UNIVERSIDADE FEDERAL DE SANTA CATARINA
CENTRO DE CIÊNCIAS FÍSICAS E MATEMÁTICAS

Teorema do Hexágono de Pascal
Teorema de Pappus

TRABALHO DE CONCLUSÃO DE CURSO

Kátia Regina Fraga Leimann

Florianópolis – SC
Julho – 2003

Kátia Regina Fraga Leimann

Teorema do Hexágono de Pascal
Teorema de Pappus

Trabalho de conclusão de Curso apresentado ao
Curso de Matemática – Habilitação Licenciatura
Departamento de Matemática
Centro de Ciências Físicas e Matemáticas
Universidade Federal de Santa Catarina

Orientadora: Albertina Zatelli

Florianópolis – SC
Julho – 2003

Sumário

INTRODUÇÃO ***04***

1. BIOGRAFIA DE PASCAL E PAPPUS ***05***

2. POLINÔMIOS ***09***

Definição de Polinômio ***09***
Grau de um Polinômio ***13***
O Algoritmo da Divisão ***16***
Raízes de Polinômios ***18***
Ideais Principais e Máximo Divisor Comum ***22***
Polinômios Irredutíveis e Ideais Maximais ***25***
Fatoração Única ***28***
Resultante de Dois Polinômios ***32***

3. Aplicações ***44***
Teorema de Bezout ***44***
Teorema de Pascal ***46***
Teorema de Pappus ***54***

CONCLUSÃO ***57***

REFERÊNCIAS BIBLIOGRÁFICAS ***58***

Introdução

Durante o Curso de Graduação em Matemática, habilitação licenciatura, comecei a ter grande interesse pela área de Álgebra, principalmente por polinômios. Este trabalho tem por objetivo estudar polinômios e através destes provar dois teoremas da geometria projetiva: o Teorema do Hexágono de Pascal e o Teorema de Pappus.

Neste trabalho, no capítulo 1, trazemos um breve estudo sobre a biografia desses dois grandes matemáticos, Blaise Pascal e Pappus.

No segundo capítulo, fazemos um estudo sobre polinômios, anéis de polinômios, ideais, com demonstrações de resultados importantes que serão utilizados na demonstração dos teoremas.

Finalmente, no terceiro capítulo, enunciamos e apresentamos as demonstrações do Teorema do Hexágono de Pascal, e do Teorema de Pappus.

Ao longo do trabalho, serão vistos alguns exemplos e ilustrações para a melhor compreensão dos tópicos.

Capítulo 1

Biografia de Pascal e Pappus

BLAISE PASCAL

Blaise Pascal - filósofo, matemático, físico, teólogo e escritor de origem francesa, nasceu em Clermont-Ferrand, região de Auvergne, na França, em 19 de junho de 1623, mas aos nove anos de idade foi morar com toda a sua família em Paris. Era filho de Etienne Pascal, um matemático e alto funcionário do Estado, que se dedicou com muita eficiência na formação educacional de seus filhos, Blaise Pascal e Jacqueline.

Pascal aos doze anos começou a trabalhar em Geometria, chegando a descobrir que a soma dos ângulos de um triângulo é igual a dois ângulos retos.

Etienne Pascal mesmo não sendo uma pessoa totalmente ortodoxa, freqüentava reuniões na casa do Padre franciscano Marin Mersenne, filósofo e físico francês, onde se discutia religião e outros assuntos, como: Filosofia, Física, Matemática, etc., do qual participavam, também muitas personalidades importantes. Foi quando, com aproximadamente quatorze anos, Pascal decidiu acompanhar seu pai nessas reuniões e aos dezesseis anos apresentou vários teoremas de Geometria Projetiva, entre os quais constava o hoje conhecido "Hexagrama Místico" em que demonstra que " se um hexágono estiver inscrito numa cônica, então as interseções de cada um dos três pares de lados opostos são colineares",

onde em fevereiro de 1640 escreveu “Ensaio sobre as cônicas”, baseado no estudo de Girard Desargues.

A contribuição de Pascal às ciências é bem menos metódica e fecunda do que brilhante.

Faz parte desse estudo das cônicas o Teorema de Pascal: " O hexágono inscrito em uma cônica tem a propriedade de que os pontos de interseção dos lados opostos estão em linha reta ". Em trabalho posterior e extraviado, o " Traité des coniques ", conhecido apenas através de Leibniz, Pascal aborda o que chama de " hexagrama místico "; por meio de projeções, demonstra que todo hexágono provém de uma cônica correspondente e que, por sua vez, qualquer cônica origina um hexágono. O hexagrama serve-lhe de ponto de partida à obtenção, em quatrocentos corolários, das propriedades peculiares às cônicas.

O fato de seu pai ser nomeado coletor de impostos da Normandia Superior, em 1639, fez com que toda a família deixasse Paris e fosse morar em Rouen (sede da região da Alta Normandia, localizada na França), onde realizou suas primeiras pesquisas no campo da Física, escrevendo um tratado sobre acústica, sendo um dos pioneiros da experimentação física. Nessa época, inventou, também, uma pequena máquina de calcular, chamada Pascalinne, conservada, atualmente no Conservatório de Artes e Medidas de Paris.

Em 1651, com a morte do seu pai, Pascal teve um período de contatos com a vida mundana, convivendo com a nobreza da época. Escreveu para uma de suas irmãs uma carta relatando tudo sobre a morte de seu querido pai com um profundo significado cristão em face de sua família ser devota e adotar princípios católicos rigorosos.

Em Física destacou-se pelo seu trabalho "Tratado sobre o equilíbrio dos líquidos" relacionado com a pressão dos fluídos e hidráulica. O princípio de Pascal diz que a pressão em qualquer ponto de um fluido é a mesma, de forma a que a pressão aplicada num ponto é transmitida a todo o volume do contentor. Este é o princípio do macaco e do martelo hidráulicos.

Ainda em 1654, Pascal estudou e demonstrou um trabalho matemático intitulado “tratado do triângulo Aritmético” o qual foi publicado neste mesmo ano, onde estabelece as séries

1
1 1
1 2 1
1 3 3 1
1 4 6 4 1
1 5 10 10 5 1

que possibilitam o cálculo das combinações de 'm' elementos tomados 'n' à 'n' e das potências semelhantes nos termos de uma progressão aritmética. Antes de Pascal, Tartaglia usara o referido triângulo nos seus trabalhos e, muito antes, os matemáticos árabes e chineses já o utilizavam. Podemos aumentar indefinidamente, este triângulo, bastando, para isso, aumentar o número de linhas da seguinte maneira: cada número é igual à soma do par de números acima de si. Este triângulo é conhecido como Triângulo de Pascal ou Triângulo de Tartaglia, apresentando inúmeras propriedades e relações, entre as quais a Sucessão de Fibonacci em que as somas dos números dispostos ao longo das diagonais do triângulo geram a referida série.

Em correspondência com Fermat, durante o Verão de 1654, Pascal estabeleceu os fundamentos da Teoria das Probabilidades. O seu último trabalho foi sobre a Ciclóide – a curva traçada por um ponto da circunferência que gira, sem escorregar, ao longo de uma linha reta. Durante esse ano desinteressou-se pela ciência; passou os últimos anos da vida a praticar caridade e decidiu dedicar-se a Deus e à religião. Faleceu com 39 anos devido a um tumor maligno que tinha no estômago ter se estendido ao cérebro.

PAPPUS DE ALEXANDRIA

Pappus de Alexandria é o último dos grandes geometras gregos e um dos seus teoremas é citado como a base da geometria projetiva moderna. Nosso conhecimento sobre a vida de Pappus é quase nulo. Segundo Suídas, Pappus viveu em fins do século IV da nossa era. É famoso, pela sua Coleção Matemática, que durante muitos séculos foi a obra mais manuseada pelos matemáticos.

Esta coleção foi escrita em oito livros, dos quais se perdeu o primeiro e parte do segundo. Sua principal importância é esclarecer as dificuldades deixadas em aberto pelos seus antecessores, analisando e comentando numerosas passagens fielmente escritas. Sendo por isso uma preciosa fonte para o conhecimento de obras que de outra maneira não teriam chegado até nós.

Inédito durante muito tempo, o seu nome não alcançou a popularidade de muitos dos seus contemporâneos; não era, porém, totalmente desconhecido, como prova o fato de que a Geometria de Descartes está baseada em grande parte na resolução de um problema de

Pappus de Alexandria. Além disso, já em 1588 Comandino tinha apresentado uma excelente tradução que exerceu certa influência no desenvolvimento da geometria do séc. XVII. Além da obra já citada, Suídas atribuiu-lhe diversos escritos geográficos, uma obra sobre presságios e os sonhos e um Comentário sobre a Sintaxis de Tolomeu. Finalmente na coleção dos Alquimistas Gregos aparece com o seu nome um Juramento que trata de questões religiosas. A generalização dos escritos de Pappus de Alexandria demonstrou que o teorema conhecido pelo nome de Guldin e atribuído durante muito tempo a este matemático, pertence na verdade ao matemático grego.

O teorema de Pappus, foi demonstrado pela primeira vez por Pappus de Alexandria por volta do ano 300, é um teorema de características completamente projetista, e pode ser enunciado como: "Se os pontos A, B e C estão em uma reta, os pontos A', B' e C' estão em outra reta concorrente e as retas AB', BC' e CA' cortam as retas BA', CB' e AC' respectivamente, então os pontos de interseção são colineares."

A obra de Pappus é de imenso valor, não só pelo seu valor informativo mas também pelas contribuições originais, onde se encontram soluções que muitos séculos depois foram reelaboradas como definitivas, no campo da Matemática.

Capítulo 2

Polinômios

Neste capítulo veremos algumas notações, definições e resultados importantes sobre polinômios.

Quase todas as demonstrações foram feitas, principalmente aquelas que não foram vistas durante o curso de graduação.

Definição de Polinômio

Definição 2.1: Seja $\boldsymbol{A}$ um anel comutativo com unidade. Chamamos de polinômio sobre $\boldsymbol{A}$, na indeterminada x, à uma expressão formal

$p = a_o + a_1x^1 + a_2x^2 + ... + a_nx^n + ...$, onde cada $a_i \in \boldsymbol{A}$ e existe $k \in N$ tal que $a_j = 0$ para todo $j \geq k$.

Designaremos por $\boldsymbol{A}[x]$ o conjunto de todos os polinômios sobre a indeterminada x.

Dois polinômios são iguais se, e somente se, os coeficientes correspondentes a mesma potência de x são iguais.

Sejam:

$p = a_0 + a_1x^1 + ... + a_nx^n + ...$ e

$q = b_0 + b_1x^1 + ... + b_mx^m + ...,$

definimos adição e produto de polinômios do seguinte modo:

$p + q = (a_0 + b_0) + (a_1 + b_1)x^1 + ... + (a_k + b_k)x^k + ...$ e

$p.q = c_0 + c_1x^1 + ... + c_kx^k + ...$ onde:

$$\begin{cases} c_0 = a_0b_0 \\ c_1 = a_0b_1 + a_1b_0 \\ \quad \vdots \\ c_k = a_0b_k + a_1b_{k-1} + ...+ a_kb_0 \\ \quad \vdots \end{cases}$$

isto, é $c_k = \sum_{i=0}^{k} a_i b_{k-i}$ para cada $k \in \boldsymbol{N}$.

Usando as propriedades do anel ***A*** podemos provar que:

Definição 2.2: O polinômio $\boldsymbol{0} = 0 + 0x^1 + 0x^2 + ... + 0x^n + ...$ é denominado de polinômio nulo e $\boldsymbol{1} = 1 + 0x^1 + ... + 0x^n + ...$ é denominado de polinômio constante *1*.

Teorema 2.1: O conjunto ***A****[x]* é um anel comutativo com unidade.

Demonstração:

Tomemos, *p, q* e *h* polinômios em ***A****[x]:*

$p = a_o + a_1x^1 + a_2x^2 + ... + a_nx^n + ...$
$q = b_o + b_1x^1 + b_2x^2 + ... + b_mx^m + ...$
$h = d_o + d_1x^1 + d_2x^2 + ... + d_kx^k + ...$

1) $p + (q + h) = (p + q) + h$.

De fato,

$$p + (q + h) = (a_o + a_1x^1 + a_2x^2 + \dots) + ((b_o + d_o) + (b_1 + d_1)x^1 + (b_2 + d_2)x^2 + \dots)$$
$$= (a_o + (b_o + d_o)) + (a_1 + (b_1 + d_1))x^1 + (a2 + (b_2 + d_2))\, x^2 + \dots$$
$$= ((a_o + b_o) + d_o) + ((a_1 + b_1) + d_1)x^1 + ((a_2 + b_2) + d_2)x^2 + \dots$$
$$= (p + q) + h.$$

2) $p + q = q + p.$

De fato,

$$p + q = (a_o + b_o) + (a_1 + b_1)x^1 + (a_2 + b_2)\, x^2 + \dots$$
$$= (b_o + a_o) + (b_1 + a_1)x^1 + (b_2 + a_2)\, x^2 + \dots$$
$$= q + p.$$

3) Existe $\boldsymbol{0} = 0 + 0x^1 + 0x^2 + \dots + 0x^n + \dots \in \boldsymbol{A}[x]$ (polinômio nulo) tal que $\boldsymbol{0} + p = p, \ \forall\ p \in \boldsymbol{A}[x]$.

De fato:

$$\boldsymbol{0} + p = (0 + a_0) + (0 + a_1)x^1 + (0 + a_2)x^2 + \dots + (0 + a_n)x^n + \dots$$
$$= a_0 + a_1x^1 + a_2x^2 + \dots + a_nx^n + \dots$$
$$= p$$

Portanto $\boldsymbol{0} = 0 + 0x^1 + 0x^2 + \dots + 0x^n + \dots$ é o elemento neutro para adição de polinômios.

4) Dado $p \in \boldsymbol{A}[x]$ existe $-p \in \boldsymbol{A}[x]$ tal que $p + (-p) = \boldsymbol{0}$.

De fato: tomemos

$$-p = (-a_o) + (-a_1)x^1 + (-a_2)x^2 + \dots + (-a_n)x^n + \dots, \text{ então}$$
$$p + (-p) = (a_o - a_o) + (a_1 - a_1)x^1 + (a_2 - a_2)x^2 + \dots + (a_n - a_n)x^n + \dots$$
$$= 0 + 0x^1 + 0x^2 + \dots + 0x^n + \dots$$
$$= \boldsymbol{0} \text{ (polinômio nulo).}$$

Assim, $-p \in \boldsymbol{A}[x]$ é o elemento inverso de p com respeito a adição.

5) $p.(q.h) = (p.q).h$

De fato, tomemos

$p = (a_i)$, $q = (b_j)$, $h = (c_k)$, $q.h = (d_l)$, $p.(q.h) = (e_m)$, $p.q = (x_n)$ e $(p.q).h = (y_m)$ temos:

$$e_m = \sum_{i+l=m} a_i d_l = \sum_{i+l=m} a_i(\sum_{j+k=l} b_j c_k) = \sum_{i+j+k=m} a_i(b_j c_k) = \sum_{i+j+k=m} (a_i b_j) c_k =$$

$$\sum_{n+k=m} (\sum_{i+j=n} a_i b_j) c_k = \sum_{n+k=m} x_n c_k = y_m, \forall m \in N.$$

6) $p.(q + h) = p.q + p.h$

De fato, sejam

$$p.(q + h) = e_0 + e_1x^1 + ... + e_nx^n + ...$$

$$p.q = k_0 + k_1x^1 + ... + k_nx^n + ...$$

$$p.h = g_0 + g_1x^1 + ... + g_nx^n + ...$$

Logo $e_n = \sum_{i=0}^{n} a_i(b_{n-i} + c_{n-i}) = \sum_{i=0}^{n} a_i b_{n-i} + \sum_{i=o}^{n} a_i c_{n-i} = k_n + g_n$

Portanto, segue da igualdade de polinômios que $p.(q + h) = p.q + p.h$.

Analogamente prova-se que $(p + q).h = p.h + q.h$.

7) $p.q = q.p$

De fato, sejam

$$p.q = k_0 + k_1x^1 + ... + k_nx^n + ...$$

$$q.p = e_0 + e_1x^1 + ... + e_nx^n + ...$$

Assim, temos que

$$k_n = \sum_{i=0}^{n} a_i b_{n-i} = a_0b_n + a_1b_{n-1} + ... + a_nb_0$$

$$e_n = \sum_{i=0}^{n} b_i a_{n-i} = b_0a_n + b_1a_{n-1} + ... + b_na_0$$

Logo $k_n = e_n$. Portanto da igualdade de polinômios segue que $p.q = q.p$.

8) Existe $\mathbf{1} = 1 + 0x^1 + 0x^2 + ... + 0x^n + ... \in \mathbf{A}[x]$ que é elemento unidade.

De fato,

$\mathbf{1} = b_o + b_1x^1 + b_2x^2 + ... + b_nx^n + ...$, onde $b_0 = 1$ e $b_i = 0, \forall\ i > 0$.

$\mathbf{1}.p = c_o + c_1x^1 + c_2x^2 + ... + c_kx^k + ...$ onde

$c_i = a_0b_i + a_1b_{i-1} + ... + a_ib_0$, então

$c_0 = a_0b_0 = b_0a_0 = a_0$

$c_1 = a_0b_1 + a_1b_0 = b_0a_1 = a_1$

$c_2 = a_0b_2 + a_1b_1 + a_2b_0 = b_0a_2 = a_2$

$:$

$:$

$c_i = b_0a_i = a_i$

Assim, $\mathbf{1}.p = p$.

