Universidade Federal da Bahia - UFBA
Instituto de Matemática e Estatística - IME
Sociedade Brasileira de Matemática - SBM
Mestrado Profissional em Matemática em Rede Nacional - PROFMAT
Dissertação de Mestrado

Divisão de Polinômios: uma Nova Abordagem para o Ensino Médio

Marcelo Lopes Monteiro

Salvador-Bahia
Abril-2017

Divisão de Polinômios: uma Nova Abordagem para o Ensino Médio

Marcelo Lopes Monteiro

Dissertação de Mestrado apresentada à Comissão Acadêmica Institucional do PROFMAT-UFBA como requisito parcial para obtenção do título de Mestre em Matemática.

Orientador: Prof. Dr. Carlos Eduardo Nogueira Bahiano.

Salvador - Bahia
Abril-2017

Modelo de ficha catalográfica fornecido pelo Sistema Universitário de Bibliotecas da UFBA para ser confeccionada pelo autor

Lopes Monteiro, Marcelo
DIVISÃO DE POLINÔMIOS: UMA NOVA ABORDAGEM PARA O ENSINO MÉDIO / Marcelo Lopes Monteiro. -- Salvador, 2017.
66 f. : il

Orientador: Prof. Dr. Carlos Eduardo Bahiano.
Dissertação (Mestrado - PROFMAT) -- Universidade Federal da Bahia, Universidade Federal da Bahia, Instituto de Matemática e Estatística UFBA, 2017.

1. Polinômios. 2. Divisão de Polinômios. 3. Polinômios em duas ou mais variáveis. 4. Pseudodivisão de Polinômios. I. Bahiano, Prof. Dr. Carlos Eduardo. II. Título.

Divisão de Polinômios: Uma nova abordagem para o Ensino Médio

Marcelo Lopes Monteiro

Dissertação de Mestrado apresentada à comissão Acadêmica Institucional do PROFMAT-UFBA como requisito parcial para obtenção do título de Mestre em Matemática, aprovada em 07/04/2017.

Banca Examinadora:

Carlos Eduardo N. Bahiano
Prof. Dr. Carlos Eduardo Nogueira Bahiano (orientador)
UFBA

Marco Cerami
Prof. Dr. Marco Cerami
UFBA

Elaís Cidely Souza Malheiro
Profª. Dra.Elaís Cidely Souza Malheiro
UFBA

À minha esposa Flávia e a meus filhos: Arthur e Alice, com muio carinho e amor

AGRADECIMENTOS

Agradeço primeiramente à Deus, pois sem ele eu não estaria aqui. À minha esposa por estar sempre comigo nos momentos que mais precisei. Aos meus familiares, principalmente à minha mãe Maria Crisina Santos por acreditar em mim, aos meus colegas de curso: Etinevaldo, Leandro e Ivanilton, aos professores dessa instituição que contribuíram bastante para o bom andamento do curso e ao meu orientador Carlos Bahiano, pela paciência, disponibilidade e atenção dispensados à minha pessoa.

"A Matemática não mente. Mente
quem faz mau uso dela".
Albert Einstein

RESUMO

O presente trabalho busca apresentar um novo modelo de Ensino Aprendizagem ao conteúdo de polinômios, especificamente abordado, em geral, no 3° ano do Ensino Médio. Logicamente acrescentando esse novo modelo, aos modelos já existentes, que são tradicionalmente trabalhados e inseridos no contexto do ensino de Polinômios. A escolha do tema foi devido à importância do mesmo e também com o intuito de estender esse aprendizado a partir da introdução de novos conceitos e aplicabilidades, que não são trabalhados no ensino médio. A proposta é realmente desenvolver uma nova abordagem no ensino de polinômios e um dos tópicos a serem trabalhados com mais ênfase é a pseudo divisão de Polinômios de duas ou mais variáveis, portanto será necessário que os alunos adquiram o conhecimento relativo ao conceito de polinômios de duas ou mais variáveis e como desenvolver as operações com esse tipo de polinômio.

Palavras-chave: Polinômios, Divisão de Polinômios, Operações com polinômios de duas ou mais várias variáveis

ABSTRACT

The present work seeks to present a new model of Teaching Learning to the content of polynomials, specifically discussed, in general, in the 3rd year of Brazilian High School. Logically, by adding this new model to existing models that have traditionally been developed and inserted in the context polynomials. The choice of this topic was due to it's importance and also in order to extend the common sense that is usual, by introducting new concepts and applicabilities. We aim to presents to teachers a new approach and tecnique for discuss the theme with their students; More precisaly, we suggest the discussion of polynomials with up 1 to 3 variables and real coefficients and their main operations. Was due to importance of the theme and also in order to extend this learning from the introduction of new concepts and applicabilities. The proposal is really to develop a new approach in the teaching of polynomials and one of the technicians, to be worked with more emphasis, and the pseudo-division of Polynomials of two or more variables,Therefore it will be necessary for students to acquire knowledge about the concept of polynomials of two or more variables and how to develop operations with this type of polynomial.

Key words: Polynomials, Division of Polynomials, Operations with polynomials of two or more variables

SUMÁRIO

INTRODUÇÃO

A Matriz curricular nacional para o ensino da Matemática, inserida nos Parâmetros Curriculares Nacionais, foi estabelecida para dar uma orientação ou sugestão de como devem ser ensinados os conteúdos matemáticos e quais, objetivamente, devem ser abordados [1]. A álgebra está entre as preocupações dos educadores matemáticos, sobretudo pela forma com que esse ramo tão importante da matemática é tratado em sala de aula, ou seja: quase sempre dando ênfase puramente às manipulações algébricas, sem contextualizar e sem abordar as conexões com outros temas da matemática. Isso torna o processo de ensino aprendizagem desestimulante para os alunos.

O ensino da álgebra, faz parte da Competência 5 da Matriz Curricular Nacional, estando descrita assim:*Modelar e resolver problemas que envolvem variáveis socioeconômicas ou técnico-científicas, usando representações algébricas*[2]. Essa competência traz cinco habilidades especificas e necessárias para a sua composição, que são elas:

- I) *"Identificar representações algébricas que expresem relações entre grandezas"*.Essa habilidade exige que os estudantes saibam encontrar uma equação que relacione grandezas, independentemente de serem proporcionais ou não;

- II) *"Interpretar gráfico cartesiano que represente relações entre grandezas"*. Como todas as relações entre as grandezas x, y e z geram um gráfico, o estudante precisa reconhecer de qual função ele foi originado;

- III) *"Resolver situação-problema cuja modelagem envolva conhecimentos algébricos"*. Essa habilidade exige que o estudante saiba chegar ao resultado esperado por meio da aplicação dos dados do problema em uma fórmula;

- IV) *"Utilizar conhecimentos algébricos/geométricos como recurso para a construção de argumentação"*.É essencial identificar qual a argumentação correta, por meio das próprias questões;

- V) *"Avaliar propostas de intervenção na realidade utilizando conhecimentos algébricos"*. O estudante deve pontuar qual a alteração que deve ser feita em uma situação-problema para que o resultado se altere de acordo com o que é pedido.

Ao tomar posse do conhecimento dessa competência e das habilidades concernentes, percebe-se logo, nas primeiras palavras, a inserção de elementos que não são exclusivos da álgebra e até mesmo da matemática, como a modelagem e variáveis socioeconômicas ou técnico-científicas, o que deixa bem claro que a proposta fundamental é a utilização da álgebra como uma ferramenta representativa e bastante útil, para a resolução de problemas que envolvam variáveis.

Desse modo, se faz presente a necessidade de propostas que envolvam novas abordagens para o ensino da álgebra em todos os seus conteúdos correlacionados, com o pré-requisito de que essas propostas de trabalhos estejam de acordo com as competências e as habilidades atribuídas para esse ramo da matemática.

O tema desse presente trabalho tem como uma de suas finalidades a inserção de novos conceitos e aplicações para as divisões polinomiais (assunto que faz parte do conteúdo da álgebra). Essa nova abordagem busca tornar o processo de ensino aprendizagem mais interessante e significativo para os alunos, sem deixar de estar inserida nas competências do ensino da álgebra.

No capítulo 1 serão abordados todos os aspectos dos conteúdos que já são tradicionalmente trabalhados na educação básica, ou seja: as divisões polinomiais com uma variável, utilizando a divisão euclidiana e outros métodos de divisão como: método de Descartes (ou dos coeficientes a determinar) e as divisões imediatas, também serão abordados alguns teoremas como o Teorema do Resto e o Teorema de DAlembert, e as divisões por binômios do 1° grau utilizando o algoritmo de Briot-Ruffini. No final do capítulo, a abordagem terá como foco as equações algébricas e algumas aplicações, utilizando a divisão polinomial com uma variável, aplicações essas, que não são usualmente trabalhadas no ensino médio, como, por exemplo: o método das divisões sucessivas de Euclides, que permite encontrar o M.D.C. entre Polinômios.

O capítulo 2 será destinado à introdução de mais uma variável, em cada polinômio envolvido na divisão. O que se espera é que os alunos, a princípio, tenham alguma dificuldade em resolver essa operação, e comecem a despertar a curiosidade em conhecer um método que busque a solução desse tipo de divisão. A partir daí se faz necessária a introducão do conceito de Ordens Monomiais. Em seguida, será apresentado o algoritmo para a divisão de polinômios com duas ou mais variáveis, através do conceito de termo líder; O objetivo é que os alunos aprendam a dividir esses polinômios (inclusive, com dois polinômios no divisor), de acordo com a ordem monomial escolhida. Será possível, a partir dos resultados obtidos, com a utilização desse algoritmo citado, desenvolver com os alunos as aplicações desse tipo de divisão. Para que isso ocorra com eficácia, será preciso definir os conceitos de resultante e suas propriedades, além do teorema de intersecccão de Bézout.

Para o capítulo 3 serão apresentados sugestões de atividades e em que momento essas atividades deverão ser abordadas em sala de aula.

No capítulo final, serão feitas as considerações finais do trabalho, evidenciando os principais itens que merecem maior importância, entre outras observações apropriadas.

CAPÍTULO 1

CONCEITOS BÁSICOS

Um Polinômio $p(x)$ com coeficientes em $\mathbb{R}$ e variável em x é uma expressão do tipo:

$$p(x) = a_0 + a_1x + a_2x^2 + ... + a_nx^n = \sum_{i=0}^{n} a_ix^i, \text{ em que } n \in \mathbb{N}, \quad a_i \in \mathbb{R}, \text{ para } 0 \leq i \leq n$$

.

1.1 Grau

Definição 1.1.1. *Seja $p(x) = a_0 + a_1x + a_2x^2 + ... + a_nx^n$ um polinômio não nulo. Chama-se de grau de p e representa-se por $gr(p)$ o número natural l, tal que $a_l \neq 0$ e $a_i = 0$, $\forall i > l$. Lembrando que o polinômio em que todos os coeficientes a_i são zeros é denominado de polinômio nulo*

Assim grau de um polinômio p é o maior expoente em x de termo não nulo em p.

Vale afirmar que dois polinômios são iguais quando possuem exatamente os mesmos coeficientes nos termos de mesmo "grau".

Para o propósito desse trabalho, a abordagem das operações polinomiais se dará maior foco à divisão de polinômios, em detrimento das outras operações, tais como: adição, subtração e multiplicação.

1.2 Divisão de Polinômios

Definição 1.2.1. *Dados dois polinômios f (dividendo) e $g \neq 0$ (divisor), dividir f por g é determinar dois outros polinômios q(quociente) e r (resto) de modo que se verifiquem as duas condições:*

I) $q \cdot g + r = f$;

II) $gr(r) < gr(g)$, ou $r = 0$.

Exemplo 1.2.1. *Para $f = x^4 + 2x^3 - 3x + 2$ por $g = x^3 + 2x^2 + 2x - 1$, obtém-se $q = x$ e $r = -2x^2 - 2x + 2$ que satisfazem as duas seguintes condições:*

I) $q \cdot g + r = x(x^3 + 2x^2 + 2x - 1) + (-2x^2 - 2x + 2) = x^4 + 2x^3 - 3x + 2;$

II) $gr(r) = 2$ *e* $gr(g) = 3 \Longrightarrow gr(r) < gr(g).$

Exemplo 1.2.2. *Para* $f = 3x^3 - 4x^2 - 2x - 4$ *por* $g = x - 2$, *obtém-se* $q = 3x^2 + 2x + 2$ *e* $r = 0$ *que satisfazem as duas seguintes condições:*

I) $q \cdot g + r = (3x^2 + 2x + 2) \cdot (x - 2) + 0 = 3x^3 - 4x^2 - 2x - 4 = f;$

II) $r = 0.$

1.2.1 Divisões imediatas

Analisando o polinômio $qg + r$, onde $g \neq 0$ e $gr(r) < gr(q)$ ou $r = 0$, tem-se que:

i) Se $q = 0$ e $r = 0$, então $gq + r = 0.g + 0 = 0$;

ii) Se $q = 0$ e $r \neq 0$, então $gq + r = 0 \cdot g + r = r$, portanto, $gr(gq + r) = gr(r) < gr(g)$;

iii) Se $q \neq 0$ então $gr(gq) = gr(g) + gr(q) \geq gr(g)$, portanto, $gr(gq + r) \geq gr(g)$ pois a parcela r tem grau menor que q ou é nula.

Há dois casos em que a divisão de f por g é imediata:

- 1 ° Caso: $f = 0$: Nesse caso, tem-se que $gq + r = 0$ e, como foi visto, isso ocorre somente se $q = 0$ e $r = 0$ portanto: $f = 0 \Longrightarrow q = 0$ e $r = 0$;

- 2 ° Caso: $gr(f) < gr(g)$: Nesse caso, tem-se que:

$$gq + r = f \Longrightarrow gr(gq + r) = gr(f) \Longrightarrow gr(gq + r) < gr(g)$$

  e como já foi visto, isto ocorre quando $q = 0$ e $r \neq 0$, logo é imediato que, se $gr(f) < gr(g)$ então $q = 0$ e $r = f$.

  Observe a seguir, dois exemplos da utilização das divisões imediatas:

Exemplo 1.2.3. *a) Dividindo* $f = 0$ *por* $g = x^3 - 2x^2 + 5$, *obtém-se:* $q = 0$ *e* $r = 0$.

b) Dividindo $f = 4x^2 + 3x - 2$ *por* $g = 3x^3 + x^2 + 5x - 9$,*obtém-se:* $q = 0$ *e* $r = 4x^2 + 3x - 2$.

Para divisões onde o $gr(f) > gr(g)$, aparece de imediato o seguinte questionamento: como é possível obter q e r? para obter essa resposta é necessário tratar dois métodos de divisões a seguir: o método das chaves e o método de Descartes (ou método dos coeficientes a determinar).

1.2.2 Método da Chave

Para efetuar a divisão de dois polinômios, pode-se aplicar a mesma ideia da divisão de dois números naturais usando o método da chave que é um dos métodos mais comumente utilizados. Dividir um polinômio $f(x)$ por um polinômio $g(x)$ significa encontrar um polinômio $q(x)$(quociente) e um polinômio $r(x)$ (resto) da seguinte forma:

$$\begin{array}{r|l} \text{Dividendo} & \text{Divisor} \\ \cline{2-2} \text{Resto} & \text{Quociente} \end{array}$$

Ou seja, pode-se escrever na forma:

$$\begin{array}{r|l} f(x) & g(x) \\ \cline{2-2} -\vdots & q(x) \\ \cline{1-1} r(x) & \end{array}$$

O que resulta em: $f(x) = q(x) \cdot g(x) + r(x)$. Além disso, $n = 0$ ou o grau de $r(x)$ deve ser menor que o grau de $q(x)$.

Teorema 1.2.1. *Dados os polinômios* $f = a_m x^m + a_{m-1}x^{m-1} + a_{m-2}x^{m-2} + ... + a_1 x + a_0$, *com coeficientes feais ou complexos, e* $a_m \neq 0$, $g = b_n x^n + b_{n-1}x^{n-1} + b_{n-2}x^{n-2} + ... + b_1 x + b_0$, *com* $b_n \neq 0$. *Existe um único polinômio* q *e um único polinômio* r *tais que* $gq + r = f$ *e* $gr(r) < gr(g)$ *ou* $r = 0$

Demonstração. Deve-se primeiramente provar a existência dos polinômios q e r:

I) Existência

- i) Operação base: (cancelamento do termo líder: Formar o monômio $\dfrac{a_m}{b_n} = q_0$ e construir o polinômio:
$$r_1 = f - (q_0 x^{m-n}) \cdot g \tag{1.1}$$
Chamando r_1 de 1º resto parcial, nota-se que:
$$r_1 = (a_m x^m + a_{m-1}x^{m-1} + \ldots + a_0) - \frac{a_m}{b_n} \cdot x^{m-n} \cdot (b_n x^n + b_{n-1}x^{n-1} + \ldots + b_0).$$
O que prova o cancelamento de $a_m x^m$ (pelo menos), portanto, $gr(r_1) = \alpha < m$ ou $r_1 = 0$. Por conveniência, escreve-se:
$$r_1 = c_\alpha x^\alpha + c_{\alpha-1}x^{\alpha-1} + c_{\alpha-2}x^{\alpha-2}x^{\alpha-2} + \ldots + c_1 x + c_0;$$

- ii) Caso $r_1 \neq 0$ repete-se a operação considerando-se r_1 em lugar de f, até que o resultado obtido na etapa anterior enquanto o resultado tiver $gr(f) \geq gr(g)$. Percebe-se assim que, em cada etapa, o grau do resto parcial diminui pelo menos uma unidade, concluí-se então que, um certo número p de operações resulta em um resto parcial r_p de grau inferior ao de g ou então $r_p = 0$ e
$$r_p = r_{p-1} - (q_{p-1}x^{\epsilon-n})g \tag{1.2}$$
Adicionando membro a membro as igualdades de (1) a (p):
$$\begin{aligned} r_1 &= f - (q_0 x^{m-n})g \\ r_2 &= r_1 - (q_1 x^{\alpha-n})g \\ r_3 &= r_2 - (q_2 x^{\beta-n})g \\ &\vdots \\ r_p &= r_{p-1} - (q_{p-1}x^{\epsilon-n})g \end{aligned}$$
concluí-se que: $r_p = f - (q_0 x^{m-n} + q_1 x^{\alpha-n} + q_2 x^{\beta-n} + ... + q_{p-1}x^{\epsilon-n})g$. E então $f = qg + r$ com $gr(r) < gr(g)$ ou $r = 0$.

Deve-se agora, provar a unicidade desses polinômios q e r:

II)Unicidade

Considerando a existência de dois quocientes q_1 e q_2 e dois restos r_1 e r_2 na divisão de f por g, prova-se que $q_1 = q_2$ e $r_1 = r_2$. Pela definição de divisão, tem-se que:

$f = q_1 g + r_1$ e $f = q_2 g + r_2$ igualando as equações e colocando o fator comum em evidência, tem-se que: $(q_1 - q_2)g = (r_2 - r_1)$

Se $q_1 \neq q_2$ ou $r_2 \neq r_1$ prova-se que a igualdade $(q_1 - q_2)g = r_2 - r_1$ não se verifica:

- (i) $gr[(q_1 - q_2)g] = gr(q_1 - q_2) + gr(g) \geq gr(g)$

- (ii) $gr(r_2 - r_1) \leq \max\{gr(r_2), gr(r_1)\} < gr(g)$.

Igualando (i) com (ii), tem-se: $gr(g) \leq \max\{gr(r_2), gr(r_1)\}$, em contradição com a premissa que $gr(g) > \max\{gr(r_2), gr(r_1)\}$, portanto deve-se ter: $q_1 = q_2$ e $r_1 = r_2$. $\square$

Exemplificamos, através do próximo exercício o passo a passo da divisão de dois polinômios utilizando o método da chave

Exercício 1.2.1. *Divida $P = 8x^4 - 2x^3 + 4x - 9$ por $D = 2x^2 + 1$ de modo a encontrar o quociente Q e o resto da divisão R.*

Solução:

Primeiramente escreve-se ordenadamente o dividendo P e o divisor D segundo as potências decrescentes de x, completando-os se necessário, com termos de coeficiente zero.

$$\begin{array}{r|l} 8x^4 - 2x^3 \qquad\quad + 4x - 9 & 2x^2 + 1 \\ \cline{2-2} & \end{array}$$

Dividindo o termo de maior grau de P pelo termo de maior grau de D, obtém-se o primeiro termo de Q que é $4x^2$.

$$\begin{array}{r|l} 8x^4 - 2x^3 \qquad\quad + 4x - 9 & 2x^2 + 1 \\ \cline{2-2} & 4x^2 \end{array}$$

Multiplicando o termo encontrado pelo divisor e subtraindo do dividendo,obtém-se o resto parcial $-2x^3 - 4x^2 + 4x$.

$$\begin{array}{rrrrr|l} 8x^4 & -2x^3 & & +4x & -9 & 2x^2 + 1 \\ \cline{6-6} -8x^4 & & -4x^2 & & & 4x^2 \\ \cline{1-3} & -2x^3 & -4x^2 & +4x & & \end{array}$$

Dividindo o termo de maior grau do resto parcial $(-2x^3)$ pelo termo de maior grau do divisor $(2x^2)$, obtém-se assim o próximo termo do quociente $(-x)$. Repetindo o passo anterior para obter um novo resto parcial.

$$\begin{array}{rrrrr|l} 8x^4 & -2x^3 & & +4x & -9 & 2x^2 + 1 \\ \cline{6-6} -8x^4 & & -4x^2 & & & 4x^2 - x \\ \cline{1-3} & -2x^3 & -4x^2 & +4x & & \\ & 2x^3 & & +x & & \\ \cline{2-4} & & -4x^2 & +5x & -9 & \end{array}$$

A divisão finaliza quando o grau do resto é menor do que o grau do divisor, ou quando o resto é igual a zero.

$$\begin{array}{rrrr|l}
8x^4 - 2x^3 & & +4x & -9 & 2x^2+1 \\ \cline{5-5}
-8x^4 & -4x^2 & & & 4x^2 - x - 2 \\ \cline{1-2}
-2x^3 & -4x^2 & +4x & & \\
2x^3 & & +x & & \\ \cline{1-3}
 & -4x^2 & +5x & -9 & \\
 & 4x^2 & & +2 & \\ \cline{2-4}
 & & 5x & -7 &
\end{array}$$

Logo concluí-se que o quociente é $Q(x) = 4x^2 - x - 2$ *e o resto é* $R(x) = 5x - 7$*.*

1.2.3 Método de Descartes

Também chamado de método dos coeficientes a determinar, esse método consiste em obter os coeficientes dos polinômios quociente e divisor a partir da relação: $f(x) = q(x).g(x) + r(x)$, onde f é um polinômio não nulo, baseando-se nos seguintes fatos:

I) q é zero ou $gr(q) = gr(f) - gr(g)$, pois pela definição, verifica-se que: $gq + r = f$,como r é zero ou $gr(r) < gr(g) \leq gr(gq)$ segue que $gr(q) + gr(g) = gr(f)$;

II) $gr(r) < gr(g)$ (ou $r = 0$).

