Universidade Federal de Uberlândia
Faculdade de Matemática

Programa de Mestrado Profissional em Matemática em Rede Pública

RESOLUÇÃO DE PROBLEMAS DA GEOMETRIA EUCLIDIANA PLANA USANDO POLINÔMIOS

Adriana de Souza

Uberlândia-MG
2021

Adriana de Souza

RESOLUÇÃO DE PROBLEMAS DA GEOMETRIA EUCLIDIANA PLANA USANDO POLINÔMIOS

Dissertação apresentada ao Programa de Mestrado Profissional em Matemática em Rede Nacional da Faculdade de Matemática da Universidade Federal de Uberlândia, como requisito parcial para obtenção do título de Mestre em Matemática.

Orientador: Prof. Dr. Aldicio José Miranda

Uberlândia-MG

2021

Ficha Catalográfica Online do Sistema de Bibliotecas da UFU
com dados informados pelo(a) próprio(a) autor(a).

S729 Souza, Adriana de, 1977-
2021 Resolução de problemas da geometria euclidiana plana usando polinômios [recurso eletrônico] : resolução de problemas geométricos no ensino médio / Adriana de Souza. - 2021.

Orientador: Aldicio José Miranda .
Dissertação (Mestrado) - Universidade Federal de Uberlândia, Pós-graduação em Matemática.
Modo de acesso: Internet.
Disponível em: http://doi.org/10.14393/ufu.di.2021.709
Inclui bibliografia.
Inclui ilustrações.

1. Matemática. I. , Aldicio José Miranda,1977-, (Orient.). II. Universidade Federal de Uberlândia. Pós-graduação em Matemática. III. Título.

CDU: 51

Bibliotecários responsáveis pela estrutura de acordo com o AACR2:

Gizele Cristine Nunes do Couto - CRB6/2091

UNIVERSIDADE FEDERAL DE UBERLÂNDIA
Coordenação do Programa de Pós-Graduação em Matemática - Mestrado Profissional em Rede Nacional
Av. João Naves de Ávila, 2121, Bloco 1F - Bairro Santa Mônica, Uberlândia-MG, CEP 38400-902
Telefone: (34) 3230-9452 - www.famat.ufu.br - profmat@famat.ufu.br

ATA DE DEFESA - PÓS-GRADUAÇÃO

Programa de Pós-Graduação em:	Mestrado Profissional em Matemática em Rede Nacional - PROFMAT UFU				
Defesa de:	Dissertação de Mestrado Profissional, 4, PROFMAT				
Data:	nove de dezembro de dois mil e vinte e um	Hora de início:	14:00	Hora de encerramento:	16:00
Matrícula do Discente:	11912PFT001				
Nome do Discente:	Adriana de Souza				
Título do Trabalho:	Resolução de Problemas da Geometria Euclidiana Plana Usando Polinômios				
Área de concentração:	Matemática				
Linha de pesquisa:	Geometria				
Projeto de Pesquisa de vinculação:	Não há.				

Reuniu-se em web conferência pela plataforma Google Meet a Banca Examinadora, aprovada pelo Colegiado do Programa de Pós-graduação em Matemática - Mestrado Profissional em Matemática em Rede Nacional (PROFMAT), assim composta pelos professores doutores: Thiago Henrique de Freitas - UTFPR; Luis Renato Gonçalves Dias - FAMAT/UFU e Aldicio José Miranda - FAMAT/UFU, orientador da candidata.

Iniciando os trabalhos o presidente da mesa, Dr. Aldicio José Miranda, apresentou a Comissão Examinadora e a candidata agradeceu a presença de todos. Posteriormente, o presidente concedeu à Discente a palavra para a exposição do seu trabalho. A duração da apresentação da Discente e o tempo de arguição e resposta foram conforme as normas do Programa.

A seguir o senhor presidente concedeu a palavra aos examinadores que passaram a arguir a candidata. Ultimada a arguição, que se desenvolveu dentro dos termos regimentais, a Banca, em sessão secreta, atribuiu o resultado final, considerando a candidata:

Aprovada.

Esta defesa faz parte dos requisitos necessários à obtenção do título de Mestre.

O competente diploma será expedido após cumprimento dos demais requisitos, conforme as normas do Programa, a legislação pertinente e a regulamentação interna da UFU.

Nada mais havendo a tratar foram encerrados os trabalhos. Foi lavrada a presente ata que após lida e achada conforme foi assinada pela Banca Examinadora.

Documento assinado eletronicamente por **Thiago Henrique de Freitas**, **Usuário Externo**, em 09/12/2021, às 15:36, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 8.539, de 8 de outubro de 2015.

Documento assinado eletronicamente por **Luis Renato Gonçalves Dias**, **Professor(a) do Magistério Superior**, em 09/12/2021, às 15:38, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 8.539, de 8 de outubro de 2015.

Documento assinado eletronicamente por **Aldicio José Miranda**, **Professor(a) do Magistério Superior**, em 09/12/2021, às 15:38, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 8.539, de 8 de outubro de 2015.

A autenticidade deste documento pode ser conferida no site https://www.sei.ufu.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **3216781** e o código CRC **B2B3267D**.

Referência: Processo nº 23117.082633/2021-59 SEI nº 3216781

Dedico esta grande conquista à minha mãe Ozélia, pelo seu exemplo de vida, em memória da minha irmã Maria das Graças que sempre esteve presente em todas as minhas conquistas e que partiu no decorrer desta jornada e ao meu orientador professor Dr. Aldicio pois sem sua atenção, paciência e estímulo este trabalho não teria sido possível.

Agradecimentos

Em primeiro lugar agradeço a Deus por ter me dado força, determinação, sabedoria e tudo aquilo de que precisei nesta caminhada para estar realizando mais este sonho. Só Ele sabe o quanto foi difícil superar todas as dificuldades para ingressar e conseguir terminar mais esta etapa.

Agradeço especialmente à minha mãe Ozélia que é meu exemplo de vida, mulher guerreira e batalhadora por todas as orações, apoio, carinho e amor que me deu durante toda a vida e por compreender todos os momentos de ausência necessários para dedicar aos estudos.

Ao meu professor orientador Dr. Aldicio José Miranda, pela paciência, incentivo, ensinamentos, colaboração e disponibilidade em me atender todas as vezes em que precisei, agradeço por ter sido exigente comigo, estimulando-me a não desistir no desenvolvimento deste estudo e por ter acreditado no meu potencial, conduzindo-me para esta realização, suas propostas me desafiaram e me fizeram evoluir.

A minha família, especialmente meus irmãos Sônia, Sirlene, Maria das Graças, Tânia e Djalma que sempre me apoiaram e me deram forças para seguir em frente, foram momentos de muita luta, muito esforço, momentos de ausência, viagens para cumprir disciplinas e avaliações, mas sempre pude contar com vocês.

Ao meu namorado Rogério, pelo seu companheirismo e compreensão dos momentos em que estive ausente para me dedicar às atividades do mestrado e pelo carinho nas horas mais difíceis dessa jornada.

A todos os meus colegas do PROFMAT pelo companheirismo, incentivo, apoio e amizade, por tornarem nossos sábados de muito estudo em momentos especiais de muita alegria, pois sem a nossa união seria impossível chegar à reta final.

A todos os professores do PROFMAT da Universidade Federal de Uberlândia UFU, pelos conhecimentos compartilhados, contribuindo imensamente para minha formação.

Agradeço aos amigos e colegas de trabalho pelo apoio, paciência e compreensão por ouvirem meus desabafos e me animarem nos momentos de angústia com sábios conselhos.

Por fim, agradeço a todos que fizeram parte dessa etapa, que me incentivaram, torceram por mim ou contribuíram de alguma maneira para a concretização deste sonho, a minha eterna gratidão.

"A persistência é o caminho do êxito".

"Lute com determinação, abrace a vida com paixão, perca com classe e vença com ousadia, porque o mundo pertence a quem se atreve e a vida é muito bela para ser insignificante".

(Charles Chaplin)

Resumo

Palavras-chave: Geometria euclidiana plana, anéis de polinômios, álgebra computacional, conjunto algébrico afim, resolução de problemas geométricos.

O principal objetivo deste trabalho é resolver problemas e demonstrar teoremas da geometria euclidiana plana usando polinômios. Isso será realizado através do estudo de anéis de polinômios, sistemas polinomiais e conjuntos algébricos afins. Estes conceitos nos permitem ligar a Álgebra à Geometria. Assim, por exemplo, introduzindo coordenadas cartesianas no plano euclidiano, as hipóteses e conclusões de uma grande classe de teoremas geométricos podem ser expressados com equações polinomiais. Também faremos uso de uma importante ferramenta computacional, o sistema de álgebra computacional Singular.

Abstract

Keywords: Plane Euclidean geometry, polynomial rings, computational algebra, affine algebraic set, geometric problem solving.

The main objective of this work is to solve problems and demonstrate theorems of euclidean plane geometry using polynomials. This will be done through the study of polynomial rings, polynomial systems and affins algebraic sets. These concepts makes it possible to link Algebra to Geometry. Thus, for example, by introducing cartesian coordinates into the euclidean plane, the hypotheses and conclusions of a large class of geometric theorems can be expressed with polynomial equations. We will also make use of an important computational tool, the computational algebra system Singular.

Sumário

1. Introdução

O principal objetivo deste trabalho é demonstrar teoremas e resolver problemas da geometria euclidiana plana usando polinômios. Esta apresentação bem como suas resoluções estão descritas no Capítulo 5. Para isso, precisamos estudar anéis de polinômios de várias variáveis, conjuntos algébricos afins e também fazer uso de um sistema algébrico computacional.

No ensino médio e até mesmo em disciplinas da graduação, os problemas da geometria euclidiana plana são resolvidos usando os axiomas ou postulados de Euclides, apresentado pelo grande matemático Euclides de Alexandria em uma das suas maiores obras primas intitulada "Os Elementos" a qual é constituída por treze livros que contemplam tópicos como aritmética, geometria e álgebra. A obra "Os Elementos" é um dos mais influentes na história. Nele, Euclides introduz o método axiomático que consiste em assumir como verdadeiras certas afirmações, conceitos e proposições sem necessidade de prova apresentando proposições deduzidas a partir de axiomas e postulados. Euclides refere-se a axioma como fatos de caráter geral, amplo para qualquer ciência, proposições evidentes por si mesmas e já postulado refere-se a teoria específica, tipo geométrica ou de determinado tema, proposições aceitas sem demonstrações. Atualmente axiomas e postulados têm o mesmo sentido, são hipóteses admitidas como verdadeiras sem precisar de uma demonstração.

No Capítulo 2 definimos grupos, anéis, corpos e ideais que são essenciais para o estudo de anéis de polinômios que serão abordados nos outros capítulos. O principal anel que vamos trabalhar é sobre o anel de polinômios em várias variáveis sobre o corpo dos números racionais. Inicialmente, discutiremos polinômios em uma variável para abrir caminho no entendimento de algumas definições e algoritmos da divisão em várias variáveis que serão utilizados nos cálculos envolvendo conjuntos algébricos afins. Além de definirmos o algoritmo da divisão em anéis de polinômios em várias variáveis, vários exemplos serão calculados.

Muitos problemas do Capítulo 5 também serão resolvidos com auxílio de uma importante ferramenta computacional algébrica, o Singular. Assim, no Capítulo 3 apresentaremos uma breve introdução ao Singular, [6]. O Singular é um sistema de álgebra computacional, designado para cálculos com polinômios. Os principais objetos que podemos trabalhar no Singular, são ideais e módulos sobre uma grande variedade de anéis, em particular sobre o anel de polinômios de várias variávies sobre o corpo do números racionais.

No Capítulo 4 será abordado o conceito de conjunto algébrico afim, que é definido por equações polinomiais. Por exemplo, a equação $x^2 + y^2 - 1 = 0$ define um conjunto algébrico afim, no caso, uma circunferência de raio 1 e centro na origem no plano cartesiano xy. A base

para trabalhar com conjuntos algébricos afins ou variedades afins é um "pouco" de álgebra e ideais em anéis de polinômios. Um exemplo importante vindo da álgebra linear é discutido no Capítulo 4, com o objetivo de distinguir e definir um anel somente com variáveis e um anel com variáveis e parâmetros.

O interessante é que o estudo de polinômios e sistemas de polinômios sobre um corpo permite ligar a álgebra à geometria. Logo, este conceito de conjunto algébrico afim nos permite reformular problemas geométricos em termos algébricos e vice-versa. Esta relação será tratada com exemplos práticos no Capítulo 5. Mais precisamente, introduzindo coordenadas cartesianas no plano euclidiano, as hipóteses e conclusões de uma grande classe de teoremas geométricos podem ser expressados com equações polinomiais entre as coordenadas de uma coleção de pontos de acordo com o problema apresentado. Por exemplo: como provar que as diagonais de um paralelogramo se cruzam ao meio usando polinômios? Faremos uso de ferramentas computacionais para resolver ou simplificar os sistemas polinomiais de acordo com cada problema apresentado. Ressaltamos que para entender e construir as hipóteses e teses relacionados a um determinado problema mostrado no Capítulo 5, é necessário saber os axiomas da geometria euclidiana plana, distâncias entre pontos, Teorema de Pitágoras, Teorema de Tales, equação da reta, equação da circunferência e outros mais.

2. Anéis e polinômios

Neste capítulo apresentaremos alguns conceitos da teoria de anéis, corpos, grupos e ideais que são essenciais para o estudo de anéis de polinômios que serão abordados nos próximos capítulos. Os conteúdos abordados neste capítulo foram baseados nas referências [2], [3] e [4].

Os anéis mais conhecidos são os dos números inteiros $\mathbb{Z}$ e o anel dos polinômios em uma variável sobre um corpo.

Definiremos o algoritmo da divisão em anéis de polinômios em várias variáveis, e por último uma breve apresentação sobre o que podemos fazer com o Singular.

Definição 1. *Dizemos que um anel é uma estrutura algébrica que consiste em um conjunto não vazio A associado a duas operações binárias adição e multiplicação, que satisfazem as seguintes condições:*

Adição (denotada por $+$) $A \times A \to A : (a, b) \to a+b$.
Multiplicação (denotada por $\cdot$) $A \times A \to A : (a, b) \to a \cdot b$.

i) ***Associatividade em relação a*** $(+)$***:*** *para quaisquer $a, b, c \in A$ temos:*

$$(a + b) + c = a + (b + c).$$

ii) ***Comutatividade em relação a*** $(+)$***:*** *para quaisquer $a, b \in A$ temos:*

$$a + b = b + a.$$

iii) ***Elemento Neutro*** (e) ***em relação a*** $(+)$***:*** *para todo $a \in A$, existe $e \in A$ tal que*

$$a + e = e + a = a.$$

iv) ***Elemento Simétrico em relação a*** $(+)$***:*** *para todo $a \in A$, existe um elemento $b \in A$ tal que*

$$a + b = b + a = e.$$

Observe que para cada a, b é único. Logo, denotaremos o elemento simétrico de a por $-a$.

v) ***Associatividade em relação a*** $(\cdot)$***:*** *para quaisquer* $a, b, c \in A$ *temos:*

$$(a \cdot b) \cdot c = a \cdot (b \cdot c) \cdot$$

vi) ***Distributividade em relação a*** $(\cdot)$***:*** *para todo* $a, b, c \in A$*, temos:*

$$a \cdot (b + c) = a \cdot b + a \cdot c.$$

$$(a + b) \cdot c = a \cdot c + b \cdot c.$$

vii) ***Elemento Neutro*** (1) ***em relação a*** $(\cdot)$***:*** *para todo* $a \in A$*, existe* $1 \in A$ *tal que*

$$a \cdot 1 = 1 \cdot a = a.$$

Daqui em diante, $(A, +, \cdot)$ denotará um anel A com as operacões $+$ e $\cdot$.

Definição 2. *Seja* G *um conjunto não vazio munido de uma operação binária*

$$+ : G \times G \to G.$$

Dizemos que G *munido da operação* $+$*, denotado por* $(G, +)$*, é um grupo se valem os axiomas* (i)*,* (ii)*,* (iv) *e se valer também* (iii) *então* $(G, +)$ *é chamado de grupo abeliano.*

Um anel é completamente diferente de um grupo, pois em um anel são definidas duas operações. Comumente, essas operações são chamadas de adição e multiplicação, enquanto um grupo é munido de uma única operação.

O conjunto dos números inteiros $\mathbb{Z}$, com as operações de adição e multiplicação usuais, é um anel comutativo com unidade.

Definição 3. *Seja* A *um anel.* A *é dito ser um corpo se qualquer elemento não nulo* $a \in A$ *é uma unidade, isto é, existe* $b \in A$ *tal que* $ab = 1 \neq 0$*. Note que um corpo é um anel com unidade em que todo elemento diferente de* 0 *(não nulo) possui um elemento inverso com relação à multiplicação.*

O conjunto dos números racionais com as operações usuais de adição e multiplicação de números racionais é um anel comutativo com unidade. Além disso, os números racionais diferentes de 0 formam um grupo abeliano com relação a multiplicação, com esta última propriedade é denominada um corpo.

