$ não são os únicos corpos que se podem trabalhar, existem uma inúmeros deles. Segundo Gonçalves (1939, p. 35) "[...] $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, $\mathbb{Q}[\sqrt{2}]$ e $\mathbb{Z}_p$, p primo são todos exemplos de corpos, sendo que os $\mathbb{Z}_p$, p primos ≥ 2, nos dão uma infinidade de exemplos de corpos finitos]'.

Segundo Kalasas (2009.2, p. 99) "[...] Um corpo K é dito uma extensão de F se K contém F como um subcorpo [...]".

Por exemplo, dado um polinômio qualquer $P(x) = ax^2 + b$ em *K[x]*, observe que *P(x)* não possui raízes reais. De fato, se *P(x) = 0* temos que $ax^2 + b = 0$, então $x = \sqrt{\frac{-b}{a}}$, com $a \neq 0$. Como não existe raiz de índice par de números negativos, então $x \notin \mathbb{R}$. No entanto podemos encontrar as raízes de *P(x)*, sendo elas reais ou não em $\mathbb{C}$[20]. Esse processo que fazemos de estender o conjunto $\mathbb{R}$ para o conjunto $\mathbb{C}$, na verdade estamos ampliando o corpo $\mathbb{R}$ para o corpo $\mathbb{C}$. Portanto $\mathbb{C}$ é uma extensão algébrica de $\mathbb{R}$.

[20] $\mathbb{C}$ designa o conjunto dos números complexos.

Dado um elemento μ de E de tal forma que exista um *H(x)* em *K[x]*, polinômio não nulo em *K[x]*, onde μ é raiz de *H(x)*, dizemos que μ é algébrico sobre o corpo *K*.

Por exemplo, seja o polinômio $P(x) = x^3 - \alpha$ em *K[x]* temos que $P(\sqrt[3]{\alpha}) = 0$, então dizemos que $\sqrt[3]{\alpha}$ é elemento algébrico de *P(x)* sobre *K*. Portanto as extensões algébricas nos permite determinar os elementos algébricos de certos polinômios com maior facilidade, pois nos permite a ampliação de um corpo *K* para um corpo *K'* e dessa maneira encontrar as possíveis raízes de um polinômio *P(x)*.

APÊNDICE C – A IMPORTÂNCIA DOS NÚMEROS COMPLEXOS

Os números complexos tem uma grande importância em relação à resolução de equações polinomiais, mas quanto a sua criação muitos matemáticos achavam desnecessária sua criação, principalmente em questões sobre raízes quadradas.

> Por volta de 1500 d. C., a impressão que se tinha é que, com a criação dos números reais – que tinham representação para a solução de todos os problemas de medida -, não seria mais necessária à ampliação de nenhum campo numérico. O pensamento era que "um número negativo não é raiz quadrada de nenhum número; logo, não existe raiz quadrada de número negativo". (GIOVANNI, 2005, P. 136).

Mas entre estudiosos que discordavam da criação de tais números, existiam aqueles que afirmavam que a utilização desses números seria impossível resolver alguns problemas relacionados a raízes de polinômios, pois sem a utilização dos números complexos aos cálculos para se extrair raízes negativas de polinômios ficariam de certa forma travados.

> Quando surgiram os primeiros problemas nos quais havia sentido material falar-se em raízes negativas (como ocorre, por exemplo, ao tratarmos de débitos automáticos em questões de contabilidade), passou-se a chamar as raízes positivas de raízes verdadeiras e as negativas de raízes falsas. Ripoll (2006, p. 221 e 222)

Dessa forma foi possível encontrar raízes negativas de polinômios por meio da utilização dos números complexos.

Segundo Brusamarello (2009, p. 7) "muitos acreditam que os números complexos surgiram para resolver equações de 2° grau, mas isto não é verdade". O surgimento dos números complexos deu-se por meio das tentativas de se resolver equações de 3° grau.

Com a criação dos números complexos foi possível não apenas determinar raízes de números negativos, mas também facilitar os processos de resoluções de problemas encontrados nos cursos de Cálculo, problemas encontrados em funções trigonométricas,

funções exponenciais, todos podem ser resolvidos facilmente com a aplicação de números complexos.