O método é aplicado da seguinte forma:

i) Calculam-se $gr(q)$ e $gr(r)$;

ii) Constroem-se os polinômios q e r deixando incógnitos seus coeficientes;

iii) Determinam-se os coeficientes, impondo a igualdade $gq + r = f$

Exercício 1.2.2. *Obter o quociente e o resto da divisão de* $f = 2x^4 - x^3 + 6x - 1$ *por* $g = 2x^3 - x^2 + 5x - 2$*, pelo método de Descartes.*

Solução:

Primeiramente obtém-se o provável grau do quociente: $gr(q) = 4 - 3 = 1$ *o que leva a* $q = ax + b$ *com* $gr(r) < 3$*, portanto na pior das hipóteses tem-se que:* $gr(r) = 2$*, então escreve-se* r *na forma:* $r = cx^2 + dx + e$ *com* $gq + r = f$*, obtendo a equação:* $(ax+b)(2x^3-x^2+5x-2)+(cx^2+dx+e) = 2x^4-x^3+6x-1$*. Desenvolvendo a equação, segue para todo* x*:* $2ax^4+(2b-a)x^3+(5a-b+c)x^2+(-2a+5b+d)x+(-2b+e) = 2x^4-x^3+6x-1$*, o que resulta em:*

$$\begin{cases} 2a = 2 \\ 2b - a = -1 \\ 5a - b + c = 0 \\ -2a + 5b + d = 6 \\ -2b + e = -1 \end{cases}$$

Portanto, ao resolver o sistema, obtém-se: $a = 1, b = 0, c = -5, d = 8, e = -1$*, logo o quociente é :* $q = x$ *e o resto é:* $r = -5x^2 + 8x - 1$*.*

No conteúdo de divisão polinomial, existe um tópico muito importante, pois trata especificamente da divisão de um polinômio p por um binômio do 1^o grau. Esse tipo de divisão deu origem à vários métodos de divisões especificas que se tornaram ferramentas bastante úteis ao cálculo com polinômios, além disso alguns teoremas importantes na álgebra (Teorema do Resto e Teorema de D'Alembert, por exemplos) foram desenvolvidos a partir desse tema, e serão vistos na próxima seção.

1.2.4 Divisão por Binômio do 1° grau

Neste tópico serão abordadas as divisões em que o dividendo é um polinômio f de grau maior ou igual a 1 e o divisor é um polinômio g de grau 1, observa-se que nesse tipo de divisão, o resto r é sempre uma constante, pois $gr(g) = 1$, portanto: $gr(r) = 0$ ou $r = 0$. Verifica-se que, numericamente. Neste caso, o valor de r é independente do número a que fora substituído no lugar de x, isto é, $r(a) = r, \forall a \in \mathbb{R}$.

Veja a seguir, um exemplo de divisão pelo método convencional da chave, desenvolvendo também, no mesmo exercício, o cálculo do valor numérico específico de um polinômio $p(x)$.

Exercício 1.2.3. *Divida o polinômio $P(x) = 3x^3 + 2x + 1$ pelo binômio $x - 5$, em seguida calcule $P(5)$.*

Solução:

Primeiramente escreve-se ordenadamente o dividendo P e o divisor $x - 5$ segundo as potências decrescentes de x, completando-os se necessário, com termos de coeficiente zero.

$$\begin{array}{rrr|l} 3x^3 & +2x & +1 & x-5 \\ \cline{4-4} & & & \end{array}$$

Dividindo o termo de maior grau de P pelo termo de maior grau de $x-5$, obtém-se o primeiro termo do quociente que é $3x^2$.

$$\begin{array}{rrr|l} 3x^3 & +2x & +1 & x-5 \\ \cline{4-4} & & & 3x^2 \end{array}$$

Multiplicando o termo encontrado pelo divisor e subtraindo do dividendo,obtém-se o resto parcial $15x^2 + 2x$.

$$\begin{array}{rrr|l} 3x^3 & +2x & +1 & x-5 \\ \cline{4-4} -3x^3+15x^2 & & & 3x^2 \\ \cline{1-1} 15x^2 & +2x & & \end{array}$$

Dividindo o termo de maior grau do resto parcial $(15x^2)$ pelo termo de maior grau do divisor x, obtém-se assim o próximo termo do quociente $(15x)$. Repetindo o passo anterior para obter um novo resto parcial.

$$\begin{array}{rrr|l} 3x^3 & +2x & +1 & x-5 \\ \cline{4-4} -3x^3+15x^2 & & & 3x^2+15x \\ \cline{1-1} 15x^2 & +2x & & \\ -15x^2 & +75x & & \\ \cline{1-2} & 77x & +1 & \end{array}$$

A divisão finaliza quando o grau do resto é menor do que o grau do divisor, ou quando o resto é igual a zero.

$$
\begin{array}{rrrr|l}
3x^3 & & +2x & +1 & x-5 \\ \cline{5-5}
-3x^3 & +15x^2 & & & 3x^2+15x+77 \\ \cline{1-2}
& 15x^2 & +2x & & \\
& -15x^2 & +75x & & \\ \cline{2-3}
& & 77x & +1 & \\
& & -77x & +385 & \\ \cline{3-4}
& & & 386 &
\end{array}
$$

Logo concluí-se que o quociente é $3x^2 + 15x + 77$ *e o resto é* 386*.*

Cálculo de $P(5)$*:*

$$
\begin{aligned}
P(5) &= 3 \cdot (5)^3 + 2 \cdot (5) + 1 \\
P(5) &= 375 + 10 + 1 \\
P(5) &= 386
\end{aligned}
$$

Verifica-se portanto que o valor de $P(5)$ é igual ao resto da divisão de $P(x)$ pelo binômio $(x - 5)$. Isso remete ao próximo teorema a ser abordado, que é bastante útil nas divisões de um polinômio por um binômio do tipo $(x - a)$.

Teorema 1.2.2 (Teorema do Resto)**.** *O resto da divisão de um polinômio* p *por* $x - a$ *é numericamente igual ao valor de* p *em* a*. Ou seja: dado um polinômio* p *com grau maior ou igual a* 1*, o resto da divisão de* p *por* $x - a$ *é igual ao valor numérico* $p(a)$

Demonstração. De acordo com a definição de divisão

$$q \cdot (x - a) + r = p \tag{1.3}$$

onde q e r são, respectivamente, o quociente e o resto da divisão de p por $x - a$. Como $x - a$ tem grau 1, o resto r ou é nulo ou tem grau zero, logo r é um polinômio constante. Fazendo o cálculo dos valores dos polinômios, tem-se na igualdade (1.5) em a:

$$q(a) \cdot (a - a) + r(a) = p(a) \Longrightarrow r = p(a)$$

$\square$

Observem dois exemplos da utilização do Teorema do Resto:

Exemplo 1.2.4. *Obter o resto da divisão de* $f = 3x^3 - 2x^2 + 4x - 6$ *por* $g = x - 2$ *sem efetuar a divisão*

Basta utilizar o teorema do resto. Como o número que anula o divisor g *é* $x = 2$*, substituindo esse valor em* f *tem-se:*

$$
\begin{aligned}
f(2) &= 3 \cdot (2)^3 - 2 \cdot (2)^2 + 4 \cdot 2 - 6 \\
f(2) &= 24 - 8 + 8 - 6 \\
f(2) &= 18
\end{aligned}
$$

Exemplo 1.2.5. *Se o resto da divisão de* $(m+2)x^3+3mx-4$ *por* $x+3$ *é* 14*, então determine o valor de* m

Anulando o divisor g*, tem-se* $x=-3$*, e sabendo que, pelo teorema do resto,* $r=p(a)$ *então substituindo* a *em* x *e igualando ao resto dado, obtém-se:*

$$\begin{aligned}
14 &= (m+2)\cdot(-3)^3+3m\cdot(-3)-4\\
14 &= (m+2)\cdot(-27)-9m-4\\
14 &= -27m-54-9m-4\\
36m &= -58-14\\
36m &= -72\\
m &= -2
\end{aligned}$$

Um teorema bastante importante é o Teorema de D'Alembert, que leva o nome do matemático, filósofo e físico francês: Jean le Rond D'Alembert $(1717-1783)$. O Teorema de dAlembert é uma consequência imediata do Teorema do Resto, ambos os teoremas são voltados para a divisão de polinômio por um binômio do tipo (xa).

Teorema 1.2.3 (Teorema de d'Alembert)**.** *Um polinômio* $P(x)$ *é divisível por* $(x-a)$ *se, e somente se,* a *é raiz de* $P(x)$*, istoé* $P(a)=0$.

Demonstração. De fato, $P(x)$ é divisível por $x-a$, se e somente se o resto r dessa divisão é igual a zero, e pelo teorema do resto, tem-se que $r=P(a)$ é o resto da divisão de $P(x)$ por $(x-a)$. Logo $P(x)$ é divisível por $(x-a)\Leftrightarrow r=0$, ou seja, $P(a)=0\Leftrightarrow a$ é raiz de $P(x)$, finalizando a demonstração. □

Observe, nos dois exercícios seguintes, como é simples e prático a utilização desse teorema:

Exercício 1.2.4. *Sem efetuar as divisões, verifique se* $P=x^4-4x^3+4x^2-4x+3$ *é divisível por* $g=x-3$.

Solução:

$$\begin{aligned}
P(3) &= 3^4-4\cdot(3)^3+4\cdot(3)^2-4\cdot3+3\\
P(3) &= 81-108+36-12+3\\
P(3) &= 0
\end{aligned}$$

Então conclui-se que P *é divisível por* g.

Exercício 1.2.5. *Determine o valor de* a*, de modo que* $f=x^3+3ax^2-(2+a)x+8$*, seja divisível por* $x-4$.

Solução:

Utilizando o teorema de D'Alembert, queremos que $f(4)=0$*, desse modo, devemos ter:*

$$\begin{aligned}
f(4) &= 4^3+3a\cdot(4)^2-(2+a)\cdot(4)+8\\
f(4) &= 64+48a-8-4a\\
0 &= 44a+56\\
-44a &= 56
\end{aligned}$$

portanto $a = -\frac{56}{44} = -\frac{14}{11}$.

Existe ainda um outro método bastante simples e que facilita a divisão de um polinômio $P(x)$ por um binômio na forma $x-a$, trata-se do dispositivo, que será apresentado a seguir.

1.2.5 Dispositivo prático de Briot-Ruffini

O dispositivo prático de Briot-Ruffini é uma ótima ferramenta para realizar a divisão de um polinômio qualquer por binômios do tipo $x-a$. O algoritmo que representa o dispositivo foi desenvolvido por dois matemáticos: Paulo Ruffini (Itália/1765 – 1822) e Charles Auguste Briot (França, 1817 – 1882).

Esse método utiliza apenas coeficientes do dividendo $P(x)$, onde $P(x) = a_nx^n + a_{n-1}x^{n-1} + a_{n-2}x^{n-2} + ... + a_1x + a_0$, e o valor de a que é a raiz do divisor $(x-a)$. Observe como devem ser arranjados os coeficientes nesse dispositivo:

$$\begin{array}{c|cccccc|c} a & a_n & a_{n-1} & a_{n-2} & \dots & a_2 & a_1 & a_0 \\ \hline & q_{n-1} & q_{n-2} & q_{n-3} & \dots & q_1 & q_0 & R \end{array}$$

Na primeira linha e coluna do dispositivo encontra-se o zero do divisor, representado por a, nas demais colunas da mesma linha encontram-se os coeficientes do dividendo $P(x)$ e são representados por: $a_n, a_{n-1}, a_{n-2}, \dots, a_2, a_1$ e a_0. Já na segunda linha, a partir da segunda coluna até a penúltima, se encontram os coeficientes do quociente, obtidos através da resolução do dispositivo e que são representados por: $q_{n-1}, q_{n-2}, q_{n-3}, \dots, q_1, q_0$. Finalmente na última coluna da segunda linha, se encontra o resto da divisão, representado por R. A resolução do dispositivo de Briot-Ruffini se processa da seguinte forma:

Sendo Q o quociente da divisão de $P(x)$ por $(x-a)$, então:

$$Q = q_{n-1}x^{n-1} + q_{n-2}x^{n-2} + q_{n-3}x^{n-3} + ... + q_1 + q_0$$

Em seguida, aplicando o método dos coeficientes a determinar, tem-se:

$$\begin{aligned} Q \cdot (x-a) &= (q_{n-1}x^{n-1} + q_{n-2}x^{n-2} + q_{n-3}x^{n-3} + ... + q_0) \cdot (x-a) \\ &= q_{n-1}x^n + q_{n-2}x^{n-1} + q_{n-3}x^{n-2} + \ldots + q_0x - aq_{n-1}nx^{n-1} - \ldots - aq_1x - aq_0 \\ &= q_{n-1}x^n + (q_{n-2} - aq_{n-1})x^{n-1} + (q_{n-3} - aq_{n-2})x^{n-2} + ... + (q_0 - aq_1)x - aq_0 \end{aligned}$$

Assim, escrevendo $f = Q.(x-a) + r$, verificam-se as igualdades:

$$\begin{array}{rcl} q_{n-1} & = & a_n \\ q_{n-2} - aq_{n-1} = a_{n-1} & \text{logo} & q_{n-2} = aq_{n-1} + a_{n-1} \\ q_{n-3} - aq_{n-2} = a_{n-2} & \text{logo} & q_{n-3} = aq_{n-2} + a_{n-2} \\ & \vdots & \\ q_1 - aq_2 = a_2 & \text{logo} & q_1 = aq_2 + a_2 \\ q_0 - aq_1 = a_1 & \text{logo} & q_0 = aq_1 + a_1 \\ R - aq_0 = a_0 & \text{logo} & R = aq_0 + a_0. \end{array}$$

Observe agora um exercício que mostra o passo a passo da utilização desse dispositivo.

Exercício 1.2.6. *Determine o quociente e o resto da divisão de* $P(x) = 2x^3 + x^2 - 4x + 1$ *por* $x - 2$ *utilizando o dispositivo de Briot-Ruffini.*

Solução:

Primeiramente, para montar o dispositivo, dispõem-se os valores que participam do cálculo, escrevendo os coeficientes do dividendo $P(x)$ *na linha de cima e o valor de* a *na linha de baixo.*

$$\begin{array}{c|cccc} & 2 & 1 & -4 & 1 \\ 2 & & & & \\ \hline & & & & \end{array}$$

Em seguida é feita a multiplicação do valor de a *por esse coeficiente, somando o produto obtido com o próximo coeficiente de* $P(x)$ *e colocando o resultado abaixo dele.*

$$\begin{array}{c|cccc} & 2 & 1 & -4 & 1 \\ 2 & & 4+ & & \\ \hline & 2 & 5 & & \end{array}$$

Multiplicando o valor de a *por esse coeficiente, somando o produto obtido com o próximo coeficiente de* $P(x)$ *e colocando esse novo resultado abaixo desse coeficiente, obtém-se:*

$$\begin{array}{c|cccc} & 2 & 1 & -4 & 1 \\ 2 & & 4+ & 10+ & \\ \hline & 2 & 5 & 6 & \end{array}$$

Repete-se o processo até o último coeficiente de $P(x)$*, que está separado à direita.*

$$\begin{array}{c|cccc} & 2 & 1 & -4 & 1 \\ 2 & & 4+ & 10+ & 12 \\ \hline & 2 & 5 & 6 & \end{array}$$

O último resultado é o resto da divisão e os demais números obtidos são os coeficientes do quociente, dispostos ordenadamente segundo as potências decrescentes de x.

$$\begin{array}{c|cccc} & 2 & 1 & -4 & 1 \\ 2 & & 4+ & 10+ & 12+ \\ \hline & 2 & 5 & 6 & \boxed{13} \end{array}$$

Com esse procedimento, conclui-se que, o quociente é $Q(x) = 2x^2 + 5x + 6$ *e o resto* $R(x) = 13$.

O teorema seguinte é bastante útil na divisão de um polinômio por um binômio, podendo utilizar, de forma estendida, o dispositivo de Briot-Ruffini.

Teorema 1.2.4. *Se um polinômio* f *é divisível por* $x - a$ *e divisível por* $x - b$*, com* $a \neq b$ *então* f *é divisível pelo produto* $(x - a) \cdot (x - b)$.

Demonstração. Sejam q o quociente e $r = cx+d$, o resto da divisão de f por $(x-a)\cdot(x-b)$, então:

$$f = q(x-a)\cdot(x-b) + (cx+d) \tag{1.4}$$

Fazendo os cálculos numéricos desses polinômios em a e sabendo que f é divisível por $x-a$, então $f(a) = 0$. Da mesma forma, tem-se que f é divisível por $x-b$, então $f(b) = 0$, logo, substituindo $f(a)$ e $f(b)$ na equacão (1.6), tem-se:

$$q(a)\cdot\underbrace{(a-a)}_{0}\cdot(a-b) + (ca+d) = \underbrace{f(a)}_{0} \tag{1.5}$$

$$q(b)\cdot(b-a)\cdot\underbrace{(b-b)}_{0}+(cb+d) = \underbrace{f(b)}_{0} \tag{1.6}$$

Com as equações (1.7) e (1.8) faz-se o sistema:

$$\begin{cases} ca+d=0 \\ cb+d=0 \end{cases}$$

Donde vem $c = 0$ e $d = 0$, gerando $r = 0$. □

Seguem dois exercícios de aplicação desse teorema.

Exercício 1.2.7. *Determine a e b reais de modo que o polinômio $P(x) = x^3+2x^2+(2a-b)x+(a-b)$ seja divisível por $d(x) = x^2-x$.*

Solução:

Fatorando o polinômio $d(x)$ tem-se $d(x) =x\left(x-1\right)$, se $P(x)$ é divisível por $d(x)$, então em particular $p(x)$ tem que ser divisível por $x-1$ e por x, utilizando o teorema do resto, tem-se que obter $P(1) = 0$ e $P(0) = 0$, sendo assim:

$$\begin{aligned} P(0) &= 0^3+2\cdot(0)^2+(2a-b)\cdot 0+(a-b) \\ P(0) &= 0+a-b \\ 0 &= a-b \\ a &= b. \\ P(1) &= 1^3+2\cdot(1)^2+(2a-b)\cdot 1+(a-b) \\ P(1) &= 1+2+3a-2b \\ 0 &= 3+3a-2a \\ a &= -3. \end{aligned}$$

Portanto, como $a = b$, então $b = -3$.

Exercício 1.2.8. *Verifique se $P(x) = x^3-3x^2-6x+8$ é divisível por $(x+2)(x-4)$. Caso seja, obtenha o quociente e o resto de $P(x)$ por esse produto.*

Solução:

Pode-se escrever $P(x)$ como: $P(x) = q(x)\cdot(x+2)(x-4)+R(x)$ em que $R(x) = cx+d$, para algum $c, d \in \mathbb{R}$. Sem efetuar a divisão, primeiramente verificando se $P(x)$ é divisível por $x+2$, tem-se que: $P(-2) = (-2)^3-3\cdot(-2)^2-6\cdot(-2)+8 = 0$. Verificando *agora se $P(x)$ é divisível por $x-4$, tem-se que:$P(4) = (4)^3 - 3\cdot(4)^2 - 6\cdot 4 + 8 = 0$. A segunda parte do exercício, consiste em obter o quociente e o resto da divisão de $P(x)$ pelo produto $(x+2)(x-4)$, efetuando sucessivamente as divisões por $(x+2)$ e por $(x-4)$ pelo dispositivo de Briot-Ruffini.*

Dividindo $P(x)$ por $(x+2)$ tem-se:

$$\begin{array}{c|cccc}
 & 1 & -3 & -6 & 8 \\
-2 & & -2 & 10 & -8 \\
\hline
 & 1 & -5 & 4 & \boxed{0}
\end{array}$$

portanto x^2-5x+4 é o quociente que representa a divisão de $P(x)$ pelo binômio $(x+2)$. O próximo passo é dividir o quocienente x^2-5x+4 por $(x-4)$, utilizando o dispositivo de Briot-Ruffini.

$$\begin{array}{c|ccc}
 & 1 & -5 & 4 \\
4 & & 4 & -4 \\
\hline
 & 1 & -1 & \boxed{0}
\end{array}$$

obtendo assim o quociente $Q(x) = x-1$ e o resto $R(x) = 0$. Portanto, verifica-se que:

$$x^3 - 3x^2 - 6x + 8 = \overbrace{(x-1)}^{quociente} \cdot \overbrace{(x-2)(x+4)}^{divisor}.$$

Na próxima seção discutiremos a resolução de equações algébricas. Vários matemáticos deram suas contribuições para esse importante tópico da álgebra, tais como: Al-Khowarizmi $(780-850)$ que fez os primeiros registros relacionando as equações de primeiro e segundo graus; Os italianos: Girolamo Cardano $(1501-1576)$, Niccolo Tartaglia $(1499-1557)$ e Ludovico Ferrari $(1522-1565)$ que iniciaram estudos sobre equações de terceiro e quarto graus. Também se destacaram por grandes demonstrações que são de extrema importância para a álgebra, até hoje, os seguintes matemáticos: Niels Henrik Abel (Noruega/$1802-1829$), Carl Friedrich Gauss (Alemanha/$1777-1855$) e o francês Evarist Galois $(1811-1832)$.