Logo $\mathbf{1} = 1 + 0x^1 + ... + 0x^n + ...$ é elemento unidade do anel de polinômios $\mathbf{A}[x]$. □

Observação 2.1: Um polinômio $p = a_o + a_1x^1 + a_2x^2 + ... + a_nx^n + ... \in \mathbf{A}[x]$ tal que $a_i = 0$ para todo i > n passará a ser indicado por $p = a_o + a_1x^1 + a_2x^2 + ... + a_nx^n$.

Grau de um Polinômio

Definição 2.3: Seja $p = a_o + a_1x^1 + a_2x^2 + ... + a_nx^n \in \mathbf{A}[x]$ tal que $a_n \neq 0$ (em particular $p \neq 0$) então diz-se que ***p tem grau n*** (denotaremos por $grau(p) = n$).

Observação 2.2: O grau do polinômio nulo não está definido, diremos então que o polinômio nulo não tem grau.

Observação 2.3: Quando mencionarmos o grau de um polinômio p estaremos assumindo que p é um polinômio não nulo.

Pode-se provar facilmente que $grau(p + q) \leq máx\{grau(p),grau(q)\}$ e que $grau(p.q) \leq grau(p) + grau(q)$. Além disso, se $\boldsymbol{A}$ um domínio prova-se que $grau(p.q) = grau(p) + grau(q)$.

Vamos provar que grau $(p + q) \leq máx\{grau(p), grau(q)\}$.

Sejam p e q polinômios, tais que

$$p = a_o + a_1x^1 + a_2x^2 + ... + a_nx^n$$

$$q = b_o + b_1x^1 + b_2x^2 + ... + b_mx^m$$

onde $a_n \neq 0$, $b_m \neq 0$, $a_j = 0$ *para* $j > n$ e $b_r = 0$ *para* $r > m$.

Sendo $k = máx(n,m)$ temos que $k \geq n$ e $k \geq m$ então:

$a_j = 0$ para todo $j > k \geq n$

$b_r = 0$ para todo $r > k \geq m$

Assim,

$p + q = (a_o + b_o) + (a_1 + b_1)x^1 + (a_2 + b_2)\, x^2 + ... +(a_k + b_k)x^k$

Logo $grau\ (p + q) \leq k = máx\{grau(p), grau(q)\}$. □

Vamos provar que $grau(p.q) \leq grau(p) + grau(q)$.

$p.q = c_0 + c_1x^1 + c_2x^2 + ... +c_lx^l +$, onde $l = n + m$

$c_i = a_0b_i + a_1b_{i-1} + ... + a_ib_0$

$c_{n+m} = a_0b_{n+m} + a_1b_{n+m-1} + ... + a_nb_m + a_nb_{m-1} + ... + a_{m+n}b_0$.

Temos ainda que $a_j = 0$ para $j > n$ e $b_r = 0$ para $r > m$.

Então $a_0b_{n+m} = 0$

$a_1b_{n+m-1} = 0$

$\vdots$

$a_{n-1}b_{m+1} = 0$

a_nb_m

$na_{+1}b_{m-1} = 0$

$\vdots$

$a_{m+n}b_0 = 0$

Logo $c_{n+m} = a_nb_m$

Agora seja $k > n + m$

$c_k = a_0b_k + a_1b_{k-1} + ... + a_nb_{k-n} + ... + a_{n+1}b_{k-n-1} + ... + a_kb_0$.

Para $0 \leq j \leq n$ temos que $-n \leq -j$, donde segue que $m < k - n \leq k - j$, assim, $b_{k-j} = 0$, além disso, $a_{n+j} = 0$ para qualquer que seja j. Logo $c_k = 0$. Portanto $grau(p.q) \leq n + m = grau(p) + grau(q)$. Se $\boldsymbol{A}$ for domínio temos que $c_{n+m} = a_nb_m \neq 0$ de modo que neste caso teremos $grau(p.q) = n + m = grau(p) + grau(q)$. □

Exemplo 2.1: $p = 1 + x^2$

$q = 1 + x^1 + x^3$

$p.q = (1 + x^2).(1 + x^1 + x^3)$

$p.q = 1 + x^1 + x^3 + x^2 + x^3 + x^5$

$p.q = 1 + x^1 + x^2 + 2x^3 + x^5$

Portanto $grau(p.q) = 2 + 3 = grau(p) + grau(q)$.

Teorema 2.2: Se $\boldsymbol{A}$ um domínio então $\boldsymbol{A}[x]$ é domínio.

Demonstração: Basta provar que $p \neq 0$ e $q \neq 0$ então $p.q \neq 0$.

Tomemos,

$p = a_o + a_1x^1 + a_2x^2 + ... + a_nx^n$

$q = b_o + b_1x^1 + b_2x^2 + ... + b_mx^m$

onde $a_n \neq 0$ e $b_m \neq 0$ então $pq = c_0 + c_1x^1 + c_2x^2 + ... + c_{n+m}x^{n+m}$ onde $c_{n+m} = a_nb_m$.

Como $a_n \neq 0$, $b_m \neq 0$ e $\boldsymbol{A}$ é domínio temos que $a_nb_m \neq 0$. Concluímos que $c_{n+m} \neq 0$.

Logo $p.q \neq 0$.

Portanto $\boldsymbol{A}[x]$ é domínio. □

O Algoritmo da Divisão

Proposição 2.1: Sejam $(\boldsymbol{A}, +, .)$ um anel comutativo com unidade e $\boldsymbol{A}[x]$ o anel de polinômios numa variável sobre $\boldsymbol{A}$. Sejam $f \in \boldsymbol{A}[x]$ e $g = b_m x^m + ... + b_1 x^1 + b_0$ um polinômio em $\boldsymbol{A}[x]$ com b_m invertível em $\boldsymbol{A}$. Então:

(i) Existem $t, r \in \boldsymbol{A}[x]$ tais que $f = g.t + r$, com
$grau(r) < grau(g)$ *ou* $r = 0$.

(ii) Tais t e r podem ser efetivamente calculados.

(ii) Tais t e r são unicamente determinados.

Demonstração:

(i) e (ii) Se $f = 0$ ou se $grau(f) < grau(g)$ acabou: tome $t = 0$ e $r = f$.

Se $grau(f) \geq grau(g) = m$, escreva $f = a_n x^n + ... + a_0$ com $n \geq m$ e $a_n \neq 0$. Por hipótese, b_m é invertível em $\boldsymbol{A}$, logo $(1/b_m) \in \boldsymbol{A}$ e portanto $(1/b_m).a_n x^{n-m} \in \boldsymbol{A}[x]$. Notemos que $(1/b_m).a_n x^{n-m}$ é o polinômio pelo qual precisamos multiplicar o primeiro termo de g para se obter o primeiro termo de f. Temos então $f - (1/b_m).a_n x^{n-m}.g = (a_{n-1} - a_n b_{m-1}/b_m)x^{n-1} + ... + (a_{n-m} - a_n b_0/b_m)x^{n-m} + h$ *(onde* $h = 0$ *ou* $grau(h) < n\text{-}m)$ $= f_1 \in \boldsymbol{A}[x]$, assim $f = g.(1/b_m).a_n x^{n-m} + f_1$. Observe que $(1/b_m).a_n$ e f_1 foram efetivamente calculados.

Se $f_1 = 0$ ou se $grau(f_1) < grau(g) = m$, acabou: tome $t = (1/b_m).a_n x^{n-m}$ *e* $r = f_1$.

Se $p = grau(f_1) \geq m$, repete-se o processo com f_1 no lugar de f e g, isto é, escreva $f_1 = c_p x^p + ... + c_0$ com $n - 1 \geq p \geq m$ e $c_p \neq 0$ e tome $f_2 = f_1 - (1/b_m)c_p x^{p-m}.g$; temos então $f = g[(1/b_m).a_n x^{n-m} + (1/b_m)c_p x^{p-m}] + f_2$ com $(1/b_m).a_n$, $(1/b_m).c_p$ e f_2 efetivamente calculáveis.

Se $f_2 = 0$ ou se $grau(f_2) < m$, acabou, se não, repetimos todo o processo novamente, até obtermos depois de um número finito de passos um polinômio f_k nulo ou de grau menor que m. Tome $r = f_k$.

(iii) Se existem $t_1, r_1, t_2, r_2 \in \boldsymbol{A}[x]$ tais que $f = g.t_1 + r_1 = g.t_2 + r_2$ com $grau(r_1) < grau(g)$ *(ou* $r_1 = 0$*) e* $grau(r_2) < grau(g)$ *(ou* $r_2 = 0$*).*

Então temos $g[t_1 - t_2] = r_2 - r_1$. Suponha que $t_1 - t_2 \neq 0$; então pelo fato de g ter coeficiente inversível, vem que $g(t_1 - t_2) \neq 0$, daí, $r_2 - r_1 \neq 0$, temos então $grau(r_2 - r_1) = grau(g[t_1 - t_2]) = grau(g) + grau(t_1 - t_2)$, pois o coeficiente do termo de maior grau de g não é divisor de zero em $\boldsymbol{A}$ já que ele é invertível em $\boldsymbol{A}$; assim, temos $grau\ (r_2 - r_1) \geq grau(g)$, o que é absurdo pois $grau(r_2 - r_1) \leq máx\{grau(r_1), grau(r_2)\} < grau(g)$. □

Exemplo 2.2: Dividir o polinômio $f = x^4 + 4x^3 + 4x^2 + 9$ pelo polinômio $g = x^2 + x - 1$ em $\boldsymbol{Z}[x]$.

Resolução:

$f = x^4 + 4x^3 + 4x^2 + 0x + 9 \quad | x^2 + x - 1 = g$

$-x^4 - x^3 + x^2 \quad\quad x^2 + 3x + 2 = t$

$3x^3 + 5x^2 + 0x$

$-3x^3 - 3x^2 + 3x$

$2x^2 + 3x + 9$

$-2x^2 - 2x + 2$

$x + 11 = r.$

Desta divisão temos que: $x^4 + 4x^3 + 4x^2 + 9 = (x^2 + x - 1)(x^2 + 3x + 2) + x + 11$ onde grau $(r) = 1 < 2 = grau(g)$.

Definição 2.4: Seja $\boldsymbol{D}$ um domínio. Dizemos que $\boldsymbol{D}$ é domínio Euclidiano se existe uma função $\varphi: \boldsymbol{D}^* \to \boldsymbol{N}$ tal que

i) Dados $f, g \in \boldsymbol{D}$, $g \neq 0$; existem $q, r \in \boldsymbol{D}$ tais que $f = q.g + r$ onde $r = 0$ ou $\varphi(r) < \varphi(g)$.

ii) $\varphi(a.b) \geq \varphi(a), \forall\, a, b \in \boldsymbol{D}^*$.

Notação: $(\boldsymbol{D}, \varphi)$ é domínio euclidiano.

Sejam $\boldsymbol{K}$ um corpo e $\boldsymbol{K}[x]$ o domínio dos polinômios sobre $\boldsymbol{K}$ na indeterminada x. Vamos provar que $\boldsymbol{K}[x]$ é um domínio Euclidiano.

Teorema 2.3: (Algoritmo da divisão). Seja $\boldsymbol{K}$ um corpo e sejam $f, g \in \boldsymbol{K}[x]$ com $g \neq 0$. Então existem únicos $q, r \in \boldsymbol{K}[x]$ tais que:

$$f(x) = q(x).g(x) + r(x) \quad \text{com} \begin{cases} graur(x) < graug(x) \\ ou \\ r(x) = 0. \end{cases}$$

Ou seja o teorema afirma que $(\boldsymbol{K}[x], grau(\,.\,))$ é domínio euclidiano.

Definição 2.5: Nas condições do teorema 2.3 onde f é chamado dividendo, g é chamado divisor, e r é chamado de resto.

Demonstração: (teorema 2.3)

A demonstração segue como corolário da proposição 2.1, basta observar que se $grau(g) = m$ teremos que $g = b_m x^m + ... + b_1 x^1 + b_0 \in \boldsymbol{K}[x]$ é um polinômio com b_m invertível em $\boldsymbol{K}$ (visto que num corpo todo elemento diferente de zero é invertível). □

Notemos que a demonstração da proposição 2.1 generaliza o processo usual da divisão de polinômios o qual é usualmente demonstrado em $\boldsymbol{K}[x]$.

Raízes de Polinômios

Definição 2.6: Se $f = a_o + a_1 x^1 + a_2 x^2 + ... + a_n x^n$ é um polinômio não nulo em $\boldsymbol{A}[x]$ e $\alpha \in \boldsymbol{A}$ definimos $f(\alpha) = a_o + a_1 \alpha^1 + a_2 \alpha^2 + ... + a_n \alpha^n \in \boldsymbol{A}$. Dizemos que α é uma raiz de f em $\boldsymbol{A}$ se tivermos que $f(\alpha) = 0$.

Proposição 2.2: Sejam $\boldsymbol{A}$ um anel, e $f \in (\boldsymbol{A}[x] - \{0\})$ e $\alpha \in \boldsymbol{A}$ então existe $q \in \boldsymbol{A}[x]$ tal que $f = (x - \alpha).q + f(\alpha)$.

Demonstração:

Seja $(x - \alpha) \in \boldsymbol{A}[x]$, assim pela proposição 2.1 existem $q, r \in \boldsymbol{A}[x]$ tal que $f = g.(x - \alpha) + r$ onde $r = 0$ ou $grau(r) < 1$, ou seja, $r \in \boldsymbol{A}$.

Assim temos que $f(\alpha) = g(\alpha).(\alpha - \alpha) + r$, donde segue que $f(\alpha) = r$.

Logo $f = q(x - \alpha) + f(\alpha)$. □

Corolário 2.1: Seja $\boldsymbol{A}$ um anel. $\alpha \in \boldsymbol{A}$ é raiz de f, *se e somente se*, $(x-\alpha)$ divide f, ou seja $\alpha \in \boldsymbol{A}$, $f(\alpha)=0 \Leftrightarrow f = g.(x - \alpha)$, com $g \in \boldsymbol{A}[x]$.

Aplicando o corolário 2.1 um número finito de vezes temos que existem $g \in \boldsymbol{A}[x]$ e um número natural $1 \leq k \leq grau(f)$ tais que $f = (x - \alpha)^k.g$ com $g(\alpha) \neq 0$.

Definição 2.7: Sejam $\boldsymbol{A}$ um anel, $f \in \boldsymbol{A}[x]$ e $\alpha \in \boldsymbol{A}$. Dizemos que α é uma raiz de f com multiplicidade $k \geq 1$ se $(x - \alpha)^k$ divide f mas $(x - \alpha)^{k+1}$ não divide f.

Corolário 2.2: Sejam $\boldsymbol{A}$ um anel, $f \in \boldsymbol{A}[x]$ e $\alpha \in \boldsymbol{A}$. Então as seguintes afirmações são equivalentes:

i) α é uma raiz de f com multiplicidade k.

ii) Existe $h \in \boldsymbol{A}[x]$ tal que $f = (x - \alpha)^k.h$ com $h(\alpha) \neq 0$.

Demonstração:

(i)⇒(ii) Sendo α uma raiz de f com multiplicidade k temos que $(x - \alpha)^k$ divide f, assim existe $h \in \boldsymbol{A}[x]$ tal que $f = (x - \alpha)^k.h$. Se por absurdo tivermos $h(\alpha) \neq 0$, existirá $g \in \boldsymbol{A}[x]$ tal que $h = (x - \alpha).g$ resultando que $f = (x - \alpha)^{k+1}.g$. Isto é uma contradição, pois $(x - \alpha)^{k+1}$ não divide f.

(ii) $\Rightarrow$(i) Como $f = (x - \alpha)^k.h$ temos que α é raiz de f com multiplicidade maior ou igual a k, assim $(x - \alpha)^k$ divide f. Devemos mostrar que $(x - \alpha)^{k+1}$ não divide f. Suponhamos por absurdo que $(x - \alpha)^{k+1}$ divide f, temos então que $(x - \alpha)^k.h = f = (x - \alpha)^{k+1}.g$ para algum $g \in \boldsymbol{A}[x]$. Logo $(x - \alpha)^k.h - (x - \alpha)^{k+1}.g = 0 \Rightarrow (x - \alpha)^k.[h - (x - \alpha).g] = 0$. Como $(x - \alpha)^k$ é um polinômio mônico, temos que $[h - (x - \alpha).g)] = 0$, onde $h = (x - \alpha).g$, então $h(\alpha) = 0$, o que contradiz a hipótese. □

Corolário 2.3: Sejam $\boldsymbol{D}$ um domínio e $0 \neq f \in \boldsymbol{D}[x]$. Então, o *número de raízes de f* em $\boldsymbol{D}$ (contando as multiplicidades) *é menor ou igual ao grau(f).*

Demonstração:

Seja $n = grau(f)$. Vamos usar o segundo princípio de indução sobre n.

Se $n = 0$ então f não possui raízes em $\boldsymbol{D}$, assim não há nada a demonstrar.

Suponha o resultado válido para todo polinômio q *tal* que $grau(q) < n$.

Vamos provar que vale para todo polinômio f tal que $grau(f) = n$.