Definição 4. *Sejam* A *um anel e* I *um subconjunto não vazio de* A*. Dizemos que* I *é um ideal de* A *se*

i) $f, g \in I \Rightarrow f + g \in I$.

ii) $f \in I, a \in A \Rightarrow af \in I$.

O conceito de ideais é fundamental no estudo de geometria algébrica (estudo de objetos geométricos definidos por equações polinomiais, usando meios algébricos). O anel principal que trataremos aqui é o anel de polinômios em várias variáveis.

Definição 5. *Seja A um anel.*

i) Um ***monômio*** *em n variáveis, $x_1, \ldots, x_n$, é um produto da forma*

$$x^\alpha = x_1^{\alpha_1} \cdot \ldots \cdot x_n^{\alpha_n}, \quad \alpha = (\alpha_1, \ldots, \alpha_n) \in \mathbb{N}^n.$$

ii) Um ***termo*** *é um monômio vezes um coeficiente (elemento de A), escrito da forma*

$$ax^\alpha = ax_1^{\alpha_1} \cdot \ldots \cdot x_n^{\alpha_n}, a \in A.$$

iii) Um polinômio sobre A é uma combinação linear finita de monômios, com coeficientes em A, e é escrito da forma

$$f = \sum_\alpha a_\alpha x^\alpha = \sum_{\alpha \in \mathbb{N}^n}^{finita} a_{\alpha_1 \ldots \alpha_n} x_1^{\alpha_1} \cdot \ldots \cdot x_n^{\alpha_n}, a_\alpha \in A.$$

Para $\alpha \in \mathbb{N}^n$, colocamos $|\alpha| := \alpha_1 + \cdots + \alpha_n$. Se $f \neq 0$, chamamos de ***grau*** *de f, o inteiro definido por* $\text{grau}(f) := max\{|\alpha|, a_\alpha \neq 0\}$. *Se $f = 0$, colocamos* $\text{grau}(f) = -1$. *O termo lider de um polinômio, é o termo de maior grau. O coeficiente do termo lider é chamado de coeficiente lider.*

iv) O anel polinomial $A[x] = A[x_1, \ldots, x_n]$ em n variáveis sobre A é o conjunto de todos os polinômios juntamente com as operações usuais de soma e multiplicação:

$$\sum_\alpha a_\alpha x^\alpha + \sum_\alpha b_\alpha x^\alpha := \sum_\alpha (a_\alpha + b_\alpha) x^\alpha,$$

$$\left(\sum_\alpha a_\alpha x^\alpha \right) \left(\sum_\beta b_\beta x^\beta \right) := \sum_\gamma \left(\sum_{\alpha+\beta} a_\alpha b_\beta \right) x^\gamma.$$

Note que $A[x_1, \ldots, x_n]$ é um anel comutativo com unidade $1 = x_1^0 \cdot \ldots \cdot x_n^0$, que identificamos com a unidade $1 \in A$. Elementos de $A \subset A[x]$ são chamados de polinômios constantes.

Usamos x, y e x, y, z para as variáveis no caso quando $n = 2$ ou $n = 3$, respectivamente.

Exemplo 1. Considere o anel $\mathbb{K}[x, y, z]$, $\mathbb{K} = \mathbb{Q}$, onde $\mathbb{Q}$ representa o conjunto do números racionais ou $\mathbb{K} = \mathbb{R}$, onde $\mathbb{R}$ representa o conjunto do números reais. Seja $p(x, y, z) = x^3y + 5xy^2 - 2x^2yz^2$, logo p é um polinômio contendo 3 termos e o grau de p é 5.

Dada uma coleção finita de polinômios $f_1, \ldots, f_s \in \mathbb{K}[x_1, \ldots, x_n]$, podemos criar outros polinômios dependentes destes através de uma multiplicação por polinômios arbitrários em $\mathbb{K}[x_1, \ldots, x_n]$ e tomando a soma.

Definição 6. *Seja $f_1, \ldots, f_s \in \mathbb{K}[x_1, \ldots, x_n]$. Pomos $\langle f_1, \ldots, f_s \rangle$ para denotar a coleção*

$$\langle f_1, \ldots, f_s \rangle = \{p_1 f_1 + \cdots + p_s f_s : \quad p_i \in \mathbb{K}[x_1, \ldots, x_n], i = 1, \ldots, s\}.$$

Teorema 1. *A coleção $\langle f_1, \ldots, f_s \rangle$ é um ideal de $\mathbb{K}[x_1, \ldots, x_n]$ e é gerado por $f_1, \ldots, f_s$.*

Demonstração:

Dados $f = p_1 f_1 + \cdots + p_s f_s$ e $g = q_1 f_1 + \cdots + q_s f_s$ dois elementos de $\langle f_1, \ldots, f_s \rangle$, então:

$$f + g = (p_1 + q_1) f_1 + \cdots + (p_s + q_s) f_s \in \langle f_1, \ldots, f_s \rangle.$$

Também para $f \in \langle f_1, \ldots, f_s \rangle$ e $a \in \mathbb{K}[x_1, \ldots, x_n]$ temos que

$$af = ap_1 f_1 + \cdots + ap_s f_s$$

$$af = (ap_1) f_1 + \cdots + (ap_s) f_s \in \langle f_1, \ldots, f_s \rangle.$$

Logo, as propriedades $i)$ e $ii)$ da Definição 4 estão satisfeitas.

□

Exemplo 2. Temos que $x^2 \in \langle x - y^2, xy \rangle$ em $\mathbb{K}[x, y]$, pois $x^2 = p_1(x - y^2) + p_2 xy$, com $p_1 = x$ e $p_2 = y$.

Um resultado importante que não provaremos aqui é o Teorema de Basis de Hilbert.

Teorema 2 (Hilbert Basis Theorem)**.** *Todo ideal $I \in \mathbb{K}[x_1, \ldots, x_n]$ tem um conjunto finito de geradores.*

Este Teorema nos diz que, dado um ideal $I \in \mathbb{K}[x_1, \ldots, x_n]$, existe um número finito de polinômios $\{f_1, \ldots, f_s\} \in \mathbb{K}[x_1, \cdots, x_n]$ tal que $I = \langle f_1, \ldots, f_s \rangle$.

2.1 Algoritmo da divisão

A divisão de polinômios é fundamental no estudo de ideais em anéis polinomiais. Por exemplo, precisamos do algoritmo da divisão juntamente com bases de Groebner (que pode ser aprofundada no livro de referência [2]) para verificar se um dado polinômio pertence a um ideal. Nesta subseção, definiremos o algoritmo em um anel de polinômios com uma e com várias variáveis.

2.1.1 Algoritmo da divisão em $\mathbb{K}[x]$

Relembre que um polinômio f na variável x, é uma expressão da forma

$$f(x) = a_n x^n + a_{n-1} x^{n-1} + ... + a_2 x^2 + a_1 x + a_0,$$

onde n é um número inteiro não negativo com $a_0, \ldots, a_n$ elementos de $\mathbb{K}$, chamados de coeficientes de f, se $a_n \neq 0$ dizemos que a_n é o coeficiente líder.

Em anéis de polinômios em uma única variável, o algoritmo da divisão de Euclides nos permite dividir polinômios, isto é, dados dois polinômios $f, g \in \mathbb{K}[x]$, com $g \neq 0$, então existem únicos polinômios $q, r \in \mathbb{K}[x]$ tal que

$$f = qg + r, \text{ com } r = 0 \text{ ou } \text{grau}(r) < \text{grau}(g).$$

Assim, como todo ideal $I \subset \mathbb{K}[x]$ é principal (gerado por um único gerador), se $I = \langle g \rangle$, isto é, I ser gerado por um único polinômio g, teremos $f \in I$ se $r = 0$, ou seja, o resto da divisão de f por g for o polinômio nulo. Caso, $f = qg + r$, com $r \neq 0$, segue que $f \notin I$. Assim, verificar se um polinômio f pertence a um ideal I, é facilmente resolvido no caso de anel de polinômios em uma única variável.

Note que todo polinômio pode ser escrito de modo único como a soma de seus termos a menos da ordem da posição de seus termos, devido a propriedade comutativa da adição nesses anéis. Em um anel polinomial em uma única variável, podemos escrever de modo único um polinômio de acordo com o grau de cada monômio. Assim, para efetuar divisão de polinômios precisamos primeiro estabelecer uma ordem, para que possamos escrever de modo único tal polinômio.

Ao dividir um polinômio f por um polinômio g esperamos encontrar dois novos polinômios, o quociente q e o resto r, sendo que o $\text{grau}(r) < \text{grau}(g)$. No algoritmo da divisão quando o anel dos coeficientes é um corpo $\mathbb{K}$, o polinômio divisor sempre tem coeficiente líder invertível, ou seja, um coeficiente que quando multiplicado por um número apropriado resulta em 1 de modo que a divisão seja sempre possível.

Teorema 3 (Algoritmo da divisão de Euclides)**.** *Seja A um corpo. Dados $f(x), g(x) \in A[x]$ em que $g(x) \neq 0$. Então existem $q(x), r(x) \in A[x]$ tais que*

$$f(x) = g(x)q(x) + r(x),$$

com $r(x) = 0$ ou $\text{grau}(r(x)) < \text{grau}(g(x))$.

Demonstração:

Temos três casos a considerar:

i) $f(x) = 0$.

ii) $f(x) \neq 0$ **e** $\text{grau}(f(x)) < \text{grau}(g(x))$.

iii) $f(x) \neq 0$ **e** $\text{grau}(f(x)) \geq \text{grau}(g(x))$.

Suponhamos que $f(x) = a_m x^m + a_{m-1}x^{m-1} + \cdots + a_1 x + a_0$, com $\text{grau}(f(x)) = m$ e $g(x) = b_n x^n + b_{n-1}x^{n-1} + \cdots + b_1 x + b_0$, em que $\text{grau}(g(x)) = n$.

No primeiro caso, se $f(x) = 0$, basta tomar $q(x) = r(x) = 0$.

No segundo caso, sendo $f(x) \neq 0$, grau$(f(x)) <$ grau$(g(x))$ e como $f(x) = 0g(x) + f(x)$ basta tomar $q(x) = 0$ e $r(x) = f(x)$.

Portanto, resta considerarmos o caso em que o $f(x) \neq 0$ e grau$(f(x)) \geq$ grau$(g(x))$.

A ideia é multiplicar $g(x)$ por um polinômio apropriado $q(x)$ e subtrair o resultado de $f(x)$, afim de conseguirmos um outro polinômio $r(x)$ que é o polinômio nulo ou de grau menor que o grau de $g(x)$

$$r(x) = f(x) - g(x)q(x).$$

A maneira de encontrar o polinômio $q(x)$ é via um algoritmo que passamos a descrever a partir de agora. Defina:

$$q_1(x) = a_m b_n^{-1} x^{m-n}.$$

Observe a forma como $q_1(x)$ é definido: $q_1(x)$ é um monômio e seu único coeficiente é o produto do coeficiente líder de $f(x)$ pelo inverso do coeficiente líder de $g(x)$ e o expoente de x é grau$(f(x))-$ grau$(g(x))$.

Multiplique $g(x)$ por $q_1(x) = a_m b_n^{-1} x^{m-n}$ e subtraia este resultado de $f(x)$, obtendo outro polinômio $f_1(x)$.

Mais precisamente, $f_1(x) = f(x) - q_1(x)g(x)$. Note que

$$\begin{aligned} q_1(x)g(x) &= (a_m b_n^{-1} x^{m-n})(b_n x^n + b_{n-1}x^{n-1} + \cdots + b_1 x + b_0) \\ &= a_m b_n^{-1} b_n x^{m-n+n} + \cdots + a_m b_n^{-1} b_1 x^{m-n+1} + a_m b_n^{-1} b_0 x^{m-n} \\ &= a_m x^m + \cdots + a_m b_n^{-1} b_1 x^{m-n+1} + a_m b_n^{-1} b_0 x^{m-n}. \end{aligned}$$

Como os polinômios $f(x)$ e $q_1(x)g(x)$ tem o mesmo grau m e o mesmo coeficiente líder a_m temos que a diferença $f(x) - q_1(x)g(x)$ é um polinômio $f_1(x)$ de grau menor que m, portanto:

Se $f_1(x) = 0$, então tomamos $q(x) = q_1(x)$ e $r(x) = 0$.

Se grau$(f_1(x)) <$ grau$(g(x))$, então tomamos $q(x) = q_1(x)$ e $r(x) = f_1(x)$.

Se grau$(f_1(x)) \geq$ grau$(g(x))$, então executamos o processo anterior colocando $f_1(x)$ no lugar de $f(x)$ e repete o processo.

Seja $f_1(x) = c_p x^p + \cdots + c_1 x + c_0$, com $c_p \neq 0$ e grau$(f_1(x)) \geq$ grau$(g(x))$ ou seja $p \geq n$, então multiplicamos $g(x)$ por $q_2(x) = c_p b_n^{-1} x^{p-n}$ (observe que $q_2(x)$ tem o mesmo padrão de $q_1(x)$) e subtraímos este resultado de $f_1(x)$ obtendo um outro polinômio $f_2(x)$ dado por:

$$\begin{aligned} f_2(x) &= f_1(x) - c_p b_n^{-1} x^{p-n} g(x) \\ &= f_1(x) - q_2(x)g(x). \end{aligned}$$

Uma análise análoga a anterior mostra que grau$(f_2(x)) <$ grau$(f_1(x))$.

Substituindo $f_1(x) = f(x) - q_1(x)g(x)$ na igualdade anterior obteremos

$$\begin{aligned} f_2(x) &= f(x) - q_1(x)g(x) - q_2(x)g(x) \\ &= f(x) - [q_1(x) + q_2(x)]g(x) \\ &= f(x) - [a_m b_n^{-1} x^{m-n} + c_p b_n^{-1} x^{p-n}]g(x). \end{aligned}$$

Se $f_2(x) = 0$ tomemos $q(x) = q_1(x) + q_2(x) = a_m b_n^{-1} x^{m-n} + c_p b_n^{-1} x^{p-n}$ e $r(x) = 0$.

Se $\text{grau}(f_2(x)) < \text{grau}(g(x))$, então tomemos $q(x) = q_1(x) + q_2(x)$ e $r(x) = f_2(x)$.

Se $\text{grau}(f_2(x)) \geq \text{grau}(g(x))$, repetimos o processo anterior.

A demonstração dada acima é construtiva e o argumento usado para obter $f_i(x)$ constitui o primeiro passo no algoritmo da divisão polinomial. O algoritmo consiste em primeiro multiplicar o polinômio divisor por outro polinômio de forma que o polinômio do resultado da multiplicação tenha o mesmo grau e coeficiente líder do polinômio dividendo, isso é possível pois o coeficiente líder do polinômio divisor pertence a um corpo, ou seja, possui inverso multiplicativo. Com isso, ao realizar a subtração de ambos, obteremos um polinômio de grau menor. Em seguida, realizamos novamente o procedimento com o polinômio obtido no lugar do polinômio dividendo e repetimos o procedimento com o polinômio obtido novamente, com repetições sucessivas desse argumento, até que se obtenha ou o polinômio nulo ou um polinômio de grau menor do que o divisor. A cada passo o grau do polinômio $f_i(x)$ encontrado diminui estritamente, de modo que após um número finito de (no máximo m) passos, obteremos $f_i(x) = 0$ ou $\text{grau}(f_i(x)) < \text{grau}(g(x))$.

Logo, tomaremos $r(x) = f_i(x)$ e $q(x)$ conforme a soma dos $q_{i's}(x)$ provando a existência dos polinômios $q(x)$ e $r(x)$.

□

Teorema 4 (Unicidade do Algoritmo da Divisão)**.** *Seja A um corpo. Dados $f(x), g(x) \in A[x]$ com $g(x) \neq 0$, existem $q(x), r(x) \in A[x]$ únicos tais que $f(x) = g(x)q(x) + r(x)$ com $r(x) = 0$ ou* $\text{grau}(r(x)) < \text{grau}(g(x))$.