1.3 Equações Polinomiais

Definição 1.3.1. *Equação polinomial ou algébrica é toda equação na forma:*

$$a_n x^n + a_{n-1}x^{n-1} + a_{n-2}x^{n-2} \ldots + a_2x^2 + a_1x + a_0 = 0$$

sendo x a incógnita e $a_n, a_{n-1}, a_{n-2}, \ldots, a_2, a_1, a_0$, os coeficientes reais. Para a qual se busca valores numéricos para x que satisfaçam a equação. Observa-se também que essa equação com $a_n \neq 0$, é um polinômio $P(x)$ de grau n, ou seja: a equação algébrica tem grau n.

Exemplo 1.3.1. *a) A equação $x^5 + 2x^3 - 3x^2 + x - 1 = 0$ é de grau 5.*

b) $kx^3 + 5x + 7$ é de grau 3 se $k \neq 0$ e de grau 1 se $k = 0$.

1.3.1 Raiz de uma Equação Polinomial

A raiz de uma equação algébrica $P(x) = 0$ de grau n é todo número complexo α que é raiz de $P(x)$, ou seja:

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

Resolver uma equação algébrica consiste em determinar os valores de x em um dado conjunto universo, que a tornam verdadeira. O exercício seguinte ajuda a entender, de forma prática, o conceito de raiz.

Exercício 1.3.1. *Verifique se os números: -2 e 4 são raízes da equação $f(x) = x^3 - 2x^2 - 9x + 4 = 0$.*

Solução:

Para $x = -2$, tem-se: $(-2)^3 - 2 \cdot (-2)^2 - 9 \cdot (-2) + 4 = -16 + 22 = 6$, logo o número -2 não é raiz de f.

Para $x = 4$, tem-se: $4^3 - 2 \cdot (4)^2 - 9 \cdot 4 + 4 = 68 - 68 = 0$, logo o número 4 é raiz de f.

O conjunto solução de uma equação algébrica, é o conjunto de todas as raízes dessa equação que pertencem ao conjunto universo considerado. Aprender a encontrar essas raízes nas resolucões dos mais diversos tipos de equações, é o objetivo principal no estudo das equações algébricas.

Importante também salientar que, na transformação de uma equação polinomial para a forma $P(x) = 0$ podem ocorrer dois casos notáveis:

- $1°$ caso: $P(x)$ é identicamente nulo, isto é:

  $$0.x^n + 0.x^{n-1} + 0.x^{n-2} + \ldots + 0.x + 0 = 0$$

  Essa sentença é verdadeira para todo número complexo x, assim, chamando de S o conjunto solução da equação, tem-se que $S = \mathbb{C}$;

- $2°$ caso: $P(x)$ é constante e não nula, isto é:

  $$0.x^n + 0.x^{n-1} + 0.x^{n-2} + \ldots + 0.x + k = 0$$

  Essa sentença é falsa para todo número x, logo o conjunto solução é $S = \emptyset$ (conjunto vazio).

Seguindo com o conceito de raiz, é necessário também, ter o conhecimento sobre número de raízes de uma equação e o que isso pode representar na solução das equações algébricas.

1.3.2 Raízes Complexas em polinômios de coeficientes reais

Ao resolver uma equação polinomial $p(x) = 0$, pode-se verificar a existência de várias raízes, inclusive raízes complexas na forma: $z = \alpha + \beta i$ com $\beta \neq 0$. O aparecimento dessas raízes, quando os coeficientes são reais, sempre ocorrem aos pares, em razão de seus conjugados. Os teoremas seguintes demonstrarão as relações entre a raiz $z = \alpha + \beta i$ com o seu conjugado $\overline{z} = \alpha - \beta i$, ambos com $\beta \neq 0$.

Teorema 1.3.1. *Se uma equação polinomial de coeficientes reais admite como raiz o número complexo $z = \alpha + \beta i$ com $\beta \neq 0$, então também admite como raiz o número $\overline{z} = \alpha - \beta i$, chamado de conjugado de z.*

Demonstração. Seja a equação $P(x) = a_n x^n + a_{n-1}x^{n-1} + a_{n-2}x^{n-2} + \ldots + a_1 x + a_0 = 0$ de coeficientes reais, admitindo a raiz z, ou seja $P(z) = 0$. Prova-se que $\overline{z}$ também é raiz, isto é $P(\overline{z}) = 0$:

$$\begin{aligned}
P(\overline{z}) &= a_n(\overline{z})^n + a_{n-1}(\overline{z})^{n-1} + a_{n-2}(\overline{z})^{n-2} + \ldots + a_1\overline{z} + a_0 = \\
&= a_n(\overline{z^n}) + a_{n-1}(\overline{z^{n-1}}) + a_{n-2}(\overline{z^{n-2}}) + \ldots + a_1\overline{z} + a_0 = \\
&= \overline{a_n}(\overline{z^n}) + \overline{a_{n-1}}(\overline{z^{n-1}}) + \overline{a_{n-2}}(\overline{z^{n-2}}) + \ldots + \overline{a_1}\ \overline{z} + \overline{a_0} = \\
&= \overline{a_n z^n} + \overline{a_{n-1}z^{n-1}} + \overline{a_{n-2}z^{n-2}} + \ldots + \overline{a_1 z} + \overline{a_0} = \\
&= \overline{a_n z^n + a_{n-1}z^{n-1} + a_{n-2}z^{n-2} + \ldots + a_1 z + a_0} = \overline{P(z)} \\
&= \overline{0} = 0
\end{aligned}$$

□

Lembrando que, se $gr(p) = n$ então tem-se duas situações: $i)$ Se $n = 2k + 1$, p tem k fatores de grau 2 e um fator de grau 1. $ii)$ Se $n = 2k$ então p tem k fatores de grau 2. Também pode-se relacionar o teorema acima quando ocorrer a multiplicidade das raízes numa equação polinomial de coeficientes reais. O corolário seguinte demonstra essa relação.

Corolário 1.3.1. *Se uma equação polinomial de coeficientes reais, admite a raiz $z = \alpha + \beta i$, com $\beta \neq 0$ e multiplicidade p, então também admite a raiz $\overline{z} = \alpha - \beta i$ com multiplicidade p.*

Demonstração. Supondo que $P(x) = 0$ com coeficientes reais admita a raiz $z = \alpha + \beta i$ com $\beta \neq 0$, de multiplicidade p e a raiz $\overline{z} = \alpha - \beta i$ de multiplicidade $(p' \neq p)$, prova-se que esse fato leva a uma contradição. Seja m o menor dos números p e p'. Como o polinômio P é divisível por $(x - z)^p$ e $(x - \overline{z})^{p'}$, P é divisível por $(x - z)^m$ e $(x - \overline{z})^m$, como $z \neq \overline{z}$, conclui-se que P é divisível por $(x - z)^m \cdot (x - \overline{z})^m$, logo:

$$\begin{aligned}
P &= [(x - z)^m \cdot (x - \overline{z})^m] \cdot Q \\
&= [(x - z)(x - \overline{z})]^m \cdot Q \\
&= [x^2 - (z + \overline{z})x + z\overline{z}]^m \cdot Q \\
&= [x^2 - 2\alpha x + (\alpha^2 + \beta^2)]^m \cdot Q
\end{aligned}$$

Como P e $[x^2 - 2\alpha x + (\alpha^2 + \beta^2)]^m$ possuem coeficientes reais, segue-se que Q possui coeficientes reais, com possibilidades de existir dois casos:

1 caso: $m = p < p'$

Portanto Q não é divisível por $x - z$ e é divisível por $x - \overline{z}$, isto é, $Q(z) \neq 0$ e $Q(\overline{z}) = 0$. O que é um absurdo, pois contraria o teorema anterior;

$2caso : m = p' < p$

Portanto Q não é divisível por $x - \overline{z}$ e é divisível por $x - z$, isto é, $Q(\overline{z}) \neq 0$ e $Q(z) = 0$. O que também é um absurdo, pois contraria o teorema anterior.

Para evitar essa contradição, tem-se necessariamente que $p = p'$. □

Vale lembrar que:

1 - Os dois teoremas anteriores só se aplicam às equações polinomiais de coeficientes reais, observando, por exemplo a equação: $x^2 - ix = 0$, tem como raízes: $x = 0$ e $x = i$, mas não tem $-i$ como raiz, que é o conjugado de i;

2 - Para uma equação polinomial de coeficientes reais, tem-se que toda raiz complexa $z = \alpha + \beta i$ admite uma raiz complexa conjugada $\overline{z} = \alpha - \beta i$, então o número de raízes complexas não reais de $P(x) = 0$ é necessariamente par;

3 - Se uma equação polinomial de coeficientes reais, tem grau ímpar, então ela admite um número ímpar de raízes reais. Por exemplo: se a, b, c e d são coeficientes reais então toda equação $ax^3 + bx^2 + cx + d = 0$ possui uma ou três raízes reais, pois o número de raízes complexas e não reais é par.

Serão vistos agora dois exercícios que exemplificam bem a utilização dos dois teoremas acima.

Exercício 1.3.2. *Determine o menor grau que pode ter uma equação polinomial de coeficientes reais, para admitir as raízes:* $1, i$ *e* $3 + i$*, esta última com multiplicidade dupla.*

Solução:

Como cada raiz complexa tem que vir acompanhado de uma raiz complexa conjugada, então tem-se que $-i$ *é raiz com multiplicidade simples e* $3 - i$ *é raiz com multiplicidade dupla, logo tal equação terá no mínimo sete raízes:* $1, i, -i, 3+i, 3+i, 3-i, 3-i$*, portanto terá no mínimo grau* 7

Exercício 1.3.3. *Verifique se* $1 + \sqrt{2}i$ *é raiz do polinômio* $f = x^4 - x^3 + 2x^2 + x + 3$.

Solução:

Se $1 + \sqrt{2}i$ *for raiz de um polinômio* g *de coeficientes reais, então o seu conjugado* $1 - \sqrt{2}i$ *também é raiz do polinômio* g*. Utilizando a forma fatorada, tem-se:*

$$\begin{aligned}
[x - (1 + \sqrt{2}i)] \cdot [x - (1 - \sqrt{2}i)] &= [(x - 1) - \sqrt{2}i] \cdot [(x - 1) + \sqrt{2}i)] \\
&= (x - 1)^2 - (\sqrt{2}i)^2 \\
&= (x - 1)^2 - 2(i)^2 \\
&= (x - 1)^2 + 2 \\
&= x^2 - 2x + 3
\end{aligned}$$

portanto $1 - \sqrt{2}i$ *e* $1 + \sqrt{2}i$ *são as raízes de* $g = x^2 - 2x + 3$*, deve-se agora verificar se* g *divide* f*. Fazendo a divisão pelo método da chave:*

$$\begin{array}{rrrrr|l}
x^4 & -x^3 & +2x^2 & +x & +3 & x^2 - 2x + 3 \\
\cline{6-6}
-x^4 & +2x^3 & -3x^2 & & & x^2 + x + 1 \\
\cline{1-3}
 & x^3 & -x^2 & +x & & \\
 & -x^3 & +2x^2 & -3x & & \\
\cline{2-4}
 & & x^2 & -2x & +3 & \\
 & & -x^2 & +2x & -3 & \\
\cline{3-5}
 & & & & 0 &
\end{array}$$

verifica-se que o polinômio $g = x^2 - 2x + 3$ divide f, concluindo assim, que $1 + \sqrt{2}i$ é uma das raízes de f, pois é raiz de g.

Exercício 1.3.4. *Resolva a equação $x^4 - 2x^3 + 6x^2 + 22x + 13 = 0$ sabendo que uma das raízes é $2 + 3i$.*

Solução:

Como a equação tem todos os coeficientes reais, resulta que uma outra raiz é $2 - 3i$, logo o polinômio dado é divisível por $(x - 2 - 3i)(x - 2 + 3i)$, portanto é divisível por $x^2 - 4x + 13$. Utilizando a divisão euclidiana entre os dois polinômios: $x^4 - 2x^3 + 6x^2 + 22x + 13$ e $x^2 - 4x + 13$, encontra-se o outro termo do polinômio fatorado:

$$
\begin{array}{rrrrr|l}
x^4 & -2x^3 & +6x^2 & +22x & +13 & x^2 - 4x + 13 \\
\cline{6-6}
-x^4 & +4x^3 & -13x^2 & & & x^2 + 2x + 1 \\
\cline{1-3}
 & 2x^3 & -7x^2 & +22x & & \\
 & -2x^3 & +8x^2 & -26x & & \\
\cline{2-4}
 & & x^2 & -4x & +13 & \\
 & & -x^2 & +4x & -13 & \\
\cline{3-5}
 & & & & 0 &
\end{array}
$$

Conclui-se que a equação dada se escreve na forma: $(x^2 - 4x + 13)(x^2 + 2x + 1) = 0$. As raízes de $x^2 + 2x + 1 = 0$ são as que faltam. Como:

$$x^2 + 2x + 1 = 0 \Longleftrightarrow (x + 1)^2 = 0$$

Tem-se a raiz $x = -1$, com multiplicidade dupla. Assim sendo, o conjunto solução da equação é formado pelos números: $2 + 3i, 2 - 3i$ e -1.

Na próxima seção será abordado um dos conteúdos que raramente é visto na educação Básica, trata-se do *M.D.C.* entre dois polinômios com uma variável.

1.3.3 Número de Raízes

Sabe-se que toda equação polinomial pode ser escrita na forma $P(x) : a_n x^n + a_{n-1}x^{n-1} + a_{n-2}x^{n-2} + \ldots + a_1 x + a_0 = 0$. chamando de r, a raiz dessa equação, então tem-se que $P(r) = 0$. Com relação ao estudo das raízes de uma equação Polinomial, alguns teoremas são importantes, um deles é o Teorema Fundamental da Álgebra (T.F.A.), esse teorema foi publicado no ano de 1799 (em Helmstädt) por Johann Carl Friedrich Gauss (Alemanha/$1777 - 1855$) em sua tese de doutorado. Embora seja um dos maiores teoremas da álgebra, a demonstração apresentada em sua tese baseia-se em parte nos conceitos de Análise (como a noção de continuidade). Posteriormente, Gauss dedicou-se na busca de uma prova inteiramente algébrica (tal empenho gerou mais três versões de provas publicadas). Atualmente existem mais de 100 provas a respeito do teorema que é importante para o entendimento das relações entre raízes e a forma fatorada de um polinômio.

Teorema 1.3.2 (Teorema Fundamental da Álgebra (T.F.A.))**.** *Todo Polinômio de grau $n > 1$ e coeficientes reais (ou complexos) admite ao menos uma raiz complexa. Como a demonstração desse teorema foge do escopo desse trabalho, então considera-se como válido esse teorema, sem necessidade de demonstração.*

O próximo teorema é uma consequência imediata do Teorema Fundamental da Álgebra.

Teorema 1.3.3 (Teorema da Decomposição)**.** *Seja $P(x)$ um polinômio de coeficientes reais e de grau n, com $n \geq 1$, dado por:*

$$P(x) = a_n x^n + a_{n-1} x^{n-1} + \ldots + a_1 x + a_0 \ (a_n \neq 0)$$

Então, $P(x)$ pode ser decomposto em n fatores do 1° grau sob a forma:

$$P(x) = a_n \cdot (x - r_1) \cdot (x - r_2) \cdot \ldots \cdot (x - r_n)$$

em que $r_1, r_2, \ldots, r_n$ são as raízes de $P(x)$ e a_n é o coeficiente dominante de $P(x)$. Desconsiderando a ordem dos fatores, tal decomposição é única.

Demonstração. 1^a Parte: Existência:

a) Considere P um polinômio de grau $n \geq 1$, pelo *T.F.A.*, P tem ao menos uma raiz complexa r_1. Desse modo $P(r_1) = 0$, portanto, de acordo com o Teorema de d'Alembert, $P(x)$ é divisível por $x - r_1$:

$$(i)\ P(x) = (x - r_1).Q_1(x)$$

Chamando Q_1 um polinômio de grau $n - 1$, com coeficiente dominante a_n (pois o divisor $x - r_1$ tem coeficiente dominante unitário), tem-se que:

- a) Se $n = 1$, então $Q_1(x)$ é um polinômio de grau $1 - 1 = 0$, ou seja, $Q_1(x)$ é um polinômio constante, dado por $Q_1(x) = a_n$, e substituindo em (i) vem que $P(x) = a_n(x - r_1)$, e o teorema fica demonstrado;

- b) Caso $n \geq 2$, então $n - 1 \geq 1$ e o T.F.A. se aplica ao polinômio $Q_1(x)$, ou seja: $Q_1(x)$ tem pelo menos uma raiz complexa r_2, portanto: $Q_1(r_2) = 0$ e $Q_1(x)$ é divisível por $x - r_2$:

  $$(ii)\ Q_1(x) = (x - r_2) \cdot Q_2(x)$$

  Substituindo (i) em (ii), verifica-se que:

  $$(iii)\ P(x) = (x - r_1) \cdot (x - r_2) \cdot Q_2(x)$$

  onde $Q_2(x)$ é um polinômio de grau $n - 2$ e coeficiente dominante a_n.

  Caso $n = 2$, $Q_2(x)$ é um polinômio de grau 0 dado por $Q_2(x) = a_n$, segue que: $P_2(x) = a_n(x - r_1)(x - r_2)$, e o teorema fica demonstrado;

- c) Daí por diante, após sucessivas aplicações do T.F.A, chega-se na igualdade:

  $$P(x) = (x - r_1)(x - r_2)(x - r_3) \ldots (x - r_n).Q_n(x) \tag{1.7}$$

  em que $Q_n(x)$ é um polinômio de grau $n - n = 0$, com coeficiente dominante a_n, logo: $Q_n(x) = a_n$ e:

  $$P(x) = a_n(x - r_1)(x - r_2)(x - r_3) \ldots (x - r_n)$$

  P fatora em $n = 2k + 1$ fatores, onde, tem-se: k fatores de grau 2 e um fator de grau 1 ou P fatora em k fatores de grau 2

2^a Parte: Unicidade:

Supondo que P admita duas decomposições:

$$\begin{array}{rcl} P(x) & = & a_n(x-r_1)(x-r_2)(x-r_3)\ldots(x-r_n) \\ P(x) & = & a'_m(x-r'_1)(x-r'_2)(x-r'_3)\ldots(x-r'_m) \end{array}$$

Expandindo e ordenando os dois segundos membros, tem-se:

$$a_nx^n - a_nS_1.x^{n-1} + \ldots = a'_mx^m - a'_mS'_1.x^{m-1} + \ldots$$

Da igualdade de polinômios, verifica-se necessariamente: $n = m$ e $a_n = a'_m$ obtendo a igualdade:

$$(x-r_1)(x-r_2)(x-r_3)\ldots(x-r_n) = (x-r'_1)(x-r'_2)(x-r'_3)\ldots(x-r'_m)(I)$$

Impondo $x = r_1$, tem-se:

$$0 = (r_1 - r'_1)(r_1 - r'_2)(r_1 - r'_3)\ldots(r_1 - r'_n)$$

E se o produto é nulo, então um dos fatores $r_1 - r'_j$ também é nulo. Convenientemente fazendo uma mudança na ordem dos fatores pode-se escrever: $r_1 = r'_1$. A igualdade (I) se transforma em:

$$(x-r_1)(x-r_2)(x-r_3)\ldots(x-r_n) = (x-r_1)(x-r'_2)(x-r'_3)\ldots(x-r'_m)$$

e em seguida em:

$$(x-r_2)(x-r_3)\ldots(x-r_n) = (x-r'_2)(x-r'_3)\ldots(x-r'_m)$$

Impondo $x = r_2$, verifica-se que:

$$0 = (r_2 - r'_2)(r_2 - r'_3)\ldots(r_2 - r'_n)$$

De modo análogo, verifica-se que um dos fatores $r_2 - r'_k$ é nulo, convenientemente fazendo uma mudança na ordem dos fatores, pode-se escrever, $r_2 = r'_2$.

Assim sucessivamente, concluí-se que $r_i = r'_i$, $\forall i \in \{1, 2, 3 \ldots, n\}$. Com isso as igualdades ficam assim constituídas: $m = n, a'_m = a_n, r'_1 = r_1, r'_2 = r_2, r'_3 = r_3, \ldots, r'_n = r_n$ são a prova da unicidade da decomposição.

□

Corolário 1.3.2. *Toda equação polinomial de grau n com $(n \geq 1)$ e coeficientes reais ou complexos admite exatamente n raízes complexas.*

Demonstração. Sendo $P(x) = a_nx^n + a_{n-1}x^{n-1} + a_{n-2}x^{n-2} + \ldots + a_1x + a_0 = 0$ pela demonstração da existência da decomposição, verifica-se que P admite as raízes $r_1, r_2, r_3, \ldots, r_n$ que podem ser distintas ou não, além disso foi provado na unicidade da decomposição, que apenas essas são as raízes de P. □

Algumas observações sobre o Teorema da Decomposição:

- 1^a) Todo polinômio de grau $n(n \geq 1)$ pode ser visto como o desenvolvimento de um produto de n fatores de 1° grau com um fator constante a_n chamado de coeficiente dominante em P[5]

$$P(x) = a_n(x-r_1)(x-r_2)(x-r_3)\ldots(x-r_n)$$

- 2^a) Pode ocorrer que a decomposição de P apresente fatores iguais, desse modo, obtém-se:

$$P(x) = a_n(x-r_1)^{m_1}(x-r_2)^{m_2}(x-r_3)^{m_3}\ldots(x-r_p)^{m_p}$$

Onde

$$\begin{cases} m_1 + m_2 + m_3 + \ldots + m_p = n \\ r_1, r_2, r_3, \ldots, r_p \ \text{ são dois a dois distintos} \end{cases}$$

Neste caso P é divisível separadamente por cada polinômio:

$$(x-r_1)^{m_1}, (x-r_2)^{m_2}, (x-r_3)^{m_3}, \ldots, (x-r_p)^{m_p}.$$

Os exercícios abaixo, apresentam aplicações da utilização do T.FA. e do Teorema da Decomposição

Exercício 1.3.5. - *Fatore o polinômio* $P(x) = 4x^5 - 4x^4 - 64x + 64$ *sabendo que suas raízes são* $1, -2, 2, -2i, 2i$.