Se não existe $\alpha \in \boldsymbol{D}$ tal que $f(\alpha) = 0$ o resultado é válido.

Suponha que existe $\alpha \in \boldsymbol{D}$ tal que $f(\alpha) = 0$. Então pelo corolário 2.2 existem $q \in \boldsymbol{A}[x]$ e $k \geq 1$ tais que $f = (x - \alpha)^k.q$ com $q(\alpha) \neq 0$ (notemos que $grau(q) = n - k$).

Se não existe $\beta \neq \alpha$ tal que $f(\beta) = 0$, temos que o *número de raízes de f é k* e $grau(f) \geq k$, logo o número de raízes de f é menor ou igual ao $grau(f)$.

Se existe $\beta \neq \alpha$ tal que $f(\beta) = 0$. Então $0 = f(\beta) = (\beta - \alpha).q(\beta)$ onde $\beta - \alpha \neq 0$, então β é raiz de q (pois $\boldsymbol{D}$ é um domínio) mas $grau(q) = n - k$.

Por hipótese de indução temos que q tem no máximo $n - k$ raízes em $\boldsymbol{D}$ (contando as multiplicidades). Então f tem no máximo $(n - k) + k = n$ raízes em $\boldsymbol{D}$.

Logo o número de raízes de f em $\boldsymbol{D}$ (contando as multiplicidades) é menor ou igual ao $grau(f)$. □

Exemplo 2.3: $f = x^4 + 3x^3 + x^2 - 3x - 2 \in \boldsymbol{Z}[x]$

Fatorando f temos: $f = (x + 2).(x + 1)^2.(x - 1)$

$grau(f) = 4$

Número de raízes de f *em* $\boldsymbol{Z} = 4$

Portanto $grau(f) \geq$ *número de raízes de f.*

Exemplo 2.4: $f = x^5 + 6x^3 + 4x^4 + 6x^2 + 5x + 2 \in \boldsymbol{Z}[x]$

Fatorando f temos: $f = (x + 2).(x + 1)^2.(x^2 + 1)$

$grau(f) = 5$

Número de raízes de f *em* $\boldsymbol{Z} = 3$

Portanto $grau(f) \geq$ *número de raízes de f.*

Definição 2.8: Sejam $\boldsymbol{K}$ e $\boldsymbol{L}$ dois corpos. Dizemos que $\boldsymbol{L}$ é uma extensão de $\boldsymbol{K}$ se $\boldsymbol{K} \subseteq \boldsymbol{L}$.

Colorário 2.4: Seja $f = a_o + a_1x^1 + a_2x^2 + ... + a_nx^n$ um polinômio não nulo de *grau n* (isto é, $a_n \neq 0$) em $\boldsymbol{K}[x]$. Então f possui no máximo n raízes em qualquer extensão $\boldsymbol{L}$ de $\boldsymbol{K}$.

Demonstração:

Como $f \in \boldsymbol{K}[x]$ e sendo $\boldsymbol{L}$ uma extensão de $\boldsymbol{K}$, temos que $\boldsymbol{K} \subset \boldsymbol{L}$ então $f \in \boldsymbol{L}[x]$, pelo corolário 2.3 temos que $grau(f)$ tem no máximo n raízes em $\boldsymbol{L}$. □

Corolário 2.5: Sejam f *e* $g \in \boldsymbol{K}[x]$ onde $\boldsymbol{K}$ é um corpo com um número infinito de elementos. Então $f = g \Leftrightarrow f(b) = g(b) \ \forall b \in \boldsymbol{K}$.

Demonstração:

($\Rightarrow$) Trivial pela definição de igualdade de polinômios.

($\Leftarrow$) Seja $h = f - g \in \boldsymbol{K}[x]$. Assim, por hipótese, temos, $h(b) = 0, \forall b \in \boldsymbol{K}$, e como $\boldsymbol{K}$ é infinito segue imediatamente do Corolário 2.3 que $h = 0$, ou seja, $f = g$ como queríamos demonstrar. □

Ideais Principais e Máximo Divisor Comum

Definição 2.7: Seja $\boldsymbol{I} \subset \boldsymbol{A}$. Dizemos que $\boldsymbol{I}$ é um ideal de $\boldsymbol{A}$ se as seguintes condições são satisfeitas:

(i) $0 \in \boldsymbol{I}$

(ii) $(x - y) \in \boldsymbol{I}, \forall x, y \in \boldsymbol{I}$

(iii) $b.x \in \boldsymbol{I}$ *e* $x.b \in \boldsymbol{I}, \forall b \in \boldsymbol{A}, \forall x \in \boldsymbol{I}$.

Definição 2.9: Seja $\boldsymbol{A}$ anel comutativo com unidade e $a.\boldsymbol{A} = \{a.x: x \in \boldsymbol{A}\}$.

No que segue vamos mostrar que $a.\boldsymbol{A}$ é um ideal:

(i) $0 \in a.A$, pois $a.0 = 0$

(ii) Sejam $x, y \in a.A$, sendo que temos

$$\begin{cases} x = a.z_1 \\ y = a.z_2 \end{cases} \text{ onde } z_1, z_2 \in \boldsymbol{A}$$

Temos que: $(x - y) = (a.z_1 - a.z_2) = a.(z_1 - z_2)$, onde $(z_1 - z_2) \in \boldsymbol{A}$.

Logo $(x - y) \in a.\boldsymbol{A}$.

(iii) Seja $b \in \boldsymbol{A}$ então $b.x = b.(a.z_1) = (b.a).z_1 = (a.b).z_1 = a.(b.z_1)$. Por outro lado temos $b.x = x.b = (a.z_1).b = a.(z_1.b)$. Logo $b.x \in a.\boldsymbol{A}$ *e* $x.b \in a.\boldsymbol{A}$.

Portanto $a.\boldsymbol{A}$ é ideal de $\boldsymbol{A}$. □

Definição 2.10: O ideal $a.A$ é denominado ideal gerado por a.

Observação 2.4: Usualmente denota-se o ideal $a.A$ por $[a]$.

Definição 2.11: Seja I ideal de A (A anel comutativo com unidade). Quando $I = a.A = \{ax: x \in A\}$ para algum $a \in A$, diz-se que I é um ideal principal.

Observação 2.5: Se I é ideal de um anel com unidade A e suponhamos que $1 \in I$ então $I = A$ pois, $I \subset A$ e para qualquer que seja $a \in A$, $a = a.1 \in I$ donde $A \subset I$. Logo $I = A$.

Teorema 2.4: Todo ideal de $K[x]$ é principal.

Demonstração:

Seja I um ideal de $K[x]$. Se $I = \{0\}$ então $I = 0K[x]$, e neste caso I é gerado por 0. Suponhamos que $I \neq \{0\}$ então existe $0 \neq p \in I$.

Tomemos $S = \{grau(p): p \in I\}$ assim $S \neq \phi$ pois $p \in I$.

Pelo Principio da Boa Ordem existe um elemento mínimo em S, isto é, existe $p_0 \in I$ tal que $grau(p_0) \leq grau(p)$, $\forall p \in I$.

Vamos provar que $I = p_0.K[x] = K[x]p_0$. Notemos que $p_0 \neq 0$ pois p_0 tem grau.

Seja $f \in I$. Então pelo algoritmo de Euclides temos que existem g e r em $K[x]$ tais que $f = g.p_0 + r$ onde $r = 0$ ou $grau(r) < grau(p_0)$. Como $f, p_0 \in I$ segue imediatamente que $r = (f - g.p_0(x_0)) \in I$. Se $r \neq 0$ temos que $grau(r) < grau(p_0)$ contrariando a escolha de p_0, assim temos que $r = 0$, portanto $f = g.p_0 \in K[x].p_0$.

Consequentemente $I \subset K[x].p_0$.

Mas $K[x].p_0 = \{f.p_0 : f \in K[x]\} \subset I$.

Logo $I = K[x].p_0$.

Assim concluímos que todo ideal de $\boldsymbol{K}[x]$ é principal. □

Antes de enunciarmos o próximo teorema vamos definir a noção de divisibilidade em $\boldsymbol{K}[x]$.

Sejam $f, g \in \boldsymbol{K}[x]$, $g \neq 0$. Dizemos que g é um divisor de f em $\boldsymbol{K}[x]$ (ou g divide f em $\boldsymbol{K}[x]$) se existe $h \in \boldsymbol{K}[x]$ tal que $f = h.g$.

Se g é um divisor de f em $\boldsymbol{K}[x]$ escreveremos $g \backslash f$ em $\boldsymbol{K}[x]$.

Se $p_1, ..., p_m \in \boldsymbol{K}[x]$ e como a soma de ideais é ideal, temos que $\boldsymbol{I} = \boldsymbol{K}[x].p_1 + ... + \boldsymbol{K}[x].p_m = \{f_1.p_1 + ... + f_m.p_m : f_i \in \boldsymbol{K}[x], i = 1,2,3,...,m\}$, é o ideal de $\boldsymbol{K}[x]$ gerado por $p_1, ... , p_m \in \boldsymbol{K}[x]$.

Teorema 2.5: (Existência de MDC). Sejam $p_1, ..., p_m \in \boldsymbol{K}[x] - \{0\}$ e seja o ideal $\boldsymbol{I} = \boldsymbol{K}[x].p_1 + ... + \boldsymbol{K}[x].p_m$, isto é, $\boldsymbol{I}$ é o ideal de $\boldsymbol{K}[x]$ gerado pelos polinômios não nulos $p_1, ..., p_m$.

Se $d \in \boldsymbol{K}[x]$ é tal que $\boldsymbol{I} = \boldsymbol{K}[x].d$ então são válidas as seguintes propriedades:

a) $\exists\ r_1, ..., r_m \in \boldsymbol{K}[x]$ tais que $d = r_1.p_1 + ... + r_m.p_m$.

b) d é um divisor comum dos polinômios $p_1, p_2, ..., p_m$.

c) Se d' é um divisor comum qualquer dos polinômios $p_1, p_2, ... p_m$ então d' é também um divisor de d.

Observação 2.6: Um polinômio que satisfaz as condições (b) e (c) citadas acima, chama-se um *MDC* de $p_1, ..., p_m$ em $\boldsymbol{K}[x]$. E se d é um *MDC* de $p_1, ..., p_m$ em $\boldsymbol{K}[x]$ e $a \in \boldsymbol{K}$, $a \neq 0$ então $a.d$ é também um *MDC* em $\boldsymbol{K}[x]$ desses mesmos polinômios.

Demonstração: (do teorema 2.5)

a) Da igualdade $\boldsymbol{K}[x].d = \boldsymbol{K}[x].p_1 + ... + \boldsymbol{K}[x].p_m$ temos que existem polinômios $r_1, ..., r_n \in \boldsymbol{K}[x]$ tais que $d = r_1.p_1 + ... + r_n.p_n \in \boldsymbol{I}$.

b) Seja $i \in \{1, 2, ..., m\}$ e $\boldsymbol{K}[x].d = \boldsymbol{K}[x].p_1 + ... + \boldsymbol{K}[x].p_m$. Então, $p_i \in \boldsymbol{K}[x].p_i \subset \boldsymbol{K}[x].p_1 + ... + \boldsymbol{K}[x].p_m = \boldsymbol{K}[x].d$ e portanto $\exists\, r_i \in \boldsymbol{K}[x]$ tal que $p_i = r_i.d$, ou seja, d é um divisor de cada p_i, $i = 1,2,...,m$.

c) Seja d' um divisor comum em $\boldsymbol{K}[x]$, de $p_1, ...,p_m$, isto é, existe $r_i \in \boldsymbol{K}[x]$ tal que $p_i = r_i.d'$, para $i = 1,2,...,m$.

Assim, $\boldsymbol{K}[x].p_i \subset \boldsymbol{K}[x].d'$ qualquer que seja $i \in \{1,2,..,m\}$ daí segue que, $\boldsymbol{K}[x].d = \boldsymbol{K}[x].p_1 + ... + \boldsymbol{K}[x].p_m \subset \boldsymbol{K}[x].d'$, ou seja, existe $r \in \boldsymbol{K}[x]$ tal que $d = r.d'$. □

Se $p_1, ..., p_m \in \boldsymbol{K}[x] - \{0\}$ então pode-se provar que existe um único polinômio mônico que é um MDC de $p_1, ..., p_m$ *em* $\boldsymbol{K}[x]$, o qual denotamos por $MDC_{\mathbf{K}}\{p_1, ..., p_m\}$.

Definição 2.12: Se $MDC_{\mathbf{K}}\{p_1, ..., p_m\} = 1$ dizemos que os polinômios são relativamente primos em $\boldsymbol{K}[x]$.

Observação 2.7: Se $MDC_{\mathbf{K}}\{p_1, ..., p_m\} = 1$ então existem $r_1, ..., r_m \in \boldsymbol{K}[x]$ tais que $r_1p_1 + ... + r_mp_m = 1$ (veja itam a) do teorema 2.5).

Polinômios irredutíveis e ideais maximais.

Seja $\boldsymbol{K}$ um corpo e $\boldsymbol{K}[x]$ o domínio dos polinômios sobre $\boldsymbol{K}$ na indeterminada x.

Definição 2.13: Seja $f \in \boldsymbol{K}[x]$ tal que *grau* $f \geq 1$. Dizemos que f é um polinômio irredutível sobre $\boldsymbol{K}$ se toda vez que $f = g.h$, sendo que $g \in \boldsymbol{K}[x]$ e $h \in \boldsymbol{K}[x]$ então temos $g = a$ constante não nula em $\boldsymbol{K}$, ou $h = b$ constante não nula em $\boldsymbol{K}$. Se f não for irredutível sobre $\boldsymbol{K}$ dizemos que f é redutível sobre $\boldsymbol{K}$.

Observação 2.8: Todo polinômio de *grau 1* é irredutível.

Demonstração:

Seja $f \in \boldsymbol{K}[x]$ onde $grau(f) = 1$, se $f = g.h$ temos então que $grau(f) = grau(g) + grau(h)$. Como $grau(f) = 1$ então $1 = grau(g) + grau(h)$ e daí $grau(g) = 0$ ou $grau(h) = 0$. Conseqüentemente g $\in \boldsymbol{K}$ *ou* $h \in \boldsymbol{K}$. □

Definição 2.14: Seja $\boldsymbol{A}$ um anel comutativo com unidade e $\boldsymbol{I}$ um ideal de **A**. Então dizemos que ***I é ideal maximal***, se e somente se, $\boldsymbol{I} \neq \boldsymbol{A}$ e para todo ideal $\boldsymbol{M}$ de $\boldsymbol{A}$ tal que $\boldsymbol{I} \subset M \subset \boldsymbol{A}$, tivermos $\boldsymbol{M} = \boldsymbol{I}$ ou $\boldsymbol{M} = \boldsymbol{A}$.

Teorema 2.6: Se $\boldsymbol{A}$ é anel comutativo com unidade. Então $\boldsymbol{I}$ é ideal maximal, se e somente se, $\boldsymbol{A/I}$ é um corpo.

Demonstração:

($\Rightarrow$) Suponhamos $\boldsymbol{I}$ ideal maximal de $\boldsymbol{A}$, e seja $[0] \neq [a] \in \boldsymbol{A/I}$. Devemos provar que existe $[b] \in \boldsymbol{A/I}$ tal que $[a].[b] = [1]$. Se $\boldsymbol{L} = \boldsymbol{A}.a$ ideal principal de $\boldsymbol{A}$ gerado por a, temos que: $\boldsymbol{I} + \boldsymbol{L} = \{x + y: x \in \boldsymbol{I}, y \in \boldsymbol{L}\}$ é um ideal de $\boldsymbol{A}$ contendo $\boldsymbol{I}$, e mais $[a] \neq 0$ se e somente se $a \notin \boldsymbol{I}$. Como $a = 1.a \in \boldsymbol{L} \subset \boldsymbol{I} + \boldsymbol{L}$ temos que $\boldsymbol{I} + \boldsymbol{L}$ é um ideal que contêm $\boldsymbol{I}$ e mais $\boldsymbol{I} + \boldsymbol{L} \neq \boldsymbol{I}$.

Pela maximalidade de $\boldsymbol{I}$ segue que $\boldsymbol{A} = \boldsymbol{I} + \boldsymbol{L}$ e daí vem, $1 \in \boldsymbol{I} + \boldsymbol{L} \Rightarrow \exists\ u \in \boldsymbol{I}, v \in \boldsymbol{L}$ tais que $1 = u + v$.

Mas $v \in \boldsymbol{L} = \boldsymbol{A}.a$ e temos que $v = b.a$ para algum $b \in \boldsymbol{A}$, ou seja, $\exists\, b \in \boldsymbol{A}$, $\exists\, u \in \boldsymbol{I}$ tais que $1 = u + b.a$.

Ora tomando as classes em ambos os membros, segue que, $[1] = [u + b.a] = [u] + [b].[a] = [0] + [b].[a]$, isto é, $[a].[b] = [1]$.

($\Leftarrow$)Suponhamos que $\boldsymbol{A/I}$ seja um corpo. Assim $[0],[1] \in \boldsymbol{A/I} \Rightarrow \boldsymbol{I} \neq \boldsymbol{A}$.