Demonstração:
Pelo Teorema 3, resta provar a unicidade de $q(x)$ e $r(x)$. Sejam $q(x), q^*(x), r(x), r^*(x) \in A[x]$ tais que

$$f(x) = g(x)q(x) + r(x) \text{ e } f(x) = g(x)q^*(x) + r^*(x), \text{ com}$$

$$r(x) = r^*(x) = 0 \text{ ou } \text{grau}(r(x)), \ \text{grau}(r^*(x)) < \text{grau}(g(x)).$$

Então,

$$g(x)q(x) + r(x) = g(x)q^*(x) + r^*(x)$$

$$r(x) - r^*(x) = [q^*(x) - q(x)]g(x).$$

Admitamos que $q(x) \neq q^*(x)$. Assim, $q(x) - q^*(x) \neq 0$ e $g(x) \neq 0$, portanto a diferença entre $r(x) - r^*(x)$ tem grau, logo:

$$\begin{aligned} \text{grau}(r(x) - r^*(x)) &= \text{grau}[q(x) - q^*(x)]g(x) \\ &= \text{grau}(q(x) - q^*(x)) + \text{grau}(g(x)) \\ &\geq \text{grau}(g(x)). \end{aligned}$$

Porém, como $\text{grau}(r(x)),\ \text{grau}(r^*(x)) < \text{grau}(g(x))$ temos que

$$\text{grau}(r(x) - r^*(x)) \leq \max\{\text{grau}(r(x)), \text{grau}(r^*(x)\} < \text{grau}(g(x)).$$

O que é absurdo! Então, $q(x) = q^*(x)$ e, portanto, $r(x) = r^*(x)$. Logo, são únicos os polinômios $q(x)$ e $r(x)$, tais que $f(x) = g(x)q(x) + r(x)$.

□

Exemplo 3. Sejam $f(x) = 6x^6 + 7x^5 + 8x^4 + 1$ e $g(x) = x^4 + x + 1$ em $\mathbb{R}[x]$. Vamos determinar o quociente e o resto da divisão euclidiana de $f(x)$ por $g(x)$, aplicando os passos do algoritmo da divisão polinomial.

Solução: Temos que

$$m = \text{grau}(f(x)) = 6, n = \text{grau}(g(x)) = 4, a_m = 6 \text{ e } b_n = 1,$$

logo:

$q_1(x) = a_m b_n^{-1} x^{m-n} = 6.1.x^{6-4} = 6x^2.$

$$\begin{aligned} f_1(x) &= f(x) - q_1(x)g(x) \\ &= f(x) - 6x^2(x^4 + x + 1) \\ &= 6x^6 + 7x^5 + 8x^4 + 1 - (6x^6 + 6x^3 + 6x^2) \\ &= 7x^5 + 8x^4 - 6x^3 - 6x^2 + 1. \end{aligned}$$

Como $\text{grau}(f_1(x)) > \text{grau}(g(x))$, então executamos o processo anterior novamente colocando $f_1(x)$ no lugar de $f(x)$.

$q_2(x) = c_p b_n^{-1} x^{p-n} = 7.1.x^{5-4} = 7x.$

$$\begin{aligned} f_2(x) &= f_1(x) - q_2(x)g(x) \\ &= f_1(x) - 7x(x^4 + x + 1) \\ &= 8x^4 - 6x^3 - 13x^2 - 7x + 1. \end{aligned}$$

Como $\text{grau}(f_2(x)) > \text{grau}(g(x))$, então executamos o processo anterior novamente colocando $f_2(x)$ no lugar de $f_1(x)$.

$q_3(x) = d_s b_n^{-1} x^{s-n} = 8.1.x^{4-4} = 8.$

$$\begin{aligned} f_3(x) &= f_2(x) - q_3(x)g(x) \\ &= f_2(x) - 8(x^4 + x + 1) \\ &= -6x^3 - 13x^2 - 15x - 7. \end{aligned}$$

Como grau$(f_3(x)) <$ grau$(g(x))$ o processo finaliza e obtemos

$r(x) = f_3(x) = -6x^3 - 13x^2 - 15x - 7$ e $q(x) = q_1(x) + q_2(x) + q_3(x) = 6x^2 + 7x + 8$.

O procedimento acima pode parecer complexo, mas, na verdade, é esse algoritmo que utilizamos desde o ensino fundamental conhecido como método da chave, como podemos indentificar no próximo exemplo.

Exemplo 4. Sejam $f(x) = 6x^6 + 7x^5 + 8x^4 + 1$ e $g(x) = x^4 + x + 1$ em $\mathbb{R}[x]$, vamos aplicar o algoritmo da divisão de $f(x)$ por $g(x)$, utilizando o método da chave.

Solução:

$$\begin{array}{rl} f(x) \to & 6x^6 + 7x^5 + 8x^4 + 1 \;\big|\; x^4 + x + 1 \quad \leftarrow g(x) \\ -q_1(x)g(x) \to & \underline{-6x^6 - 6x^3 - 6x^2} \qquad\qquad 6x^2 + 7x + 8 \;\leftarrow q(x) \\ r_1(x) \; ------ \to & 7x^5 + 8x^4 - 6x^3 - 6x^2 + 1 \qquad\quad \uparrow \quad \uparrow \quad \uparrow \\ -q_2(x)g(x) --- \to & \underline{-7x^5 - 7x^2 - 7x} \qquad\qquad q_1(x)\; q_2(x)\; q_3(x) \\ r_2(x) ------- \to & 8x^4 - 6x^3 - 13x^2 - 7x + 1 \\ -q_3(x)g(x) \; ------ \to & \underline{-8x^4 - 8x - 8} \\ r_3(x) \; -------- \to & -6x^3 - 13x^2 - 15x - 7 \leftarrow r(x). \end{array}$$

Sendo assim,

$$q(x) = q_1(x) + q_2(x) + q_3(x) = 6x^2 + 7x + 8$$

e

$$r(x) = r_3(x) = -6x^3 - 13x^2 - 15x - 7.$$

Note que:

$q_1(x)$ é obtido dividindo o termo de maior grau de $f(x)$ pelo termo de maior grau de $g(x)$.

$q_2(x)$ é obtido dividindo o termo de maior grau de $r_1(x)$ pelo termo de maior grau de $g(x)$.

$q_3(x)$ é obtido dividindo o termo de maior grau de $r_2(x)$ pelo termo de maior grau de $g(x)$.

Logo, $f(x) = g(x)q(x) + r(x)$. Portanto,

$$f(x) = (x^4 + x + 1)(6x^2 + 7x + 8) + (-6x^3 - 13x^2 - 15x - 7).$$

Definição 7. *Dizemos que $f(x)$ é divisível por $g(x)$ quando na divisão de $f(x)$ por $g(x)$ o resto for o polinômio nulo.*

Abaixo os comandos do SINGULAR para efetuar a divisão entre polinômios do Exemplo 4.

```
> ring A = 0, (x), dp;
> poly f = 6x6 + 7x5 + 8x4 + 1;
```

```
> f;
6x6+7x5+8x4+1
> poly g = x4 + x + 1;
> division(f,g);
[1]:
   _[1,1]=6x2+7x+8
[2]:
   _[1]=-6x3-13x2-15x-7
[3]:
   _[1,1]=1
```

Note que a primeira entrada do comando `division(f,g)` retornou o quociente $q(x) = 6x^2 + 7x + 8$ e a segunda entrada retornou o resto $r(x) = -6x^3 - 13x^2 - 15x - 7$ da divisão de $f(x)$ por $g(x)$.

Falaremos mais sobre os principais comandos básicos do SINGULAR no Capítulo 3.

2.1.2 ORDEM MONOMIAL

Antes de descrever um algoritmo da divisão em um anel de polinômios em várias variáveis $\mathbb{K}[x_1, \ldots, x_n]$, precisamos de uma maneira para ordenar os monômios do polinômio. Ordenar monômios em n variáveis é o mesmo que ordenar sobre $\mathbb{N}^n$. Podemos tornar esta ordem única escolhendo uma ordem total sobre o conjunto dos monômios. O objetivo aqui é apenas apresentar a definição e fazer exemplos. Veja mais sobre ordens monomiais no livro da referência [2].

Definição 8. *Uma ordem monomial é uma ordem total $>$ sobre o conjunto dos monômios $Mon_n = \{x^\alpha | \alpha \in \mathbb{N}^n\}$ em n variáveis satisfazendo o seguinte:*

$$x^\alpha > x^\beta \Longrightarrow x^\gamma x^\alpha > x^\gamma x^\beta$$

para todo $\alpha, \beta, \gamma \in \mathbb{N}^n$. Dizemos que $>$ é uma ordem monomial sobre $A[x_1, \ldots, x_n]$, A um anel, considerando que $>$ é uma ordem monomial sobre Mon_n.

Identificamos Mon_n com $\mathbb{N}^n$, e então uma ordem monomial é uma ordem total sobre $\mathbb{N}^n$.

Uma ordem típica e importante é a **ordem lexicográfica** sobre $\mathbb{N}^n$, definida por: $x^\alpha > x^\beta$ se, e somente se, a primeira entrada não nula de $\alpha - \beta$ é positiva.

Trabalhar com uma determinada ordem, nos permite representar um polinômio em um computador como uma lista ordenada de coeficientes, tornando testes de igualdade simples e rápidos.

Vamos considerar um exemplo usando a ordem lexicográfica denotada por `lp` no SINGULAR. Lembrando, que no SINGULAR antes de definir objetos, primeiro devemos definir um anel.

```
> ring A=0,(x,y,z),lp;
```

A linha de comando acima, significa que $A = \mathbb{Q}[x, y, z]$, onde: 0 é a característica do anel; os coeficientes de A pertencem ao corpo do números racionais $\mathbb{Q}$; x, y e z são as variáveis de A e `lp` define a ordem lexicográfica com $x > y > z$.

```
> poly f = y6z3+4x3y3z2+3x5-z5+3y2;      //definindo o polinômio f no anel A
> f;                                      //apenas mostrando f
3x5+4x3y3z2+y6z3+3y2-z5
```

Observe que, quando colocamos o comando `> f` acima, o SINGULAR mostra f com os monômios obedecendo a ordem `lp`. Como $3x^5$ e $4x^3y^3z^2$ correspondem respectivamente às listas $\alpha = (5, 0, 0)$ e $\beta = (3, 3, 2)$, segue que $\alpha - \beta = (2, -3, -2)$, e como o primeiro termo não nulo é positivo, então $3x^5 > 4x^3y^3z^2$. Analogamente, $4x^3y^3z^2 > y^6z^3 > 3y^2 > z^5$.

Os comandos abaixo são usados para operações com polinômios no SINGULAR.

```
> leadmonom(f);       //monômio lider de f
x5
> leadexp(f);        //lista com os expoentes do monômio lider de f
5,0,0
> lead(f);           //termo lider de f
3x5
> leadcoef(f);      //coeficiente do termo lider de f
3
```

2.1.3 ALGORITMO DA DIVISÃO EM $\mathbb{K}[x_1, \ldots, x_n]$

Fixamos primeiro uma ordem monomial em $\mathbb{N}^n$. Suponha que são dados um polinômio f e um conjunto ordenado $(g_1, \ldots, g_s)$ de polinômios em $\mathbb{K}[x_1, \ldots, x_n]$. O algoritmo da divisão encontra polinômios $a_1, \ldots, a_s$ e r em $\mathbb{K}[x_1, \ldots, x_n]$ tal que

$$f = a_1g_1 + \cdots + a_sg_s + r, \tag{2.1}$$

onde $r = 0$ ou nenhum monômio em r é divisível por qualquer $LT(g_i), i = 1 \ldots s$, (LT significa termo lider).

Veja o algoritmo da divisão:

DADOS DE ENTRADA: $g_1, \ldots, g_s, f$
$a_i := 0; \quad i = 1 \ldots s; \quad r := 0; \quad p := f;$
ENQUANTO $p \neq 0$ FAÇA
$i := 1;$
DNE := false (DNE = divisão não efetuada)
(ENQUANTO $i \leq s$ e DNE = false) FAÇA
SE ($LT(g_i)$ DIVIDE $LT(p)$) ENTÃO
$a_i := a_i + LT(p)/LT(g_i);$
$p := p - (LT(p)/LT(g_i))g_i;$
DNE = true
SENÃO
$i := i + 1;$
SE (NDE = false) ENTÃO
$r := r + LT(p)$
$p := p - LT(p)$
DADOS DE SAÍDA: $a_1, \ldots, a_s, r$

ALGORITMO DA DIVISÃO EM $\mathbb{K}[x_1, \ldots, x_n]$.

Observação 1. 1. De acordo com a equação 2.1, se $r = 0$, então $f \in \langle g_1, \ldots, g_s \rangle$.

2. O resto r depende da ordem dos g_i.

Note que no algoritmo acima, na linha "SE ($LT(g_i)$ DIVIDE $LT(p)$) ENTÃO", o índice i varia de 1 até s, logo uma vez fixada a posição dos g_i o algoritmo deverá rodar até o final.
Vamos explicar o funcionamento deste algoritmo através de exemplos.

Exemplo 5. Sejam os polinômios $f := x^2y + xy^2 + y^2$, $g_1 := xy - 1$ e $g_2 := y^2 - 1$. Vamos efetuar a divisão de f por g_1 e g_2 usando a ordem lexicográfica ($x > y$).

$p : x^2y + xy^2 + y^2$	$g_1 : xy - 1$	**Passo 1**: $LT(g_1) = xy$ divide $LT(p) = x^2y$
$\underline{x^2y - x}$	$\underline{g_2 : y^2 - 1}$	Então, $a_1 := (LT(p)/LT(g_1)) = x$
$xy^2 + x + y^2$	$a_1 : x$	
	$a_2 : 0$	
	$r : 0$	

$p : xy^2 + x + y^2$	$g_1 : xy - 1$	**Passo 2**: $LT(g_1) = xy$ divide $LT(p) = xy^2$
$\underline{xy^2 - y}$	$\underline{g_2 : y^2 - 1}$	Então, $a_1 := a_1 + (LT(p)/LT(g_1)) = a_1 + y$
$x + y^2 + y$	$a_1 : x + y$	
	$a_2 :$	
	$r : 0$	

$$\begin{array}{rl|l|l} p: & x + y^2 + y & g_1 : xy - 1 & \textbf{Passo 3}: LT(g_1) = xy \text{ não divide } LT(p) = x \\ p: & y^2 + y & \underline{g_2 : y^2 - 1} & LT(g_2) = y^2 \text{ não divide } LT(p) = x \\ & & a_1 : x + y & \text{neste caso, movemos o } LT(p) = x \text{ para o resto } r \\ & & a_2 : & \\ & & r : x & \end{array}$$

$$\begin{array}{rl|l|l} & y^2 + y & g_1 : xy - 1 & \textbf{Passo 4}: LT(g_1) = xy \text{ não divide } LT(p) = y^2 \\ p: & \underline{y^2 - 1} & \underline{g_2 : y^2 - 1} & LT(g_2) = y^2 \text{ divide } LT(p) = y^2 \\ & y + 1 & a_1 : x + y & \text{Então, } a_2 := (LT(p)/LT(g_2)) = 1 \\ & & a_2 : 1 & \\ & & r : x & \end{array}$$

$$\begin{array}{rl|l|l} & y + 1 & g_1 : xy - 1 & \textbf{Passo 5}: LT(g_1) = xy \text{ não divide } LT(p) = y \\ p: & & \underline{g_2 : y^2 - 1} & LT(g_2) = y^2 \text{ não divide } LT(p) = y \\ p: & 1 & a_1 : x + y & \text{neste caso, movemos o } LT(p) = y \text{ para o resto } r \\ & & a_2 : 1 & \\ & & r : x + y & \end{array}$$

$$\begin{array}{rl|l|l} & & g_1 : xy - 1 & \textbf{Passo 6}: LT(g_1) = xy \text{ não divide } LT(p) = 1 \\ p: & 1 & \underline{g_2 : y^2 - 1} & LT(g_2) = y^2 \text{ não divide } LT(p) = 1 \\ p: & 0 & a_1 : x + y & \text{neste caso, movemos o } LT(p) = 1 \text{ para o resto } r \\ & & a_2 : 1 & \text{---------------------------------} \\ & & r : x + y + 1 & p := 0 \text{ e o algoritmo da divisão termina.} \end{array}$$

Portanto,

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

Os polinômios do Exemplo 5 são os mesmos do Exemplo 6, apenas permutamos a posição de g_1 e g_2.