Solução:

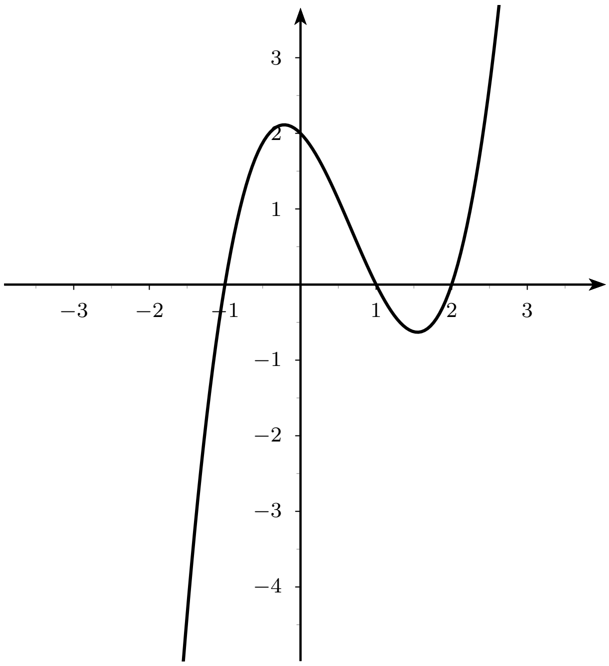
Como o coeficiente dominante é $a_5 = 4$, *pelo teorema da decomposição, tem-se que* $P(x) = a_5(x-r_1)(x-r_2)(x-r_3)(x-r_4)(x-r_5)$, *logo:* $4(x+2i)(x-2i)(x-1)(x-2)(x+2) = P(x)$ *que também pode ser escrito como:* $P(x){=}\left(4x^2+16\right)\left(x-1\right)\left(x-2\right)\left(x+2\right)$.

Exercício 1.3.6. *Determine o conjunto Solução da equação* $5(x-2)^4(x+2)^2(x-5) = 0$. *Qual o grau dessa equação?*

Solução:

Igualando cada termo fatorado à zero, obtém-se as raízes de P *que são:* $2, 2, 2, 2, -2, -2, 5$, *assim verifica-se que a equação dada é do* 7° *grau e o conjunto solução é* $S = \{-2, 2, 5\}$

Exercício 1.3.7. *Obter o polinômio de menor grau possível, tal que* $P(3) = 8$ *e cujo gráfico é representado a seguir:*



Solução:

Como $P(-1) = P(1) = P(2) = 0$, *verifica-se que* $-1, 1$ *e* 2 *são as raízes de* $P(x)$. *Admitindo que cada raiz é unica e supondo que* $P(x)$ *tem o menor grau para se obter essas raízes, então, resta agora encontrar o valor do coeficiente dominante* a_n, *como* $P(3) = 8$, *pelo teorema da decomposição tem-se que* $P(x) = a_3(x-r_1)(x-r_2)(x-r_3)$,*logo* $8 = a_3(3+1)(3-1)(3-2)$, *tem-se então* $a_3 = 1$ *como coeficiente dominante e* r_1, r_2,r_3 *são as raízes de* $P(x)$, *logo:* $P(x) = (x+1)(x-1)(x-2) = x^3 - 2x^2 - x + 2$

No penúltimo exercício, nota-se que as raízes repetidas de uma equação algébrica, interfere diretamente na fatoração da equação algébrica, portanto merece atenção, por sua relevância, o estudo do tema seguinte.

1.3.4 Multiplicidade de uma raiz

Definição 1.3.2. *O número complexo* r *é raiz de multiplicidade* m, *com* ($m \in \mathbb{N}, m \geq 1$) *da equação* $P(x) = 0$ *se* $P(x)$ *é da forma:*

$$P(x) = (x-r)^m \cdot Q(x) \text{ com } Q(r) \neq 0$$

Ou seja: r *é raiz de multiplicidade* m *de* $P(x)$, *se* $(x-r)^m$ *divide o polinômio* P *mas*$(x-r)^{m+1}$ *não divide* P. *Portanto, na decomposição de* P *existem extamente* m *fatores iguais a* $x - r$. *No caso de* $m = 1$, *dizemos que* r *é raiz simples; se* $m = 2$ *dizemos que* r *é raiz dupla; se* $m = 3$, *dizemos que* r *é raiz tripla, etc.*

Os dois exemplos seguintes verificam a utilização do conceito de multiplicidade das raízes.

Exemplo 1.3.2. *A equação* $x^3(x-2)^2(x+1)^2 = 0$ *admite as raízes:* 0 *com multiplicidade* 3, 2 *com multiplicidade* 2 *e a raiz* -1 *com multiplicidade* 2, *logo embora seja uma equação do* 7° *grau, a solução dessa equação só possui três elementos:* $S = \{0, 2, -1\}$.

Exemplo 1.3.3. *O Conjunto Solução da equação polinomial* $P(x) = 0$ *de coeficiente dominante* k *que possui as raízes* $1, 0$ *e* -2*, com multiplicidade* 3*,* 4 *e* 2 *respectivamente, é determinado na forma:*

$$0 = k(x-1)^3x^4(x+2)^2 \text{ com } k \in \mathbb{C} \text{ e } k \neq 0,$$

Portanto, a equação possui grau 9.

O entendimento das relações existentes entre os coeficientes de uma equação polinomial e as raízes dessa equação, em muitos casos, ajudam a encontrar a solução da equação. E uma das relações mais importantes e mais utilizadas na álgebra são as relações de Girard, que é o tema da próxima seção.

1.3.5 Relações entre Coeficientes e Raízes

As relações de Girard foram propostas por Albert Girard(França $1595 - 1632$) que estudou as relações existentes entre os coeficientes e suas raízes. Para efeito de demonstração, serão deduzidas a seguir as relações existentes entre os coeficientes e as raízes de uma equação polinomial de grau n, com $n \geq 1$.

Dada a equação:

$$P(x) = a_nx^n + a_{n-1}x^{n-1} + a_{n-2}x^{n-2} + \ldots + a_1x + a_0 \ (a_n \neq 0)$$

com raízes $r_1, r_2, r_3, \ldots, r_n$, tem-se então:

$$\begin{aligned}
P(x) &= a_n(x-r_1)(x-r_2)(x-r_3), \ldots (x-r_n)\\
&= a_n[x(x-r_2)(x-r_3)\ldots(x-r_n) - r_1(x-r_2)(x-r_3)\ldots(x-r_n)]\\
&= a_nx^n - a_n\underbrace{(r_1+r_2+r_3+\ldots+r_n)}_{S_1}x^{n-1}+\\
&+ a_n\underbrace{(r_1r_2+r_1r_3+\ldots+r_{n-1}r_n)}_{S_2}x^{n-2}-\\
&- a_n\underbrace{(r_1r_2r_3+r_1r_2r_4+\ldots+r_{n-2}r_{n-1}r_n)}_{S_3}x^{n-3}+\ldots+\\
&+ (-1)^ha_nS_hx^{n-h}+\ldots+(-1)^na_n\underbrace{(r_1r_2r_3\ldots r_n)}_{S_n}, \forall x
\end{aligned}$$

Em que S_n é a soma de todos os produtos de h elementos $r_{i_1}, r_{i_2}, \ldots, r_{i_n} \in \{r_1, r_2, r_3, \ldots\}$ com $i_1 < i_2 < \ldots < i_n$. Portanto, aplicando a condição de identidade:

$$\begin{aligned}
S_1 &= r_1+r_2+r_3+\ldots+r_n = -\frac{a_{n-1}}{a_n}\\
S_2 &= r_1r_2+r_1r_3+r_1r_4+\ldots+r_{n-1}r_n = \frac{a_{n-2}}{a_n}\\
S_3 &= r_1r_2r_3+r_1r_2r_4+\ldots+r_{n-2}r_{n-1}r_n = -\frac{a_{n-3}}{a_n}\\
&\vdots\\
S_n &= r_1r_2r_3\ldots r_n = (-1)^n\ \frac{a_0}{a_n}
\end{aligned}$$

Se pensarmos $r_1, r_2, \ldots, r_n$ como variáveis, denominamos S_i de i-ésimo polinômio de Girard em n variáveis.

A resolução dos dois exercícios seguintes, ajudam a compreender melhor à importância da utilização das relacões de Girard no contexto das equações algébricas.

Exercício 1.3.8. *Calcule a soma e o produto das raízes da equação* $3x^4 + 4x^3 - 2x^2 + 5x - 2 = 0$

Solução:

$$r_1 + r_2 + r_3 + r_4 = -\frac{a_3}{a_4} = -\frac{4}{3}$$
$$r_1 \cdot r_2 \cdot r_3 \cdot r_4 = (-1)^4\, \frac{a_0}{a_4} = -\frac{2}{3}$$

Exercício 1.3.9. *Resolva a equação* $x^3 - 13x^2 + 50x - 56 = 0$, *através das Relações de Girard, sabendo que uma das raízes é o dobro da outra [4]:*

Solução:

Para essa equação, tem-se os coeficientes: $a_3 = 1, a_2 = -13, a_1 = 50$ *e* $a_0 = -56$, *considerando* r_1, r_2 *e* r_3 *as raízes e* S_1, S_2, S_3 *as somas, verifica-se que:*

$$S_1 = r_1 + r_2 + r_3 = (-1)^1 \frac{a_2}{a_3} = 13$$
$$S_2 = r_1 \cdot r_2 + r_1 \cdot r_3 + r_2 \cdot r_3 = (-1)^2 \frac{a_1}{a_3} = 50$$
$$S_3 = r_1 \cdot r_2 \cdot r_3 = (-1)^3 \frac{a_0}{a_3} = 56$$

Tendo então as equações:

$$r_1 + r_2 + r_3 = 13 \tag{1.8}$$
$$r_1 \cdot r_2 + r_1 \cdot r_3 + r_2 \cdot r_3 = 50 \tag{1.9}$$
$$r_1 \cdot r_2 \cdot r_3 = 56 \tag{1.10}$$

Como $r_2 = 2r_1$ *e substituindo na equação*(1.8)*:*

$$r_1 + 2r_1 + r_3 = 13$$
$$3r_1 + r_3 = 13$$
$$r_3 = 13 - 3r_1$$

Fazendo a substituição em (1.9)*:*

$$r_1 \cdot 2r_1 + r_1 \cdot r_3 + 2r_1 \cdot r_3 = 50$$
$$2r_1^2 + 3r_1 \cdot r_3 = 50$$

Sabe-se que $r_3 = 13 - 3r_1$, *logo:*

$$2r_1^2 + 3r_1 \cdot (13 - 3r_1) = 50$$
$$2r_1^2 + 39r_1 - 9r_1^2 = 50$$
$$-7r_1^2 + 39r_1 - 50 = 0$$

Resolvendo essa última equação do segundo grau, obtém-se as raízes: $r_1' = 2$ *e* $r_1'' = \dfrac{25}{7}$*, mas ao substituir* $r_1'' = \dfrac{25}{7}$ *na equação* $x^3 - 13x^2 + 50x - 56 = 0$*, verifica-se que* $\dfrac{25}{7}$ *não é raiz, pois,* $\left(\dfrac{25}{7}\right)^3 - 13 \cdot \left(\dfrac{25}{7}\right)^2 + 50 \cdot \left(\dfrac{25}{7}\right) - 56 = \dfrac{792}{343} \neq 0$*, ao passo que, substituindo* $r_1' = 2$*, tem-se então* $2^3 - 13 \cdot 2^2 + 50 \cdot 2 - 56 = 0$*, logo 2 é raiz da equação e como* $r_2 = 2r_1$*, então* $r_2 = 2 \cdot 2 = 4$*, resta encontrar o valor de* r_3*. Como:* $r_3 = 13 - 3r_1$*, então* $r_3 = 13 - 3 \cdot 2 = 13 - 6 = 7$*, logo as raízes da equação são:* $2, 4$ *e* 7*.*

1.3.6 Máximo Divisor Comum

Definição 1.3.3. *Dados dois polinômios de coeficiente reais não nulos f e g, afirma-se que o polinômio h é um máximo divisor comum de f e g se, e somente se, forem satisfeitas às seguintes condições:*

I) h é mônico,ou seja, possui coeficiente do termo dominante igual a 1

II) h é divisor de f e de g;

III) Se qualquer outro polinômio h_1 é divisor comum de f e de g, então h_1 também é divisor de h.

Será utilizada a notação $h = mdc(f, g)$, para representar o máximo divisor comum dos dois polinômios f e g. Os exemplos seguintes, dão uma ideia de como obter esse máximo divisor comum, apenas testando as três condições citadas

Exemplo 1.3.4. *a) Se* $f = (x-1)(x-4)$ *e* $g = (x+1)(x-1)^2(x-4)^4$ *então* $h = (x-1)(x-4)$ *satisfaz às condições:* I, II *e* III*, logo* $h = mdc(f, g)$

Exemplo 1.3.5. *b) Se* $f = 2x^4 - 2$ *e* $g = x^4 - 3x^3 + 3x^2 - 3x + 2$ *então* $mdc(f, g) = x^3 - x^2 + x - 1$ *pois fatorando os polinômios f e g, obtém-se:*

$$f = 2(x^2+1)(x+1)(x-1) \text{ e } g = \left(x^2+1\right)\left(x-1\right)\left(x-2\right)$$

Como: $h = (x^2+1)(x-1) = x^3 - x^2 + x - 1$*, então* $h = mdc(f, g)$*.*

Nos próximos tópicos, serão abordadas as possibilidades de se obter o máximo divisor comum entre dois polinômios, sem precisar testar as três condições citadas.

Lema 1.3.1. *Se f e g são polinômios não nulos, com $f = hg + r$ e r é o resto da divisão de f por g, então, $mdc(f, g) = mdc(g, r)$*

Demonstração. Seja $h = mdc(f, g)$, então, por definição, tem-se que h é divisor de f e g, logo:

$$f = q_1 \cdot h \;\text{ e }\; g = q_2 \cdot h \tag{1.11}$$

sendo q_1 quociente da divisão de f por h e q_2 quociente da divisão de g por h. Como r é o resto da divisão de f por g então:

$$r = f - q \cdot g. \tag{1.12}$$

Substituindo 1.11 em 1.12 obtém-se:

$$r = q_1 \cdot h - q \cdot q_2 \cdot h = (q_1 - q \cdot q_2) \cdot h$$

isto é, h é divisor de r. Por outro lado, seja $h_1 = mdc(g, r)$. Como h é divisor de g e de r, então h é divisor de h_1. Será provado agora que $h = h_1$, para isso é preciso mostrar que h_1 também é divisor de h. Por definição tem-se que h_1 é divisor de g e de r, portanto:

$$g = q_3 \cdot h_1 \quad \text{e} \quad r = q_4 \cdot h_1 \tag{1.13}$$

sendo q_3 quociente da divisão de g por h_1 e q_4 quociente da divisão de r por h_1. Substituindo 1.12 na equação 1.13 e isolando o f, tem-se:

$$f = gq + r = q \cdot q_3 \cdot h_1 + q_4 h_1 = (q \cdot q_3 + q_4)h_1$$

isto é, h_1 é divisor de f, como já era divisor de g, então h_1 é divisor de h, concluindo que h é divisor de h_1 e h_1 é divisor de h, portanto existe $\alpha \in \mathbb{R}$, tal que $h = \alpha h_1$, como h e h_1 são mônicos, temos $\alpha = 1$ e consequentemente $h = h_1$ logo $mdc(f, g) = mdc(g, r)$. □

A principal aplicação deste teorema é o método das divisões sucessivas, para o cálculo do *mdc*. Esse método permite obter o $mdc(f, g)$

1.3.7 Método das Divisões Sucessivas para cálculo do *mdc*

Proposição 1.3.1. *Dados dois polinômios não nulos f e g com $gr(f) \geq gr(g)$,considere a sequência de polinômios $h_0, h_1, h_2, \dots$ dados por $h_0 = f, h_1 = g$ e para $i \geq 2, h_i$ é o resto da divisão de h_{i-2} por h_{i-1}. Nestas condições tem-se que, existe $k \in \mathbb{N}$, tal que:*

(1) $h_{k+1} = 0$ e $h_k \neq 0$

(2) $mdc(f, g) = mdc(h_k, 0)$

Demonstração. Temos

$$\begin{aligned} f &= q_1 g + h_2 \\ g &= q_2 h_2 + h_3 \\ &\vdots \\ h_i &= q_{i-1} h_{i-1} + h_{i+2} \end{aligned}$$

com $gr(h_i) < gr(h_{i-1})$ ou $h_i = 0$.

Percebe-se em cada etapa que o grau diminui ao menos em 1 unidade. Logo eventualmente após um número finito de passos obtemos um resto zero, digamos $h_{k+1} = 0$ e $h_k \neq 0$. Além disso, pelo lema 1.3.1 temos: $mdc(f, g) = mdc(h_0, h_1) = mdc(h_1, h_2) = \ldots = mdc(h_i, h_{i+1}) = \ldots = mdc(h_k, 0)$. □

Os próximos exercícios demonstram essa aplicação das divisões sucessivas para a obtenção do máximo divisor comum entre dois polinômios.

Exercício 1.3.10. *Obtenha um mdc dos polinômios $f = x^4 + 4x^3 + 3x^2 - 4x - 4$ e $g = x^3 - 2x^2 - 5x + 6$.*

Solução:

Dividindo f por g obtém-se:

$$\begin{array}{r|l}
x^4+4x^3\;+3x^2\;-4x\;-4 & x^3-2x^2-5x+6 \\ \cline{2-2}
-x^4+2x^3\;+5x^2\;-6x\qquad & x+6 \\ \cline{1-1}
6x^3\;+8x^2-10x\;-4 & \\
-6x^3+12x^2+30x-36 & \\ \cline{1-1}
20x^2+20x-40 &
\end{array}$$

Fazendo agora a divisão de g por $r_1 = 20x^2 + 20x - 40$ obtém-se:

$$\begin{array}{r|l}
x^3-2x^2-5x+6 & 20x^2+20x-40 \\ \cline{2-2}
-x^3\;-x^2+2x\quad & \frac{1}{20}x-\frac{3}{20} \\ \cline{1-1}
-3x^2-3x+6 & \\
3x^2+3x-6 & \\ \cline{1-1}
0 &
\end{array}$$

Verifica-se que $q_2 = \dfrac{1}{20}x - \dfrac{3}{20}$ *e* $r_2 = 0$*, portanto:* $mdc(f,g) = \dfrac{1}{20} \cdot r_1 = x^2 + x - 2$

Observação 1.3.1. *Se $mdc(f,g) = 1$, então os polinômios f e g são ditos relativamente primos.*

Exemplo 1.3.6. *Na divisão entre os polinômios: $f = x^4 - x^3 - 4x^2 + 21x - 50$ e $g = x^2 + 2x - 1$, tem-se que $mdc(f,g) = 1$ pois dividindo f por g:*

$$\begin{array}{r|l}
2x^4\;-x^3\;-4x^2+21x-50 & x^2+2x-1 \\ \cline{2-2}
-2x^4-4x^3\;+2x^2\qquad\qquad & 2x^2-5x+8 \\ \cline{1-1}
-5x^3\;-2x^2+21x\quad & \\
5x^3+10x^2\;-5x\quad & \\ \cline{1-1}
8x^2+16x-50 & \\
-8x^2-16x\;+8 & \\ \cline{1-1}
-42 &
\end{array}$$

fazendo agora a divisão de $g = x^2 + 2x - 1$ por $r_1 = -42$ obtém-se

$$\begin{array}{r|l}
x^2+2x-1 & -42 \\ \cline{2-2}
-x^2\qquad\quad & -\frac{1}{42}x^2-\frac{1}{21}x+\frac{1}{42} \\ \cline{1-1}
2x\quad & \\
-2x\quad & \\ \cline{1-1}
-1 & \\
1 & \\ \cline{1-1}
0 &
\end{array}$$

Logo $mdc(f,g) = mdc(-42, 0) = -\dfrac{1}{42} \cdot (-42) = 1$

1.3.8 Teorema de Bézout

Este Teorema é muito importante para ampliar o conceito de máximo divisor comum e ajuda a compreender melhor as propriedades envolvendo *mdc*. A seguir temos $K = \mathbb{Q}, \mathbb{R}$ ou $\mathbb{C}$

Teorema 1.3.4 (Teorema de Bezout)**.** *Dados dois polinômios $f(x)$ e $g(x) \in K[x]$ existem polinômios $A(x)$ e $B(x) \in K[x]$, tais que:*

$$f(x)A(x) + g(x)B(x) = mdc(f(x), g(x))$$

Demonstração. Considerando o conjunto $L = \{f(x)A(x)+g(x)B(x)|A(x), B(x) \in K[x]\}$, seja d, mônico de menor grau em L, portanto $d = f(x)A(x)+g(x)B(x)$, para convenientes valores de $A(x)$ e $B(x) \in K[x]$ deve-se provar que d é o máximo divisor comum de $f(x)$ e $g(x)$

- (i) Considerando a divisão euclidiana de f por d. o que é possivel pois $d \neq 0$ temos $f = qd + r$ onde $r = 0$ ou $gr(r) < gr(d)$, mas como $d = f(x)A(x) + g(x)B(x)$, então

  $$f(x) = [(f(x)A(x) + g(x)B(x)]q + r$$

  Daí tem-se que

  $$r = f(x)[1 - qA(x)] + g(x)[-qB(x)]$$

  o que mostra que r é um elemento de L, e como grau de d é o menor possível entre os graus dos elementos de L, r não pode ter grau, logo $r = 0$, portanto, $f(x) = dq$. Ou seja $d|f(x)$.