Se $\boldsymbol{M} \neq \boldsymbol{I}$ é um ideal de $\boldsymbol{A}$ e $\boldsymbol{I} \subset M \subset \boldsymbol{A}$, então temos que existe $a \in \boldsymbol{M}$, $a \notin \boldsymbol{I}$, ou seja, $[a] \neq [0]$. Como $\boldsymbol{A/I}$ é corpo $\exists\, b \in \boldsymbol{A}$ tal que $[a].[b] = [1]$; ou ainda, $a.b \equiv 1 \ (mod\ \boldsymbol{I})$.

Mas, $a.b \equiv 1 \ (mod\ \boldsymbol{I})$ se e somente se $a.b - 1 \in \boldsymbol{I}$. Logo existem $\exists\, u \in \boldsymbol{I}$ tal que $a.b - 1 = u$, e isto nos diz que, $1 = a.b - u$.Como $a \in \boldsymbol{M}$ segue $a.b \in \boldsymbol{M}$ e como $u \in \boldsymbol{I} \subset \boldsymbol{M}$ temos também $u \in \boldsymbol{M}$. Logo concluímos que $1 = a.b - u \in \boldsymbol{M}$ e imediatamente temos $\boldsymbol{M} = \boldsymbol{A}$. Portanto $\boldsymbol{I}$ é ideal maximal de $\boldsymbol{A}$.□

Teorema 2.7: Sejam $\boldsymbol{K}$ um corpo e $p \in \boldsymbol{K}[x]$. Então as seguintes condições são equivalentes:

a) p é irredutível sobre $\boldsymbol{K}$.

b) $I = \boldsymbol{K}[x].p$ é um ideal maximal em $\boldsymbol{K}[x]$

c) $\boldsymbol{K}[x]/\boldsymbol{I}$ é um corpo, onde $\boldsymbol{I} = \boldsymbol{K}[x].p$.

Demonstração:

Queremos mostrar que $\boldsymbol{I} = [p] = p.\boldsymbol{K}[x]$ é ideal maximal em $\boldsymbol{K}[x]$.

a)$\Rightarrow$ b). Seja $\boldsymbol{I} = \boldsymbol{K}[x].p = \{g.p : g \in \boldsymbol{K}[x]\}$.

Como $grau(p) \geq 1$ temos imediatamente que $\boldsymbol{I} \neq \boldsymbol{K}[x]$, pois $1 \notin \boldsymbol{I}$.

Seja $\boldsymbol{J} = \boldsymbol{K}[x].h$ (lembremos que todo ideal de $\boldsymbol{K}[x]$ é ideal principal) um ideal de $\boldsymbol{K}[x]$ tal que $\boldsymbol{I} \subset \boldsymbol{J}$ vamos provar que $\boldsymbol{J} = \boldsymbol{I}$ ou $J = \boldsymbol{K}[x]$. De fato, $p \in \boldsymbol{K}[x].p \subset \boldsymbol{K}[x].h$, nos diz que, $p = g.h$ para algum $g \in \boldsymbol{K}[x]$. Como p é irredutível temos que $g \in \boldsymbol{K}^*$ ou $h \in \boldsymbol{K}^*$.

Se $g \in \boldsymbol{K}^*$ temos que $h = g^{-1}.p$ e portanto $J = \boldsymbol{K}[x].h \subset \boldsymbol{K}[x].p = \boldsymbol{I}$. Logo $\boldsymbol{J} = \boldsymbol{I}$.

Se $h \in \boldsymbol{K}^*$ temos que $1 \in \boldsymbol{J}$, logo $\boldsymbol{J} = \boldsymbol{K}[x]$.

b)⇒a) Seja $\boldsymbol{I} = \boldsymbol{K}[x].p$ um ideal maximal em $\boldsymbol{K}[x]$. Assim $\boldsymbol{I} \neq \boldsymbol{K}[x]$ temos que $grau(p) \geq 1$.

Suponhamos g e $h \in \boldsymbol{K}[x]$ e $p = g.h$. Segue então que $\boldsymbol{I} \subset \boldsymbol{J} = \boldsymbol{K}[x].h$ e como $\boldsymbol{I}$ é maximal temos que $\boldsymbol{I} = \boldsymbol{J}$ ou $\boldsymbol{J} = \boldsymbol{K}[x]$.

Se $\boldsymbol{I} = \boldsymbol{J}$ então $h \in \boldsymbol{I} = \boldsymbol{K}[x].p$ então temos que $h = f.p$ para algum $f \in \boldsymbol{K}[x]$. Daí segue que $p = g.f.p$. Como $p \neq 0$ e $\boldsymbol{K}[x]$ é um domínio de integridade teremos $1 = g.f$, ou seja, $g \in \boldsymbol{K}^*$ (pois $grau(g) = 0$).

Se $\boldsymbol{J} = \boldsymbol{K}[x]$ teremos que $1 \in \boldsymbol{J}$, então existe $t \in \boldsymbol{K}[x]$ *tal que* $t.h = 1$, ou seja, $h \in \boldsymbol{K}^*$. Consequentemente p é irredutível em $\boldsymbol{K}$.

b) ⇔ c) A equivalência sai diretamente do teorema 2.6. □

Fatoração única

Definição 2.15: Seja $\boldsymbol{D}$ um domínio, dizemos que ***D é um domínio de fatoração*** **única** se todo elemento $x \in \boldsymbol{A} - \{0\}$ pode ser escrito na forma, $f = u.r_1...r_m$ (tendo a possibilidade de $f = u$ quando $m = 0$) onde os $r_{i's}$ são elementos irredutíveis (não necessariamente distintos) e u *é um elemento inversível de* $\boldsymbol{A}$. Essa expressão é única a menos da constante u e da ordem dos elementos $r_1...r_m$.

Vamos provar agora que $\boldsymbol{K}[x]$ é um domínio de fatoração única.

Teorema 2.8: Seja $\boldsymbol{K}$ um corpo. Então todo polinômio $f \in \boldsymbol{K}[x] - \{0\}$ pode ser escrito na forma, $f = u.p_1...p_m$ onde os $p_{i's}$ são polinômios irredutíveis sobre $\boldsymbol{K}$ (não necessariamente distintos) e $u \in \boldsymbol{K}\text{-}\{0\}$. Essa expressão é única a menos da constante u e da ordem dos polinômios $p_1...p_m$.

Demonstração:

Seja $f \in \boldsymbol{K}[x] - \{0\}$. Provaremos por indução sobre $grau(f) = n$.

Se $n = 0$ teremos $f = u$, sendo uma constante não nula. Assim, podemos assumir $grau(f) = n \geq 1$.

Se f é irredutível não há nada para demonstrar (toma-se $m = 1$, $u = 1$ e $p_1 = f$). Se não, f é um polinômio redutível sobre $\boldsymbol{K}$. Assim, existem polinômios $g, q \in \boldsymbol{K}[x]$, onde $1 \leq grau(g) < n$, e $1 \leq grau(q) < n$ tais que $f = g.q$.

Por hipótese de indução temos que $g = a.p_1....p_r$, com $a \in \boldsymbol{K}[x] - \{0\}$ e $p_1,...,p_r$ polinômios irredutíveis sobre $\boldsymbol{K}$. Também temos que $h = bp_{r+1}...p_m$, $b \in k - \{0\}$ e $p_{r+1},....,p_m$ polinômios irredutíveis sobre $\boldsymbol{K}$. Deste modo

$$p = (ab).p_1....p_r\ p_{r+1}....p_m$$

sendo $u = a.b$ uma constante não nula e os $p_{i's}$ polinômios irredutíveis sobre $\boldsymbol{K}$.

Demonstraremos agora a unicidade da expressão.

Suponhamos $f = u.p_1...p_m = u'.q_1....q_s$ onde u e $u' \in \boldsymbol{K} - \{0\}$ e $p_1,...,p_m$, $q_1,...,q_s$ são polinômios irredutíveis sobre $\boldsymbol{K}$.

Usaremos indução sobre m.

Se $m = 0$ temos que $s = 0$ pois os $q_{i's}$ são polinômios irredutíveis sobre $\boldsymbol{K}$, resultando que $f = u$ onde $u \in \boldsymbol{K}-\{0\}$.

Suponhamos $m \geq 1$.

Assim temos, $p_1 \setminus (q_1 ..q_s)$ daí segue que existe $u_i \in \boldsymbol{K} - \{0\}$ tal que $q_i = u_i.p_1$.

De $p_i = u_i.p_1$ e sendo $\boldsymbol{K}[x]$ um domínio temos que: $u.p_2...p_m = (u.u_i).(q_1...q_{i-1})(.q_{i+1}...q_s)$ daí segue pela hipótese de indução que $m - 1 = s - 1$ (ou seja, $m = s$) e cada q_i está associado com algum p_i através de uma constante.

Isto finaliza a demonstração do teorema. □

Corolário 2.6: Sejam $\boldsymbol{K}$ um corpo e $f_1, f_2 \in \boldsymbol{K}[x]$ dois polinômios primos entre si; seja $h \in \boldsymbol{K}[x]$. Então:

1) É possível calcular efetivamente $g_1, g_2 \in \boldsymbol{K}[x]$
   tais que $h = g_1.f_1 + g_2.f_2$.
2) Se $grau(h) < grau(f_1) + grau(f_2)$, tais g_1 e g_2 podem ser tomados com
   $\{grau(g_1) < grau(f_2)$ (ou $g_1 = 0)$ $grau(g_2) < grau(f_1)$ (ou $g_2=0)$

Demonstração:

1) Sabemos que a divisão em $\boldsymbol{K}[x]$ é efetiva. Como f_1 e f_2 são primos entre si, podemos efetivamente encontrar (pelo teorema 2.5) dois polinômios φ_1 e $\varphi_2 \in \boldsymbol{K}[x]$ tais que $1 = \varphi_1.f_1 + \varphi_2.f_2$, logo para qualquer polinômio $h \in \boldsymbol{K}[x]$ temos que $h = h.\varphi_1.f_1 + h.\varphi_2 f_2$. Portanto basta tomarmos $g_1 = h.\varphi_1$ e $g_2 = h.\varphi_2$.

2) Pela proposição 2.1 podemos efetivamente encontrar $q, r \in \boldsymbol{K}[x]$ tais que $g_1 = f_2.q + r$ com $grau(r) < grau(f_2)$ *ou* $r = 0$.

Tem-se então $h = r.f_1 + [f_1.q + g_2].f_2$ como $grau(h) < grau(f_1) + grau(f_2)$ e também $grau(r.f_1) < grau(f_1) + grau(f_2)$ *(ou* $r = 0$*)*, então temos que $grau([f_1 q + g_2].f_2) < grau(f_1) + grau(f_2)$ (ou $f_1.q + g_2 = \boldsymbol{0}$), portanto, $f_1.q + g_2$ tem grau menor que grau de f_1 (ou é o polinômio nulo). Logo os polinômios r e $(f_1.q + g_2)$ têm as propriedades desejadas. □

Definição 2.16: Seja $F(x) = a_n x^n + ... + a_1 x \in \boldsymbol{D}[x]$. O conteúdo de $f(x)$ é o $M.D.C.\{a_n, ..., a_0\}$, e será denotado por $c(f(x))$. Dizemos que $f(x)$ é primitivo em $\boldsymbol{D}[x]$ se o conteúdo de $f(x)$ é um elemento invertível de $\boldsymbol{D}$, isto é, de maneira equivalente, se $f(x)$ não tem fator não-trivial de grau zero.

Lema 2.1 (Gauss): Sejam $\boldsymbol{D}$ um domínio fatorial e $\boldsymbol{K}$ seu corpo de frações.

1) Se $g \in \boldsymbol{D}[x]$ tem $grau \geq 1$, então:
   a) g não é um produto de dois fatores de $grau \geq 1$ em $\boldsymbol{D}[x]$ se e somente se g não é um produto de dois fatores de $grau \geq 1$ em $\boldsymbol{K}[x]$ (isto é g é irredutivel em K[x])
   b) g é irredutível em $\boldsymbol{D}[x]$ se e só se g é primitivo em $\boldsymbol{D}[x]$ e g é irredutível em $\boldsymbol{K}[x]$
2) Sejam g, h polinômios primitivos em $\boldsymbol{D}[x]$. Então g e h são associados em $\boldsymbol{D}[x]$ se e somente se g e h são associados em $\boldsymbol{K}[x]$
3) Se f e $g \in \boldsymbol{D}[x]$, então $c.(f.g) = c.(f).c.(g)$

Demonstração: Ver referência [4]

Teorema 2.9 (Gauss): Seja $\boldsymbol{D}$ um domínio fatorial. Então $\boldsymbol{D}[x]$ é um domínio fatorial.

Demonstração

Seja $f(x) \in \boldsymbol{D}[x] \subset \boldsymbol{K}[x]$.

Existência de uma fatoração em elementos irredutíveis em $\boldsymbol{D}[x]$. Escreva $f = d.f_1$, onde $d \in \boldsymbol{D}$ é o conteúdo de f e f_1 é primitivo em $\boldsymbol{D}[x]$. Como $\boldsymbol{D}$ é fatorial, d possui uma fatoração $d = p_1...p_t$ com $p_1...p_t$ irredutiveis em $\boldsymbol{D}$ e portanto irredutíveis em $\boldsymbol{D}[x]$. Como $f_1 \in \boldsymbol{D}[x] \subset \boldsymbol{K}[x]$, f_1 possui uma fatoração em $\boldsymbol{K}[x]$, digamos $f_1 = q_1...q_r$ com $q_i \in \boldsymbol{K}[x]$, q_i irredutível em $\boldsymbol{K}[x]$ $\forall\, i = 1,...,r$. Escreva $q_i = (a_i/b_i).q_i'$ com $a_i,\ b_i \in \boldsymbol{D}$, com $b_i \neq 0$ e $q_i' \in \boldsymbol{D}[x]$ primitivo; q_i sendo irredutível em $\boldsymbol{K}[x]$, q_i' é irredutível em $\boldsymbol{K}[x]$, logo pelo lema 2.1, q_i' é irredutível em $\boldsymbol{D}[x]$. Temos então $f_1 = q_1...q_r = (a_1...a_r/b_1...b_r).q_i'...q_r'$ e portanto $b_1....b_r.f_1 = a_1...a_r.q_i'...q_r'$.

Como f_1 *e* q_i' são primitivos, temos que $b_1...b_r$ e $a_1...a_r$ são associados em $\boldsymbol{D}$. Logo $(a_1...a_r/b_1...b_r)$ é um elemento invertível de $\boldsymbol{D}$. Denotando este elemento por η, temos que $f = \eta.p_1...p_t.q_1'...q_r'$ é uma fatoração de f em elementos irredutíveis de $\boldsymbol{D}[x]$.

Unicidade da fatoração.

Sejam $f = p_1....p_t.q_1...q_r$, (onde $p_1...p_t$ são fatores irredutíveis de *grau 0* e $q_1...q_r$ são fatores irredutíveis de *grau* ≥ 1) duas fatorações de f em $\boldsymbol{D}[x]$. Como $p_1...p_t$ e $u_1...u_t'$ são ambos conteúdos de f, logo $p_1...p_t = \varepsilon u_1...u_t'$ com ε invertível em $\boldsymbol{D}$. Pela unicidade da fatoração em $\boldsymbol{D}$, temos que $t = t'$, módulo a ordem, e que p_i e u_i são associados em $\boldsymbol{D}$ e logo também em $\boldsymbol{D}[x]$. Agora temos que $\varepsilon.q_1...q_r = v_1...v_r$, por hipótese os q_i e os v_i são irredutíveis em $\boldsymbol{D}[x]$ e de *grau* ≥ 1, logo pelo lema 2.1 são irredutíveis em $\boldsymbol{K}[x]$. Pela unicidade da fatoração em $\boldsymbol{K}[x]$ obtemos $r = r'$ e, módulo a ordem, que q_i e v_i são associados em $\boldsymbol{K}[x]$ e irredutíveis em $\boldsymbol{D}[x]$ de *grau* ≥ 1, então eles são primitivos em $\boldsymbol{D}[x]$, e portanto, são associados em $\boldsymbol{D}[x]$ (pelo lema 2.1). □

Resultante de dois Polinômios

Definição 2.17: Seja ***D*** um domínio. Sejam $f = a_0x^n + a_1x^{n-1} + ... + a_n$, com $a_0 \neq 0$ e $g = b_0x^m + b_1x^{m-1} + ... + b_m$, com $b_0 \neq 0$ dois polinômios em $\boldsymbol{D}[x]$ de *grau* ≥ 1. A resultante de *f*, *g*, denotada por $R_{f,g}$, é o elemento do domínio ***D*** dado pelo determinante da seguinte matriz:

$$R = \begin{bmatrix} a_0 & a_1 & \ldots & a_{n-1} & a_n & & \\ & a_0 & a_1 & \ldots & a_{n-1} & a_n & \\ & & \vdots & & \ldots & & \\ & & & a_0 & a_1 & \ldots & a_{n-1} & a_n \\ b_0 & b_1 & \ldots & b_{n-1} & b_n & & \\ & b_0 & b_1 & \ldots & b_{n-1} & b_n & \\ & & & \vdots & & & \\ & & & b_0 & b_1 & \ldots & b_{n-1} & b_n \end{bmatrix}$$

Ou seja, $R_{f,g} = \det(R)$.

sendo que existem m linhas de a_i's e *n* linhas de b_i's as quais são completadas com zeros. A resultante entre um polinômio *f* e sua derivada *f'* (quando *f'* não é constante) é chamada discriminante de *f*.