Exemplo 6. Sejam os polinômios $f := x^2y + xy^2 + y^2$, $g_1 := y^2 - 1$ e $g_2 := xy - 1$. Como no Exemplo 5, faremos a divisão de f por g_1 e g_2 usando a ordem lexicográfica ($x > y$) e concluíremos que o resto é $r := 2x + 1$.

$$\begin{array}{rl|l|l} p: & x^2y + xy^2 + y^2 & g_1 : y^2 - 1 & \textbf{Passo 1}: LT(g_1) = y^2 \text{ não divide } LT(p) = x^2y \\ & & \underline{g_2 : xy - 1} & LT(g_2) = xy \text{ divide } LT(p) = x^2y \\ & \underline{x^2y - x} & a_1 : 0 & \text{Então, } a_2 := (LT(p)/LT(g_2)) = x \\ & xy^2 + x + y^2 & a_2 : x & \\ & & r : 0 & \end{array}$$

$$\begin{array}{r|l|l} & g_1 : y^2-1 & \textbf{Passo 2}\text{: } LT(g_1)=y^2 \text{ divide } LT(p)=xy^2 \\ p : xy^2+x+y^2 & \underline{g_2 : xy-1} & \text{Então, } a_1 := (LT(p)/LT(g_1)) = x \\ \underline{xy^2-x} & a_1 : x & \\ 2x+y^2 & a_2 : x & \\ & r : 0 & \end{array}$$

$$\begin{array}{r|l|l} & g_1 : y^2-1 & \textbf{Passo 3}\text{: } LT(g_1)=y^2 \text{ não divide } LT(p)=2x \\ p : \ 2x \ + \ y^2 & \underline{g_2 : xy-1} & LT(g_2)=xy \text{ não divide } LT(p)=2x \\ p : \ y^2 & a_1 : x & \text{neste caso, movemos o } LT(p)=2x \text{ para o resto } r \\ & a_2 : x & \\ & r : 2x & \end{array}$$

$$\begin{array}{r|l|l} & g_1 : y^2-1 & \textbf{Passo 4}\text{: } LT(g_1)=y^2 \text{ divide } LT(p)=y^2 \\ p : y^2 & \underline{g_2 : xy-1} & \text{Então, } a_1 := (LT(p)/LT(g_1)) = 1 \\ \underline{y^2-1} & a_1 : x+1 & \\ 1 & a_2 : x & \\ & r : 2x & \end{array}$$

$$\begin{array}{r|l|l} & g_1 : y^2-1 & \textbf{Passo 5}\text{: } LT(g_1)=y^2 \text{ não divide } LT(p)=1 \\ p : 1 & \underline{g_2 : xy-1} & LT(g_2)=xy \text{ não divide } LT(p)=1 \\ p : 0 & a_1 : x+y & \text{neste caso, movemos o } LT(p)=1 \text{ para o resto } r \\ & a_2 : x & \hline \\ & r : 2x+1 & p := 0 \text{ e o algoritmo da divisão termina.} \end{array}$$

Portanto,

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

Como podemos observar se alterarmos a ordem dos polinômios divisores g_1 e g_2, obtemos restos diferentes.

Exemplo 7. Sejam os polinômios $f := xy^2 - x$, $g_1 := y^2 - 1$ e $g_2 := xy + 1$. Usando a ordem lexicográfica ($x > y$), mostre que f dividido por g_1 e g_2 tem resto $r := 0$.

$$\begin{array}{r|l|l} & g_1 : y^2-1 & \textbf{Passo 1}\text{: } LT(g_1)=y^2 \text{ divide } LT(p)=xy^2 \\ p : xy^2-x & \underline{g_2 : xy+1} & \text{Então, } a_1 := (LT(f)/LT(g_1)) = x \\ \underline{xy^2-x} & a_1 : x & \\ 0 & a_2 : 0 & \\ & r : 0 & \end{array}$$

Portanto, temos uma divisão exata

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

Exercício 1. Sejam os polinômios $f := xy^2 - x$, $g_1 := xy + 1$ e $g_2 := y^2 - 1$. Usando a ordem lexicográfica ($x > y$), mostre que f dividido por g_1 e g_2 tem resto $r := -x - y$.

No Exemplo 7, o resto é $r := 0$, logo podemos concluir que $f := xy^2 - x$ pertence ao ideal gerado por $g_1 := y^2 - 1$ e $g_2 := xy + 1$. Mas, pelo Exercício 1, usando os mesmos g_1 e g_2 (porém permutados), temos $r \neq 0$, e não podemos concluir se f pertence ao ideal gerado por eles. Assim, o algoritmo da divisão (da forma que está definido acima) não fornece um teste para saber se um polinômio f pertence a um ideal. Felizmente, é possível resolver este problema usando bases de Groebner.

Bases de Groebner é uma ferramenta de extrema importância, pois permite resolver problemas sobre ideais polinomiais, e consequentemente sobre o estudo de variedades afins. Usando bases de Groebner é sempre possível (dependendo da memória do computador) decidir se um polinômio pertence ou não a um determinado ideal. Não abordaremos sobre essas bases de Groebner neste texto, porém, faremos uso dessas bases pois elas estão implementadas no SINGULAR. O objetivo é usar essas bases para simplificar ideais e efetuar o algoritmo da divisão em anéis de polinômios de várias variáveis. Veja mais sobre bases de Groebner nos livros da referência [1, 2].

3. Introdução ao Singular

Neste capítulo apresentaremos uma breve introdução ao sistema de álgebra computacional Singular, [6].

A maioria do texto deste capítulo foi extraído de [5], [4], e do manual online do Singular. Para maiores detalhes o leitor poderá pesquisar o manual do Singular, que está disponibilizado online.

O Singular, é um sistema de álgebra computacional, designado para cálculos com polinômios. Este sistema foi desenvolvido para dar suporte a pesquisa matemática, principalmente nas áreas de álgebra comutativa, geometria algébrica e teoria de singuladidades. Os principais objetos que podemos trabalhar no Singular, são ideais e módulos sobre uma grande variedade de anéis. Esses anéis, por exemplo, poderão ser: anéis de polinômios sobre corpos finitos e sobre o corpo dos números racionais, entre outros anéis.

O Singular contém implementado um dos mais rápidos e mais gerais algoritmos para calcular bases de Groebner. Além do mais, podemos fatorar polinômios, calcular resultantes, realizar decomposição primária de ideais e muitas outras funcionalidades.

O Singular está disponível livremente para a maioria das plataformas. Versões do Singular poderão ser baixadas através dos sites https://www.singular.uni-kl.de/download.html. Também é possível usar uma interface web do Singular, criado por Franziska Hinkelmann, Lars Kastner and Mike Stillman, através da página https://www.singular.uni-kl.de:8003/.

3.1 Primeiros passos

Primeiros passos para usar o Singular.

1. Uma vez que o SINGULAR é iniciado, aparece o prompt “>” a partir daí podemos digitar os comandos.

2. Todo comando ou sentença deverá ser terminado com “;” . O símbolo ponto e vírgula diz que o comando deverá ser interpretado.

3. Todos os objetos tem um tipo, por exemplo, uma variável inteira é definida pela palavra `int`.

```
> int k = 12;
```

4. Uma associação é feita usando o símbolo "=".

5. Para testar uma igualdade o conjunto de símbolos "==" é usado.

6. Testes para desigualdade é feito usando "! =" ou "<>", onde 0 representa a variável boleana com valor FALSE (falso), e qualquer outro valor retornado, representa a variável boleana TRUE (verdadeiro).

```
> k == 12;
1;
> k != 12;
0;
```

7. Para ver o valor de um objeto, pasta escrever o nome do objeto e executar o comando (apertando a tecla ENTER).

```
> k;
12;
```

8. O comando

```
> help;  //abre um arquivo de ajuda do Singular
```

9. Textos escritos depois de // denota um comentário que é ignorado nos cálculos.

Variáveis do tipo string também podem ser definidas e elas são delimitadas por dupla aspas. São importantes para comentar os resultados de saída de alguma computação.

No SINGULAR podemos definir aneis de polinômios sobre os seguintes corpos:

1. corpo do números racioanis $\mathbb{Q}$;

2. corpos finitos F_p, onde p é um número primo ≤ 2147483629;

3. extensões algébricas simples de $\mathbb{Q}$ ou F_p;

4. números em ponto flutuante real (precisão simples);

5. números em ponto flutuante real (precisão arbitrária pescrita);

6. números em ponto flutuante complexo (precisão arbitrária pescrita).

Observação 2. Na verdade, cálculos sobre corpos finitos, sobre o conjunto dos números inteiros, sobre o corpo dos números racionais são exatos, limitado somente pela memória interna do computador. Por outro lado, números em pontos flutuantes (floating point numbers), não representam o corpo dos números reais ou complexos. Por exemplo, devido a erros de arredondamentos, o produto entre dois números não nulos (ou a diferença de dois números não nulos distintos) podem resultar em zero. Porém, em muitos casos com o conhecimento técnico e teórico podemos confiar nos resultados, lembrando que a responsabilidade é sempre do usuário em analisar os dados, mesmo em computadores de alta precisão.

Para realizar operações no SINGULAR, primeiramente precisamos definir um anel.

Abaixo uma lista de exemplos de alguns anéis que podemos definir e trabalhar no SINGULAR.

1. **Computação sobre o corpo dos números racionais:**

```
> ring A=0, x, dp;
> number n = 2/3;
> n^3;
8/27;
```

`> ring A=0, x, dp;` este comando define o anel de polinômios da variável x, característica zero, com coeficientes em $\mathbb{Q}$, e ordem monomial global `dp`.

2. **Computação sobre corpos finitos:**

```
> ring A1=32003, (x), dp;
> number n=1010253;
> n^8;
3451;
```

`> ring A1=32003, x, dp;` este comando define o anel A1= $\mathbb{Z}_p[x]$, anel de polinômios em x e de característica $p = 32003$ com coeficientes no corpo $\mathbb{Z}_p$.

3. **Computação em números de ponto flutuante,** 100 **dígitos de precisão:**

```
> ring r=(real,100),(x),dp;
> number n=2/5;
> n^9000;
0.3466745429523766868669875201719137528580444595048549101118260943266639
  8570683829345681486475986936 89e-3581
>
```

Temos um número com 3581 dígitos depois do ponto. Entretanto, somente 100 dígitos são computados.

4. **Computação em números complexos em ponto flutuante,** 20 **dígitos de precisão:**

```
> ring R1=(complex, 20,i), (x), dp;
> number n = 123456.0+0.021i;
> n^7;
0.43710463467674779545e+36+i*0.52046381947051861 05e+31;
```

O resultado é um número complexo com parte real e imaginária respectivamente com 36 e 31 dígitos. Entretanto, somente 20 dígitos são computados.

5. **Computação em anéis polinomiais (sobre $\mathbb{Q}$)**

```
> ring R=0,(x,y,z), lp;
> poly f=x4+zy2;
> f*f-2*f;
x8+2x4y2z-2x4+y4z2-2y2z
>
```

$R = \mathbb{Q}[x, y, z]$ é um anel polinomial de característica 0 sobre $\mathbb{Q}$, nas variáveis (x, y, z). (`lp` é uma ordem monomial global lexicográfica.)

6. **Mais exemplos de anéis que podemos definir no SINGULAR.**

   i. `> ring r1=integer,(a,b),lp;`
   Anel de inteiros nas variáveis a e b.

   ii. `> ring r2=(integer, 20),(a,b),lp;`
   Anel de inteiros módulo 20, variáveis a e b.

   iii. `> ring r3 = 0,(x(1..48)),dp;`
   Anel sobre $\mathbb{Q}$, de característica 0 e variáveis $x(1), \ldots, x(48)$.

   iv.
   ```
   > ring r4 = 0,(x,y,z),dp;
   > ideal I=x^2,y,z^2;
   > qring r6 = std(I);  \\ anel quociente módulo I
   ```
   O anel $r6$ é o anel quociente módulo I, $r6 = \frac{\mathbb{Q}[x,y,z]}{\langle x^2,y,z^2\rangle}$.

   v. `> ring r=(0,a,b),(x,y,z),lp;`
   Anel de polinômios nas variáveis x, y, z, onde os coeficiente são frações nas variáveis a e b, $r = \mathbb{Q}(a, b)[x, y, z]$.

No SINGULAR, podemos definir vários anéis no mesmo ambiente. Para passar de um anel para outro, devemos usar a função `setring`. Por exemplo, se estamos no anel r e desejarmos ir para o anel r_1, basta digitar

```
> setring r1;
```

Agora, o anel atual é o anel r_1, porém os dados do anel r não se alteram e nem são deletados.

No SINGULAR, também é possível programar, criar procedimentos, bibliotecas, e a sintaxe é baseada na linguagem C. A distribuição do SINGULAR contém diversas bibliotecas com procedimentos e rotinas que podem ser carregadas quando necessárias.

```
> LIB "all.lib"; //carrega todas as bibliotecas do Singular.
```

Objetos definidos em um anel podem ser transportados para outros anéis sem a necessidade de redefini-los novamente.

`imap` é uma aplicação entre anéis que é uma identidade entre as variáveis e parâmetros de mesmo nome e 0 de outro modo.

`fetch` é uma aplicação entre anéis que que é a identidade sobre a posição das variáveis, isto é, a i-ésima variável do anel fonte (anel de saída) é mapeada na i-ésima variável no anel meta (anel de chegada). Os corpos coeficientes devem ser compatíveis.

```
> ring r1=0,(x,y,z),dp;
> ring r2=0,(y,x,z),dp;
> ring r3=0,(a,b,c),dp;
> setring r1;
> poly f = x2+y3+z2+xz+y2z;
> f;
y3+y2z+x2+xz+z2
> setring r2;
> poly f=imap(r1,f);f;
y3+y2z+x2+xz+z2                    \\usa o nome das variáveis
> poly g=fetch(r1,f);g;
x3+x2z+y2+yz+z2                    \\usa a posição das variáveis
> setring r3;
> poly f=imap(r1,f);f;
0
> poly g=fetch(r1,f);g;
b3+b2c+a2+ac+c2
```

"Maps" são aplicações entre anéis. O anel meta da aplicação `map` é sempre o anel atual. Aplicações com corpos diferentes são possíveis.

```
> ring r1=0,(x,y,z),dp;
> ring r3=0,(a,b,c),dp;
> setring r1;
> ideal i=x2+y2+z;
```

```
> setring r3;
> map M=r1, a2,b,c+1;
> ideal j=M(i);j;
j[1]=a4+b2+c+1
```

Neste exemplo, temos que M é a aplicação:

$$\begin{array}{rccc} M & : & r_1 & \longrightarrow & r_3 \\ & & x & \longmapsto & a^2 \\ & & y & \longmapsto & b \\ & & z & \longmapsto & c+1 \end{array}$$

Então, $M(i) = (a^2)^2 + b^2 + c + 1 = a^4 + b^2 + c + 1$.

Bases de Groebner ou bases Standard, são usadas por exemplo, para verificar se uma função polinomial se anula sobre um conjunto algébrico, ou em termos algébricos, se um polinômio pertence a um ideal. Para isto, usamos os comandos `groebner` ou `std`.

```
> LIB "standard.lib";   \\biblioteca para bases standard ou de Groebner
> ring r=0,(x,y),lp;
> ideal I=xy-1,y2-1;
> ideal G=groebner(I); \\retorna uma base de Groebner do ideal I
> G;
G[1]=y2-1
G[2]=x-y
```

Abaixo alguns comandos muito úteis disponíveis no SINGULAR.

O comando `reduce`, reduz um polinômio, um vetor, ideal ou módulo para sua forma normal a respeito a um outro ideal ou módulo.

```
> ring r=0,(x,y),ds;
> ideal I=x2+y2,xy;
> ideal J=std(I);
> reduce(yx2+y3+x2y,J);
0                        //significa que yx2+y3+x2y é um elemento de I
> reduce(x+y,J);
x+y                      //significa que x+y não é um elemento de I
```

O comando `division`, calcula a divisão com resto entre dois ideais.

Exemplo 8. Considere o polinômio definido por $f(x,y) = x^2y + xy^2 + y^2$ e seja o ideal $I = \langle y^2 - 1, x - y\rangle$. Encontrar a_1, a_2, r tal que $f = a_1(y^2-1) + a_2(x-y) + r$, onde r é o resto.

```
> ring r=0,(x,y),lp;
> ideal I=y2-1,x-y;
> poly f=x2y+xy2+y2;
> list L=division(f,I);
> L[1]; //retorna ai's
_[1,1]=2x+1
_[2,1]=xy+2
> L[2]; //retorna o resto r
_[1]=2y+1
```

Portanto,

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

Note que, `reduce(f,std(I))`, retorna o resto acima $r = 2y + 1$.

```
> ring r=0,(x,y),lp;
> ideal I=y2-1,x-y;
> poly f=x2y+xy2+y2;
> reduce(f,std(I));
2y+1                    //igual ao resto r obtido acima
```

O comando `factorize`, computa os fatores irredutíveis de um polinômio.

```
> ring r=0,(x,y),dp;
> poly i=(x-1)^2*(y^2+1);
> factorize(i);
[1]:
   _[1]=1
   _[2]=x-1
   _[3]=y2+1
[2]:
   1,2,1      //o fator (x-1) tem multiplicidade 2
              //o fator y^2+1 é irredutível em Q[x]
```

O terceito item da primeira entrada do comando `factorize(i)` acima, retornou o fator $y^2 + 1$. Este fator é irredutível em $\mathbb{Q}[x]$. Mas podemos fatorá-lo com coeficientes complexos conforme mostrado abaixo.

```
> ring q=(0,i),y,dp;
> minpoly =i2+1;
> poly p=y2+1;
> factorize(p);
```

```
[1]:
   _[1]=1
   _[2]=y+(i)
   _[3]=y+(-i)
[2]:
   1,1,1
```

O resultado do comando `factorize(p)`, diz que

$$y^2 + 1 = (y + i)(y - i),$$

onde, i é um número complexo, $i = \sqrt{-1}$.