  De maneira análoga se demonstra que $d|g(x)$;

- (ii) se $d'|f(x)$ e $d'|g(x)$ então $d'|d$ uma vez que $d = f(x)A(x) + g(x)B(x)$.

□

Alguns teoremas demonstram propriedades envolvendo o *mdc* entre polinômios. Serão abordados a seguir,alguns deles

Teorema 1.3.5. *α é uma raiz comum aos polinômios f e g,se e somente se, α é uma raiz do $mdc(f, g)$*

Demonstração. Aplicando o Teorema de Bézout, pondo $h = mdc(f, g)$, temos que existem polinômios A, B tais que

$$h = Af + Bg$$

Calculando h em α temos

$$h(\alpha) = A(\alpha) \cdot f(\alpha) + B(\alpha) \cdot g(\alpha)$$

Se α é raiz de f e g então $f(\alpha) = 0$ e $g(\alpha) = 0$, logo $h(\alpha) = 0$, portanto $x = \alpha$ é raiz de $h = mdc(f, g)$ Reciprocamente como $h|g$ e $h|f$, se $h(\alpha) = 0$ então $f(\alpha) = g(\alpha) = 0$. □

Exercício 1.3.11. *Obter as raízes comuns aos polinômios $f = x^3 - 6x^2 + 5x + 12 = 0$ e $g = x^3 - 5x^2 - 2x + 24 = 0$.*

Solução

Fazendo as divisões sucessivas até obter um resto nulo:

$$
\begin{array}{r|l}
x^3 - 6x^2 + 5x + 12 & x^3 - 5x^2 - 2x + 24 \\ \cline{2-2}
-x^3 + 5x^2 + 2x - 24 & 1 \\ \cline{1-1}
-x^2 + 7x - 12 &
\end{array}
$$

$$
\begin{array}{r|l}
x^3 - 5x^2 \quad - 2x + 24 & -x^2 + 7x - 12 \\ \cline{2-2}
-x^3 + 7x^2 - 12x \quad\quad & -x - 2 \\ \cline{1-1}
2x^2 - 14x + 24 & \\
-2x^2 + 14x - 24 & \\ \cline{1-1}
0 &
\end{array}
$$

Logo $mdc(f,g) = -x^2 + 7x - 12 = (x-3)(x-4)$ *e igualando cada termo fatorado à zero, obtém-se que* $x = 3$ *e* $x = 4$ *são as raízes comuns de* f *e* g*.*

Teorema 1.3.6. *Se* f *e* g *são polinômios divisíveis por* $(x-\alpha)^m$*, então o* $mdc(f,g)$ *também é divisível por* $(x-\alpha)^m$*.*

Demonstração. Pondo $h = mdc(f,g)$, aplicando o Teorema de Bézout, onde

$$h = Af + Bg$$

Sendo os polinômios A e $B \in K[x]$, tem-se que: $f = (x-\alpha)^m \cdot q_1$ e $g = (x-\alpha)^m \cdot q_2$, logo $h = A \cdot q_1 \cdot (x-\alpha)^m + B \cdot q_2 \cdot (x-\alpha)^m = [A \cdot q_1 + B \cdot q_2] \cdot (x-\alpha)^m$ portanto $(x-\alpha)^m | h$ □

Corolário 1.3.3. *Se* α *é raiz de* f *e de* g *com multiplicidade* m_1 *e* m_2*, respectivamente então* α *é raiz do* $mdc(f,g)$ *com multiplicidade igual ao mínimo entre* m_1 *e* m_2*.*

Demonstração. Seja $r = min\{m_1, m_2\}$. Temos $(x-\alpha)^r | mdc(f.g)$ mas $(x-\alpha)^{r+1} \nmid f$ ou $(x-\alpha)^{r+1} \nmid g$. Logo $(x-\alpha)^{r+1} \nmid mdc(f,g)$. □

O principal resultado deste Corolário é que o $mdc(f,g)$ é o polinômio unitário que representa o produto dos fatores comuns a f e a g, tomado cada fator como o menor dos expoentes com que aparecem em f e g.

Corolário 1.3.4. *Se* $f = a_n(x-\alpha_1)_1^n \cdots (x-\alpha_r)_r^n$ *e* $g = b_m(x-\alpha_1)_1^m \cdots (x-\alpha_r)_r^m$ *em que* $s_i = min\{m_i, n_i\}$*.*

Demonstração. A demonstração é imediata do corolário anterior. □

Exemplo 1.3.7. *O mdc de* $f = 2(x-2)^3(x-1)^2(x+4)^5(x-5)^4$ *e* $g = 3(x-1)^3(x+4)^4(x-2)^2$ *é o polinômio* $(x-2)^2(x+4)^4(x-1)^2$ *observa-se que os fatores que não se apresentam simultaneamente nos dois polinômios* f *e* g*, não fazem parte do mdc.*

Os exercícios seguintes ajudam a entender melhor a importância deste Corolário para a obtenção das raízes comuns e não comuns à duas ou mais equações polinomiais.

Exercício 1.3.12. *Determine as raízes comuns e as não comuns às equações:* $f : x^4 + 4x^3 + 3x^2 - 4x - 4 = 0$ *e* $g : x^3 - 2x^2 - 5x + 6 = 0$*.*

Solução

Fazendo a divisão de f *em* g*, tem-se*

$$\begin{array}{rrrrr|l}
x^4 + 4x^3 & + 3x^2 & - 4x & - 4 & & x^3 - 2x^2 - 5x + 6 \\
\cline{6-6}
- x^4 + 2x^3 & + 5x^2 & - 6x & & & x + 6 \\
\cline{1-3}
6x^3 & + 8x^2 & - 10x & - 4 & & \\
- 6x^3 & + 12x^2 & + 30x & - 36 & & \\
\cline{1-4}
 & 20x^2 & + 20x & - 40 & &
\end{array}$$

Logo temos que $f-(x+6)\cdot g = 20x^2+20x-40$, *fatorando* g, *obtém-se* $(x-1)(x+2)(x-3)$, *deve-se encontrar o valor de* α *que determinamos como raiz comum de* g *e do polinômio* $20x^2+20x-40$, *substituindo as raízes de* g *no polinômio citado, logo, para* $x=1$ *tem-se* $20\cdot(1)^2+20\cdot 1-40=0$. *Logo* $x=1$ *é raiz comum de* f *e* g, *substituindo* $x=-2$ *tem-se* $20\cdot(-2)^2+20\cdot(-2)-40=0$, *logo* $x=-2$ *é raiz comum de* f *e* g, *substituindo* $x=3$, *tem-se* $20\cdot(3)^2+20\cdot 3-40\neq 0$, *logo* $x=3$ *não é raiz comum de* f *e* g. *Portanto conclui-se que* $x=1$ *e* $x=-2$, *são as raízes comuns de* f *e* g. *Como* $f: x^4+4x^3+3x^2-4x-4 = (x-1)(x+1)(x+2)^2$, *então as raízes não comuns de* f *e* g *são* $x=-1$ *e* $x=3$.

Exercício 1.3.13. *Determinar o valor de a de modo que às equações* $f: x^3-3x^2-4x+a=0$ *e* $g: x^2-3x+2=0$ *admitam uma raiz comum*

Solução:

Fazendo a divisão de f *em* g, *tem-se*

$$\begin{array}{r|l}
x^3 - 3x^2 - 4x + a & x^2 - 3x + 2 \\
\cline{2-2}
- x^3 + 3x^2 - 2x & x \\
\cline{1-1}
- 6x &
\end{array}$$

Logo temos que $f-x\cdot g = -6x+a$, *fatorando* g, *obtém-se* $(x-1)(x-2)$, *deve-se encontrar o valor de* α *que determinamos como raiz comum de* g *e do polinômio* $-6x+a$, *substituindo as raízes de* g *em* $-6x+a$, *tem-se que:* $-6\cdot(1)+a=0$ *ou* $-6\cdot(2)+a=0$. *isto é* $a=6$ *ou* $a=12$. *Portanto para que* f *e* g *tenham raízes comuns, então:* $a=6$ *ou* $a=12$.

CAPÍTULO 2

CONCEITOS E APLICAÇÕES COM POLINÔMIOS DE DUAS OU MAIS VARIÁVEIS

Neste capítulo, serão abordados alguns conceitos e aplicações vistos no capítulo anterior, generalizando para polinômios com mais de uma variável. Para isso é importante estabelecer uma ordem para as parcelas dos polinômios, pois somente a ideia de grau não é suficiente para reproduzir algumas noções e em particular a ideia de divisão com resto não nulo.

2.1 Ordem Monomial

Uma componente importante para qualquer extensão da divisão para um processo similar para polinômios em várias variáveis é a ordenação nos termos do polinômio em $K[x_1, ..., x_n]$. Vale salientar que se pode reconstruir um monômio $x^\alpha = x_1^{\alpha_1}, x_2^{\alpha_2}, \ldots, x_n^{\alpha_n}$, a partir de n-uplas de expoentes $\alpha = (\alpha_1, \ldots, \alpha_n) \in \mathbb{Z}^n_{\geq 0}$. Esta observação estabelece uma correspondência de um para um entre o conjunto dos monômios em $k[x_1, \ldots, x_n]$ e $\mathbb{Z}^n_{\geq 0}$. Além disso, qualquer ordem $>$ estabelecida no espaço $\mathbb{Z}^n_{\geq 0}$, pode ser naturalmente entendida como nos mônomios, por exemplo: Se $\alpha > \beta$ de acordo com essa ordem, diz-se, também, que $x^\alpha > x^\beta$.

Há muitas maneiras diferentes para definir ordenações em $\mathbb{Z}^n_{\geq 0}$. Para os propósitos desse trabalho convém salientar que a maioria dessas ordenações não serão utéis em virtude de que nem sempre esses ordenamentos preservam as propriedades algébricas que são desejáveis. Como por exemplo, a ordem dos termos não devem ser alteradas ao se multiplicar um polinômio por um monômio. Uma vez que um polinômio é uma soma de termos, a proposta é organizar os termos em um polinômio de forma inequívoca, por ordem descendente (ou ascendente) dos monômios correspondentes. Para fazer isso é preciso comparar cada par de monômios afim de estabelecer suas posições relativas adequadas. Assim, deve-se exigir que os agrupamentos sejam ordenações lineares ou totais. Isto significa que, para cada par de monômios x^α e x^β, exatamente uma das três afirmações seguintes deve ser verdadeira:

$$x^\alpha > x^\beta,\ x^\alpha = x^\beta \text{ ou } x^\alpha < x^\beta$$

Em seguida, deve-se levar em conta o efeito das operações de soma e produto em polinômios. Quando se soma polinômios, depois de combinar os termos semelhantes, pode-se simplesmente reorganizar os termos presentes, na ordem apropriada. Percebe-se que as somas não apresentam dificuldades, porém os produtos são mais sutis, pois ao multiplicar os termos monomiais pelos termos polinomiais, a ordem relativa dos termos poderia mudar, o motivo para esse problema é que o termo principal no produto poderia ser diferente a partir do produto do termo monomial com o termo líder do polinômio original.

Por isso, é necessária a imposição de que todos os ordenamentos monomiais tenham a seguinte propriedade adicional: Se $x^\alpha > x^\beta$ e x^γ é um termo monomial qualquer, então é necessário que $x^\alpha x^\gamma > x^\beta x^\gamma$. Em termos dos vetores expoentes, esta propriedade significa que, se $\alpha > \beta$ em $\mathbb{Z}^n_{\geq 0}$, então $\forall \gamma \in \mathbb{Z}^n_{\geq 0}$, $\alpha + \gamma > \beta + \gamma$. Com essas considerações em mente, pode-se apresentar a definição de Ordem Monomial e posteriormente detalhar duas dessas ordens.

Definição 2.1.1. *Uma ordem monomial em $K[x_1, x_2, \ldots, x_n]$ é uma relação $>$ em $\mathbb{Z}^n_{\geq 0}$ (ou de forma equivalente à toda relação sobre o conjunto de monômios x^α, com $\alpha \in \mathbb{Z}^n_{\geq 0}$) satisfazendo às seguintes condições:*

(i) $>$ é uma ordem total (ou linear) em $\mathbb{Z}^n_{\geq 0}$;

(ii) Se $\alpha > \beta$ e $\gamma \in \mathbb{Z}^n_{\geq 0}$ então $\alpha + \gamma > \beta + \gamma$;

(iii) $>$ é uma boa ordenação em $Z^n_{\geq 0}$. Isto significa que cada subconjunto não vazio de elementos em $Z^n_{\geq 0}$ elementos, admite um menor elemento.

O lema abaixo ajuda a entender melhor à condição de boa ordenação.

Lema 2.1.1. *Uma relação de ordem $>$ em $\mathbb{Z}^n_{\geq 0}$é uma boa ordenação se, e somente se, cada sequência estritamente decrescente em $\mathbb{Z}^n_{\geq 0}$.*

$$\alpha(1) > \alpha(2) > \alpha(3) > \cdots \text{ eventualmente termina .}$$

Demonstração. Prova-se na forma contrapositiva. Se $>$ não é uma boa ordenação, então algum subconjunto não vazio $S \subset \mathbb{Z}^n_{\geq 0}$ não tem menor elemento. Escolhendo $\alpha(1) \in S$, como $\alpha(1)$ não é o menor elemento, pode-se encontrar $\alpha(2)$ onde $\alpha(1) > \alpha(2)$ em S. Em seguida observa-se que $\alpha(2)$ também não é o menor elemento, pois pode-se encontrar um $\alpha(3)$ tal que $\alpha(2) > \alpha(3)$ prosseguindo da mesma forma, temos uma sequência infinita estritamente decrescente.

$$\alpha(1) > \alpha(2) > \alpha(3) \ldots$$

Reciprocamente, se uma sequência infinita$\{\alpha(1), \alpha(2), \alpha(3), \ldots\}$ é um subconjunto não vazio de $\mathbb{Z}^n_{\geq 0}$ que não possui menor elemento, então conclui-se que $>$ não é uma boa ordem. □

Esse Lema é de fundamental importância, sobretudo para mostrar que vários algoritmos terminam, observando que os resultados decrescem estritamente (em relação a uma ordem monomial fixa) a cada passo do algoritmo. A seguir será especificado e estudado com mais detalhes, a Ordem Lexicográfica e a Ordem Lexicográfica Graduada, duas das ordens monomiais.

Definição 2.1.2. *Ordem Lexicográfica*
Sejam $\alpha = (\alpha_1, \ldots, \alpha_n)$ e $\beta = (\beta_1 \ldots, \beta_n) \in \mathbb{Z}^n_{\geq 0}$ diz-que $\alpha >_{lex} \beta$ se na diferença do vetor $\alpha - \beta \in \mathbb{Z}^n$, o mais à esquerda é não nulo,logo a entrada é positiva. Escreve-se $x^\alpha >_{lex} x^\beta$ se $\alpha >_{lex} \beta$.

Alguns exemplos do uso da ordem lexicográfica:

a) $(1,2,0) >_{lex} (0,3,4)$ uma vez que $\alpha - \beta = (1,-1,-4)$;

b) $(4,3,3) >_{lex} (4,3,2)$ uma vez que $\alpha - \beta = (0,0,1)$;

Na prática, quando trabalhamos com polinômios em duas ou três variáveis, chamaremos as variáveis x, y, z em vez de x_1, x_2, x_3. Também devemos assumir que a ordem alfabética, ou seja: A ordem $x > y > z$ nas variáveis é usada para definir a ordem lexicográfica, a menos que seja determinado o contrário.

Para finalizar, deve-se verificar se a ordem lexicográfica satisfaz às três condições de definição de ordem monomial.

Proposição 2.1.1. *A ordem lexicográfica é uma ordem monomial*

Demonstração. (i) $>_{lex}$ é uma ordem total (ou linear), segue diretamente da definição e do fato da ordem numérica em $\mathbb{Z}^n_{\geq 0}$, ser uma ordem total;

(ii) Se $\alpha >_{lex} \beta$, então a coordenada não nula mais à esquerda em $\alpha - \beta$, digamos $\alpha_k - \beta_k$, é positiva. Porém $x^\alpha \cdot x^\gamma = x^{\alpha+\gamma}$ e $x^\beta \cdot x^\gamma = x^{\beta+\gamma}$ então tem-se $(\alpha+\gamma)-(\beta+\gamma) = \alpha - \beta$ a coordenada não nula mais à esquerda é mais uma vez $\alpha_k - \beta_k > 0$;

(iii) Supondo que $>_{lex}$ não seja uma boa ordem. Então pelo lema 2.1.1 deve haver uma sequência infinita estritamente decrescente $\alpha(1) >_{lex} \alpha(2) >_{lex} \alpha(3) \ldots$, de elementos $\mathbb{Z}^n_{\geq 0}$ que levará a uma contradição. Considerando a primeira coordenada de cada um dos vetores $\alpha(i) \in \mathbb{Z}^n_{\geq 0}$ pela definição de ordem lexicográfica, estas formam uma sequência de números inteiros não negativos e portanto devem estabilizar, isto é, existe um m tal que a primeira coordenada de vetores $\alpha(i)$ com $i \geq m$ são iguais. Começando em $\alpha(m)$ as segundas coordenadas são as que determinam a ordem lexicográfica graduada. As segundas coordenadas de $\alpha(m), \alpha(m+1), \ldots$, formam uma sequência não crescente. Pela mesma razão anterior, as segundas coordenadas, também devem se estabilizar. Continuando assim, verifica-se que para algum l,tem-se que $\alpha(l), \alpha(l+1), \ldots$, são todos iguais. Isto contradiz o fato de que $\alpha(l) > \alpha(l+1)$.

$\square$

Definição 2.1.3. *Ordem Lexicográfica Graduada*
Sejam $\alpha, \beta \in \mathbb{Z}^n_{\geq 0}$ diz-que $\alpha >_{grlex} \beta$ se:

i) $|\alpha| = \sum_{i=1}^{n} \alpha_i > \sum_{i=1}^{n} \beta_i = |\beta|$ *ou*

ii) $|\alpha| = |\beta|$ *e* $\alpha >_{lex} \beta$ *na sequência* $\alpha_1 - \beta_1, \alpha_2 - \beta_2, \ldots, \alpha_n - \beta_n$, *o primeiro elemento não nulo é positivo [8]*

A ordem lexicográfica graduada tem por característica ordenar inicialmente pelo grau total e, quando estes são iguais, pela ordem lexicográfica, ou seja: As variáveis: $x_1, x_2, \ldots, x_n$, são ordenadas da maneira usual pela ordenação de lex: $(1,0,\ldots,0) >_{lex} (0,1,0,\ldots,0) >_{lex} (0,\ldots,0,1)$. Então $x_1 >_{lex} x_2 > \ldots >_{lex} x_n$. Na prática, ao trabalhar com polinômios em duas ou três variáveis, chamaremos as variáveis de x, y, z ao invés de x_1, x_2, x_3. Assumindo também, que a ordem alfabética: $x > y > z$ nas variáveis é usada para definir a ordem lexicográfica.

Vale lembrar que, existem $n!$ ordens *grlex* sobre n variáveis, dependendo de como as variáveis são ordenadas. Alguns exemplos do uso da ordem lexicográfica graduada:

a) $(1,3,4) >_{grlex} (4,2,1)$ pois $|(1,3,4)| = 8 > |(4,2,1)| = 7$;

b) $(2,2,3) >_{grlex} (2,1,4) >$ pois $|(2,2,3)| = |(2,1,4)|$ e $|(2,2,3)| >_{lex} |(2,1,4)|$

Proposição 2.1.2. *A ordem lexicográfica graduada é uma ordem monomial*

Demonstração. (i) $>_{grlex}$ é uma ordem total (ou linear) pelo fato da ordem numérica em $\mathbb{Z}$, ser uma ordem total;

(ii) Se $\alpha >_{grlex} \beta$, então a coordenada não nula mais à esquerda em $|\alpha| > |\beta|$, digamos $|\alpha_k| - |\beta_k|$, é positiva. Porém $|x|^\alpha |x|^\gamma = |x|^{\alpha+\gamma}$ e $|x|^\beta |x|^\gamma = |x|^{\beta+\gamma}$ então em $(\alpha + \gamma) - (\beta + \gamma) = \alpha - \beta$ a coordenada não nula mais à esquerda é mais uma vez $|\alpha_k| - |\beta_k| > 0.$;

(iii) Supondo que $>_{grlex}$ não seja uma boa ordem. Então pelo lema 2.1.1 deve haver uma sequência infinita estritamente decrescente $|\alpha(1)| >_{grlex} |\alpha(2)| >_{grlex} |\alpha(3)| \ldots$, de elementos $\mathbb{Z}^n_{\geq 0}$ que levará a uma contradição. Considerando a primeira coordenada de cada um dos vetores $|\alpha(i)| \in \mathbb{Z}^n_{\geq 0}$ pela definição de ordem graduada lexicográfica, estas formam uma sequência de números inteiros não negativos e portanto devem estabilizar, isto é, existe um m tal que a primeira coordenada de vetores $\alpha(i)$ com $i \geq m$ são iguais. Começando em $\alpha(m)$ as segundas coordenadas são as que determinam a ordem lexicográfica graduada. As segundas coordenadas de $\alpha(m), \alpha(m+1), \ldots$, formam uma sequência não crescente. Pela mesma razão anterior, as segundas coordenadas, também devem se estabilizar. Continuando assim, verifica-se que para algum l,tem-se que $\alpha(l), \alpha(l+1), \ldots$, são todos iguais. Isto contradiz o fato de que $\alpha(l) > \alpha(l+1)$.

□

Essa seção será encerrada com um exemplo de aplicação do ordenamento lexicográfico graduado, em um polinômio de mais de uma variável.