Exemplo 2.5: Seja $f = ax^2 + bx + c$. Vamos calcular o discriminante de *f:*

Solução: $f = ax^2 + bx + c$

$f' = 2ax + b$

$$R = \begin{bmatrix} a & b & c \\ 2a & b & 0 \\ 0 & 2a & b \end{bmatrix}$$

$$Det(R): = -a(b^2 - 4*a*c)$$

Notemos que quando *"a"* é diferente de zero o discriminante de f é igual a zero, se e somente se, $b^2 - 4*a*c = 0$ que coincide com o discriminante da fórmula de Báskara.

Teorema 2.10: Seja $\boldsymbol{D}$ um domínio. Sejam $f = a_0x^n + a_1x^{n-1} + ... + a_n$, com $a_0 \neq 0$ e $g = b_0x^m + b_1x^{m-1} + ... + b_m$, com $b_0 \neq 0$ dois polinômios em $\boldsymbol{D}[x]$ de *grau* ≥ 1 . Então:

1) As seguintes condições são equivalentes:

   (i) $R_{f,g} = 0$

   (ii) Existem polinômios $0 \neq f_1 \in \boldsymbol{D}[x]$ de *grau* $\leq (n-1)$, $0 \neq g_1 \in \boldsymbol{D}[x]$ de *grau* $\leq (m-1)$ tais que $f_1.g = g_1.f$.

2) Se $\boldsymbol{D}$ é um domínio fatorial, essas condições são também equivalentes a:

   (iii) f e g possuem um fator comum em $\boldsymbol{D}[x]$ de *grau* ≥ 1.

Antes de demonstrarmos o teorema 2.10 vamos fazer um exemplo para melhor compreensão da demonstração.

Exemplo 2.6: Sejam $f = x^5 + 3x^3 + x^2 + 2x + 1$ e $g = x^4 + 3x^3 + 3x^2 + 3x + 2$

$$R = \begin{bmatrix} 1 & 0 & 3 & 1 & 2 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 3 & 1 & 2 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 3 & 1 & 2 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 3 & 1 & 2 & 1 \\ 1 & 3 & 3 & 3 & 2 & 0 & 0 & 0 & 0 \\ 0 & 1 & 3 & 3 & 3 & 2 & 0 & 0 & 0 \\ 0 & 0 & 1 & 3 & 3 & 3 & 2 & 0 & 0 \\ 0 & 0 & 0 & 1 & 3 & 3 & 3 & 2 & 0 \\ 0 & 0 & 0 & 0 & 1 & 3 & 3 & 3 & 2 \end{bmatrix}$$

$$R_{f,g} = 0$$

Queremos encontrar $f_1 \neq 0$ e $g_1 \neq 0$ tais que $f_1.g = g_1.f$.

Vamos tomar f_1 e g_1 genéricos, sendo $f_1 = a_1x^4 + a_2x^3 + a_3x^2 + a_4x + a_5$ e $g_1 = b_1x^3 + b_2x^2 + b_3x + b_4$, vamos calcular $h = f_1.g$ e $h_1 = g_1.f$, ou seja,.

$$h := 3\,a_1\,x^6 + a_2\,x^7 + 3\,a_1\,x^5 + 3\,a_4\,x^3 + 3\,a_4\,x^2 + a_5\,x^4 + 3\,a_5\,x^3 + 3\,a_5\,x^2 + 3\,a_5\,x + 3\,a_2\,x^6 + 3\,a_2\,x^5 + 3\,a_2\,x^4 + a_3\,x^6 + 3\,a_3\,x^5 + 3\,a_3\,x^4 + 3\,a_3\,x^3 + a_4\,x^5 + 3\,a_4\,x^4 + 2\,a_5 + 2\,a_1\,x^4 + 2\,a_2\,x^3 + 2\,a_3\,x^2 + 2\,a_4\,x + a_1\,x^8 + 3\,a_1\,x^7$$

$$h1 := b_1\,x^8 + 3\,b_1\,x^6 + b_1\,x^5 + 2\,b_1\,x^4 + b_1\,x^3 + b_2\,x^7 + 3\,b_2\,x^5 + b_2\,x^4 + 2\,b_2\,x^3 + b_2\,x^2 + b_3\,x^6 + 3\,b_3\,x^4 + b_3\,x^3 + 2\,b_3\,x^2 + b_3\,x + b_4\,x^5 + 3\,b_4\,x^3 + b_4\,x^2 + 2\,b_4\,x + b_4$$

A igualdade de polinômios nos leva ao seguinte sistema homogêneo,

$$a_1 = b_1$$

$$a_2 + 3\,a_1 = b_2$$

$$3\,a_1 + 3\,a_2 + a_3 = 3\,b_1 + b_3$$

$$3\,a_1 + 3\,a_2 + 3\,a_3 + a_4 = b_1 + 3\,b_2 + b_4$$

$$a_5 + 3\,a_2 + 3\,a_3 + 3\,a_4 + 2\,a_1 = 2\,b_1 + b_2 + 3\,b_3$$

$$3\,a_4 + 3\,a_5 + 3\,a_3 + 2\,a_2 = b_1 + 2\,b_2 + b_3 + 3\,b_4$$

$$3\,a_4 + 3\,a_5 + 2\,a_3 = b_2 + 2\,b_3 + b_4$$

$$3\,a_5 + 2\,a_4 = b_3 + 2\,b_4$$

$$2\,a_5 = b_4$$

cuja matriz é

$$M = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & -1 & 0 & 0 & 0 \\ 3 & 1 & 0 & 0 & 0 & 0 & -1 & 0 & 0 \\ 3 & 3 & 1 & 0 & 0 & -3 & 0 & -1 & 0 \\ 3 & 3 & 3 & 1 & 0 & -1 & -3 & 0 & -1 \\ 2 & 3 & 3 & 3 & 1 & -2 & -1 & -3 & 0 \\ 0 & 2 & 3 & 3 & 3 & -1 & -2 & -1 & -3 \\ 0 & 0 & 2 & 3 & 3 & 0 & -1 & -2 & -1 \\ 0 & 0 & 0 & 2 & 3 & 0 & 0 & -1 & -2 \\ 0 & 0 & 0 & 0 & 2 & 0 & 0 & 0 & -1 \end{bmatrix}$$

Comparando a matriz do sistema homogêneo com a matriz da resultante percebemos que as quatro primeiras linhas da matriz da resultante são iguais as quatro ultimas colunas

da matriz do sistema respectivamente multiplicadas por -1, e que as cinco últimas linhas da matriz da resultante são iguais as cinco primeiras colunas da matriz do sistema. Conclusão $0 = R_{f,g} = \pm det(M)$. Logo vão existir f_1 e g_1, ambas não nulas tais que $f_1 g = g_1 f$. resolvendo o sistema encontramos uma solução particular, $f_1 = 4x^4 - 13x^3 + 8x^2 - 22x - 13$ e $g_1 = 4x^3 - x^2 - 31x - 26$. Mas sabemos que existem infinitas soluções possíveis.

Demonstração: (Teorema 2.10)

1) Encontrar $0 \neq f_1 = \alpha_1 x^{n-1} + \alpha_2 x^{n-2} + ... + \alpha_n$ e $0 \neq g_1 = \beta_1 x^{m-1} + \beta_2 x^{m-2} + ... + \beta_m$ em $\boldsymbol{D}[x]$ tais que $f_1.g = g_1.f$, ou seja, encontrar uma solução não-trivial em $\boldsymbol{D}$ do seguinte sistema de $(n + m)$ equações nas incógnitas $\beta_1, \beta_2, ..., \beta_m, \alpha_1, \alpha_2, ..., \alpha_n$:

$$\begin{array}{ll} \text{(termo em } x^{n+m-1}\text{)} & a_0.\,\beta_1 - b_0.\alpha_1 = 0 \\ \text{(termo em } x^{n+m-2}\text{)} & a_1.\,\beta_1 + a_0.\,\beta_2 - b_1.\,\alpha_1 - b_0.\alpha_2 = 0 \\ \text{.....} & \text{.....} \\ \text{.....} & \text{.....} \\ \text{(termo constante)} & a_n.\,\beta_m - b_m.\,\alpha_n = 0 \end{array}$$

Agora, podemos ver que existe uma solução não trivial deste sistema em $\boldsymbol{D}$ se e só se existe uma tal solução no corpo de frações $\boldsymbol{K}$ de $\boldsymbol{D}$, ou seja, pela regra de Cramer, se e só se o determinante da matriz M dos coeficientes do sistema é nulo. Isto ocorre, se e só se $R_{f,g} = 0$. De fato, cada coluna $1 \geq j \leq n$ de M é igual a linha correspondente da matriz usada na definição de $R_{f,g}$ e cada coluna $n+1 \geq j \leq n+m$ de M é igual a linha correspondente da matriz usada na definição de $R_{f,g}$ multiplicada por (-1), deste modo temos que $det(M) = \pm R_{f,g}$.

2) iii)$\Rightarrow$ii) Como f e g possuem um fator comum p em $\boldsymbol{D}[x]$ de $grau \geq 1$, então temos:

$f = p.f_1$ com $f_1 \in \boldsymbol{D}[x]$, $grau(f_1) < n$

$g = p.g_1$ com $g_1 \in \boldsymbol{D}[x]$, $grau(g_1) < m$

e, claramente, $f_1.g = g_1.f$.

ii)⇒iii) Sejam $f_1, g_1 \in \boldsymbol{D}[x]$ tais que $f_1.g = g_1.f$. Sendo $\boldsymbol{D}[x]$ um domínio fatorial, todos os fatores irredutíveis de *grau* ≥ 1 de f aparecem no produto $f_1.g$, nem todos eles podem aparecer em f_1 pois, por hipótese, temos *grau* f_1 < *grau(f)*; assim, pelo menos um dos fatores irredutíveis de *grau* ≥ 1 de f aparece em g. □

Exemplo 2.7: Seja $f = x^2 + 2x + 1$ *e* $g = x^3 + x^2 \in \boldsymbol{Z}[x]$, determine $R_{f,g}$.

Solução: $f = x^2 + 2x + 1$, $n = 2$ onde $a_0 = 1$, $a_1 = 2$ e $a_2 = 1$

$g = x^3 + x^2 + 0x + 0$, $m = 3$, onde $b_0 = 1$, $b_1 = 1$, $b_2 = 0$ e $b_3 = 0$

$$A = \begin{bmatrix} 1 & 2 & 1 & 0 & 0 \\ 0 & 1 & 2 & 1 & 0 \\ 0 & 0 & 1 & 2 & 1 \\ 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 \end{bmatrix}$$

$$R_{f,g} = det(A) = 0$$

Como $R_{f,g} = 0$, então temos que f e g possuem um fator comum em $\boldsymbol{D}[x]$ de *grau* ≥ 1.

Fatorando as expressões teremos:

$f = x^2 + 2x + 1 = (x + 1)^2$ e $g = x^3 + x^2 = (x + 1)x^2$

Logo, o fator comum entre f e g é $(x + 1)$.

Exemplo 2.8: Seja $f = x^3 + 7x^2 + 16x + 12$ e $g = x^5 - 2x^3 - 2x^2 + 4 \in \boldsymbol{Z}[x]$, determine $R_{f,g}$:

Solução: $f = x^3 + 7x^2 + 16x + 12$ onde $a_0 = 1$, $a_1 = 7$, $a_2 = 16$ e $a_3 = 12$

$g = x^5 + 0x^4 - 2x^3 - 2x^2 + 0x + 4$ onde $b_0 = 1$, $b_1 = 0$, e $b_2 = -2$, $b_3 = -2$,

$b_4 = 0$ e $b_5 = 4$.

$$R = \begin{bmatrix} 1 & 7 & 16 & 12 & 0 & 0 & 0 & 0 \\ 0 & 1 & 7 & 16 & 12 & 0 & 0 & 0 \\ 0 & 0 & 1 & 7 & 16 & 12 & 0 & 0 \\ 0 & 0 & 0 & 1 & 7 & 16 & 12 & 0 \\ 0 & 0 & 0 & 0 & 1 & 7 & 16 & 12 \\ 1 & 0 & -2 & -2 & 0 & 4 & 0 & 0 \\ 0 & 1 & 0 & -2 & -2 & 0 & 4 & 0 \\ 0 & 0 & 1 & 0 & -2 & -2 & 0 & 4 \end{bmatrix}$$

$$R_{f,g} = det(R) = -81200$$

Como $R_{f,g} = -81200 \neq 0$, temos que f e g não possuem um fator comum. Se fatorarmos as expressões temos:

$f = x^3 + 7x^2 + 16x + 12 = (x + 2)^2(x + 3)$

$g = x^5 - 2x^3 - 2x^2 + 4 = (x^2 - 2)(x^3 - 2)$. Portanto, pela fatoração verificamos novamente que f e g não possuem um fator comum.

Corolário 2.7: Sejam $\boldsymbol{D} \subset \boldsymbol{D'}$ dois domínios, $\boldsymbol{D}$ fatorial. Sejam $f, g \in \boldsymbol{D}[x]$ de $grau \geq 1$. Então, f e g têm um fator comum de $grau \geq 1$ em $\boldsymbol{D}[x]$ se e só se eles têm um fator comum de $grau \geq 1$ em $\boldsymbol{D'}[x]$.

Demonstração:

Se f e g têm um fator comum de $grau \geq 1$ em $\boldsymbol{D'}[x]$ então pela implicação iii)⇒ii) do teorema 2.10 temos que $R_{f,g} = 0$ (pois não precisa supor $\boldsymbol{D'}$ fatorial). Logo f e g têm um fator comum de $grau \geq 1$ em $\boldsymbol{D}[x]$ (pela implicação i)⇒iii) do teorema 2.10).

Como f e g têm um fator comum de $grau \geq 1$ em $\boldsymbol{D}[x]$ (pela implicação i)⇒iii) do teorema 2.10) e por hipótese temos que $\boldsymbol{D}[x] \subset \boldsymbol{D'}[x]$, logo f e g têm um fator comum de $grau \geq 1$ em $\boldsymbol{D'}[x]$. □

Observação 2.9: Dados dois polinômios $f, g \in \boldsymbol{D}[x]$ de *grau* ≥ 1, é sempre possível calcular a resultante deles e consequentemente, quando $\boldsymbol{D}$ for fatorial, é possível determinar se eles têm ou não um fator comum de *grau* ≥ 1 (pelo teorema 2.10).

Proposição 2.3: Seja $\boldsymbol{D}$ um domínio. Sejam $f = a_0x^n + a_1x^{n-1} + ... + a_n$, $a_0 \neq 0$ e $g = b_0x^m + b_1x^{m-1} + ... + b_m$, $b_0 \neq 0$ dois polinômios em $\boldsymbol{D}[x]$ de *grau* ≥ 1. Então:

1) A resultante $R_{f,g}$ é uma soma de termos do tipo $\pm a_{i1},....,a_{im}b_{j1}...b_{jn}$ *com* $i_1 + ... + i_m + j_1 + ... + j_n = n.m$.

Demonstração:

1) $R_{f,g} = det(c_{ij})$ $1 \leq i, j \leq m + n$ onde

para $1 \leq i \leq m$, $c_{ij} = \begin{cases} a_{j-i} \text{ se } i \leq j \leq i + n \\ 0, \text{ caso contrário} \end{cases}$

para $m + 1 \leq i \leq m + n$, $c_{ij} = \begin{cases} b_{m+j-i} \text{ se } i - m \leq j \leq i \\ 0, \text{ caso contrário} \end{cases}$

Agora, $det(c_{ij})$ é uma soma de termos do tipo $\pm c_{1j1}.c_{2j2}...c_{mjm}.c_{m+1jm+1}...c_{m+njm+n}$, com $\{j_1,...,j_m,j_{m+1},...,j_{m+n}\} = \{1, 2 ,..., m + n\}$. Um tal termo é igual a zero ou igual a $\pm a_{j1-1}.a_{j2-2}...aj_{m-m}.b_{m+jm+1-(m+1)}...b_{m+jm+n-(m+n)}$.

A soma S dos índices deste termo é igual a:

$$S = (j_1 - 1) + (j_2\text{-}2) + ... + (j_m - m) + (j_{m+1} - 1) + ... + (j_{m+n} - n) =$$

$$= \sum_{k=1}^{m+n} j_k - \sum_{u=1}^{m} u - \sum_{v=1}^{n} v = \sum_{l=1}^{m+n} l - \sum_{u=1}^{m} u - \sum_{v=1}^{n} v = \left(\frac{n+m}{2}\right)(n+m+1) - \frac{m}{2}(m+1) - \frac{n}{2}(n+1) =$$

$$= \left(\frac{n}{2} + \frac{m}{2}\right)(n+m+1) - \frac{m^2}{2} - \frac{m}{2} - \frac{n^2}{2} - \frac{n}{2} = \frac{n^2}{2} + \frac{n.m}{2} + \frac{n}{2} + \frac{m.n}{2} + \frac{m^2}{2} + \frac{m}{2} - \frac{m^2}{2} -$$

$$- \frac{m}{2} - \frac{n^2}{2} - \frac{n}{2} = \frac{n.m}{2} + \frac{m.n}{2} = \frac{2.n.m}{2} = n.m \qquad \square$$

Faremos um exemplo prático para compreender melhor a relação dos elementos da matriz cujo determinante é $R_{f,g}$ (a resultante de f e g) com os coeficientes dos polinômios f e g.