O comando `subst`, substitui uma ou mais variáveis por polinômios ou constantes. Este comando é muito útil para avaliar funções.

```
>  ring r=0,(x,y,z),dp;
> poly f=x2+y3+xz2+z2+1;
> subst(f,x,y,z,1);  // x  substituido por y e z por 1
y3+y2+y+2
```

4. Conjunto algébrico afim

O conjunto de zeros em comum de uma dada família de polinômios no anel de polinômios $\mathbb{K}[x_1, \ldots, x_n]$, onde $\mathbb{K}$ é um corpo, é chamado de conjunto algébrico afim. Este conjunto de zeros está contido no espaço afim $\mathbb{K}^n = \mathbb{K} \times \cdots \times \mathbb{K}$, (n-vezes).

Pelo conceito de conjunto algébrico é possível constituir uma relação entre a álgebra e a geometria, o que permite reformular problemas geométricos em termos algébricos e vice-versa. Esta relação será tratada com exemplos práticos no Capítulo 5.

Neste capítulo, definiremos conjuntos algébricos afins acompanhados com vários exemplos. Para um estudo mais aprofundado sobre conjuntos algébricos afins, veja [2].

4.1 Definição e exemplos de conjuntos algébricos afins

O conjunto $\mathbb{K}^n = \{(a_1, \ldots, a_n) : a_1, \ldots, a_n \in \mathbb{K}\}$ é chamado de espaço afim n-dimensional sobre $\mathbb{K}$. Por exemplo, se $\mathbb{K} = \mathbb{R}$, temos o usual e conhecido espaço euclidiano $\mathbb{R}^n$. Cada polinômio $f \in \mathbb{K}[x_1, \ldots, x_n]$ define uma função $f : \mathbb{K}^n \to \mathbb{K}$. O valor de f em $(a_1, \ldots, a_n) \in \mathbb{K}^n$ é obtido substituindo x_i por a_i e calculando o resultado da expressão em $\mathbb{K}$. Mais precisamente se escrevemos $f = \sum_\alpha c_\alpha x^\alpha$ para $c_\alpha \in \mathbb{K}$, então $f(a_1, \ldots, a_n) = \sum_\alpha c_\alpha a^\alpha \in \mathbb{K}$, onde $a = (a_1, \ldots, a_n)$ e $a^\alpha = a_1^{\alpha_1} \cdots a_n^{\alpha_n}$.

Definição 9. *O conjunto de todas as soluções simultâneas $(a_1, \ldots, a_n) \in \mathbb{K}^n$ de um sistema de equações polinomiais:*

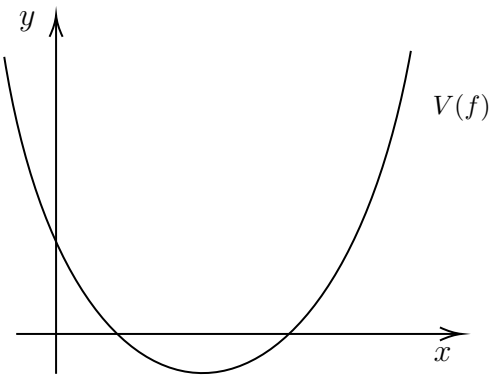
$$\begin{aligned} f_1(x_1, \ldots, x_n) &= 0 \\ f_2(x_1, \ldots, x_n) &= 0 \\ &\vdots \\ f_s(x_1, \ldots, x_n) &= 0 \end{aligned}$$

é conhecido como o conjunto algébrico afim definido por $f_1, \ldots, f_s$, e é denotado por $V(f_1, \ldots, f_s)$. Um subconjundo $V \subset \mathbb{K}^n$ é dito ser um conjunto algébrico afim se $V = V(f_1, \ldots, f_s)$ para alguma coleção de polinômios $f_i \in \mathbb{K}[x_1, \ldots, x_n]$.

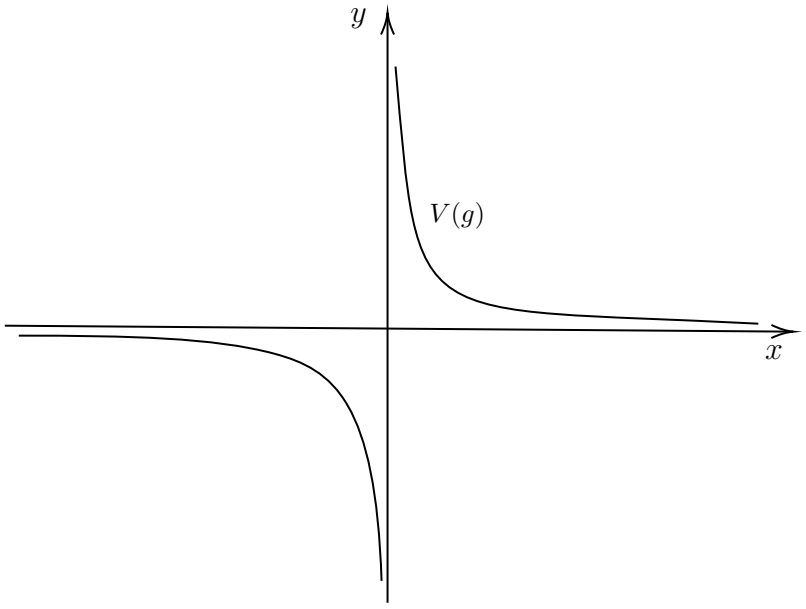
Observação 3. Quando $\mathbb{K}$ é infinito, dois polinômios definem a mesma função sobre $\mathbb{K}^n$ se, e somente se, são iguais em $\mathbb{K}[x_1, \ldots, x_n]$. Note que qualquer equação $p = q$, onde $p, q \in \mathbb{K}[x_1, \ldots, x_n]$, pode ser reescrita da forma $p - q = 0$, então é usual escrever todas as equações da forma $f = 0$.

Exemplo 9 (Cônicas)**.** As cônicas: parábolas, elipses e hipérboles, são exemplos de conjuntos algébricos afins.

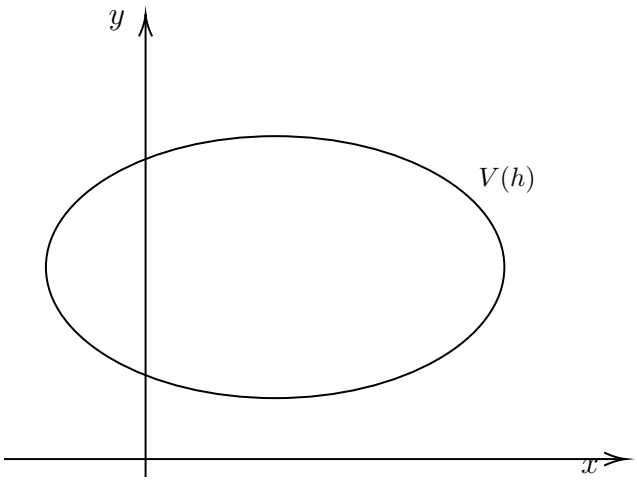
Parábola: $y - ax^2 - bx - c = 0$. Os pontos do plano $\mathbb{R}^2$ que anulam esta equação polinomial é um conjunto algébrico afim. Abaixo $V(f)$, para $f(x, y) = y - x^2 + 4x - 3 = 0$.



Hipérbole: Vamos tomar como exemplo a hipérbole $y = \frac{1}{x}$. Aqui temos uma função racional, mas como $x \neq 0$, então $y \neq 0$, logo podemos considerar a equação polinomial $g(x, y) = xy - 1 = 0$. Assim, temos o conjunto algébrico afim $V(g)$. De modo geral, gráfico de função racional pode ser visto como conjunto algébrico afim.



Elipse: Vamos tomar como exemplo a elipse $h(x,y) = 2x^2 + 9y^2 - 4x - 36y + 30 = 0$. Assim, temos o conjunto algébrico afim $V(h)$.



Note que no caso da hipérbole e da parábola, os conjuntos $V(f)$ e $V(g)$ podem ser dados como gráfico de funções, o que não ocorre no caso da elipse $V(h)$.

Em álgebra linear estudamos como resolver um sistema linear sobre um corpo $\mathbb{K}$ (geralmente $\mathbb{K} = \mathbb{R}$ ou $\mathbb{C}$). O conjunto solução de um sistema linear também é um exemplo de conjunto algébrico afim e muito importante devido suas aplicações.

Nos dois exemplos seguintes vamos analisar a solução do sistema linear

$$S: \begin{cases} x + 2y - 2z - a = 0 \\ 2x - 3y + z - b = 0 \\ -x - y + 3z - c = 0 \\ x + y + z = 0 \end{cases}$$

em dois anéis diferentes. O primeiro em um anel considerando x, y, z como variávies e a, b, c como parâmetros e no outro anel considerando x, y, z, a, b, c como variáveis. A importância desse exemplo, facilitará no entendimento das resoluções de problemas no Capítulo 5.

Exemplo 10. Considere o seguinte sistema linear S nas variáveis x, y, z e coeficientes no anel $\mathbb{R}(a,b,c)$. Lembramos que os elementos do anel $\mathbb{R}(a,b,c)$ são frações do tipo $\dfrac{f(a,b,c)}{g(a,b,c)}$ com $g(a,b,c) \neq 0$. Assim, afim de resolver o sistema S, vamos trabalhar no anel $A := \mathbb{R}(a,b,c)[x,y,z]$.

$$S: \begin{cases} x + 2y - 2z = a \\ 2x - 3y + z = b \\ -x - y + 3z = c \\ x + y + z = 0 \end{cases}$$

O sistema S possui 4 linhas e 3 colunas. Escalonando o sistema linear S, obtemos o sistema linear S_1 equivalente a S, dado por:

$$S_1 : \begin{cases} x + 2y - 2z = a \\ 7y - 5z = 2a - b & \xleftarrow{L_2=2L_1-L_2} \\ y + z = a + c & \xleftarrow{L_3=L_1+L_3} \\ y - 3z = a & \xleftarrow{L_4=L_1-L_4} \end{cases}$$

$$S_1 : \begin{cases} x + 2y - 2z = a \\ 7y - 5z = 2a - b \\ -12z = -5a - b - 7c & \xleftarrow{L_3=L_2-7L_3} \\ 4z = c & \xleftarrow{L_4=L_3-L_4} \end{cases}$$

$$S_1 : \begin{cases} x + 2y - 2z = a \\ 7y - 5z = 2a - b \\ z = \frac{5a}{12} + \frac{b}{12} + \frac{7c}{12} \\ z = \frac{c}{4} \end{cases}$$

Substituindo o valor de $z = \frac{c}{4}$ em L_2, teremos:

$$7y - 5z = 2a - b$$

$$7y - 5 \cdot \left(\frac{c}{4}\right) = 2a - b$$

$$28y - 5c = 8a - 4b$$

$$y = \frac{2a}{7} - \frac{b}{7} + \frac{5c}{28}.$$

Agora, substituindo o valor de $z = \frac{c}{4}$ e $y = \frac{2a}{7} - \frac{b}{7} + \frac{5c}{28}$ em L_1, teremos:

$$x + 2y - 2z = a$$

$$x + 2 \cdot \left(\frac{2a}{7} - \frac{b}{7} + \frac{5c}{28}\right) - 2 \cdot \left(\frac{c}{4}\right) = a$$

$$x + \frac{4a}{7} - \frac{2b}{7} + \frac{5c}{14} - \frac{2c}{4} = a$$

$$x = \frac{3a}{7} + \frac{2b}{7} + \frac{c}{7}.$$

Note que encontramos o valor de z, porém o sistema só terá solução se satisfazer a seguinte condição:

$$\frac{5a}{12} + \frac{b}{12} + \frac{7c}{12} = \frac{c}{4}$$

ou

$$5a + b + 4c = 0.$$

Para constatar essa condição através de um caso particular, vamos atribuir valores para a, b, c que satisfaça a condição $5a + b + 4c = 0$. Tomando $a = 0$, $b = -4$ e $c = 1$ e substituindo os valores nas linhas 3 e 4 do sistema encontramos o valor de z e analogamente encontraremos os valores de x e y

$$L_3 : z = \frac{5a}{12} + \frac{b}{12} + \frac{7c}{12} = 0 - \frac{4}{12} + \frac{7}{12} = \frac{1}{4}.$$

$$L_4 : z = \frac{c}{4} = \frac{1}{4}.$$

$$y = 0 + \frac{4}{7} + \frac{5}{28} = \frac{3}{4}$$

$$x = 0 - \frac{8}{7} + \frac{1}{7} = -1.$$

Observem que o sistema tem solução quando satisfeita a condição.

Agora vamos atribuir valores que não satisfaça a condição $5a + b + 4c = 0$. Considerando $a = 1, b = -4$ e $c = 1$ teremos:

$$L_3 : z = \frac{5a}{12} + \frac{b}{12} + \frac{7c}{12} = \frac{5}{12} - \frac{4}{12} + \frac{7}{12} = \frac{2}{3}$$

$$L_4 : z = \frac{c}{4} = \frac{1}{4}.$$

No entanto, para esses valores atribuídos para a, b e c, o sistema não teve solução, pois $\frac{1}{4} \neq \frac{2}{3}$.

Este exemplo mostra que em geral o sistema linear S não possui solução no anel $A := \mathbb{R}(a, b, c)[x, y, z]$, mas, se a condição $5a + b + 4c = 0$ for satisfeita, o sistema terá a seguinte única solução:

$$\text{Solução de S} = \left\{ \left(\frac{3a + 2b + c}{7}, \frac{8a - 4b + 5c}{28}, \frac{c}{4} \right), \quad a, b, c \in \mathbb{R} \right\}.$$

Vejamos a resposta do SINGULAR para este exemplo.

```
> ring r=(0,a,b,c),(x,y,z),lp;
> ideal I=x+2y-2z-a, 2x-3y+z-b, -x-y+3z-c, x+y+z;
> ideal J=std(I);
> J;
J[1]=1
```

Quando o comando `std(I)` retorna 1, significa que para valores gerais de a, b, c o sistema não possui solução.

Exemplo 11. Considere o seguinte sistema linear S_2, porém agora considerando x, y, z, a, b, c como variáveis. Neste caso, os cálculos para solução do sistema S_2 serão realizados no anel $\mathbb{R}[x, y, z, a, b, c]$:

$$S_2 : \begin{cases} x & +2y & -2z & -a & & & = 0 \\ 2x & -3y & +z & & -b & & = 0 \\ -x & -y & +3z & & & -c & = 0 \\ x & +y & +z & & & & = 0 \end{cases}$$

O sistema S_2 possui 4 linhas e 6 colunas (e não 4 linhas e 3 colunas como antes). Escalonando o sistema linear S_2, obtemos o sistema linear S_3 equivalente a S_2, dado por:

$$S_3 : \begin{cases} x & +2y & -2z & -a & & & = 0 & \\ & 7y & -5z & -2a & +b & & = 0 & \xleftarrow{L_2=2L_1-L_2} \\ & y & +z & -a & & -c & = 0 & \xleftarrow{L_3=L_1+L_3} \\ & y & -3z & -a & & & = 0 & \xleftarrow{L_4=L_1-L_4} \end{cases}$$

$$S_3 : \begin{cases} x & +2y & -2z & -a & & & = 0 & \\ & 7y & -5z & -2a & +b & & = 0 & \\ & & -12z & +5a & +b & +7c & = 0 & \xleftarrow{L_3=L_2-7L_3} \\ & & +4z & & & -c & = 0 & \xleftarrow{L_4=L_3-L_4} \end{cases}$$

$$S_3 : \begin{cases} x & +2y & -2z & -a & & & = 0 & \\ & 7y & -5z & -2a & +b & & = 0 & \\ & & 12z & -5a & -b & -7c & = 0 & \\ & & & 5a & +b & +4c & = 0 & \xleftarrow{L_4=L_3+3L_4} \end{cases}$$

Observe que dependendo do anel, o sistema muda totalmente a solução. Neste último caso, o sistema possui infinitas soluções. Isolando qualquer uma das variáveis e efetuando as respectivas substituições, temos:

$$b = -5a - 4c.$$

$$z = \frac{c}{4}.$$

$$y = a + \frac{3c}{4}.$$

$$x = -a - c.$$

$$\text{Solução de } S_3 = \left\{ \left(-a - c, a + \frac{3c}{4}, \frac{c}{4}, a, -5a - 4c, c \right), \quad a, c \in \mathbb{R} \right\}.$$

Neste exemplo, temos infinitas soluções.