Exercício 2.1.1. *Se $f = 3x^2yz + 4xy^2z - 6x^3 + 8x^2z^3 + 3z^2 \in K[x,y,z]$, ordene esse polinômio, utilizando a ordem monomial lexicográfica graduada*

Solução:

Como para a ordem lexicográfica graduada ordena-se inicialmente pelo grau total e, quando estes são iguais, ordena-se pela ordem lexicográfica, ou seja: primeiramente ao grau da variável x, em seguida de variável y e por fim com o grau da variável z. Sendo assim, o termo líder de f é $LT(f) = 8x^2z^3$, pois possui grau total igual a 5, em seguida vem o termo monomial: $3x^2yz$, com grau total igual a 4, esse termo possui o mesmo grau total do termo $4xy^2z$, porém o grau da variável x em $3x^2yz$ é maior $(2 > 1)$; O penúltimo termo é $-6x^3$ que possui grau 3 e por fim o último termo é $3z^2$ com grau 2. Portanto,tem-se o polinômio ordenado:

$$f = 8x^2z^3 + 3x^2yz + 4xy^2z - 6x^3 + 3z^2$$

2.2 Algoritmo da Pseudodivisão com Polinômios de Duas ou mais Variáveis

Nesta seção, será abordado o algoritmo da pseudodivisão, com polinômios em mais de uma variável, ou seja: em $k[x_1, \ldots, x_n]$. A ideia básica é a mesma de uma divisão com polinômios em uma variável. Ou seja, ao dividir f por $f_1, \ldots, f_s$ onde $f \in k[x_1, \ldots, x_n]$ e $f_1, \ldots, f_s \in k[x_1, \ldots, x_n]$, o objetivo é cancelar os termos de f utilizando os termos líderes de f_i de forma que os termos adicionados sejam sempre inferiores aos termos cancelados, continuando assim até que o processo não seja mais possível de ser realizado. Isso significa expressar f sob a forma $f = a_1 f_1 + \ldots + a_s f_s + r$, onde os "quocientes": $a_1, \ldots, a_s$, assim como o resto r, pertencem a $k[x_1, \ldots, x_n]$. Alguns procedimentos se fazem necessários, a fim de decidir como caracterizar o resto da divisão, daí a necessidade de utilizar um ordenamento monomial adequado.

O Teorema seguinte indica a forma geral do Algoritmo da divisão e pode também ser considerada como uma extensão do Teorema de D'Alembert, para o caso onde há mais de uma variável.

Teorema 2.2.1. (*Algoritmo da Pseudodivisão em* $k[x_1, \ldots, x_n]$) *Fixando uma ordem* $>$ *em* $\mathbb{Z}^n_{\geq 0}$ *e seja* $F = (f_1, \ldots, f_s)$ *uma* $s-$ *tupla ordenada de polinômios em* $k[x_1, \ldots, x_n]$, *então cada* $f \in k[x_1, \ldots, x_n]$ *pode ser escrito como.*

$$f = a_1 f_1 + \cdots + a_s f_s + r,$$

onde $a_i, r \in k[x_1, \ldots, x_n]$, *sendo que* $r = 0$ *ou* r *é uma combinação linear de monômios com coeficientes em* k *nenhum dos quais é divisível por qualquer dos termos líderes:* $LT(f_1), \ldots, LT(f_s)$. *Sabendo que* r *é o resto da divisão de* f *por* F, *além disso, se* $a_i \neq 0$, *então tem-se que* $multideg(f) \geq multideg(a_i f_i)$ *onde o termo* $multideg(f)$ *significa grau máximo de* f.

Demonstração. Prova-se a existência de $a_1, \ldots, a_s$ e r através de um algoritmo para a construção deles, demonstrando que ele opera corretamente sobre qualquer entrada dada, vejamos:

$impute$: $f_1, \ldots, f_s, f$
$output$: $a_1, \ldots, a_s, r$
$a_1 := 0, \ldots, a_1 = 0, r := 0; p := f$
Enquanto $p \neq 0$ Faça
$i := 1$
divisãoocorreu $:= false$
Enquanto $i \leq s$ e divisãoocorreu $= false$ Faça
Se $LT(f_i)$ divide $LT(p)$ Então
$a_i := a_i + LT(p)/LT(f_i)$
$p := p - (LT(p)/LT(f_i))f_i$
divisãoocorreu $= true$
Caso contrário
$i := i + 1$
Se divisãoocorreu $= false$ Então
$r := r + LT(p)$
$p := p - LT(p)$

Relacionando este algoritmo com o exemplo anterior observa-se que a variável p representa o dividendo intermediário para cada etapa da divisão, a variável r representa a coluna do lado esquerdo e as variáveis $a_1, \ldots, a_s$ são os quocientes. Finalmente a variável booleana "divisãoocorreu"determina quando algum $LT(f_i)$ divide o termo líder do dividendo intermediário. Observe que cada vez que é acionado o laço principal Enquanto,... Faça, precisamente uma das duas coisas acontecem:

1) (Passo da Divisão) Se algum $LT(f_i)$ divide $LT(p)$, então o algoritmo procede como o caso de uma variável;

2) (Passo do Resto) Se nenhum $LT(f_i)$ divide $LT(p)$ então o algoritmo adiciona $LT(p)$ para o resto e volta ao passo 1).

Serão desenvolvidos nos exercícios seguintes, a aplicação do algoritmo da divisão entre polinômios de duas variáveis, utilizando a ordem monomial lexicográfica graduada.

Exercício 2.2.1. *Divida o polinômio* $f : xy^2 + 1$ *pelos polinômios* $f_1 = xy + 1$ *e* $f_2 : y + 1$ *utilizando a ordem lexicográfica graduada.*

Solução:

Listando os divisores f_1, f_2*, nessa ordem, obtém-se a seguinte configuração:*

$$\begin{array}{c|c} xy^2+1 & xy+1;\ y+1 \\ \cline{2-2} \end{array}$$

Os termos líderes $LT(f_1) = xy$ *e* $LT(f_2) = y$*, dividem o termo líder* $LT(f) = xy^2$*. Como* f_1 *é listado em primeiro lugar, então, inicia-se a operação, dividindo* xy^2 *por* xy*.*

$$\begin{array}{c|c} xy^2+1 & xy+1;\ y+1 \\ \cline{2-2} -xy^2-y & y; \\ \cline{1-1} -y+1 & \end{array}$$

Continuando a divisão, verificou-se que o termo líder $LT(f_1) = xy$ *não divide o novo termo líder de* f*, representado pelo monômio* $LT(f) = -y$ *então, a divisão prossegue, dessa vez com o divisor* $f_2 = y + 1$*.*

$$\begin{array}{c|c} xy^2+1 & xy+1, y+1 \\ \cline{2-2} -xy^2-y & y;\ (-1) \\ \cline{1-1} -y+1 & \\ y+1 & \\ \cline{1-1} 2 & \end{array}$$

Já que os termos líderes $LT(f_1)$ *e* $LT(f_2)$ *não dividem 2, o resto é* $r = 2$*, finalizando assim a divisão. Logo, podemos escrever o dividendo, na forma:*

$$xy^2 + 1 = y \cdot (xy + 1) + (-1) \cdot (y + 1) + 2 \tag{2.1}$$

Mas o que acontece quando a ordem dos divisores é trocada? O resto é alterado, ou continua o mesmo? Para eliminar essas dúvidas, observe o exercicío abaixo

Exercício 2.2.2. *De acordo com o exercício anterior, trocando a ordem de* f_1 *e* f_2*, divida* $f = xy^2 + 1$ *por* $f_1 = y + 1$ *e* $f_2 = xy + 1$ *pela ordem lexicográfica graduada.*

Solução:

Escrevendo os divisores f_1, f_2*, nesssa ordem, obtém-se a seguinte configuração:*

$$\begin{array}{c|c} xy^2+1 & y+1, xy+1 \\ \cline{2-2} \end{array}$$

Os termos líderes $LT(f_1) = y$ *e* $LT(f_2) = xy$*, dividem o termo líder* $LT(f) = xy^2$*. Como* f_1 *é listado em primeiro lugar, então inicia-se a operação dividindo* xy^2 *por* y

$$\begin{array}{c|c} xy^2+1 & y+1, xy+1 \\ \cline{2-2} -xy^2-xy & xy-x \\ \cline{1-1} -xy+1 & \\ xy+x & \\ \cline{1-1} x+1 & \end{array}$$

Continuando a divisão, verificou-se que o termo líder $LT(f_1) = y$ não divide o termo líder do resultado parcial $(x+1)$, representado pelo monômio $LT(f) = x$ então, a divisão prossegue, dessa vez com o divisor $f_2 = xy+1$, porém verifica-se que o termo líder de f_2 também não divide o novo termo líder de f, pois x não divide $xy+1$, o termo x passa a integrar o resto e retomamos a divisão com 1 como resultado parcial, logo a divisão finaliza, com quociente $a_2 = 0$ e resto $r = x+1$, obtendo assim:

$$xy^2+1 = (xy-x)\cdot(y+1) + 0\cdot(xy+1) + x + 1 = x(y-1)(y+1) + x + 1. \tag{2.2}$$

Exercício 2.2.3. *Faça a divisão de $f : x^2y^3+y^4+3xy^2+x^2+2y^2+1$ por $f_1 : x^2y+2x+1$ e $f_2 = y^2+y$, utilizando a ordem lexicográfica graduada Listando os divisores f_1, f_2, nessa ordem, obtém-se a seguinte configuração:*

Solução:

$$\begin{array}{c|c} x^2y^3+y^4+3xy^2+x^2+2y^2+1 & x^2y+2x-1;\ y^2+y \\ \cline{2-2} -x^2y^3-2xy^2-y^2 & y^2; \\ \cline{1-1} y^4+xy^2+x^2+y^2+1 & \end{array}$$

Continuando a divisão, após obter o quociente y^2, verificou-se que o termo líder $LT(f_1) = x^2y$, não divide o novo termo líder de f, representado pelo monômio $LT(f) = y^4$ então, a divisão prossegue, dessa vez com o divisor $f_2 = y^2+y-1$.

$$\begin{array}{c|c} x^2y^3+y^4+3xy^2+x^2+2y^2+1 & x^2y+2x-1;\ y^2+y \\ \cline{2-2} -x^2y^3-2xy^2-y^2 & y^2;\ y^2+x-y \\ \cline{1-1} y^4+xy^2+x^2+y^2+1 & \\ -y^4-y^3 & \\ \cline{1-1} xy^2-y^3+x^2+y^2+1 & \\ -xy^2-xy & \\ \cline{1-1} -y^3+x^2-xy+y^2+1 & \\ y^3+y^2 & \\ \cline{1-1} x^2-xy+2y^2+1 & \end{array}$$

Desse modo obtém-se o segundo quociente (y^2+x-y) e o resto $r = x^2-xy+2y^2+1$ finalizando assim a divisão, podendo escrever o dividendo na forma:

$$x^2y^3+y^4+3xy^2+x^2+2y^2+1 = y^2\cdot(x^2y+2x+1)+(y^2+x-y)\cdot(y^2+y)+x^2-xy+2y^2+1$$

Exercício 2.2.4. *Dado o polinômio $f = x^2y+xy^2+y^2$ e os polinômios $f_1 = xy-1$ e $f_2 = y^2-1$. Divida f por f_1 e f_2, utilizando a ordem lexicográfica graduada.*

Solução:

Listando os divisores f_1, f_2, nessa ordem, obtém-se a seguinte configuração:

$$\begin{array}{c|l} x^2y+xy^2+y^2 & xy-1;\ y^2-1 \\ \cline{2-2} -x^2y+x & \quad x+y; \\ \cline{1-1} xy^2+x+y^2 & \\ -xy^2+y & \\ \cline{1-1} y^2+x+y \xrightarrow{resto} x & \\ \cline{1-1} y^2+y & \end{array}$$

Continuando a divisão, após obter o quociente $(x+y)$, verificou-se que o termo líder $LT(f_1) = xy$, não divide o novo termo líder de f, representado pelo monômio $LT(f) = x^2y$ então, a divisão prossegue, dessa vez com o divisor $f_2 = y^2 - 1$.

$$\begin{array}{c|l} x^2y+xy^2+y^2 & xy-1;\ y^2-1 \\ \cline{2-2} -x^2y+x & \quad x+y;\ 1 \\ \cline{1-1} xy^2+x+y^2 & \\ -xy^2+y & \\ \cline{1-1} y^2+x+y \xrightarrow{resto} x & \\ \cline{1-1} y^2+y & \\ -y^2+1 & \\ \cline{1-1} y+1 & \\ \cline{1-1} -1 \xrightarrow{resto} x+y & \\ \cline{1-1} 0 \xrightarrow{resto} x+y+1 & \end{array}$$

Assim, o segundo quociente é $a_2 = 1$ e o resto é $r = x + y + 1$,portanto pode-se escrever o dividendo na forma:

$$x^2y + xy^2 + y^2 = (x + y).(xy - 1) + 1(y^2 - 1) + x + y + 1$$

Esse último exercício é uma ilustração completa de como o algoritmo da divisão é trabalhado e também mostra qual a propriedade que se quer para o resto: nenhum dos seus termos deve ser divisível pelos termos líderes dos polinômios pelos quais está se dividindo. Esse passos correspondem exatamente ao que foi feito no Exemplo 2.2.3. Para provar que o algoritmo funciona, deve-se mostrar que:

$$f = a_1f_1 + \ldots + a_sf_s + r \tag{2.3}$$

é válido para todos as etapas da divisão. Isto é claramente verdadeiro para os valores iniciais de $a_1, \ldots, a_s, p$ e r; Agora suponha que (2.3) é válido para um passo do algoritmo. Se o próximo passo for um Passo da Divisão, então algum $LT(f_i)$divide $LT(p)$ e a igualdade

$$a_if_i + p = (a_i + LT(p)/LT(f_i)) \cdot f_i + (p - (LT(p)/LT(f_i)) \cdot f_i$$

mostra que $a_if_i + p$ é inalterado. E como todas as outras variáveis não são afetadas, temos que (2.3) é verdadeira. Por outro lado, se o próximo passo for o Passo do Resto, então p e r são mudados, mas a soma $p + r$ é inalterada já que

$$p + r = (p - LT(f_i)) \cdot f_i + (r + LT(f_i)) \cdot f_i$$

e como antes, tem-se que a igualdade (2.3) é preservada. A seguir, observe que o algoritmo pára quando $p = 0$. Nesta situação (2.3) torna-se

$$f = a_1f_1 + \ldots + a_sf_s + r$$

Já que os termos são adicionados a r somente quando eles não são divisíveis por nenhum dos $LT(f_i)$, isso segue que $a_1, \ldots a_s$ e r possui a propriedade desejada quando o algoritmo termina. É preciso mostrar que o algoritmo eventualmente termina. A observação chave é que cada vez que redefinimos a variável p, o termo líder é zero ou diminui (relativa à ordem de termos) ou se torna 0. Para ver isso, primeiro suponha que durante um Passo da divisão, p é definida por

$$p' = p - \frac{LT(p)}{LT(f_i)} f_i$$

Assim, tem-se que:

$$LT(\frac{LT(p)}{LT(f_i)} f_i) = \frac{LT(p)}{LT(f_i)} LT(f_i) = LT(p)$$

Logo a diferença deles p' tem o multi-grau estritamente menor, quando $p' \neq 0$. Caso o algoritmo nunca terminasse, então teríamos uma sequencia decrescente infinita de multi-graus. A propriedade da boa ordenação de $>$, como mostrado no Lema (2.1.1), mostra que isso não pode ocorrer, então $p = 0$ tem que ocorrer, após um número finito de passos.

Resta agora estudar a relação entre $multideg(f)$ e $multideg(a_i f_i)$. Todo termo em a_i é da forma $LT(p)/LT(f_i)$ para algum valor da variável p. O algoritmo começa com $p = f$ e foi provado que o multi-grau de p decresce. Isto mostra que $LT(p) \leq LT(f)$, e então temos que:

$$LT(p) \leq LT(f) \Longrightarrow \frac{LT(p)}{LT(f_i)} \leq \frac{LT(f)}{LT(f_i)} \Longrightarrow \frac{LT(p)}{LT(f_i)} LT(f_i) \leq \frac{LT(f)}{LT(f_i)} LT(f_i) \Longrightarrow$$

$$\Longrightarrow \alpha_i LT(f_i) \leq LT(f) \Longrightarrow multideg(a_i f_i) \leq multideg(f) \text{ quando } a_i f_i \neq 0$$

Finalizando assim, a demonstração do teorema □

A primeira propriedade importante do algoritmo da divisão em $K[x_1 \ldots, x_n]$ é que o resto não é unicamente determinado e isto foi visto nos Exemplos (2.2.1) e (2.2.2) com os restos : 2 e $x + 1$ respectivamente. Isso mostra que o resto não é único, ou seja, para cada ordem $F = (f_1, \ldots, f_s)$ existe um resto na divisão de f por F. Uma consequência dessa propriedade é um simples corolário do Teorema (2.2.1): Se após a divisão de f por $F = \langle f_1, \ldots, f_s \rangle$ obtermos um resto $r = 0$, então

$$f = a_1 f_1 + \ldots + a_s f_s$$

Contudo o próximo exemplo mostra que $r = 0$ não é condição necessária para que f seja da forma $a_1 f_1 + \ldots + a_s f_s$.

Exemplo 2.2.1. *Seja $f_1 = xy + 1, f_2 = y^2 - 1 \in K[x, y]$ com a ordem lexicográfica graduada dividindo $xy^2 - x$ por $F = (f_1, f_2)$ o resultado é:*

$$xy^2 - x = y(xy + 1) + 0(y^2 - 1) + (-x - y)$$

Mas quando se tem $F = (f_2, f_1)$, tem-se que:

$$xy^2 - x = x(y^2 - 1) + 0(xy + 1) + 0$$

O segundo cálculo mostra que $f = af_1 + bf_2$ e o primeiro cálculo mostra que, ainda assim é possível obter um resto não nulo na divisão por $F = (f_1, f_2)$.

Na próxima seção será abordada a teoria das Resultantes que é uma ferramenta fundamental, principalmente na resolução de sistema de equações polinomiais de uma ou mais variáveis.

2.3 Resultantes

Define-se o Resultante como o determinante da Matriz de Sylvester, mas antes de apresentar os elementos dessa matriz,é importante definir dois polinômios f e g em $K[x]$ de graus n e m respectivamente, tais que:

$$\begin{aligned} f &= a_0x^n + \ldots + a_n, \quad a_0 \neq 0 \\ g &= b_0x^m + \ldots + b_m, \quad b_0 \neq 0 \end{aligned}$$

A matriz de Sylvester nasce da necessidade de verificar a existência dos polinômios A e B para que $Af + Bg = 0$, com $gr(A) < gr(B)$ e $gr(B) < gr(F)$.

Escrevendo:

$$\begin{aligned} A &= c_0x^{m-1} + \ldots + c_{m-1} \\ B &= d_0x^{n-1} + \ldots + d_{n-1}. \end{aligned}$$

Substituindo as correspondentes expressões de f, g, A e B na equação $Af + Bg = 0$ e comparando os coeficientes das potências de x, obtém-se o seguinte sistema linear com incógnitas c_i, d_i e coeficientes a_i, b_i em K.

$$(1) \quad \begin{cases} a_0c_0 \quad + \quad b_0d_0 & = 0 \quad \text{coeficientes de} \quad x^{n+m-1} \\ a_1c_0 + a_0c_1 \quad + \quad b_1d_0 + b_0d_1 & = 0 \quad \text{coeficientes de} \quad x^{n+m-2} \\ \ddots \qquad\qquad \ddots & \vdots \\ a_lc_{m-1} \quad + \quad b_md_{n-1} & = 0 \quad \text{coeficientes de} \quad x^0 \end{cases} .$$

O sistema de equações acima mostra que existem $n + m$ equações lineares para $n + m$ incógnitas. A forma matricial desse sistema é:

$$\begin{bmatrix} a_0 & 0 & \ldots & 0 & b_0 & 0 & \ldots & 0 \\ a_1 & a_0 & & \vdots & b1 & b_0 & & \vdots \\ a_2 & a_1 & \ddots & 0 & b_2 & b_1 & \ddots & 0 \\ \vdots & & \ddots & a_0 & \vdots & & \ddots & b_0 \\ a_n & & & & b_m & & & \\ 0 & a_n & & \vdots & 0 & b_m & & \vdots \\ \vdots & 0 & \ddots & & \vdots & 0 & \ddots & \\ \vdots & \vdots & \vdots & a_n & \vdots & \vdots & & b_m \end{bmatrix} \cdot \begin{pmatrix} c_0 \\ c_1 \\ \vdots \\ c_{n-1} \\ d_0 \\ d_1 \\ \vdots \\ d_{n-1} \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 0 \\ 0 \\ \vdots \\ \vdots \\ 0 \end{pmatrix}$$

Sabe-se que um sistema desse tipo admite solução não trivial se, e somente se, o determinante da matriz dos coeficientes for nulo. A matriz de Sylvester de f e g com relação a x, denotada $Syl(f, g, x)$ é a matriz formada pelos coeficientes do sistema de equações (1).

Definição 2.3.1. *A matriz quadrada de ordem* $(n + m)$

$$Syl(f,g,x) = \begin{bmatrix} a_0 & 0 & \dots & 0 & b_0 & 0 & \dots & 0 \\ a_1 & a_0 & & \vdots & b1 & b_0 & & \vdots \\ a_2 & a_1 & \ddots & 0 & b_2 & b_1 & \ddots & 0 \\ \vdots & & \ddots & a_0 & \vdots & & \ddots & b_0 \\ & \vdots & & a_1 & & \vdots & & b_1 \\ a_n & & & & b_m & & & \\ 0 & a_n & & \vdots & 0 & b_m & & \vdots \\ \vdots & 0 & \ddots & & \vdots & 0 & \ddots & \\ \vdots & \vdots & \vdots & a_n & \vdots & \vdots & & b_m \end{bmatrix}$$

É chamada matriz de Sylvester de f e g e os espaços vazios que se encontram na matriz, são preenchidos por zero. A matriz de Sylvester é essencial para o cálculo da Resultante.