Exemplo 2.9: $f(x) = x^2 + 1$, $g(x) = x - 1$

$f(x) = x^2 + 0x + 1$, $m = 2$, $a_0 = 1$, $a_1 = 0$, $a_2 = 1$

$g(x) = x - 1$, $n = 1$ $b_0 = 1$ $b_1 = -1$

$$R := \begin{bmatrix} 1 & 0 & 1 \\ 1 & -1 & 0 \\ 0 & 1 & -1 \end{bmatrix}$$

$$\det(R) = 2$$

$m = 1$
$n = 2$

$$1 \le i \le 1, \begin{cases} aj\text{-}i & \text{se } i \le j \le 3 \\ 0, & \text{caso contrário} \end{cases}$$

$$2 \le i \le 3, c_{ij} = \begin{cases} b_{m+}j\text{-}i & \text{se } i - 1 \le j \le i \\ 0, & \text{caso contrário} \end{cases}$$

Assim,

$$c_{1j} = \begin{cases} aj\text{-}i, & \text{se } 1 \le j \le 3 \\ 0, & \text{caso contrário} \end{cases}$$

$c_{11} = a_{1-1} = a_0 = 1$

$c_{12} = a_{2-1} = a_1 = 0$

$c_{13} = a_{3-1} = a_2 = 1$

$$c_{2j} = \begin{cases} b_{m+}j\text{-}i, & \text{se } 1 \le j \le 2 \\ 0, & \text{caso contrário} \end{cases}$$

$c_{21} = b_{1+1-2} = b_0 = 1$

$c_{22} = b_{1+2-2} = b_1 = -1$

$c_{23} = b_{1+3-2} = b_2 = 0$

$c_{3j} = \begin{cases} bm+j-i, \text{ se } 2 \leq j \leq 3 \\ 0, \text{ caso contrário} \end{cases}$

$c_{31} = 0$

$c_{32} = b_{1+2-3} = b_0 = 1$

$c_{33} = b_{1+3-3} = b_1 = -1$

Sejam $\boldsymbol{K}$ um corpo e $\boldsymbol{K}[x,y] = \boldsymbol{K}[x][y] = \boldsymbol{K}[y][x]$. Como $\boldsymbol{K}[x]$ é domínio temos que $\boldsymbol{K}[x,y]$ é domínio. Mas como $\boldsymbol{K}[x]$ não é corpo, vamos perder alguns resultados que eram válidos em $\boldsymbol{K}[x]$. Por exemplo, veremos a seguir que $\boldsymbol{K}[x,y]$ não será anel principal.

Proposição 2.4: Seja $\boldsymbol{K}$ um corpo. Então $\boldsymbol{K}[x,y]$ não é anel principal.

Demonstração:

Lembremos que $[x,y] = \{h.x + r.y: h, r \in \boldsymbol{K}[x,y]\}$ e que $[p] = \{s.p: s \in \boldsymbol{K}[x,y]\}$.

Suponhamos por absurdo que exista $p \in \boldsymbol{K}[x,y]$ tal que $[x] + [y] = [x,y] = [p]$. Então temos que

1) Existem h_0 e r_0 em $\boldsymbol{K}[x,y]$ tais que $h_0.x + r_0.y = p$

2) Existe $s_0 \in \boldsymbol{K}[x,y]$ tal que $x = 1.x + 0.y = s_0.p$

3) Existe $s_1 \in \boldsymbol{K}[x,y]$ tal que $y = 0.x + 1.y = s_1.p$

Denotemos $gr(f)$ = grau de f na variável y. Desde que $\boldsymbol{K}[x]$ é domínio temos que $0 = gr(x) = gr(s_0p) = gr(s_0) + gr(p) \Rightarrow gr(p) = 0 \Rightarrow p \in \boldsymbol{K}[x]$.

De modo análogo deduzimos que $p \in \boldsymbol{K}[y]$. Logo $p \in \boldsymbol{K}^*$.

Como $p \in \boldsymbol{K}^*$ então $p \in U(\boldsymbol{K}[x,y])$ e assim, $[p] = \boldsymbol{K}[x,y]$ o que é absurdo pois $1 \notin \boldsymbol{K}[x,y]$. Logo $\boldsymbol{K}[x,y]$ não é principal. □

Definição 2.18: Sejam $\boldsymbol{K}$ um corpo e $\alpha \in \boldsymbol{K}$ tal que $\alpha \neq 0$, definimos o grau do monômio $(\alpha x^i y^j)$ por $grau(\alpha x^i y^j) = i + j$. Se $f(x,y)$ é um polinômio não nulo em $\boldsymbol{K}[x,y]$, definimos o $grau(f)$ como sendo o maior grau dos monômios que aparecem em $f(x,y)$.

Dados $f(x,y)$, $g(x,y)$ dois polinômios em $\boldsymbol{K}[x,y]$ de *graus* $n, m \geq 1$, escrevemos:

$$f(x,y) = a_0 y^n + a_1 y^{n-1} + \ldots + a_n$$

$$g(x,y) = b_0 y^m + b_1 y^{m-1} + \ldots + b_m,$$

onde para cada i e j temos: $a_i \in \boldsymbol{K}[x]$ é nulo ou $grau(a_i) \leq$ i, e $b_j \in \boldsymbol{K}[x]$ é nulo ou $grau\ (b_j) \leq j$.

Exemplo 2.10: $f(x,y) = x^5 + x^3y^2 + x \in \boldsymbol{R[y]}[x]$

$f(x,y) = a_0x^5 + a_1x^4 + a_2x^3 + a_3x^2 + a_4x + a_5$, onde

$a_0 = 1$

$a_1 = 0$

$a_2 = y^2$

$a_3 = 0$

$a_4 = 1$

$a_5 = 0$

Exemplo 2.11: $g(x,y) = 3y^5 + x^3y^2 + xy + x + x^5 \in \boldsymbol{R[y]}[x]$

$g(x,y) = a_0y^5 + a_1y^4 + a_2y^3 + a_3y^2 + a_4y + a_5$ onde

$a_0 = 3$

$a_1 = 0$

$a_2 = 0$

$a_3 = x^3$

$a_4 = x$

$a_5 = x + x^5$

Exemplo 2.12:

a) $f_1 = x + xy^2$

$grau(f_1) = i + j = 1 + 2 = 3$

b) $f_2 = xy + x^2y + y^2x$

$grau(f_2) = 2 + 1 = 3$

c) $f_3 = x + x^2y^2$

$grau(f_3) = 2 + 2 = 4$

Denotamos por $V_{\mathbf{R}}(f)$ o conjunto dos pontos em $\boldsymbol{R}^2$ da curva plana afim determinada por $f(x,y) \in \boldsymbol{R}[x,y]$, isto é, $V_{\mathbf{R}}(f) = \{(a,b) \in \boldsymbol{R}^2 / f(a,b) = 0\}$. No próximo capítulo mostraremos um importante resultado o Terorema de Bezout o qual estabelece uma cota superior para o número de interseções de duas curvas afins determinadas por polinômios f e g que não tem fator comum.

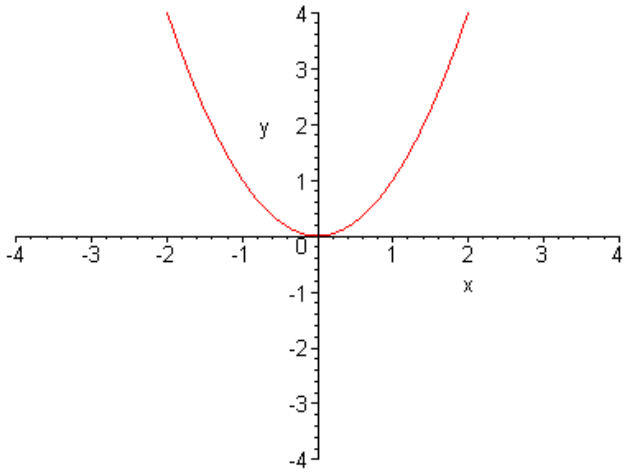
Exemplo 2.13:

$f(x,y) = x^2 - y \in \boldsymbol{R}[x,y]$

$V_{\mathbf{R}}(f) = \{(a,b) \in \boldsymbol{R}^2 / f(a,b) = 0\}$

$V_{\mathbf{R}}(f) = \{(a,b) \in \boldsymbol{R}^2 / a^2 - b = 0\}$

$V_{\mathbf{R}}(f) = \{(a,b) \in \boldsymbol{R}^2 / a^2 = b\}$ *(uma parábola)*



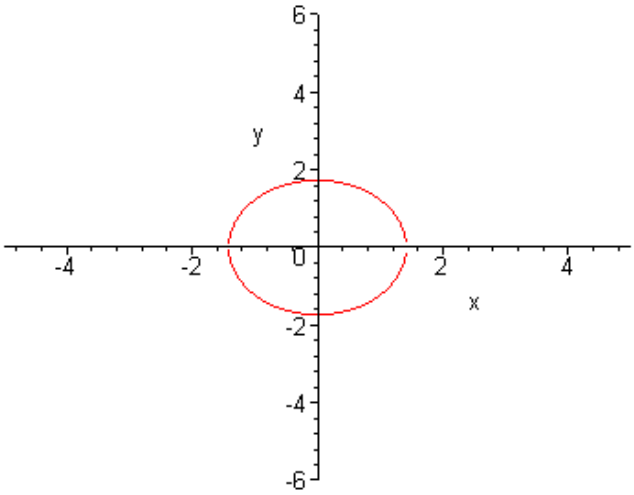
Exemplo 2.14:

$f(x,y) = x^2/2 + y^2/3 - 1 \in \mathbf{R}[x,y]$

$V_{\mathbf{R}}(f) = \{(a,b) \in \mathbf{R}^2 / f(a,b) = 0\}$

$V_{\mathbf{R}}(f) = \{(a,b) \in \mathbf{R}^2 / a^2/2 + b^2/3 - 1 = 0\}$

$V_{\mathbf{R}}(f) = \{(a,b) \in \mathbf{R}^2 / a^2/2 + b^2/3 = 1\}$ *(uma elipse).*



Capítulo 3

Aplicações

Neste capítulo faremos as demonstrações do Teorema do Hexágono de Pascal e do Teorema de Pappus.

Para isso, faremos primeiro a demonstração do Teorema de Bezout, que será a ferramenta fundamental na demonstração dos principais teoremas apresentados neste trabalho.

Teorema 3.1 (Teorema de Bezout): Seja $\boldsymbol{K}$ um corpo. Sejam $f(x,y)$ e $g(x,y)$ dois polinômios em $\boldsymbol{K}[x,y]$ de *graus* $n, m \geq 1$. Se $f(x,y)$ e $g(x,y)$ não têm fator comum em $\boldsymbol{K}[x,y]$, então $\#(V_{\mathbf{K}}(f) \cap V_{\mathbf{K}}(g)) \leq n.m$ *(sendo que # indica a cardinalidade do conjunto).*.

Demonstração:

Para provar este teorema precisamos da resultante (denotada por $R_{f,g}(y)$) de $f(x,y)$ e $g(x,y)$ considerados como polinômios em $\boldsymbol{K[y]}[x]$, onde $a_i = a_i(y)$ e $b_j = b_j(y)$. Como $f(x,y)$ e $g(x,y)$ não têm fator comum em $\boldsymbol{K[y]}[x]$, pelo corolário 2.7, segue que $f(x,y)$ e $g(x,y)$ não têm fator comum em $\boldsymbol{K}(y)[x]$. Portanto, pelo teorema 2.8, existem $a, b \in \boldsymbol{K}(y)[x]$ tais que $1 = a.f + b.g$.

$$a \in \boldsymbol{K}(y) \Rightarrow a = \frac{a_0}{c_0} + \frac{a_1}{c_1}x^1 + \ldots + \frac{a_n}{c_n}x^n \text{ onde } a_i, c_i \in \boldsymbol{K}[y], \text{ sendo } c_i \neq 0 \text{ para todo } i.$$

$$b \in \boldsymbol{K}(y) \Rightarrow b = \frac{b_0}{d_0} + \frac{b_1}{d_1}x^1 + \ldots + \frac{b_n}{d_n}x^n \text{ onde } b_i, d_i \in \boldsymbol{K}[y], \text{ sendo } d_i \neq 0 \text{ para todo } i.$$

Tomemos $d = \left(\coprod_{i=1}^{n} c_i\right)\left(\prod_{j=1}^{m} d_j\right) \in \boldsymbol{K}[y]$.

Multiplicando $1 = af + bg$ por d obtemos $d = adf + bdg = h_1.f + h_2.g$ onde $h_1, h_2 \in \boldsymbol{K}[x,y]$, e $d \in \boldsymbol{K}[y]$.

Se $(\alpha,\beta) \in \mathbf{K}^2$ é tal $f(\alpha,\beta) = 0 = g(\alpha,\beta)$, então $d(\beta) = 0$. Assim existe apenas um número finito de ordenadas possíveis para um ponto em $\mathbf{K}^2$ estar na interseção das curvas determinadas por f e g, a saber as raízes em $\mathbf{K}$ do polinômio $d(y)$.

Para uma ordenada fixa $\beta \in \mathbf{K}$, existem no máximo n pontos em $\mathbf{K}^2$ que pertencem a curva determinada por f, os pontos $(\alpha,\beta) \in \mathbf{K}^2$ tais que $f(\alpha,\beta) = 0$, donde segue que $\#(V_{\mathbf{K}}(f) \cap V_{\mathbf{K}}(g)) \leq \infty$.

Tomando uma extensão de $\mathbf{K}$ se necessário (por exemplo $\mathbf{K}(z)$ onde z é uma nova variável), podemos supor que $\mathbf{K}$ é infinito.

Como o número de pontos da interseção é finito, o número de retas passando por esses pontos também é finito.

Tomando $y = 0$ uma reta que não seja paralela a nenhuma das retas, obtemos um sistema de coordenadas no qual pontos distintos da interseção têm ordenadas distintas.

Logo: $\#(V_{\mathbf{K}}(f) \cap V_{\mathbf{K}}(g)) = \#\{\beta \in \mathbf{K}$: $f(\alpha,\beta)$ e $g(\alpha,\beta)$ tem raiz comum$\} \leq$

$\leq \#\{\beta \in \mathbf{K}$: $f(\alpha,\beta)$ e $g(\alpha,\beta)$ tem fator comum$\} =$

$= \#\{\beta \in \mathbf{K}$: $R_{f,g}(\beta)) = 0\}$ (pelo teorema 2.10) $\leq$

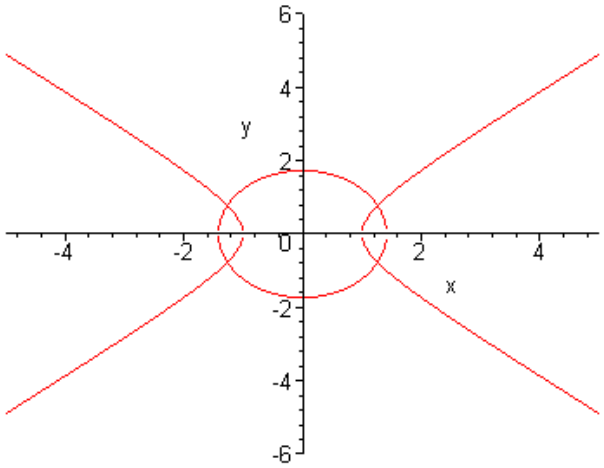
$\leq grau(R_{f,g}(y))$ (pelo corolário 2.3) $\leq$

$\leq n.m$ (proposição 2.3). □

Exemplo 3.1: $f(x,y) = x^2/2 + y^2/3 - 1$ e $g(x,y) = x^2 - y^2 - 1$ em $\mathbf{R}[x.y]$.

Como f tem *grau 2* e g tem *grau 2* e $f(x,y)$ e $g(x,y)$, temos que $\#(V_{\mathbf{R}}(f) \cap V_{\mathbf{R}}(g)) \leq 2.2$, ou seja $\#(V_{\mathbf{R}}(f) \cap V_{\mathbf{R}}(g)) \leq 4$.

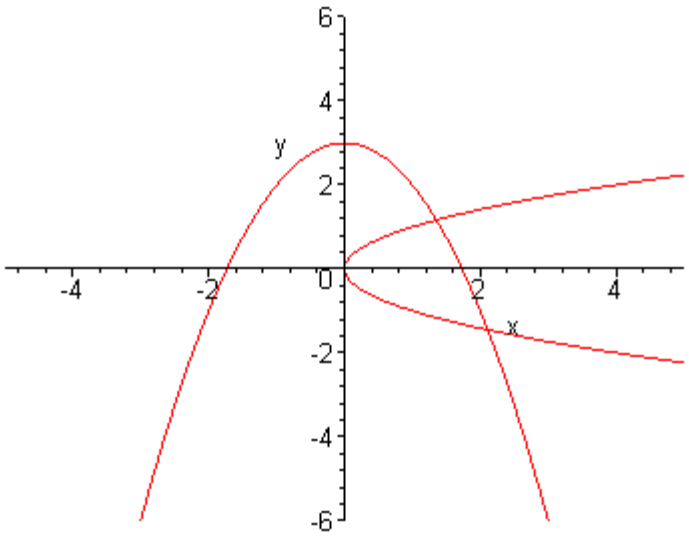
Graficamente podemos observar os quatro pontos da interseção.