Podemos resolver o sistema linear S_2, usando o Singular.

```
> ring r=0,(x,y,z,a,b,c),lp;
> ideal I=x+2y-2z-a, 2x-3y+z-b, -x-y+3z-c, x+y+z;
> ideal J=std(I);
> ideal K =simplify(J,1);
> K;
K[1]=a+1/5b+4/5c
K[2]=z-1/4c
K[3]=y+1/5z+1/5b
K[4]=x+y+z
```

Devemos ler o resultado da seguinte maneira:

$K[1] = a + \frac{1}{5}b + \frac{4}{5}c$, então $a + \frac{b}{5} + \frac{4c}{5} = 0$, ou $5a + b + 4c = 0$, ou $b = -5a - 4c$.

$K[2] = z - \frac{1}{4}c$, então $z = \frac{c}{4}$.

$K[3] = y + \frac{1}{5}z + \frac{1}{5}b$, então $y + \frac{z}{5} + \frac{b}{5} = 0$, ou $y = -\frac{c}{20} - \frac{b}{5}$, ou $y = a + \frac{3c}{4}$.

$K[4] = x + y + z$, então $x = -y - z$, ou $x = -c - a$.

Note que a solução dada pelo escalonamento e pelo Singular coincidem.

5. Problemas geométricos usando polinômios

Introduzindo coordenadas cartesianas no plano euclidiano, as hipóteses e conclusões de uma grande classe de teoremas geométricos podem ser expressadas através de equações polinomiais que dependem das coordenadas de uma coleção de pontos de acordo com o problema apresentado. Dizemos que um teorema geométrico é admissível, se ambas as hipóteses e conclusões admitem uma formulação somente em equações polinomiais. Existem muitos caminhos diferentes, porém equivalentes para formulações de um teorema admissível. Vejamos alguns exemplos interessantes.

Em todos os problemas usaremos o conhecido sistema de coordenadas no plano cartesiano xy, isto é, vamos utilizar dois eixos coordenados, eixo x e eixo y, dispostos perpendicularmente um ao outro.

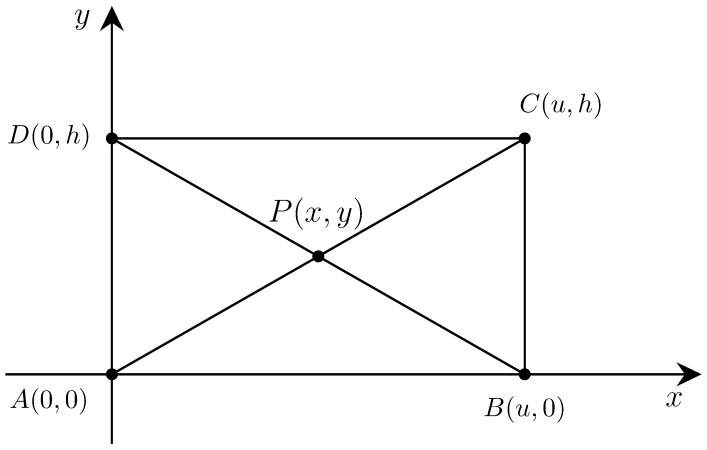
Os problemas apresentados neste capítulo foram baseados na referência [1].

5.1 Teorema das diagonais de um retângulo

Teorema 5. *As diagonais de um retângulo se intersectam no ponto médio das duas diagonais.*

Demonstração:

Utilizando o sistema cartesiano xy, faremos com que dois lados do retângulo estejam sobre os eixos coordenados x e y. Um lado do retângulo vai estar sobre o eixo x das abscissas e o outro lado sobre o eixo y das ordenadas, conforme ilustrado na figura abaixo:



Considere o retângulo $ABCD$ com coordenadas $A(0,0)$, $B(u,0)$, $C(u,h)$ e $D(0,h)$. Note que o ponto $P(x,y)$ está na interseção das diagonais do retângulo.

Observe que os pontos A, P e C estão alinhados, isso significa que as retas que passam respectivamente, por A, P e P, C têm a mesma inclinação. Vale ressaltar que o coeficiente angular de uma reta é a tangente do seu ângulo de inclinação. O coeficiente angular da reta que passa por $A(x_A, y_A)$ e $P(x_P, y_P)$ é dado por:

$$m = \tan(\alpha) = \frac{\Delta y}{\Delta x} = \frac{y_P - y_A}{x_P - x_A}.$$

A inclinação da reta que passa pelos pontos A e P é igual a

$$m = \frac{y-0}{x-0} = \frac{y}{x}.$$

E a inclinação da reta que passa pelos pontos P e C é igual a

$$m = \frac{h-y}{u-x}.$$

Como têm a mesma inclinação, obtemos:

$$\frac{y}{x} = \frac{h-y}{u-x}$$
$$x(h-y) = y(u-x)$$
$$xh - yu = 0.$$

Procedendo de maneira semelhante para a outra diagonal, temos que B, P, e D estão alinhados, logo BP e PD têm a mesma inclinação:

$$\frac{y-0}{x-u} = \frac{h-y}{0-x}$$
$$xh + yu - uh = 0.$$

Encontramos duas equações não lineares, uma vez que h e u também são variáveis, porém podemos fazer esse h e u respectivamente sendo a altura e comprimento fixo para o retângulo que estamos considerando, de modo que h e u possam ser analisados como uma constante não nula, isto nos permite resolver o sistema de equações lineares em x e y, encontrando assim o ponto P.

$$\begin{cases} xh - yu = 0 \\ xh + yu - uh = 0. \end{cases} \tag{5.1}$$

Na primeira equação isolando y encontramos $y = \frac{xh}{u}$, substituindo o valor encontrado na segunda equação temos:

$$xh - uh + uy = 0$$

$$xh - uh + \frac{uxh}{u} = 0$$
$$2xh - uh = 0$$
$$x = \frac{uh}{2h}$$
$$x = \frac{u}{2}.$$

Voltando na primeira equação encontramos $y = \frac{h}{2}$, assim obtemos o ponto $P\left(\frac{u}{2}, \frac{h}{2}\right)$.

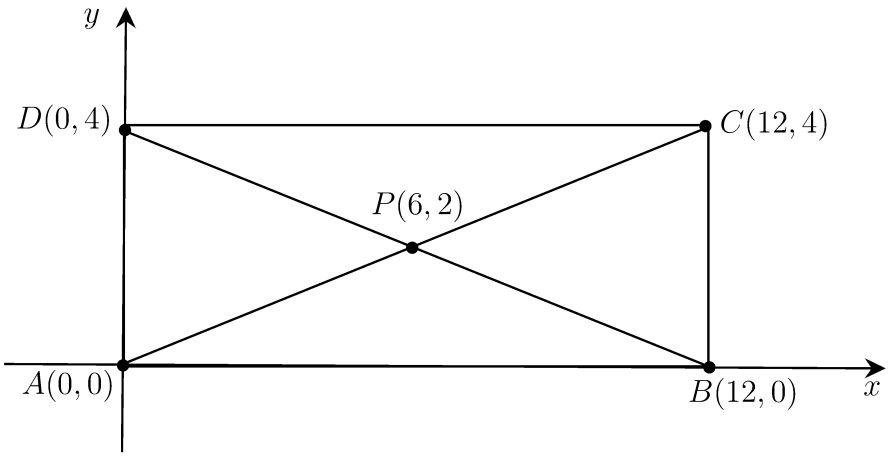
Provamos que o ponto P é mesmo o ponto médio das diagonais para qualquer retângulo.

□

Exemplo 12. Para ilustrar, vamos atribuir valores particulares para u e h (que são variáveis independentes) no sistema não linear e assim teremos um sistema linear 2×2 que é ensinado no ensino médio. Tomando $u = 12$ e $h = 4$ em 5.1, temos

$$\begin{cases} 4x - 12y = 0 \\ 4x + 12y = 48. \end{cases}$$

Resolvendo esse sistema, encontramos os valores $x = 6$ e $y = 2$, assim o ponto de encontro das diagonais é o ponto $P(6, 2)$. Esse conjunto solução é um conjunto afim e é a solução do sistema.



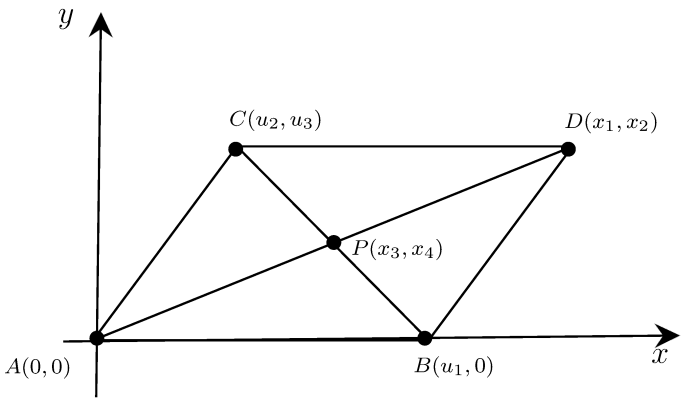
5.2 TEOREMA DAS DIAGONAIS DE UM PARALELOGRAMO

Teorema 6. *As diagonais de um paralelogramo se intersectam em um ponto P que divide ambas as diagonais em seu ponto médio.*

Demonstração:

Utilizando o sistema de coordenadas cartesianas, sem perda de generalidade podemos supor que o ponto $A(0, 0)$ é a origem do sistema e um dos vértices do paralelogramo, cuja base deve estar sobre o eixo x e os demais vértices da forma $B(u_1, 0)$, $C(u_2, u_3)$, $D(x_1, x_2)$ e $P(x_3, x_4)$

o ponto de interseção das diagonais, pois as propriedades do paralelogramo não mudam sob translações e rotações no plano, e assim podemos fazer rotações e translações até que o ponto A coincida com a origem do sistema, obtendo assim a figura abaixo:



A primeira hipótese é que os lados opostos de um paralelogramo são paralelos, então eles possuem a mesma inclinação. Sendo $AB \parallel CD$ temos que o coeficiente angular é zero, logo:

$$h_1 : \frac{x_2 - u_3}{x_1 - u_2} = 0, \text{ com } x_1 - u_2 \neq 0.$$

Sendo $AC \parallel BD$ temos que a inclinação da reta que passa pelos pontos A e C tem a mesma inclinação da reta que passa pelos pontos B e D, logo seus coeficientes angulares são iguais, ou seja:

$$m_{AC} = m_{BD}$$
$$h_2 : \frac{u_3 - 0}{u_2 - 0} = \frac{x_2 - 0}{x_1 - u_1}.$$

Assim obtemos duas equações polinomiais dadas por:

$$\begin{cases} h_1 : & x_2 & - & u_3 & & & = & 0 \\ h_2 : & x_1u_3 & - & u_1u_3 & - & x_2u_2 & = & 0. \end{cases}$$

Como o ponto P pertence à diagonal AD, então temos que os pontos A, P, D são colineares, temos:

$$h_3 : \begin{vmatrix} 0 & 0 & 1 \\ x_3 & x_4 & 1 \\ x_1 & x_2 & 1 \end{vmatrix} = 0 + 0 + x_3x_2 - x_4x_1 - 0 - 0 = 0$$

$$h_3 : x_4x_1 - x_3x_2 = 0.$$

Analogamente, o fato de P pertencer à diagonal BC, temos que:

$$h_4 : \begin{vmatrix} u_1 & 0 & 1 \\ x_3 & x_4 & 1 \\ u_2 & u_3 & 1 \end{vmatrix} = x_4u_1 + 0 + x_3u_3 - x_4u_2 + u_3u_1 - 0 = 0$$

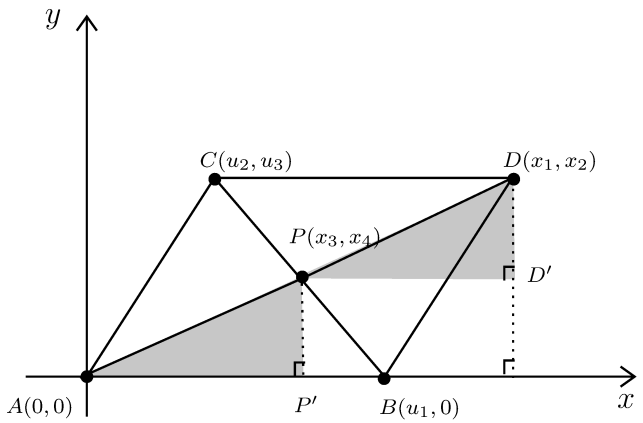
$$h_4 : x_4u_2 - x_4u_1 - x_3u_3 + u_1u_3 = 0.$$

Resultando em mais duas equações polinomiais dadas por:

$$\begin{cases} h_3 : & x_4x_1 & - & x_3x_2 & & & & = & 0 \\ h_4 : & x_4u_2 & - & x_4u_1 & - & x_3u_3 & + & u_1u_3 & = & 0. \end{cases}$$

Então, as equações h_1, h_2, h_3, h_4 são as hipóteses que vamos usar para provar que P é o ponto médio de ambas as diagonais do paralelogramo $ABCD$. As condições da tese é que P divida o segmento AD e BC em seu ponto médio. Logo, queremos provar as seguintes igualdades $AP = PD$ e $BP = PC$.

Usando o Teorema de Pitágoras nos triângulos retângulos APP' e PDD', temos:



$$|AP|^2 = |AP'|^2 + |PP'|^2$$

e

$$|PD|^2 = |PD'|^2 + |DD'|^2,$$

onde $|PD|$ significa a distândia de P até D.

Provamos o resultado se:

$$\begin{cases} g_1 : & |AP| & = & |PD| \\ g_2 : & |BP| & = & |PC|. \end{cases} \tag{5.2}$$

Temos que $|AP| = |PD|$, se:

$$x_3^2 + x_4^2 = (x_1 - x_3)^2 + (x_2 - x_4)^2$$

$$x_3^2 + x_4^2 = x_1^2 - 2x_1x_3 + x_3^2 + x_2^2 - 2x_2x_4 + x_4^2$$

$$x_1^2 - 2x_1x_3 - 2x_2x_4 + x_2^2 = 0.$$

Analogamente, temos que $|BP| = |PC|$, se:

$$(x_3 - u_1)^2 + x_4^2 = (x_3 - u_2)^2 + (x_4 - u_3)^2$$

$$x_3^2 - 2x_3u_1 + u_1^2 + x_4^2 = x_3^2 - 2x_3u_2 + u_2^2 + x_4^2 - 2x_4u_3 + u_3^2$$

$$2x_3u_1 - 2x_3u_2 - 2x_4u_3 - u_1^2 + u_2^2 + u_3^2 = 0.$$

Assim, o sistema 5.2, fica:

$$\begin{cases} g_1: & x_1^2 & - & 2x_1x_3 & - & 2x_2x_4 & + & x_2^2 & & = 0 \\ g_2: & 2x_3u_1 & - & 2x_3u_2 & - & 2x_4u_3 & - & u_1^2 & +u_2^2 & +u_3^2 = 0. \end{cases}$$

Vamos resolver este problema, com as variáveis u_1, u_2, u_3 sendo independentes, ou seja, os vértices P e D são dependentes dos vértices A, B e C, o que significa que x_1, x_2, x_3 e x_4 são dependentes de u_1, u_2 e u_3. É importante observar que neste sistema, o número de hipóteses, as equações h_i, $i = 1, 2, 3, 4$ e o número de variáveis dependentes x_j, $j = 1, 2, 3, 4$ são iguais. Com isso, atribuindo valores para as variáveis independentes u_i, $i = 1, 2, 3$, esperamos que o número de soluções, ou o número de combinações de x satisfazendo as equações seja finita.

$$\begin{cases} h_1: & x_2 & - & u_3 & & & & & = & 0 \\ h_2: & x_1u_3 & - & u_1u_3 & - & x_2u_2 & & & = & 0 \\ h_3: & x_4x_1 & - & x_3x_2 & & & & & = & 0 \\ h_4: & x_4u_2 & - & x_4u_1 & - & x_3u_3 & + & u_1u_3 & = & 0. \end{cases}$$

Em h_1 isolando x_2 teremos:

$$x_2 = u_3.$$

Substituindo x_2 em h_2:

$$x_1u_3 - u_1u_3 - u_3u_2 = 0$$

$$x_1 = \frac{u_1u_3}{u_3} + \frac{u_2u_3}{u_3}$$

$$x_1 = u_1 + u_2.$$

Analogamente em h_3 e h_4 teremos:

$$x_4(u_1 + u_2) - x_3u_3 = 0$$

$$x_3 = \frac{x_4(u_1 + u_2)}{u_3}$$

e

$$x_4u_2 - x_4u_1 - x_4\frac{(u_1 + u_2)}{u_3}u_3 + u_1u_3 = 0$$

$$x_4u_2 - x_4u_1 - x_4u_1 - x_4u_2 + u_1u_3 = 0$$

$$-2x_4u_1 = -u_1u_3$$

$$x_4 = \frac{u_3}{2}.$$

Substituindo x_4 em x_3, teremos:

$$x_3 = \frac{u_3}{2}\frac{(u_1+u_2)}{u_3}$$

$$x_3 = \frac{u_1+u_2}{2}.$$

Com isso isolamos x_1, x_2, x_3 e x_4 em função de u_1, u_2, u_3, obtendo:

$$x_1 = u_1 + u_2,$$

$$x_2 = u_3,$$
$$x_3 = \frac{u_1+u_2}{2},$$
$$x_4 = \frac{u_3}{2}.$$

Logo, P será o ponto médio se provarmos o anulamento de g_1 e g_2, substituindo os $x_{i's}$ encontrados em $g_{i's}$, temos:

$$g_1 : x_1^2 - 2x_1x_3 - 2x_2x_4 + x_2^2 = 0$$
$$g_1 : (u_1+u_2)^2 - 2(u_1+u_2)(\frac{u_1+u_2}{2}) - 2u_3\frac{u_3}{2} + u_3^2 = 0$$

$$g_1 : (u_1+u_2)^2 - (u_1+u_2)^2 - u_3^2 + u_3^2 = 0$$

$$g_1 : 0 = 0,$$

e

$$g_2 : 2x_3u_1 - 2x_3u_2 - 2x_4u_3 - u_1^2 + u_2^2 + u_3^2 = 0$$
$$g_2 : 2(\frac{u_1+u_2}{2})u_1 - 2(\frac{u_1+u_2}{2})u_2 - 2\frac{u_3}{2}u_3 - u_1^2 + u_2^2 + u_3^2 = 0$$
$$g_2 : u_1^2 + u_1u_2 - u_1u_2 - u_2^2 - u_3^2 - u_1^2 + u_2^2 + u_3^2 = 0$$

$$g_2 : 0 = 0.$$

Logo, concluímos que P é o ponto médio das diagonais de um paralelogramo.