Lema 2.3.1. *Sejam f e $g \in K[x]$ dois polinômios de graus $n > 0$ e $m > 0$ em x, respectivamente, f e g possui um fator comum não constante se, e somente se, existem polinômios A e B de modo que:*

i) *A e B são não nulos;*

ii) *A tem grau no máximo $m-1$ e B possui grau no máximo $n-1$;*

iii) *$Af + Bg = 0$.*

Demonstração. Primeiro assume-se que $w \in k[x]$ é um fator comum não constante de f e g então $f = wf_1$ e $g = wg_1$ com f_1 e $g_1 \in K[x]$. Neste caso f_1 tem grau máximo $(n-1)$ e g_1 possui grau máximo $(m-1)$, assim

$$g_1 \cdot f + (-f_1) \cdot g = g_1 \cdot wf_1 - f_1 \cdot wg_1 = 0$$

Desse modo, fazendo $A = g_1$ e $B = -f_1$ são satisfeitas as propriedades requeridas: $i)$, $ii)$ e $iii)$
Reciprocamente, supondo que A e B possui as três propriedades anteriores. De $i)$ assume-se que $B \neq 0$. Suponha que g não possua fator comum com f, então o maior divisor comum de g e f é 1. Assim sendo, pode-se encontrar polinômios $\tilde{A}$ e $\tilde{B} \in K[x]$ tal que $\tilde{A}f + \tilde{B}g = 1$ agora basta multiplicar a expressão: $\tilde{A}f + \tilde{B}g$ por B e usar $Bg = -Af$:

$$B = (\tilde{A}f + \tilde{B}g)B = \tilde{A}Bf + \tilde{B}Bg = \tilde{A}Bf - \tilde{B}Af = (\tilde{A}B - \tilde{B}A)f$$

Como f tem grau $n > 0$, então $f(\tilde{A}B - \tilde{B}A)$ possui grau $\geq n$, e pela equação acima $B = f(\tilde{A}B - \tilde{B}A)$, então verifica-se uma contradição, pois B possui grau máximo $n-1$. Logo f e g tem fator comum não constante. □

Definição 2.3.2. *O Resultante de f e g, escrito como $Res_{n,m}(f,g,x)$ é o determinante da matriz de Sylvester, ou seja: $Res_{n,m}(f,g,x) = det(Syl(f,g,x))$.*

Observa-se a seguir algumas propriedades que explicitam a importância do cálculo da Resultante. A principal de todas as propriedades do Resultante é o seguinte Teorema:

Teorema 2.3.1. *Sejam* $f = \sum_{i=0}^{n} f_i x^i, g = \sum_{i=0}^{m} g_i x^i$ *dois polinômios em* $K[x]$*, tais que* $f_n, g_m \neq 0$ *de graus em* $n \geq 1$*. Então as seguintes afirmações são equivalentes:*

i) $Res_{n,m}(f, g, x) = 0$*;*

ii) Existem polinômios não nulos $A, B \in K[x]$ *de graus menores que* n *e* m *respectivamente, tais que* $A(x) \cdot g(x) = B(x) \cdot f(x)$*;*

iii) f *e* g *tem fator comum não constante em* $K[x]$*.*

Demonstração. Suponha $Res(f, g, x) = 0$ devemos mostar a existência de polinômios não nulos $A(x) = \sum_{i=0}^{n-1} c_i x^i$ e $\tilde{B}(x) = \sum_{i=0}^{m-1} d_i x^i$, em $K[x]$ de modo que $A(x) \cdot g(x) + \tilde{B}(x) \cdot f(x) = 0$. Isso equivale a encontrar uma solução não trivial do sistema homogêneo de $n+m$ equações nas incógnitas $d_{m-1}, d_{m-2}, \ldots, d_0, c_{n-1}, c_{n-2}, \ldots, c_0$:

$$\begin{cases} \begin{array}{ccccccccl} & & a_n d_{m-1} & + & b_m c_{n-1} & & & = & 0 \text{ termo em } x^{n+m-1} \\ a_{n-1} d_{m-1} & + & a_n d_{m-2} & + & b_{m-1} c_{n-1} & + & b_m c_{n-2} & = & 0 \text{ termo em } x^{n+m-2} \\ & & & \vdots & & & & & \\ & & a_0 d_0 & + & b_0 c_0 & & & = & 0 \text{ termo constante} \end{array} \end{cases}$$

Temos que existe solução não trivial para este sistema se, e somente se o determinante da matriz dos coeficientes é nulo. Desse modo, observa-se que $i)$ e $ii)$ são equivalentes. Falta ainda mostrar que $ii)$ e $iii)$ são equivalentes. Se existem dois polinômios A e B de graus menores que m e n respectivamente, tais que

$$A(x) \cdot g(x) = B(x) \cdot f(x) \tag{2.4}$$

considerando na igualdade, a fatoração em fatores irredutíveis dos dois membros da equação (2.4) nota-se que os fatores irredutíveis de $g(x)$ dividem o lado direito da igualdade. Por hipótese, sabemos que o grau de B é menor que m, portanto nem todos os fatores de $g(x)$ podem dividir B. Sendo assim, existe algum fator irredutível de g que divide f, o que confirma que eles possuem um fator comum de grau positivo.

Analisando a recíproca, denotando por $\phi(x)$ como um fator comum de grau positivo, então pode-se escrever

$$\begin{aligned} f(x) &= \phi(x)A(x), \quad \text{grau } (A) < n \\ g(x) &= \phi(x)B(x), \quad \text{grau } (B) < m \end{aligned}$$

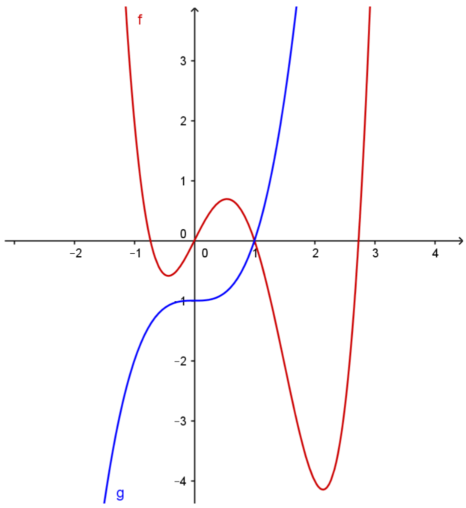
logo $A(x)g(x) = A(x)\phi(x)B(x) = B(x)f(x)$, concluindo então que $ii)$ e $iii)$ também são equivalentes. □

Exemplo 2.3.1. *Sejam* $f = x^4 - 3x^3 + 2x$ *e* $g = x^3 - 1$*, tem-se:*

Solução:

$$Res_{4,3}(f,g) = det \begin{bmatrix} 1 & 0 & 0 & 1 & 0 & 0 & 0 \\ -3 & 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & -3 & 1 & 0 & 0 & 1 & 0 \\ 2 & 0 & -3 & -1 & 0 & 0 & 1 \\ 0 & 2 & 0 & 0 & -1 & 0 & 0 \\ 0 & 0 & 2 & 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & -1 \end{bmatrix}$$

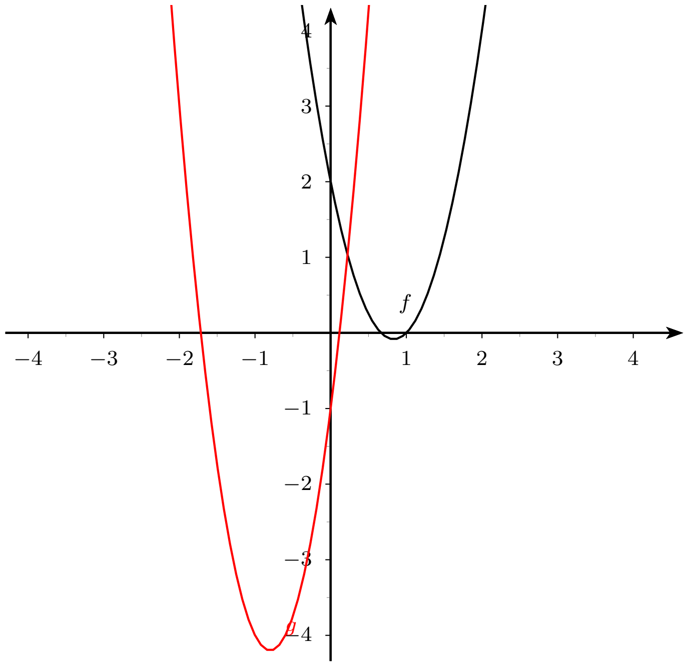
Considerando a equação $Af + Bg = 0$ e resolvendo o sistema correspondente, encontra-se: $B = (-x)(x^2 - 2x - 2)$ e $A = x^2 + x + 1$. Observe que $\frac{f}{B} = -\frac{g}{A} = x - 1$, também pode-se escrever $f = x(x-1)(x^2 - 2x - 2)$ e $g = (x-1)(x^2 + x + 1)$, como f e g tem um fator comum $(x - 1)$,pelo Teorema 2.3.1 implica que $Res_{4,3}(f,g) = 0$. Observe graficamente que f e g tem uma raiz em comum $x = 1$, e de fato, temos $mdc(f,g) = x-1$.



Exemplo 2.3.2. *Obter a resultante $Res_{2,2}(f,g)$ sendo $f = 3x^2 - 5x + 2$ e $g = 5x^2 + 8x - 1$.*

$$Res_{2,2}(f,g,x) = det \begin{bmatrix} 3 & 0 & 5 & 0 \\ -5 & 3 & 8 & 5 \\ 2 & -5 & -1 & 8 \\ 0 & 2 & 0 & -1 \end{bmatrix} = 708 \neq 0$$

Portanto não há fator comum. Além disso pode-se escrever os polinômios f e g na forma fatorada: $f = 3\left(x-1\right)\left(x - \frac{2}{3}\right)$ e $g = 5\left(x + \frac{4}{5} + \frac{\sqrt{11}}{5}\right)\left(x + \frac{4}{5} - \frac{\sqrt{11}}{5}\right)$ o que garante que não há raiz em comum a f e g, observe graficamente esse fato:

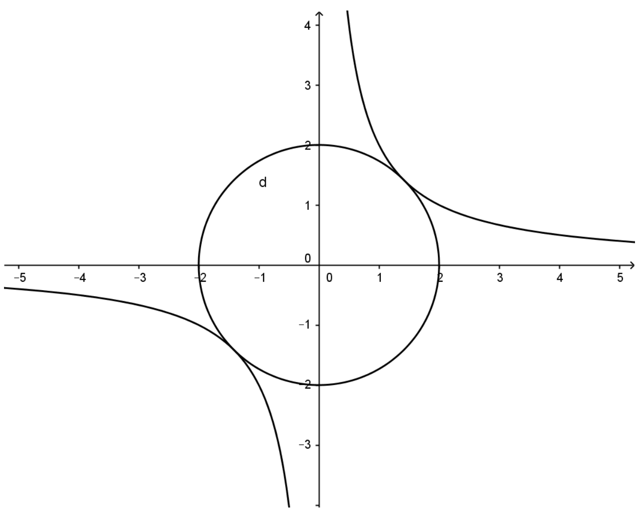


O exemplo seguinte mostra o cálculo da Resultante, utilizando polinômios em mais de uma variável. Sabendo que os polinômios f e g estão em $k[x, y]$ e x possui um grau positivo, desse modo calcula-se a $Res(f, g, x)$ com os coeficientes em x, da mesma forma, ao calcular $Res(f, g, y)$ os coeficientes do polinômio f são os que multiplicam as potências de y.

Exemplo 2.3.3. *Sejam $f = xy - 2$ e $g = x^2 + y^2 - 4$ então o resultante é*

$$Res(f, g, x) = det \begin{bmatrix} y & 0 & 1 \\ -2 & y & 0 \\ 0 & -2 & y^2 - 4 \end{bmatrix} = y^4 - 4y^2 + 4 = (y - \sqrt{2})^2(y + \sqrt{2})^2$$

Igualando cada fator a zero, obtém-se duas raízes, cada uma com multiplicidade dupla: $y = \sqrt{2}$ e $y = -\sqrt{2}$, substituindo os valores das raízes de y nos polinômios f e g,obtém-se também os valores das raízes em x, que são: $x = \sqrt{2}$ e $x = -\sqrt{2}$, com isso observa-se dois pontos: $A = (\sqrt{2}, \sqrt{2})$ e $B = (-\sqrt{2}, -\sqrt{2})$ que são os pontos em comum dos polinômios f e g. Isso pode ser verificado graficamente:



Em muitas situações, os cálculos com Resultantes podem ser facilitados utilizando algumas propriedades. As principais propriedades do resultante serão abordadas no próximo tópico.

2.3.1 Algumas Propriedades do Resultante

Para essas propriedades, define-se f e g como dois polinômios em $K[x]$, tais que:

$$f = \sum_{i=0}^{n} f_i x^i, g = \sum_{i=0}^{m} g_i x^i$$

de graus n e m, respectivamente

Propriedade 2.3.1. *A partir dos conceitos de polinômios constantes e polinômios identicamente nulos, então:*

i) $Res(f, c) = c^n$*, onde* c *é o polinômio constante não nulo;*

ii) $Res(f, 0) = 0$*, onde* 0 *é o polinômio identicamente nulo.*

Demonstração. i) Pela Definição (2.1.1), o polinômio f aparece com seus coeficientes distribuídos em colunas, com a mesma quantidade de elementos do grau do polinômio g. Como g é uma constante c, então o grau de g é zero, portanto os coeficientes de f não aparecem na matriz de Sylvester. Da mesma forma para os coeficientes de g. Como f tem grau n, então por definição, o $Res(f, c)$ é igual a:

$$Res_{n,0}(f, c) = det \begin{bmatrix} c & 0 & \dots & 0 \\ 0 & c & 0 & 0 \\ \vdots & & \ddots & \vdots \\ 0 & \dots & & c \end{bmatrix} = c^n$$

ii) O resultado dessa propriedade é diretamente demonstrado por i). □

Propriedade 2.3.2. *Se* $f_i g_i \in \mathbb{Z}[x]$*, com* $0 \leq i \leq n$ *e* $0 \leq j \leq m$ *o* $Res_{n,m}(f, g) \in \mathbb{Z}$.

Demonstração. Sabe-se que, por definição, o resultante é um determinante de uma matriz, e como os coeficientes desta matriz são números inteiros, então o resultante é um número inteiro. □

Propriedade 2.3.3. *Sendo os polinômios* $f = a_0 x^n + \ldots + a_n$ *com* $a_n \neq 0$ *e* $g = b_0 x^m + \ldots + b_m$*, com* $b_m \neq 0$*, a resultante* $Res(f, g, x)$ *pode ser dado também pela seguinte fórmula:*

$$Res(f, g, x) = det \begin{bmatrix} a_0 & a_1 & a_2 & \dots & & a_n & 0 & 0 \\ 0 & a_0 & a_1 & & \dots & & a_n & 0 \\ 0 & 0 & 0 & a_0 & a_1 & \dots & & a_n \\ b_0 & b_1 & b_2 & \dots & & b_m & & \vdots \\ 0 & b_0 & b_1 & & \dots & & b_m & 0 \\ 0 & 0 & b_0 & b_1 & & \dots & & b_m \end{bmatrix}$$

Demonstração. Sabe-se que o determinante de uma matriz é igual ao determinante da sua matriz transposta, portanto, o resultado é obvio. □

Propriedade 2.3.4. *O Resultante* $Res_{n,m}(f, g) = (-1)^{nm} Res_{m,n}(g, f)$

Demonstração. O resultado dessa propriedade é verificado pela definição de resultante, ou seja, permutando as colunas da matriz de Sylvester, o determinante é multiplicado por $(-1)^{\gamma}$, onde γ é a quantidade de permutações. Como o número de permutações é $m(m + n - 1)$, e uma vez que $(-1)^{m(m+n-1)} = (-1)^{nm}$. O resultado segue. □

Serão abordadas também algumas proposições que são fundamentais para se entender a importância do conceito e das aplicações dos resultantes, sobretudo ao se utilizar polinômios de mais de uma variável.

Teorema 2.3.2 (Teorema de Laplace para o Cálculo do Determinante)**.** *O determinante de uma matriz* $A \in M_{n\times n}$ *é igual à soma algébrica dos produtos dos elementos de uma linha (ou coluna) pelos respectivos cofatores (ou complementos algébricos). O cofator do elemento* $a_{i,j}$ *de uma matriz é o escalar* $A_{i,j}$ *definido por* $A_{i,j} = (-1)^{i+j}|M_{i,j}|$*,em que* $M_{i,j}$ *representa a matriz obtida da matriz original pela eliminação da i-ésima linha e da j-ésima coluna.Tem-se então que*

$$det(A) = a_{i,1}A_{i,1} + a_{i,2}A_{i,2} + \ldots + a_{i,n}A_{i,n}$$

Pode ser calculado também na forma:

$$det(A) = a_{1,j}A_{1,j} + a_{2,j}A_{2,j} + \ldots + a_{n,j}A_{n,j}$$

conforme seja escolhida a i-ésima linha ou a j-ésima coluna.

O teorema de Laplace é normalmente utilizado para o cálculo de determinantes de matrizes de ordem superior ou igual a 4. Apesar de também se poder aplicar a matrizes de ordem inferior.

Na prática, o que se faz é passar do cálculo do determinante de uma matriz de ordem n para o cálculo de determinantes de matrizes de ordem $n - 1$. O teorema pode ser aplicado sucessivamente até se obterem matrizes de ordem 2 ou 3, cujo determinante é mais simples de calcular.

Pode selecionar-se indiferentemente qualquer linha ou coluna da matriz para aplicar o teorema, pois todas conduzem ao mesmo resultado. No entanto, para simplificar os cálculos, é usual escolher-se a linha ou coluna que apresente mais zeros.

Na verdade, visto que o método consiste em multiplicar cada elemento da linha pelo seu cofator, no caso de o elemento ser 0, o produto é nulo, não havendo pois, necessidade de calcular o cofator do dito elemento para achar o produto.

Propriedade 2.3.5. *Dados* f *e* $g \in \mathbb{Z}[x]$ *de grau positivo, o resultante* $Res(f, g, x)$ *é uma expressão polinomial, com coeficientes inteiros, calculados nos coeficientes de* f *e* g*. Além disso,* f *e* g *possuem um fator comum em* $k[x]$ *se e somente se* $Res(f, g, x) = 0$.

Demonstração. A fórmula geral para se calcular o determinante de uma matriz $A = (a_{i,j})_{l\leq j,j\leq m}$ de ordem $n \times n$ é:

$$det(A) = \sum_{\sigma \text{ é uma permutação de } \{1,\ldots,S\}} sgn(\sigma)a_{1\sigma(1)} \cdot a_{2\sigma(2)} \ldots a_{n\sigma(n)}$$

Onde tem-se que:

$$sgn(\sigma) = \begin{cases} 1, & \text{se } \sigma \text{ é par} \\ -1, & \text{se } \sigma \text{ é ímpar} \end{cases}$$

Isso mostra que o determinante é um polinômio inteiro (na verdade, os coeficientes são $+1$ ou -1) em suas entradas, sendo assim, a primeira afirmação da proposição mostra então que o determinante é um número inteiro. Resta provar a segunda parte da proposição: Sabe-se que a resultante é zero $\Leftrightarrow$ a Matriz dos coeficientes de equações (1) possui determinante nulo $\Leftrightarrow$ equações (1) têm uma solução diferente de zero. Observou-se anteriormente que isso é equivalente à existência de A e B como no Lema 2.3.1, e então o Lema 2.3.1 completa a prova da proposição. $\square$

Proposição 2.3.1. *Dados f e $g \in k[x]$ de grau positivo, existem polinômios $A, B \in k[x]$ de modo que*

$$Af + Bg = Res(f, g, x)$$

Além disso, os coeficientes de A e B são polinômios nos coeficientes de f e g.

Demonstração. Como a definição de Resultante foi baseado na equação $Af + Bg = 0$. Se $Res(f, g, x) = 0$, o resultado segue do lema.Suponha pois que $Res(f, g, x) \neq 0$, aplicando-se os mesmos métodos da demonstração e usando o raciocínio análogo ao Lema 2.3.1. Escrevendo $f = a_0x^n + \ldots + a_n, \;\; a_0 \neq 0, g = b_0x^m + \ldots + b_m, \;\; b_0 \neq 0, A = c_0x^{m-1} + \ldots + c_{m-1}, B = d_0x^{n-1} + \ldots + d_{n-1}$, Queremos mostrar que a equação $Af + Bg = Res(f, g, x)$ tem solução, isto é que o sistema

$$(1) \quad \begin{cases} a_0c_0 & + & b_0d_0 & = & 0 & \text{coeficientes de} & x^{n+m-1} \\ a_1c_0 + a_0c_1 & + & b_1d_0 + b_0d_1 & = & 0 & \text{coeficientes de} & x^{n+m-2} \\ \ddots & & \ddots & \vdots & & & \\ & a_lc_{m-1} & + & b_md_{n-1} = & Res(f, g, x) & \text{coeficientes de} & x^0 \end{cases}$$

tem solução. A forma matricial desse sistema é:

$$\underbrace{\begin{bmatrix} a_0 & 0 & \ldots & 0 & b_0 & 0 & \ldots & 0 \\ a_1 & a_0 & & \vdots & b1 & b_0 & & \vdots \\ a_2 & a_1 & \ddots & 0 & b_2 & b_1 & \ddots & 0 \\ \vdots & & \ddots & a_0 & \vdots & & \ddots & b_0 \\ a_n & & & & b_m & & & \\ 0 & a_n & & \vdots & 0 & b_m & & \vdots \\ \vdots & 0 & \ddots & & \vdots & 0 & \ddots & \\ \vdots & \vdots & \vdots & a_n & \vdots & \vdots & & b_m \end{bmatrix}}_{Syl(f,g,x)} \cdot \begin{pmatrix} c_0 \\ c_1 \\ \vdots \\ c_{n-1} \\ d_0 \\ d_1 \\ \vdots \\ d_{n-1} \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 0 \\ 0 \\ 0 \\ \vdots \\ Res(f, g, x) \end{pmatrix}$$

Cuja matriz de coeficientees é a matriz de Sylvester de f e g e como seu determinante é não nulo (por hipótese), o sistema (1) tem solução única. $\square$

Observação 2.3.1. *Os valores dos coeficientes de A e B podem ser calculados usando-se a regra de Cramer:* $C_i = \dfrac{1}{Res(f,g,x)} \cdot det(S)$ *em que S é a matriz transposta da matriz de Sylvester quando usamos* $\begin{pmatrix} 0 \\ 0 \\ \vdots \\ 0 \\ 0 \\ 0 \\ \vdots \\ Res(f,g,x) \end{pmatrix}$ *no lugar da i-ésima coluna*

2.4 Teorema de Intersecção de Bézout

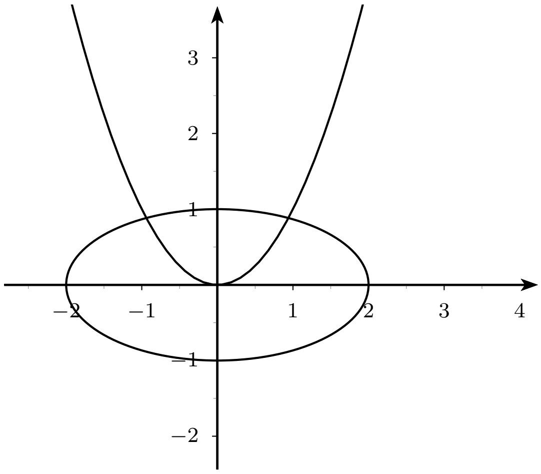
Uma das aplicações mais interessantes e importantes da utilização do conceito de resultantes está inserida no Teorema de Intersecção de Bézout. Este teorema fornece uma cota superior para o número de soluções de um sistema de equações polinomiais, através dos produtos dos graus desses polinômios. A prova mais geral desse Teorema pode ser encontrado em[10].