Exemplo 3.2: $f(x,y) = x^2 + y - 3$ e $g(x,y) = x - y^2 - 1$ em $\boldsymbol{R}[x.y]$.

Como f tem *grau 2* e g tem *grau 2*, temos que $\#(V_{\mathbf{R}}(f) \cap V_{\mathbf{R}}(g)) \leq 2.2$, ou seja $\#(V_{\mathbf{R}}(f) \cap V_{\mathbf{R}}(g)) \leq 4$.

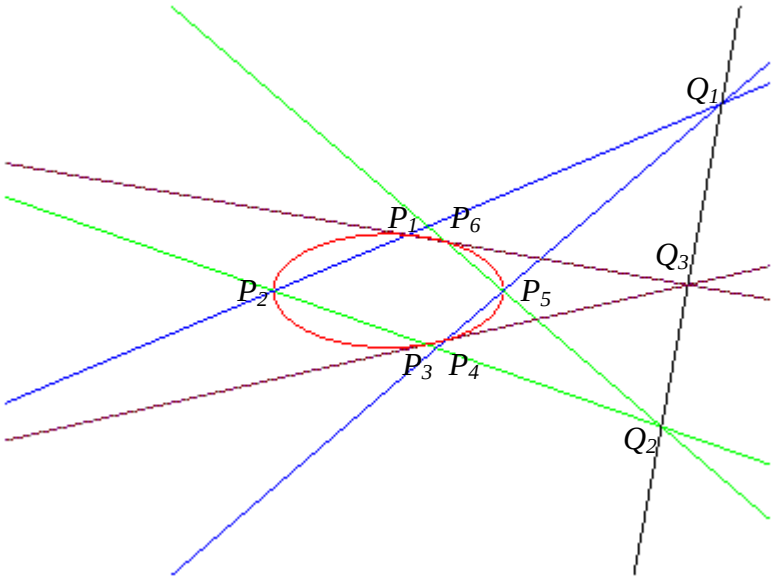
Graficamente podemos observar que neste caso existem dois pontos de interseção.



Seja $\boldsymbol{R}$ o corpo dos números reais. Lembramos que as cônicas irredutíveis em $\boldsymbol{R}^2$ são as parábolas, as elipses e as hipérboles; com uma escolha adequada de coordenadas, suas equações são do tipo $y = x^2$, $(x/a)^2 + (y/b)^2 = 1$ e $(x/a)^2 - (y/b)^2 = 1$, respectivamente.

Vamos agora aplicar o teorema de Bezout para obter o resultado seguinte: os pontos de interseção (quando eles existirem) dos lados opostos de um hexágono inscrito numa cônica irredutível são colineares. De maneira mais precisa:

Teorema 3.2(Teorema do hexágono de Pascal): Sejam $P_1,\ldots, P_6$ seis pontos distintos sobre uma cônica irredutível C. Se as retas P_1P_2 e P_4P_5 se intersectam em Q_1, se as retas P_2P_3 e P_5P_6 se intersectam em Q_2 e se as retas P_3P_4 e P_6P_1 se intersectam em Q_3, então os pontos Q_1, Q_2, Q_3 são colineares.



Demonstração:

Escolhe-se um sistema de coordenadas em $\boldsymbol{R}^2$. Seja L_i a reta P_iP_{i+1} com $i = 1,...,6$ (onde, por convenção, $P_7 = P_1$), e seja $l_i(x,y)$ a equação da reta passando pelos pontos P_i e P_{i+1}. Escolhe-se um ponto A sobre C, que seja diferente de $P_1,...P_6$, cujas coordenadas sejam (α, β).

Afirmamos que A $\notin L_i$ (e similarmente temos que $A \notin L_i$ para cada $i = 1,...,6$). De fato, se A pertencesse a L_1, então P_1, P_2 e A seriam três pontos distintos da interseção de L_1 com C, contradizendo o teorema de Bezout, onde só pode existir dois pontos na interseção de L_1 com C, pois L_1 tem *grau 1* e C é uma curva irredutível de *grau 2*.

Consideremos agora o polinômio $g(x,y) = l_1l_3l_5 + \mu l_2l_4l_6$ com $u \in R\setminus \{0\}$. Afirmamos que $grau(g) = 3$, pois $grau(l_i) = 1$ para qualquer $i = 1,....,6$. Por outro lado, os pontos P_1, P_2, Q_1 estão sobre a curva $V_{\mathbf{R}}(g)$ determinada por g, e também sobre a reta L_1. Logo pelo teorema de Bezout, ou $grau(g) \geq 3$, ou l_1 divide g. No entanto é impossível l_1 dividir g, pois, neste caso, l_1 dividiria $ul_2l_4l_6$, o que é absurdo pois $\boldsymbol{R}[x,y]$ é um domínio fatorial. Logo $grau(g) = 3$.

Podemos tomar μ de maneira que o ponto A se encontre sobre a curva $V_{\mathbf{R}}(g)$, isto é,

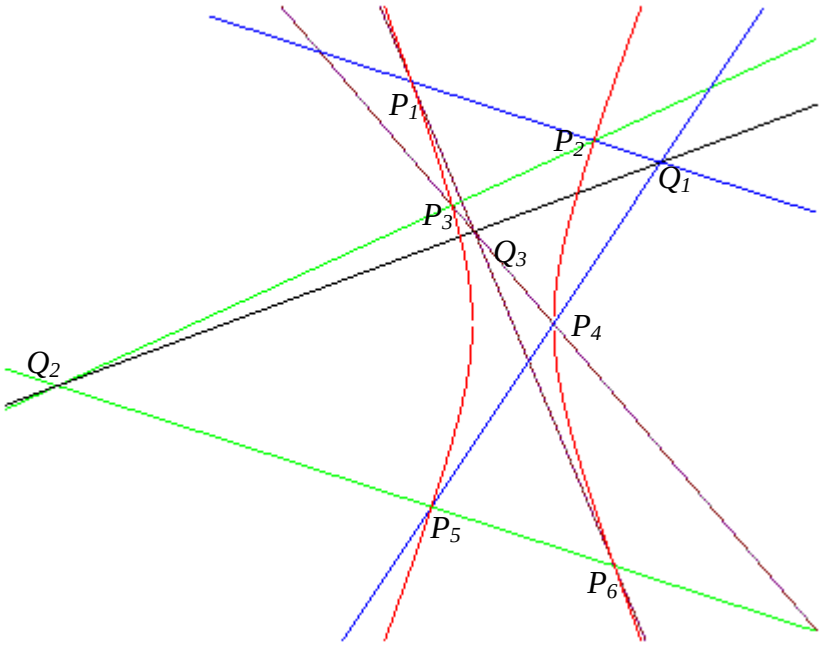
$$\mu = \frac{-l_1(\alpha,\beta).l_3(\alpha,\beta).l_5(\alpha,\beta)}{l_2(\alpha,\beta).l_4(\alpha,\beta).l_6(\alpha,\beta)}$$

notemos que $\mu \in \mathbf{R} \setminus \{0\}$, pois $A \notin L_i$ para qualquer $i = 1,...,6$. Desta maneira, os sete pontos $P_1,...,P_6$ e A se encontram na interseção de C com $V_{\mathbf{R}}(g)$, denotando a equação da cônica irredutível C por $f(x,y)$, temos, pelo teorema de Bezout, que f divide g, então, existe um polinômio $h(x,y)$ de *grau 1* tal que $g = f.h$ e portanto $V_{\mathbf{R}}(g) = V_{\mathbf{R}}(f) \cup V_{\mathbf{R}}(h)$.

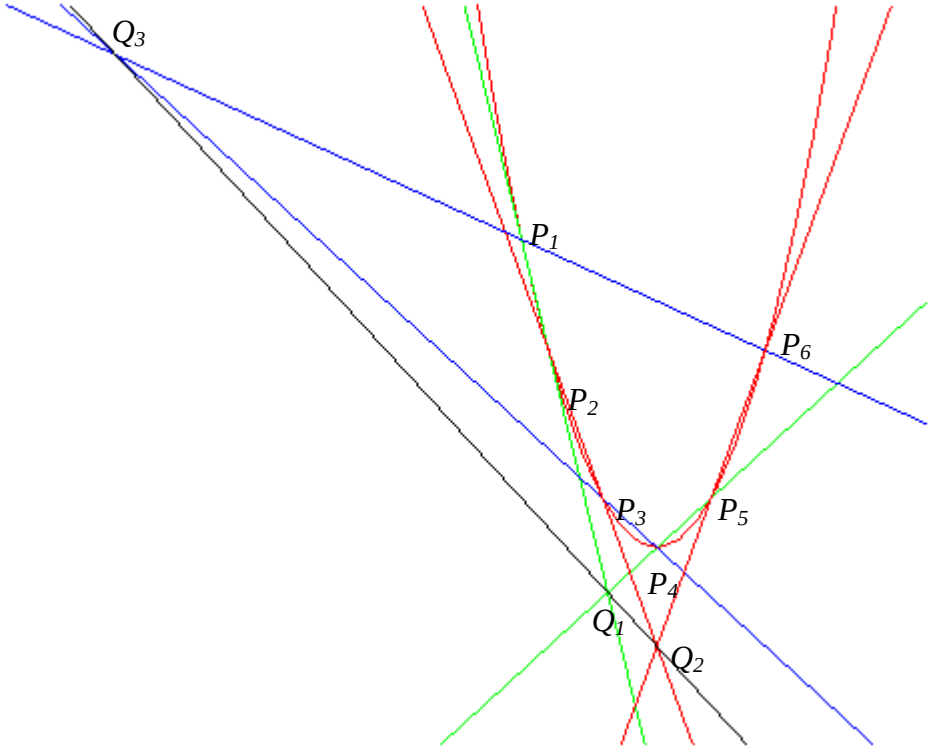
Afirmamos finalmente que Q_1, Q_2, Q_3, são colineares, de maneira mais precisa, afirmamos que Q_1, Q_2, Q_3 estão sobre a reta $V_{\mathbf{R}}(h)$. Já que Q_1, Q_2, Q_3 pertencem a $V_{\mathbf{R}}(g)$, a afirmação ficará provada se mostrarmos que Q_1, Q_2, Q_3 não pertencem a $V_{\mathbf{R}}(f) = C$.

Suponhamos por absurdo que $Q_1 \in C$, neste caso, os pontos P_1, P_2, P_4, P_5 e Q_1 seriam pontos distintos da interseção de $V_{\mathbf{R}}(l_1 l_4)$ com C, contradizendo o teorema de Bezout (visto que C é irredutível). Concluímos desta forma que $Q_1 \notin C$. O mesmo ocorre para Q_2, Q_3. □

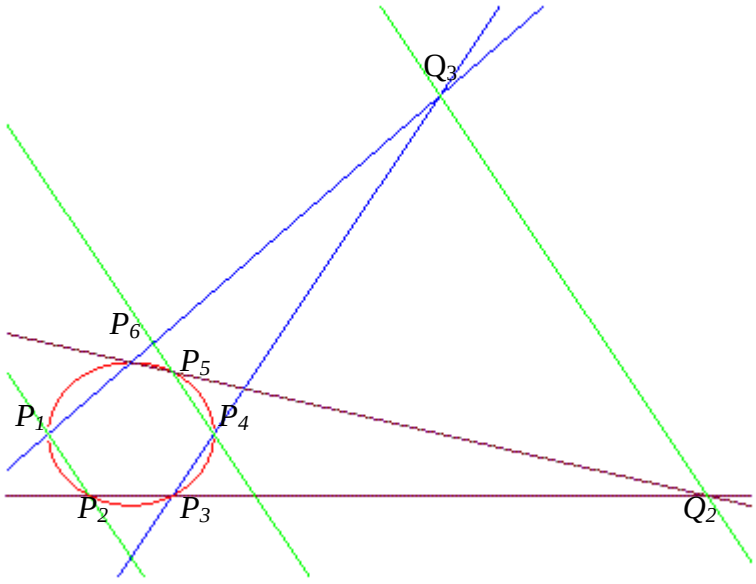
Exemplo 3.3: Para o caso da hipérbole.



Exemplo 3.4: Para o caso da parábola.



Teorema 3.3: Sejam P_1,..., P_6 seis pontos distintos sobre uma cônica irredutível C. Se as retas P_1P_2 e P_4P_5 são paralelas, se as retas P_2P_3 e P_5P_6 se intersectam em Q_2 e se as retas P_3P_4 e P_6P_1 se intersectam em Q_3, então a reta Q_2Q_3 é paralela à reta P_1P_2.



Demonstração:

Seja L_i a reta P_iP_{i+1} com $i = 1,...,6$ (onde, por convenção, $P_7 = P_1$), e seja $l_i(x,y)$ a equação da reta passando pelos pontos P_i e P_{i+1}. Seja L a reta que passa por Q_2 *e* Q_3. Suponhamos por absurdo que L intercepte L_1 em S, e que L intercepte L_4 em T. Afirmamos que $S \notin C$. De fato, caso S pertencesse a C, teríamos P_1, P_2 e S três pontos distintos da interseção de L_1 com C, contradizendo o teorema de Bezout, onde só pode existir dois pontos na interseção de L_1 com C, pois L_1 tem *grau 1* e C é uma curva irredutível de *grau 2*. Do mesmo modo $T \notin C$.

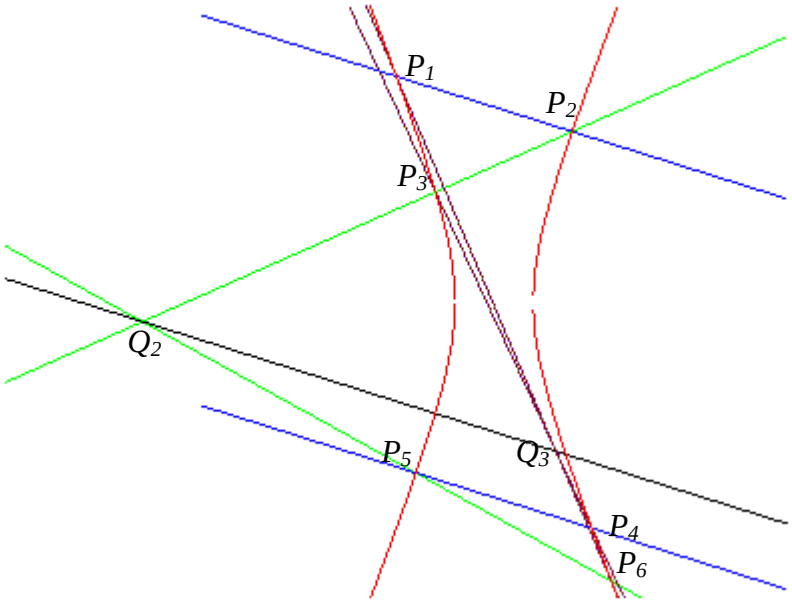
Repetindo os argumentos da demonstração do teorema 3.2, temos o polinômio $g = l_1l_3l_5 + \mu l_2l_4l_6$ de *grau 3* e o polinômio h(x,y) de *grau 1* satisfazendo $g = f.h$ onde $f(x,y)$ é a equação da cônica irredutível C.

Como no teorema 3.1 temos que Q_2 e $Q_3 \in V_{\mathbf{R}}(h = L)$. Portanto $S, T \in V_{\mathbf{R}}(h)$ *(pois* $S \in L$ *e* $T \in L)$ assim S, T, Q_2 e $Q_3 \in V_{\mathbf{R}}(g)$. Sendo $S = (s_1,s_2)$ temos então $0 = g(s_1,s_2) = l_1(s_1,s_2)l_3(s_1,s_2)l_5(s_1,s_2) + \mu l_2(s_1,s_2)l_4(s_1,s_2)l_6(s_1,s_2)$. Como $S \in L_1$ então $l_1(s_1,s_2)l_3(s_1,s_2)l_5(s_1,s_2) = 0$, donde resulta que $l_2(s_1,s_2)l_4(s_1,s_2)l_6(s_1,s_2) = 0$, ou seja, devemos ter um dos seguintes casos: $l_2(s_1,s_2) = 0$, $l_4(s_1,s_2) = 0$, ou $l_6(s_1,s_2) = 0$. Resultando que $S \in L_2$, ou $S \in L_4$ ou $S \in L_6$.

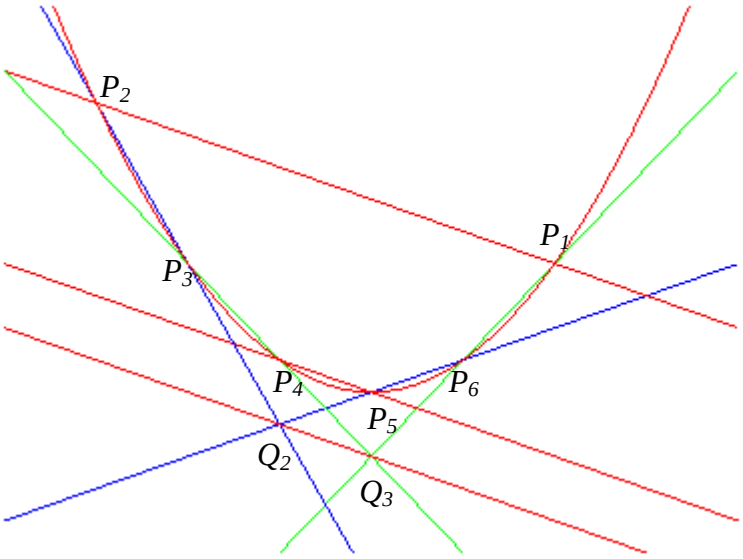
Agora suponhamos que $S \in L_2$ e lembremos que S está em L_1 (veja definição de S) então $S = P_2$, pois P_2 é o único ponto da interseção de L_1 com L_2, mas isto contradiz o fato de que $S \notin C$, logo $S \notin L_2$. De modo análogo provamos que $S \notin L_6$. Finalmente se $S \in L_4$ temos que L_1 e L_4 possuem um ponto comum, o que contradiz a hipótese de que L_1 e L_4 são retas paralelas, logo $S \notin L_4$.