□

Observamos que não existe uma única maneira de traduzir um teorema geométrico para um teorema usando polinômios como acabamos de descrever. Muitas vezes é possível simplificar, diminuindo o número de equações e o número de variáveis.

Nem sempre é possível resolver um sistema manualmente. Mas muitas vezes podemos recorrer aos recursos computacionais.

Resolvendo este problema via Singular

Vamos utilizar o Singular para encontrar o conjunto afim $V(h_1, h_2, h_3, h_4)$ e resolvemos o problema se g_1 e g_2 se anulam neste conjunto.

Quem se interessar somente com a prática, podemos resolver rapidamente este problema usando o Singular, da seguinte maneira: neste problema do paralelogramo, como supomos as variáveis u_1, u_2, u_3 arbitrárias, e as variáveis x_1, x_2, x_3, x_4 como dependentes, e o objetivo é isolar x_i, $i = 1, 2, 3, 4$ em função de u_j, $j = 1, 2, 3$, podemos realizar contas no Singular com as variáveis u_i sendo os coeficientes de polinômios em x_i. Esta análise nos diz que vamos resolver o sistema não-linear determinado pelos polinômios h_1, h_2, h_3, e h_4, no anel $\mathbb{Q}(u_1, u_2, u_3)[x_1, x_2, x_3, x_4]$.

No singular entre com os seguintes comandos:

```
> ring r=(0,u1,u2,u3),(x1,x2,x3,x4),lp;
> ideal I = x2 - u3, x1*u3- u1*u3-x2*u2,x4*x1-x3*x2,x4*u2-x4*u1-x3*u3+u1*u3;
> I;  // note que I é gerado por h1, h2, h3, h4.
I[1]=x2+(-u3)
I[2]=(u3)*x1+(-u2)*x2+(-u1*u3)
I[3]=x1*x4-x2*x3
I[4]=(-u3)*x3+(-u1+u2)*x4+(u1*u3)
> ideal J=std(I);
> option(redSB); //usada para computar bases standard reduzida
> simplify(J,1);
_[1]=x4+(-1/2*u3)
_[2]=x3+(-1/2*u1-1/2*u2)
_[3]=x2+(-u3)
_[4]=x1+(-u1-u2)
>
```

Note que no resultado do último comando, devemos ler da forma:

$$\begin{array}{rcl} x_1 & = & u_1 + u_2 \\ x_2 & = & u_3 \\ x_3 & = & \frac{u_1+u_2}{2} \\ x_4 & = & \frac{u_3}{2}. \end{array} \tag{5.3}$$

No SINGULAR usando o comando SUBST, podemos constatar que as soluções em 5.3 satisfazem os g_{is}, verificando o anulamento das teses.

```
>ideal g=x1^2-2*x1*x3-2*x2*x4+x2^2,2*x3*u1-2*x3*u2-2*x4*u3-u1^2+u2^2+u3^2;
```

```
>subst(g,x1,u1+u2,x2,u3,x3,1/2*u1+1/2*u2,x4,1/2*u3);
_[1]=0
_[2]=0
```

O comando `subst(g,f1,g1,f2,g2,...,fn,gn)`, significa que vamos substituir o objeto `fi` por `gi` no objeto `g`. Acima, substituímos x_1 por $u_1 + u_2$, x_2 por u_3, x_3 por $\frac{u_1+u_2}{2}$ e x_4 por $\frac{u_3}{2}$ nas teses de g_1 e g_2.

Exemplo 13. Para ilustrar vamos atribuir valores para os $u_{i's}$ que são as variáveis independentes para encontrar os $x_{i's}$. Fixando $u_1 = 10, u_2 = 4$ e $u_3 = 6$ e substituindo em 5.3, temos:

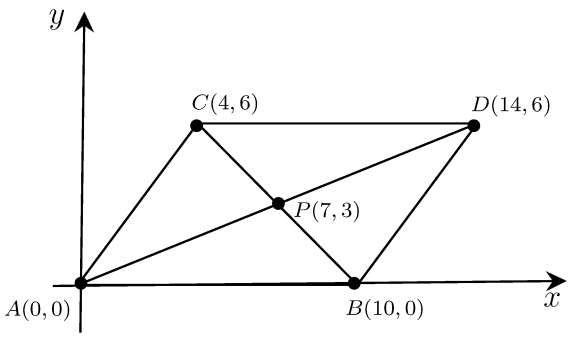
$$x_1 = 14$$

$$x_2 = 6$$

$$x_3 = 7$$

$$x_4 = 3.$$

Abaixo os pontos no sistema cartesiano, fica fácil perceber que o ponto P é o ponto médio das diagonais.

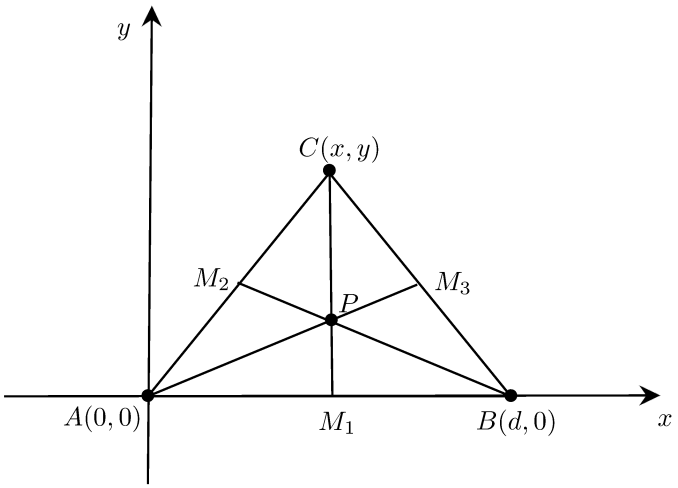


5.3 Teorema das medianas de um triângulo

Teorema 7. *A mediana de um triângulo é um segmento que une um vértice ao ponto médio do lado oposto. As três medianas de um triângulo se encontram em um único ponto, este chamado de baricentro do triângulo.*

Demonstração:

Utilizando o sistema de eixos de coordenadas, fazemos a origem do sistema coincidir com um dos vértices do triângulo de modo que um dos lados (a base) esteja sobre o eixo x (do lado positivo do eixo). Podemos assumir que a escala foi escolhida de modo que a base do triângulo tenha comprimento d. Vamos denominar os vértices do triângulo de A, B, C conforme figura abaixo:



De acordo com a figura temos $A(0,0), B(d,0), C(x,y)$. Sabemos que as coordenadas do ponto médio de um segmento AB é dada pela média aritmética das respectivas coordenadas de A e B. Assim, o ponto médio dos segmentos AB, AC e BC, são respectivamente, M_1, M_2 e M_3.

De posse destas coordenadas podemos por em ação nossa estratégia. Seja P o ponto de intersecção das medianas que passam por A e por B, digamos que P tem coordenadas (u,v). Para constatar que P está na mediana que passa por A basta igualar o coeficiente angular da reta que passa por A e P com o coeficiente angular da reta que passa por M_3 e A. Como ambas as retas têm o ponto A em comum, a igualdade dos coeficientes angulares garante que elas coincidem.

O coeficiente angular da reta que passa por $A(0,0)$ e $P(u,v)$ é dado por:

$$m = \tan(\alpha) = \frac{\Delta y}{\Delta x} = \frac{y_P - y_A}{x_P - x_A} = \frac{v-0}{u-0} = \frac{v}{u}.$$

O coeficiente angular da reta que passa por $A(0,0)$ e por $M_3(\frac{x+d}{2}, \frac{y}{2})$ é:

$$m = \tan(\alpha) = \frac{\Delta y}{\Delta x} = \frac{y_{M_3} - y_A}{x_{M_3} - x_A} = \frac{\frac{y}{2} - 0}{\frac{x+d}{2} - 0} = \frac{y}{x+d},$$

com $x + d \neq 0$.

Assim, a condição para que P esteja na mediana que passa pelo vértice A, deve satisfazer:

$$\frac{v}{u} = \frac{y}{x+d}$$
$$vx + vd = yu$$
$$vx + vd - yu = 0.$$

Seja $h_1 : vx + vd - yu = 0$, uma das hipóteses do Problema.

Procedendo de maneira análoga, expressamos a condição de que P pertença à mediana que passa pelos vértices $B(d,0)$ e $P(u,v)$.

$$m = \tan(\alpha) = \frac{\Delta y}{\Delta x} = \frac{y_P - y_B}{x_P - x_B} = \frac{v - 0}{u - d} = \frac{v}{u - d}.$$

O coeficiente angular da reta que passa por $B(d, 0)$ e por $M_2(\frac{x}{2}, \frac{y}{2})$ é:

$$m = \tan(\alpha) = \frac{\Delta y}{\Delta x} = \frac{y_{M_2} - y_B}{x_{M_3} - x_B} = \frac{\frac{y}{2} - 0}{\frac{x}{2} - d} = \frac{\frac{y}{2}}{\frac{x-2d}{2}} = \frac{y}{x - 2d},$$

com $x - 2d \neq 0$.

Assim, a condição para que P esteja na mediana que passa pelo vértice B, deve satisfazer:

$$\frac{v}{u - d} = \frac{y}{x - 2d}$$
$$vx - 2vd = yu - yd$$
$$vx - 2vd - yu + yd = 0.$$

Seja $h_2 : vx - 2vd - yu + yd = 0$, outra hipótese do Problema.

Portanto, se o ponto P pertence à intersecção das medianas pelos vértices A e B, então as equações h_1 e h_2 devem ser simultaneamente satisfeitas.

Por outro lado, o que queremos é provar que este ponto P também pertence à mediana que passa pelo vértice C.

O coeficiente angular da reta que passa por $C\,(x, y)$ e por $M_1\left(\frac{d}{2}, 0\right)$ é:

$$m = \tan(\alpha) = \frac{\Delta y}{\Delta x} = \frac{y_{M_1} - y_C}{x_{M_1} - x_C} = \frac{0 - y}{\frac{d}{2} - x} = -\frac{2y}{d - 2x}.$$

Vamos encontrar o coeficiente angular da reta que passa por $C\,(x, y)$ e por $P\,(u, v)$.

$$m = \tan(\alpha) = \frac{\Delta y}{\Delta x} = \frac{y_P - y_C}{x_P - x_C} = \frac{v - y}{u - x}.$$

Assim, a condição para que P esteja na mediana que passa pelo vértice C, deve satisfazer:

$$\frac{-2y}{d - 2x} = \frac{v - y}{u - x}$$
$$-2uy + 2xy = dv - 2vx - dy + 2xy$$
$$2vx - vd + yd - 2uy = 0.$$

Seja $g : 2vx - vd + yd - 2uy = 0$, a tese do Problema.

Precisamos mostrar que, se um ponto é zero comum de h_1 e h_2, então também é zero de g. Uma maneira de fazer isto, é supor que o vértice $C(x, y)$ esteja fixo, de modo que x e y são constantes, cujos valores não conhecemos. A partir disso tentaremos calcular u e v sob estas hipóteses:

$$h_1 : vx + vd - yu = 0.$$

$$h_2 : vx - 2vd - yu + yd = 0.$$

Como y é a altura do triângulo, certamente $y \neq 0$. Assim podemos obter o valor de u a partir da primeira equação h_1.

$$vx + vd - yu = 0$$

$$yu = vx + vd$$

$$u = \frac{v(x+d)}{y}.$$

Substituindo o valor de u na segunda equação h_2 teremos:

$$vx - 2vd - yu + yd = 0$$

$$vx - 2vd - y\frac{v(x+d)}{y} + yd = 0$$

$$vx - 2vd - vx - vd + yd = 0$$

$$-3vd + yd = 0$$

$$v = \frac{y}{3}.$$

Para encontrar o valor de u, basta substituir o valor de v em u:

$$u = \frac{v(x+d)}{y}$$

$$u = \frac{\frac{y}{3}(x+d)}{y}$$

$$u = \frac{x+d}{3}.$$

Portanto, $P(u,v) = P(\frac{x+d}{3}, \frac{y}{3})$. Para saber se este ponto pertence à terceira mediana, basta substituí-lo na equação g, como segue:

$$g : 2vx - vd + yd - 2uy = 0$$

$$g : 2 \cdot \frac{y}{3} \cdot x - \frac{y}{3} \cdot d + yd - 2 \cdot \frac{(x+d)}{3} \cdot y = 0$$

$$g : 2 \cdot \frac{xy}{3} + \frac{2yd}{3} - 2 \cdot \frac{xy}{3} - \frac{2yd}{3} = 0$$

$$g : 0 = 0.$$

Verificamos que o ponto P pertence também a terceira mediana, como duas retas se intersectam em apenas um ponto, obtivemos uma demonstração do Teorema das Medianas.