O teorema diz que, dados dois polinômios f e g em duas variáveis e de graus total n e m respectivamente, com nenhum fator em comum, a soma da multiplicidade de interseções $I(P,f,g)$ dos pontos de interseção P é no máximo $m \cdot n$, ou seja se intersectam em um número finito de pontos, em geral as curvas se intersectam no máximo em $m \cdot n$ pontos ou numa infinidade de pontos distintos[11]. Para isso monta-se uma matriz específica com seus coeficientes em x cujo determinante é a resultante $Res(f,g,x)$ e os elementos dessa matriz são polinômios na variável y. Demonstra-se que este polinômio é identicamente igual a zero ou tem grau no máximo $m \cdot n$.

Como $Res(f,g,x)$ é um polinômio de grau no máximo $m \cdot n$, então haverá no máximo $m \cdot n$ raízes distintas. A multiplidade de interseção de um ponto $P = (a,b)$ é definido como: $I(f,g,P) = 0$, Se P não é ponto comum às curvas definidas por $f = 0$ e $g = 0$, e $I(f,g,P) =$ multiplicidade de b como raiz de resultante $Res(f,g,x)$ após feitos os ajustes necessários e se P não é ponto de interseção $I(P,f,g) = 0$, sendo P pertencente a uma componente comum de f e g então $I(P,f,g) = \infty$, concluindo então que a soma das multiplicidades das raízes de $Res(f,g,x)$ é no máximo $m \cdot n$, pois o grau de $Res(f,g,x)$ é no máximo $m \cdot n$.

Seguem alguns exemplos das aplicações do Teorema de Bézout.

Exemplo 2.4.1. *As curvas* $f : y - x^2 = 0$ *(parábola) e* $g : x^2 + 4y^2 = 4$ *(elipse) se interceptam em 2 pontos,' fazendo* $x^2 = y$, *temos* $y + 4y^2 = 4$,*cujas raízes são* $y = \dfrac{-1+\sqrt{65}}{8}$ *e* $y = \dfrac{-1-\sqrt{65}}{8}$, *substituindo em x obtém-se:* $x = \sqrt{\dfrac{-1 \pm \sqrt{65}}{8}}$ *e* $x = -\sqrt{\dfrac{-1 \pm \sqrt{65}}{8}}$, *isso exemplifica o teorema de interseção de Bézout, pois os polinômios f e g, ambos tem grau 2 e o produto deles é 4, ou seja, como já foi visto, esse é o número máximo de pontos que podem ocorrer na interseção entre as curvas. Isso pode ser confirmado geometricamente:*

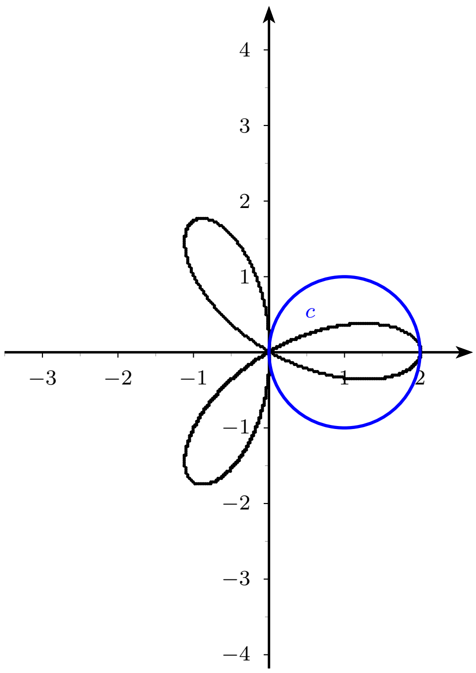


Exemplo 2.4.2. *Os polinômios* $f = x^4 - 2x^3 + 2x^2y^2 + 6xy^2 + y^4 = 0$ *e* $g = x^2 + y^2 - 2x$ *não possuem componente em comum, portanto, pelo teorema da interseção de Bézout, esses dois polinômios possuem um número máximo de pontos, igual ao produto de seus graus, ou seja 8 pontos. Pode-se resolver pelo resultante* $Res(f, g, y)$*, ou seja: resultante é [9]:*

$$Res(f,g,y) = det \begin{bmatrix} 1 & 0 & 2x^2+6x & 0 & x^4-2x^3 & 0 \\ 0 & 1 & 0 & 2x^2+6x & 0 & x^4-2x^3 \\ 1 & 0 & x^2-2x & 0 & 0 & 0 \\ 0 & 1 & 0 & x^2-2x & 0 & 0 \\ 0 & 0 & 1 & 0 & x^2-2x & 0 \\ 0 & 0 & 0 & 1 & 0 & x^2-2x \end{bmatrix} = -8x^3 + 16x^2$$

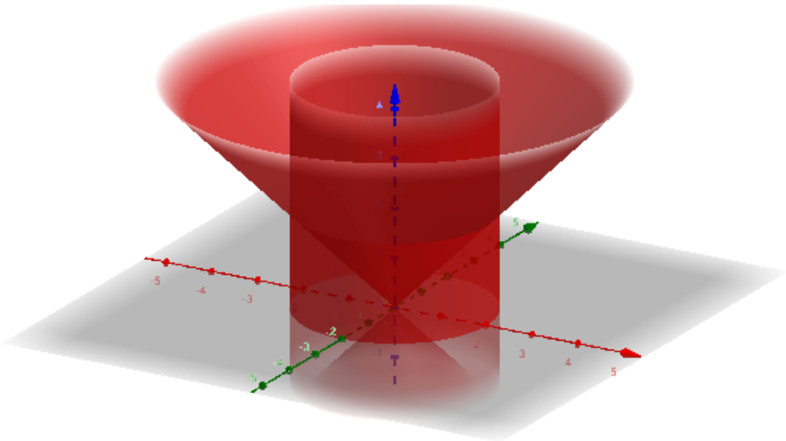
igulando a resultante a zero: $-8x^3 + 16x^2 = 0$*,obtém-se* $x = 0$ *ou* $x = 2$*, substituindo os valores de* x*, obtemos* $y = 0$ *tanto para* $x = 0$ *quanto para* $x = 2$*.*

Também pode ser determinado geometricamente as curvas projetadas por esses polinômios.



Nota-se que a rosácea de três pétalas $f : x^4 - 2x^3 + 2x^2y^2 + 6xy^2 + y^4 = 0$ *possui dois pontos em comuns com o círculo* $g : (x-1)^2 + y^2 - 1 = 0$*, são eles:* $A(0,0)$ *e* $B(2,0)$

Exemplo 2.4.3. *Os polinômios* $f = x^2 + y^2 - z^2$ *e* $g = x^2 + y^2 - 4$ *possuem componente em comum, ao substituir o termo:* $x^2 + y^2$ *em* g*, tem-se* $z^2 = 4$*, logo:* $z = 2$ *ou* $z = -2$*, ou seja:* $(x, y, 2)$ *e* $(x, y, -2)$ *gera uma infinidade de pontos em comuns. Verificando geometricamente as curvas projetadas por esses polinômios.*



Observa-se que o cilindro $g : x^2 + y^2 = 4$ *tem infinitos pontos em comuns com o cone* $f : x^2 + y^2 = z^2$.

CAPÍTULO 3

SUGESTÕES DE ATIVIDADES A SEREM DESENVOLVIDAS

Após todas essas abordagens apresentadas nos capítulos anteriores, serão sugeridas e formuladas, nesse capítulo, às seguintes atividades para serem aplicadas em sala de aula:

3.1 Atividade 1

Prof. Marcelo Lopes Monteiro
Público alvo: Alunos do 3 ° Ano do Ensino Médio.

A divisão de polinômios em duas ou mais variáveis não são trabalhadas no 3^o ano do Ensino Médio, porém os polinômios desse tipo são vistos na mesma série escolar, em geometria analítica, no formato das curvas algébricas, como por exemplo nas cônicas: Hipérboles, elipses, parábolas e circunferências. Mas como operar algebricamente com esse polinômios? Qual a ordem a ser seguida durante uma divisão? Como devem ser ordenados esses polinômios? Qual a motivação e a importância de se estudar esse conteúdo?

Para tentar responder essas perguntas propõe-se a seguinte atividade, seguindo os seguintes passos:

- 1) Primeiramente o professor(a) deverá mostrar aos alunos, vários polinômios de mais de uma variável, dando preferência para aqueles cujas curvas são mais conhecidas na geometria analítica: Elipse, Parábola, Circunfeência e Hipérbole. Sugestões de polinômios: $P = x^3 + y^3 - 6xy, P = x^2 + xy + y^2 - 3, P = x^2yz - 2x^3z^2 + y^3, P = x^2y - xz^2 - xyz + z^3, P = x^2z + 2xy - z^3 + x^3y$ e $P = 2(x^2 + y^2)^2 - 25(x^2 + y^2)$;

- 2) Em seguida o(a) discente questionará os alunos à respeito da ordem em que devem ser escritos esses polinômios, comparando com polinômios de uma variável onde os mesmos já se acostumaram a ordenar segundo às potências decrescentes da variável, nesse caso o aluno sentirá a necessidade de ordenar esses polinômios que possuem mais de uma variável. Certamente ocorrerão vários tipos de ordenações diferentes, provenientes das respostas dos alunos;

- 3) A partir dessas diferentes respostas obtidas no item anterior, cabe agora ao discente, explicar para a turma, os diferentes tipos de ordenamentos monomiais, especificando as ordens lexográfica e a lexográfica graduada, explicando o que é termo líder e como se verifica o grau total de cada monômio. Em seguida, os estudantes deverão ordenar esses polinômios, seguindo os dois tipos de ordens monomiais propostas;

- 4) Para essa etapa será proposto aos estudantes que dividam dois polinômios seguindo a ordem lexográfica graduada. No primeiro exemplo utilizando um divisor e um dividendo e nos próximos exemplos, utilizando um dividendo e dois divisores. O professor(a) questionará os alunos quanto à troca da ordem dos divisores e pedirá aos estudantes para que troquem a ordem e proceda novamente a divisão, posteriormente os estudantes deverão comparar os resultados das divisões: antes da troca e depois da troca da ordem dos divisores. Sugestões dos pares de polinômios para as divisões: $a) f = x^2y^2z^2 + xy - yz$ por $g = x - y$;
$b) f = 2y + xy^2 + y^2$ por $f_1 = y^2 - 1$ e $f_2 = xy - 1$;
$c) f = x^3 - x^2y - x^2z + x$ por $f_1 = x^2y - z$ e $f_2 = xy - 1$.

- 5) Nesta última etapa os estudantes perceberão, através dos resultados obtidos, que a troca da ordem dos divisores de fato, altera o resto da divisão, mas em ambas as situações o dividendo nada mais é do que a combinação linear do produto de cada quociente com seu divisor mais o resto, e que o resto é uma soma de monômios, sendo que nenhum dos quais é divisível pelos termos líderes de cada divisor.

3.2 Atividade 2

:

Prof. Marcelo Lopes Monteiro
Público alvo: Alunos do 3 ° Ano do Ensino Médio

A proposta é trazer para a sala de aula, os seguintes questionamentos: como proceder para achar os pontos de interseção de duas curvas f e g, formadas por polinômios com mais de uma variável? Por exemplo: como encontrar a intersecção entre uma hipérbole e uma circunferência? É possível verificar graficamente essas interseções?

Com a intenção de responder esses questionamentos, propõe-se a seguinte atividade, para cada grupo de 05 estudantes, seguindo os seguintes passos:

- 1) Cada grupo de estudantes receberá do professor, um sistema de equações com duas curvas f e g, cada grupo com duas curvas diferentes, sugestões para a dupla de curvas:
  - Grupo 1: $f = x^2 + y^2 - 2x$ e $g = y^2 - x$;
  - Grupo 2: $f = x^2 + xy^2 - y^2$ e $g = x^2 - xy$;
  - Grupo 3: $f = x^2 + y^2 - 4$ e $g = xy - 1$;
  - Grupo 4: $f = x^2 + y^2 = 2$ e $g = x - y$;
  - Grupo 5: $f = x^2 + y$ e $g = y - x^2$;
  - Grupo 6: $f = y - x$ e $g = y^2 - xy$;

  Os grupos resolverão o sistema, utilizando o método da resultante;

- 2) Resolvendo o determinante da matriz de Sylvester, contendo as duas equações com coeficientes em x ou em y (com o objetivo dos alunos perceberem qual a melhor opção de escolha da variável fixada), igualando esse determinante a zero, os alunos verificarão a quantidade de pontos da intersecção desse sistema;

- 3) Nessa etapa, o grupo utilizará o software Geogebra, que pode ser acessado por smartphones, tablets ou computadores, e verificar geometricamente os pontos de intersecções (caso existam esses pontos em comuns);

- 4) Ao final da atividade, os professor(a) deverá reunir o que cada grupo fez, verificar as resoluções, comparar os resultados e propor uma discursão entre os grupos, com base nos diversos resultados encontrados, para que os estudantes percebam a relação existente entre a resultante e os pontos de intersecção de um sistema de polinômios, além das percepção da importância da Teoria das Resultantes, como uma ferramente bastante útil nesse processo.

3.3 Atividade 3

Prof. Marcelo Lopes Monteiro
Público alvo: Alunos do 3° Ano do Ensino Médio

Um dos conteúdos raramente abordados no Ensino Médio é o $M.D.C.$ entre dois polinômios com uma variável e quando se aborda, geralmente se remete à técnica das divisões sucessivas, porém existem outros meios de obter esse máximo divisor comum, como por exemplo a teoria dos Resultantes. Quando a resultante é nula, os polinômios tem um fator comum, portanto o polinômio possui raízes comuns, mas quando a resultante não é nula, os polinômios não possuem raiz em comum, são primos entre si, ou seja, o $M.D.C.$ é 1

Para que os estudantes percebam isso, propõe-se a seguinte atividade, seguindo o passo a passo:

- 1) O professor(a) apresentará para os alunos, um par de polinômios f e g de uma variável, comeąndo com polinômios bem simples, de graus menores, o professor vai aumentando e diversificando os graus de cada polinômio (pelo menos até o 3 grau pra não dificultar muito o cálculo da resultante). Sugestões de pares de polinômios: $f = x^2 - 1$ e $g = x - 1; f = x^2 - 2x + 3$ e $g = x^2 - 4; f = x^3 - 1$ e $g = x - 2$ finalizando com $f = -x^3 + 2x^2$ e $g = 2x^2 + 5$;

- 2) Os alunos resolverão através do cálculo da resultante. Caso a resultante seja nula, os polinômios tem um fator comum, caso a resultante não seja nula, então o $M.D.C.$ é 1.

- 3) Após os cálculos das resultantes e as verificações da existência ou não de fator comum, os alunos determinarão algebricamente o $M.D.C.$ através da fatoração dos polinômios, ou então geometricamente, utilizando o software Geogebra;

- 4) Nesta última etapa, os estudantes deverão comparar os resultados obtidos, utilizando a técnica das divisões sucessivas para encontrar o máximo divsor comum, confirmando assim que realmente obtém-se os mesmos resultados.

CAPÍTULO 4

CONSIDERAÇÕES FINAIS

O intuito desse trabalho, foi de ampliar os conhecimentos dos estudantes em relação às divisões polinomiais. Esse tópico é trabalhado na educação básica apenas como mais uma das operações algébricas, ao lado da adição, subtração e multiplicação; Além disso aborda-se apenas divisões com polinômios de uma única variável.

No entanto, muitas aplicações, inclusive na própria álgebra, são desenvolvidas através da divisão de duas ou mais variáveis, que não são trabalhadas no ensino médio. Como exemplos dessas aplicações, temos: a solução de um sistema de equações não lineares de duas variáveis, o cálculo do M.D.C. entre dois polinômios e outros exemplos que foram abordados, utilizando a divisão polinomial.

O entendimento sobre ordens monomiais, divisão de polinômios de duas ou mais variáveis, resultante, Teorema de interseção de Bézout e as aplicações de todos esses conceitos, são de fundamental importância para a eficácia desse aprendizado. Vale lembrar que todos esses itens devem ser trabalhados em sala de aula, com uma linguagem matemática clara e acessível, para o aluno do ensino médio.

Com a finalidade de alcançar o objetivo e a eficácia na aprendizagem de novos conhecimentos a respeito do estudo dos polinômios, foi exibido o algoritmo da divisão de polinômios de duas ou mais variáveis e como dividi-los, simultaneamente por dois ou mais divisores, definindo suas estratégias de resolução.

Também foi introduzido o conceito de resultante, explicando à sua importância e aplicabilidade na solução de um sistema composto por polinômios de várias variáveis, especificamente nas interseções de curvas, bem como a sua utilização como uma ferramanta fundamental para os problemas relacionados ao teorema de interseção de Bézout.

A introdução, em sala de aula, desses novos tópicos dentro do contexto das divisões proporcionarão um ganho de conhecimento para os estudantes, que poderão utilizar essas abordagens n resolução de problemas envolvendo outros tópicos dentro do próprio estudo dos polinômios ou em outros temas recorrentes da matemática. Posteriormente ficou estabelecida uma conexão com a Geometria Analítica, ao identificar as possíveis interseções entre duas curvas (ex: Hipérbole e círculo) no plano.

De um modo geral, os objetivos deste trabalho foram alcançados de maneira satisfatória, considerando o fato de poder transmitir aos estudantes do 3^0 ano do Ensino Médio uma nova abordagem para um conteúdo tão importante e recorrente no ensino básico, o que tornou enriquecedora essa nova "leitura"dos co onteúdos trabalhados.

REFERÊNCIAS BIBLIOGRÁFICAS

[1] BRASIL. **Base nacional comum curricular**. MEC. Brasília, 2015. Disponível em:<http://basenacionalcomum.mec.gov.br/documentos/BNCC-APRESENTACAO.pdf >. Acesso em: 13/03/2016.

[2] BRASIL. **Parâmetros curriculares nacionais**. MEC. Brasília, p.187. 1998.

[3] IEZZI, G.. **Fundamentos da Matemática Elementar-complexos, polinômios, equações**. Atual. São Paulo, p. 151-166. 2013.

[4] PESSOA, F.Diniz. **Polinômios: Raízes e utilidade para métodos numéricos**. Dissertação (Mestrado). Universidade Federal de São João del-Rei/Campus Alto Paraopeba. Departamento de Matemática.Alto Paraopeba. 2015. Disponível em:<http://www.profmat-sbm.org.br/dissertações?polo=&título=&aluno=Fernanda+diniz.>. Acesso em 29/10/2016.

[5] MONTEIRO, L. H. Jacy. **Elementos de lgebra**. Coleção Elementos de Matemática. IMPA. Rio de Janeiro. 1970.

[6] LIMA E.L., Carvalho P.C., Wagner E., Morgado A. C.. **A Matemática do Ensino Médio, v1**. SBM. Rio de Janeiro, 2012.

[7] COX, D., Little J., OShea, D.. **Ideals, Varieties, and Algorithms, an Introduction to Computational Algebraic Geometry and Commutative Algebra**. Springer. New York, 2006.

[8] MAT.UFMG. **Ordem monomial, Algoritmo comutativo e Base de Grobner**. Universidade Federal de Minas Gerais, Instituto de Matemática. Belo Horizonte, 2013.Disponível em: < http://www.mat.ufmg.br/ pafm/alg_comut/grobner_imp.pdf >. Acesso em: 24/06/2016.

[9] VAINSENCHER, I..**Introdução as curvas algébricas planas**. Coleção Matemática Universitária. IMPA. Rio de Janeiro. 1996.

[10] SHAFAREVICH,I..**Mathematics for computer algebra**; Springer-Verlag, Berlin-Heidelberg-New York. 1977.

[11] TURA, F.C..**Resultantes, equações polinomiais e o teorema de Bezout**. Universidade Federal do Rio Grande do Sul. Instituto de Matemática. Programa de Pós-Graduação em Matemática Aplicada. Porto Alegre. 2006. Disponível em: < http://hdl.handle.net/10183/6689 >. Acesso em: 17/11/2016.