Em qualquer que seja o caso temos um absurdo, logo a reta L não pode interceptar a reta L_1. De maneira análoga concluímos que a reta L não intercepta a reta L_4. Logo a reta Q_2Q_3 é paralela à reta P_1P_2 a qual por sua vez é paralela à reta P_4P_5. □

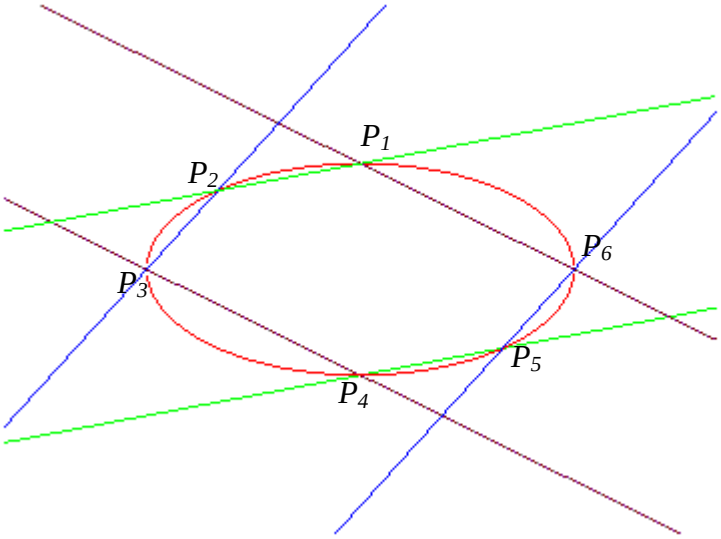
Exemplo 3.5: Para o caso da hipérbole.



Exemplo 3.6: Para o caso da parábola.



Teorema 3.4: Sejam $P_1,...,P_6$ seis pontos distintos sobre uma cônica irredutível C. Se as retas P_1P_2 e P_4P_5 são paralelas e se as retas P_2P_3 e P_5P_6 são paralelas, então as retas P_3P_4 e P_6P_1 são também paralelas.



Demonstração:

Seja L_i a reta P_iP_{i+1} com $i = 1,...,6$ (onde, por convenção, $P_7 = P_1$), e seja $l_i(x,y)$ a equação da reta passando pelos pontos P_i e P_{i+1}. Suponhamos por absurdo que as retas L_3 e L_6 se interceptem em um ponto Q. Seja $g = l_1l_3l_5 + \mu\, l_2l_4l_6$ (como no teorema3.2) sabemos que $Q \in L_3$ e $Q \in L_6$ temos que $Q \in V_{\mathbf{R}}(g)$.

Também temos que $Q \notin C$. Pois, caso Q pertencesse a C, teríamos P_1, P_6 e Q três pontos distintos da interseção de L_6 com C, contradizendo o teorema de Bezout, onde só pode existir dois pontos na interseção de L_6 com C.

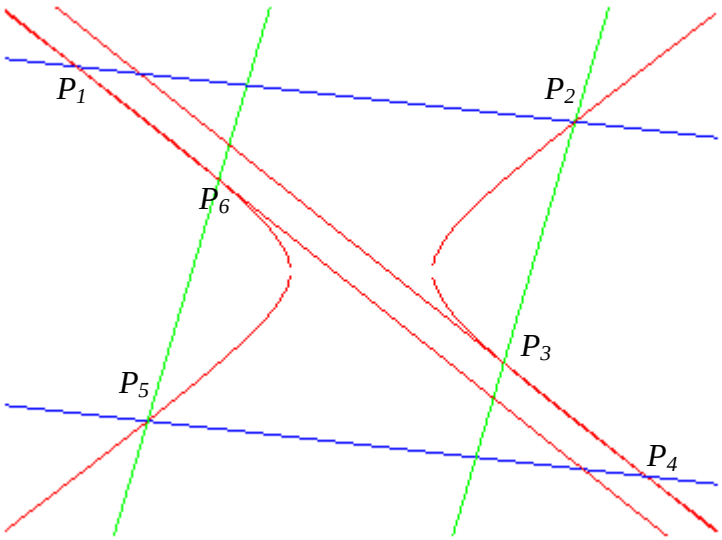
Novamente como no teorema2.3 o polinômio $g = f.h$, onde $f(x,y)$ é a equação da cônica irredutível C e $h(x,y)$ é a equação de uma L, acabamos de ver que $Q \notin C$ de modo que $Q \in L$. Além disso para qualquer $S \in L$ temos que $S \notin C$.

Afirmamos agora que existe $S_1 \in L_5 \cap L$ ou $S_1 \in L_1 \cap L$ (caso contrário teríamos $L \,//\, L_5$ e $L \,//\, L_1$ sendo assim $L_1 \,//\, L_5$, e conseqüentemente $L_1 \,//\, L_2$, o que contradiz nossa hipótese.

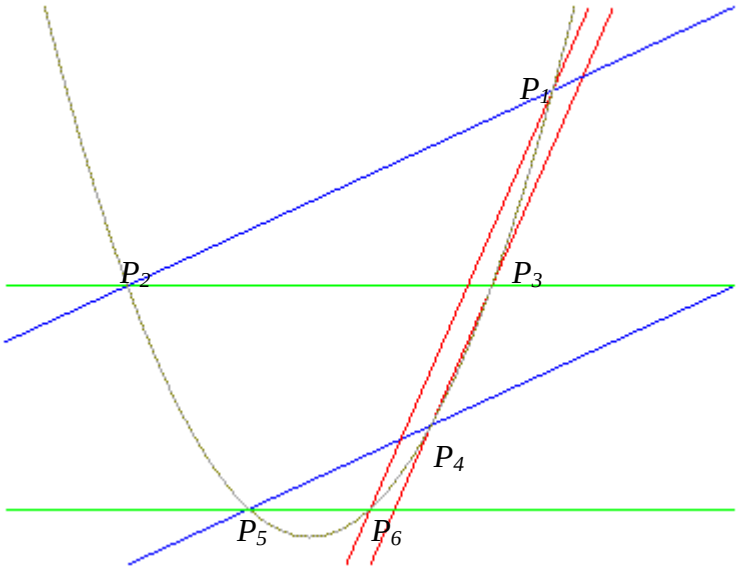
Se $S_1 \in L_5$ e $S_1 \in L$ então, $S_1 \in L_2$ ou $S_1 \in L_4$ ou $S_1 \in L_6$ (visto que $g = l_1 l_3 l_5 + \mu l_2 l_4 l_6$.). Se $S_1 \in L_2$ e $S_1 \in L_5$ então as retas L_1 e L_5 teriam um ponto em comum, contradizendo a hipótese que $L_2 \,//\, L_5$. Logo $S_1 \notin L_2$. Se $S_1 \in L_4$ e $S_1 \in L_5$ então $S_1 = P_5$, pois P_5 é o único ponto comum da interseção de L_4 com L_5, mas isto contradiz o fato que $S_1 \notin C$. Logo $S_1 \notin L_4$. Se $S_1 \in L_6$ e $S_1 \in L_5$ então $S_1 = P_6$, pois P_6 é o único ponto comum da interseção de L_5 com L_6, contradizendo novamente o fato $S_1 \notin C$. *Logo* $S_1 \notin L_6$.

Em qualquer que seja o caso temos um absurdo, logo não existe um ponto Q, tal que $Q \in L_3$ e $Q \in L_6$ de modo que a reta L_3 é paralela à reta L_6. □

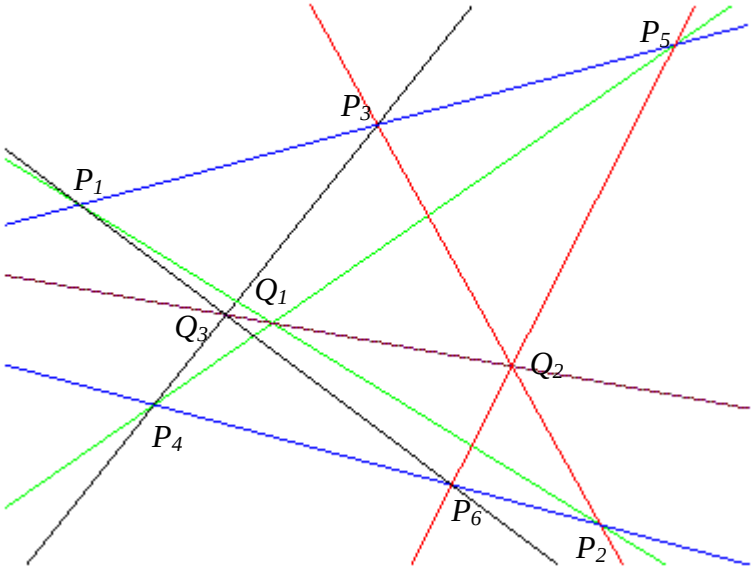
Exemplo 3.7: Para o caso da hipérbole.



Exemplo 3.8: Para o caso da parábola.



Teorema 3.5(Teorema de Pappus): Sejam Δ_1 e Δ_2 duas retas concorrentes. Sejam P_1, P_3, P_5 três pontos distintos sobre Δ_1 e sejam P_2, P_4, P_6 três pontos distintos sobre Δ_2. Se as retas P_1P_2 e P_4P_5 se intersectam em Q_1, se as retas P_2P_3 e P_5P_6 se intersectam em Q_2 e se as retas P_3P_4 e P_6P_1 se intersectam em Q_3, então os pontos Q_1, Q_2, Q_3 são colineares.



Demonstração:

Escolhe-se um sistema de coordenadas em $\mathbf{R}^2$. Seja $h_1(x,y)$ a equação de Δ_1 e $h_2(x,y)$ a equação de Δ_2. Seja L_i a reta P_iP_{i+1} com $i = 1,...,6$ (onde, por convenção, $P_7 = P_1$), e seja $l_i(x,y)$ a equação da reta passando pelos pontos P_i e P_{i+1}. Escolhe-se um ponto A na interseção das retas Δ_1 e Δ_2, sendo A diferente de $P_1,..,P_6$, e sejam (α,β) suas coordenadas.

Temos que $A \notin L_1$, pois se $A \in L_1$, então P_1, P_2 e A seriam três pontos distintos da interseção de L_1 com a reta Δ_1, contradizendo o teorema de Bezout, onde só pode existir um ponto na interseção de L_1 com a reta Δ_1, pois L_1 tem *grau 1* e Δ_1 tem *grau 1*. De modo análogo $A \notin L_i$, com $i = 1,...,6$.

Considere agora o polinômio $g(x,y) = l_1l_3l_5 + \mu l_2l_4l_6$ com $u \in R\setminus\{0\}$. Temos que $grau(g) = 3$, pois $grau(l_i) = 1$ para qualquer $i = 1,....,6$. Por outro lado, os pontos P_1, P_2, Q_1 estão sobre a curva $V_{\mathbf{R}}(g)$ determinada por g, e também sobre a reta L_1. Logo pelo teorema de Bezout, ou $grau(g) \geq 3$, ou l_1 divide g. No entanto é impossível l_1 dividir g, pois, neste caso, l_1 dividiria $\mu l_2l_4l_6$, o que é absurdo pois $\mathbf{R}[x,y]$ é um domínio fatorial. Logo $grau(g) = 3$.

Agora vamos escolher μ de maneira que o ponto A se encontre sobre a curva $V_{\mathbf{R}}(g)$, isto é,

$$\mu = \frac{-l_1(\alpha,\beta).l_3(\alpha,\beta).l_5(\alpha,\beta)}{l_2(\alpha,\beta).l_4(\alpha,\beta).l_6(\alpha,\beta)}$$

$\mu \in R\setminus\{0\}$, pois $A \notin L_i$ para qualquer $i = 1,...,6$. Desta maneira, os sete pontos $P_1,...,P_6$ e A se encontram na interseção de Δ_1 e Δ_2 com $V_{\mathbf{R}}(g)$. Como $A, P_1, P_3, P_5 \in V_{\mathbf{R}}(g)$, e como por hipótese temos que $A, P_1, P_3, P_5 \in h_1(x,y)$, então pelo teorema de Bezout, temos que $h_1(x,y)$ divide $g(x,y)$, assim existe um polinômio $h(x,y)$ de *grau 1* tal que $g = h_1(x,y).h(x,y)$ onde $h \in \mathbf{R}[x,y]$. Da mesma forma temos que $A, P_2, P_4, P_6 \in V_{\mathbf{R}}(g)$ e por hipótese temos que $A, P_2, P_4, P_6 \in h_2(x,y)$, então pelo teorema de Bezout, temos que $h_2(x,y)$ divide $g(x,y)$, então existe um polinômio $h_4(x,y)$ de *grau 1* tal que $g = h_2(x,y).h_4(x,y)$ onde $h_4(x,y) \in \mathbf{R}[x,y]$. Portanto $g(x,y) = h_2(x,y).h_4(x,y) = h_1(x,y).h(x,y)$ então $h_1(x,y) = \delta h_2(x,y)$ ou $h_1(x,y)$ divide $h_4(x,y)$. Se ocorresse $h_1(x,y) = \delta.h_2(x,y)$ então $\Delta_1 = \Delta_2$ o

que contradiz a hipótese $\Delta_1 \neq \Delta_2$, portanto $g(x,y) = h_1(x,y).h_2(x,y).h_3(x,y)$, onde $h_3(x,y)$ tem *grau 1* e portanto $V_{\mathbf{R}}(g) = V_{\mathbf{R}}(h_1) \cup V_{\mathbf{R}}(h_2) \cup V_{\mathbf{R}}(h_3)$.

Afirmamos finalmente que Q_1, Q_2, Q_3, são colineares, de maneira mais precisa, afirmamos que Q_1, Q_2, Q_3 estão sobre a reta $V_{\mathrm{R}}(h_3)$. Já que Q_1, Q_2, Q_3 pertencem a $V_{\mathbf{R}}(g)$ a afirmação ficará provada se mostrarmos que Q_1, Q_2, Q_3 não pertencem a $V_{\mathbf{R}}(h_1) \cup V_{\mathbf{R}}(h_2)$.

Se $Q_1 \in V_{\mathbf{R}}(h_1)$ os pontos P_1, P_2, P_4, P_5 e Q_1 seriam pontos distintos da interseção de $V_{\mathbf{R}}(l_1 l_4)$ com $V_{\mathbf{R}}(h_1)$ resultando que $h_1(x,y)$ divide $l_1(x,y)$ ou $h_1(x,y)$ divide $l_4(x,y)$ donde teríamos que $L_1 = \Delta_1$ ou $L_4 = \Delta_1$ o que é um absurdo. Logo $Q_1 \notin V_{\mathbf{R}}(h_1)$. Da mesma maneira $Q_1 \notin V_{\mathbf{R}}(h_2)$. O mesmo ocorre para Q_2, Q_3. Logo Q_1, Q_2, Q_3 não pertencem a $V_{\mathbf{R}}(h_1) \cup V_{\mathbf{R}}(h_2)$. □

Conclusão

Para que este trabalho fosse realizado, inicialmente foram revistos conteúdos sobre polinômios estudados durante a graduação. Após essa etapa, foram estudados conteúdos não conhecidos, que ampliaram meus conhecimentos. Abordamos no trabalho resultados importantes como a resultante de polinômios e o Teorema de Bezout, tomamos cuidado de manter o rigor matemático nas demonstrações de quase todos os teoremas apresentados. O desenvolvimento deste trabalho possibilitou aprofundar conhecimentos adquiridos em Álgebra, principalmente sobre polinômios.

Para completar o trabalho foi necessário aprender a utilizar o Equation para digitar as expressão algébricas e o Software Maple para a construção dos gráficos e construção de matrizes, o que contribuiu para uma melhor formação em informática.

REFERÊNCIAS BIBLIOGRÁFICAS

[1] DOMINGUES, Hygino H.; IEZZI, Gelson. *Álgebra Moderna*. São Paulo: Atual Editora, 1982.

[2] GONÇALVES, Adilson. *Introdução à Álgebra*. 3. Ed. Rio de Janeiro: IMPA, 1979.

[3] IEZZI, Gelson. *Fundamentos da Matemática Elementar*. Volume 6. São Paulo: Atual Editora, 1993.

[4] GARCIA, Arnaldo; LEQUAIM, Yves. *Álgebra: um curso de introdução.* 2. Ed. Rio de Janeiro: IMPA, 1988.

[5] BOYER, Carl B. *História da Matemática*, tradução: Elza F. Gomide. São Paulo, Ed. da Universidade de São Paulo, 1974.

[6] EVES, Howard. *Introdução à História da Matemática*, tradução: Hygino H. Domingues, Campinas, SP: Editora da UNICAMP, 1997.