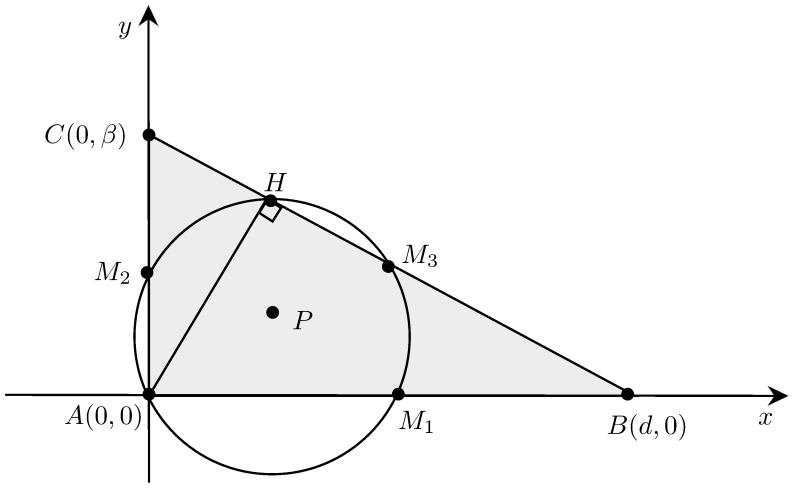
□

5.4 TEOREMA DE APOLÔNIO

Teorema 8. *O pé da altura sobre a hipotenusa e os pontos médios dos lados de um triângulo retângulo pertencem a uma mesma circunferência.*

Demonstração:

Utilizando o sistema de eixos de coordenadas cartesianas, podemos supor que os catetos do triângulo retângulo estejam sobre os eixos coordenados obtendo o triângulo ABC, de modo que $B\widehat{A}C$ seja o ângulo reto. Logo, as coordenadas do triângulo podem ser $A(0,0), B(d,0)$ e $C(0,\beta)$, conforme a figura abaixo:



Denotando por M_1 e M_2 os pontos médios dos catetos AB e AC e por M_3 o ponto médio da hipotenusa BC, então teremos:

$$M_1\left(\frac{x_A+x_B}{2},\frac{y_A+y_B}{2}\right)=M_1\left(\frac{0+d}{2},\frac{0+0}{2}\right)=M_1\left(\frac{d}{2},0\right).$$

$$M_2\left(\frac{x_A+x_C}{2},\frac{y_A+y_C}{2}\right)=M_2\left(\frac{0+0}{2},\frac{0+\beta}{2}\right)=M_2\left(0,\frac{\beta}{2}\right).$$

$$M_3\left(\frac{x_B+x_C}{2},\frac{y_B+y_C}{2}\right)=M_3\left(\frac{d+0}{2},\frac{0+\beta}{2}\right)=M_3\left(\frac{d}{2},\frac{\beta}{2}\right).$$

O segmento que une dois pontos médios dos lados de um triângulo é paralelo e mede a metade do terceiro lado do triângulo. Com isso, temos que o quadrilátero $AM_1M_3M_2$ é um retângulo inscrito na circunferência, portanto o ponto A também pertence a circunferência. Seja $P(u,v)$ o centro da circunferência que passa por M_1, M_2 e M_3. Sabendo que AP é igual ao raio da circunferência e d_{AP} significa a distância entre os pontos A e P, então:

$$d_{AP}=R=\sqrt{(x_P-x_A)^2+(y_P-y_A)^2}$$

$$R^2=(u-0)^2+(0-v)^2$$

$$R^2 = u^2 + v^2.$$

Denotaremos por h_1 a equação que expressa o fato de M_2 pertencer à circunferência de centro P que passa por M_1. Logo $d_{PM_1} = d_{PM_2}$.

$$h_1 : \sqrt{(x_P - x_{M_1})^2 + (y_P - y_{M1})^2} = \sqrt{(x_P - x_{M_2})^2 + (y_P - y_{M_2})^2}$$

$$h_1 : \left(u - \frac{d}{2}\right)^2 + (v-0)^2 = (u-0)^2 + \left(v - \frac{\beta}{2}\right)^2$$

$$h_1 : u^2 - 2u \cdot \frac{d}{2} + \frac{d^2}{4} + v^2 = u^2 + v^2 - 2v \cdot \frac{\beta}{2} + \frac{\beta^2}{4}$$

$$h_1 : -ud + \frac{d^2}{4} + v\beta - \frac{\beta^2}{4} = 0$$

$$h_1 : v\beta - \frac{\beta^2}{4} - ud + \frac{d^2}{4} = 0.$$

Denotaremos por h_2 a equação segundo a qual M_3 está sobre a mesma circunferência de centro P, logo $d_{PM_1} = d_{PM_3}$. Assim:

$$h_2 : \sqrt{(x_P - x_{M1})^2 + (y_P - y_{M1})^2} = \sqrt{(x_P - x_{M3})^2 + (y_P - y_{M3})^2}$$

$$h_2 : \left(u - \frac{d}{2}\right)^2 + (v-0)^2 = \left(u - \frac{d}{2}\right)^2 + \left(v - \frac{\beta}{2}\right)^2$$

$$h_2 : u^2 - 2u \cdot \frac{d}{2} + \frac{d^2}{4} + v^2 = u^2 - 2u \cdot \frac{d}{2} + \frac{d^2}{4} + v^2 - 2v \cdot \frac{\beta}{2} + \frac{\beta^2}{4}$$

$$h_2 : v\beta - \frac{\beta^2}{4} = 0.$$

Considere $H(\alpha, z)$ o pé da altura sobre a hipotenusa BC e r a reta que passa pelos pontos A e H. Então r tem a seguinte equação:

$$r : \begin{vmatrix} x & y & 1 \\ 0 & 0 & 1 \\ \alpha & z & 1 \end{vmatrix} = 0 + y\alpha + 0 + 0 - xz + 0 = 0$$

$$r : y\alpha - xz = 0$$

$$r : y = \frac{zx}{\alpha}.$$

Logo, o coeficiente angular de r é:

$$\frac{z}{\alpha}.$$

Considere s a reta que passa pelos pontos B e C. Então s tem a seguinte equação:

$$s : \begin{vmatrix} x & y & 1 \\ d & 0 & 1 \\ 0 & \beta & 1 \end{vmatrix} = 0 + 0 + d\beta + 0 - \beta x - dy = 0$$

$$s : dy = -\beta x + d$$

$$s : y = -\frac{\beta}{d}x + \frac{d}{d}$$

$$s : y = -\frac{\beta}{d}x + 1.$$

Logo, o coeficiente angular de s é:

$$-\frac{\beta}{d}.$$

Como m_r é o coeficiente angular da reta r e m_s é o coeficiente angular da reta s as quais são perpendiculares, então $m_r.m_s = -1$, que corresponde a equação h_3 portanto:

$$h_3 : \frac{z}{\alpha}\left(-\frac{\beta}{d}\right) = -1$$

$$h_3 : -z\beta = -\alpha d$$

$$h_3 : \alpha d - z\beta = 0.$$

Observe que H, C e B estão na mesma reta, logo a colinearidade entre esses pontos pode ser dada por h_4:

$$h_4 : \begin{vmatrix} \alpha & z & 1 \\ 0 & \beta & 1 \\ d & 0 & 1 \end{vmatrix} = \alpha\beta + zd + 0 - d\beta - 0 + 0 = 0$$

$$h_4 : \beta(\alpha - d) + zd = 0.$$

Por fim, o teorema nos diz que H pertence à mesma circunferência de centro P que passa por M_1 se a equação g for satisfeita. A equação g abaixo é satisfeita se $d_{HP} = d_{PM_1}$, ou seja, se:

$$g : \sqrt{(x_P - x_H)^2 + (y_P - y_H)^2} = \sqrt{(x_P - x_{M1})^2 + (y_P - y_{M1})^2}$$

$$g : (u - \alpha)^2 + (v - z)^2 = \left(u - \frac{d}{2}\right)^2 + (v - 0)^2$$

$$g : u^2 - 2u\alpha + \alpha^2 + v^2 - 2vz + z^2 = u^2 - 2u \cdot \frac{d}{2} + \frac{d^2}{4} + v^2$$

$$g : -2u\alpha + \alpha^2 - 2vz + z^2 + ud - \frac{d^2}{4} = 0.$$

Para concluir que H pertence à circunferência temos que provar que a equação g seja satisfeita, ou seja, que a solução do sistema abaixo satisfaça g. Para isso é necessário resolver o sistema das equações h_1, h_2, h_3 e h_4, que são as hipóteses do problema.

$$\begin{cases} h_1 : & v\beta - \frac{\beta^2}{4} - ud + \frac{d^2}{4} & = 0 \\ h_2 : & v\beta - \frac{\beta^2}{4} & = 0 \\ h_3 : & \alpha d - z\beta & = 0 \\ h_4 : & \beta(\alpha - d) + zd & = 0 \end{cases}$$

Isolando u e v em h_1 e h_2 respectivamente teremos:

$$u = \frac{d}{4}$$

e

$$v = \frac{\beta}{4}.$$

Em $h_3 : \alpha d - z\beta = 0 \rightarrow z = \frac{\alpha d}{\beta}$.

Em $h_4 : \beta(\alpha - d) + zd = 0$, substituindo o valor de z e isolando α temos:

$$\beta\alpha - \beta d + \frac{\alpha d}{\beta} d = 0$$

$$\beta\alpha - \beta d + \frac{\alpha d^2}{\beta} = 0$$

$$\beta^2\alpha - \beta^2 d + \alpha d^2 = 0$$

$$\alpha\left(\beta^2 + d^2\right) = \beta^2 d$$

$$\alpha = \frac{\beta^2 d}{\beta^2 + d^2}.$$

Como $z = \frac{\alpha d}{\beta}$ vamos substituir o valor de α encontrado:

$$z = \frac{\beta^2 d}{\beta^2 + d^2} \frac{d}{\beta}$$

$$z = \frac{\beta d^2}{\beta^2 + d^2}.$$

Note que conseguimos isolar u, v, α e z em função das duas variáveis independentes β e d. Agora vamos substituir no lado esquerdo de g para verificar se é igual a 0. De fato:

$$-2u\alpha + \alpha^2 - 2vz + z^2 + ud - \frac{d^2}{4} =$$

$$-2 \cdot \frac{d}{4}\frac{\beta^2 d}{\beta^2 + d^2} + \left(\frac{\beta^2 d}{\beta^2 + d^2}\right)^2 - 2 \cdot \frac{\beta}{4}\left(\frac{\beta d^2}{\beta^2 + d^2}\right) + \left(\frac{\beta d^2}{\beta^2 + d^2}\right)^2 + \frac{d}{4} \cdot d - \frac{d^2}{4} =$$

$$-\frac{1}{2}\left(\frac{\beta^2 d^2}{\beta^2 + d^2}\right) + \frac{\beta^4 d^2}{(\beta^2 + d^2)^2} - \left(\frac{\beta^2 d^2}{\beta^2 + d^2}\right)\frac{1}{2} + \frac{\beta^2 d^4}{(\beta^2 + d^2)^2} =$$

$$-\frac{\beta^2 d^2}{\beta^2 + d^2} + \frac{\beta^4 d^2}{(\beta^2 + d^2)^2} + \frac{\beta^2 d^4}{(\beta^2 + d^2)^2} =$$

$$\frac{-\beta^2 d^2(\beta^2 + d^2) + \beta^4 d^2 + \beta^2 d^4}{(\beta^2 + d^2)^2} =$$

$$\frac{-\beta^4 d^2 - \beta^2 d^4 + \beta^4 d^2 + \beta^2 d^4}{(\beta^2 + d^2)^2} =$$

$$\frac{0}{(\beta^2 + d^2)^2} =$$

$$0.$$

Portanto, o fato de $g : 0 = 0$, implica que H pertence à circunferência de centro P e que passa por M_1, M_2 e M_3.

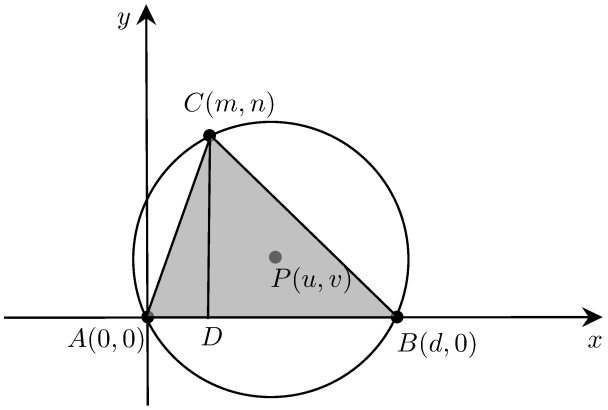
□

5.5 Teorema: Lados de um triângulo e o diâmetro da circunferência circunscrita.

Teorema 9. *O produto dos dois lados de um triângulo é igual ao produto da altura sobre o terceiro lado pelo diâmetro do círculo circunscrito.*

Demonstração:

Mais uma vez utilizando o sistema de eixos ortogonais, considere o triângulo com vértices $A(0, 0)$, $B(d, 0)$ e $C(m, n)$. Seja $P(u, v)$ o centro da circunferência circunscrita ao triângulo ABC, conforme figura abaixo.



A primeira hipótese h_1 é dada por:

$$h_1 : d_{AP} = d_{BP}$$

$$h_1 : \sqrt{(x_P - x_A)^2 + (y_P - y_A)^2} = \sqrt{(x_P - x_B)^2 + (y_P - y_B)^2}$$

$$h_1 : (u-0)^2 + (v-0)^2 = (u-d)^2 + (v-0)^2$$

$$h_1 : (u-d)^2 + v^2 - u^2 - v^2 = 0$$

$$h_1 : d^2 - 2ud = 0.$$

A segunda hipótese h_2 é dada por:

$$h_2 : d_{AP} = d_{CP}$$

$$h_2 : \sqrt{(x_P - x_A)^2 + (y_P - y_A)^2} = \sqrt{(x_P - x_C)^2 + (y_P - y_C)^2}$$

$$h_2 : (u-0)^2 + (v-0)^2 = (u-m)^2 + (v-n)^2$$

$$h_2 : (u-m)^2 + (v-n)^2 - u^2 - v^2 = 0$$

$$h_2 : m^2 + n^2 - 2um - 2vn = 0.$$

Queremos mostrar que:

$$g : d_{AC}.d_{BC} = d_{CD}.2.raio$$

$$g : \sqrt{\left[(x_C - x_A)^2 + (y_C - y_A)^2\right] \cdot \left[(x_C - x_B)^2 + (y_C - y_B)^2\right]} = n \cdot 2 \cdot \left(\sqrt{u^2 + v^2}\right)$$

$$g : \sqrt{\left[(m-0)^2 + (n-0)^2\right] \cdot \left[(m-d)^2 + (n-0)^2\right]} = n \cdot 2 \cdot \left(\sqrt{u^2 + v^2}\right)$$

$$g : \sqrt{\left[m^2 + n^2\right] \cdot \left[(m-d)^2 + n^2\right]} = 2n \cdot \left(\sqrt{u^2 + v^2}\right)$$

$$g : \left(m^2 + n^2\right) \cdot \left[(m-d)^2 + n^2\right] = 4n^2 \left(u^2 + v^2\right)$$

$$g : \left(m^2+n^2\right)\cdot\left[(m-d)^2+n^2\right]-4n^2\left(u^2+v^2\right)=0.$$

Provamos o resultado se a equação g se verifica.

Vamos resolver este problema, com as variáveis m, n, d sendo independentes e as variáveis u e v sendo dependentes de m, n e d.

$$\begin{cases} h_1 \ : \ d^2 \ - \ 2ud \ = 0 \\ \\ h_2 \ : \ m^2 \ + \ n^2 \ - \ 2um \ - \ 2vn \ = 0. \end{cases}$$

Em h_1, isolando u teremos:

$$u=\frac{d^2}{2d}$$
$$u=\frac{d}{2}.$$

Substituindo u em h_2:

$$m^2+n^2-2\cdot\frac{d}{2}\cdot m-2vn=0$$

$$m^2+n^2-dm-2vn=0$$
$$2vn=m^2+n^2-dm$$
$$v=\frac{m^2+n^2-dm}{2n},\ \text{com } n\neq 0.$$

Logo, o produto dos dois lados de um triângulo é igual ao produto da altura sobre o terceiro lado pelo diâmetro do círculo circunscrito se provarmos o anulamento de g substituindo os valores encontrados de u e v em g, temos:

$$g : \left(m^2+n^2\right)\cdot\left[(m-d)^2+n^2\right]-4n^2\left(u^2+v^2\right)=0$$

$$g : \left(m^2+n^2\right)\cdot\left[m^2-2md+d^2+n^2\right]-4n^2\cdot\left[\left(\frac{d}{2}\right)^2+\left(\frac{m^2+n^2-dm}{2n}\right)^2\right]=0$$

$$g : \left(m^2+n^2\right)\cdot\left[m^2-2md+d^2+n^2\right]-4n^2\cdot\left[\frac{d^2}{4}+\frac{(m^2+n^2-dm)\cdot(m^2+n^2-dm)}{4n^2}\right]=0$$

$$g : \left(m^2+n^2\right)\cdot\left[m^2-2md+d^2+n^2\right]-\left((m^2+n^2)(m^2-2md+d^2+n^2)\right)=0$$

$$g : 0=0.$$

Portanto, concluímos que o produto dos dois lados de um triângulo é igual ao produto da altura sobre o terceiro lado pelo diâmetro do círculo circunscrito.

□

Resolvendo este problema via Singular

Utilizando o Singular para encontrar a variedade afim $V(h_1, h_2)$ e resolvermos o problema onde g anula nesta variedade rapidamente, basta supor as variáveis m, n, d sendo independentes e as variáveis u e v sendo dependentes de m, n e d.

Esta análise nos diz que vamos resolver o sistema não-linear determinado pelos polinômios h_1 e h_2 no anel $\mathbb{Q}(m, n, d)[u, v]$.

No singular entre com os seguintes comandos:

```
> ring r= (0,m,n,d),(u,v),lp;
> option(redSB);
> ideal I=d^2-2*u*d,m^2+n^2-2*u*m-2*v*n;
> ideal J=std(I);
> simplify(J,1);
_[1]=v+(-m2+md-n2)/(2n)
_[2]=u+(-d)/2
>
```

Note que no resultado do último comando, devemos ler da forma:

$$u = \frac{d}{2}.$$

$$v = \frac{m^2 + n^2 - md}{2n}, \text{ com } n \neq 0.$$

Usando o comando `subst`, podemos constatar o anulamento da tese.

```
> poly g = (m^2+n^2)*((m-d)^2+n^2)-4*n^2*(u^2+v^2);
> subst(g,u,d/2,v,-((-m2+md-n2)/(2n)));
0
```

O comando `subst(g,f1,g1,f2,g2,...,fn,gn)`, significa que vamos substituir o objeto `fi` por `gi` no objeto `g`. Acima, substituímos u por $d/2$ e v por $-((-m2 + md - n2)/(2n)))$ no polinomio g. Se tivéssemos definido o polinomio g como ideal, o procedimento é o mesmo, ou seja,

```
> ideal g= (m^2+n^2)*((m-d)^2+n^2)-4*n^2*(u^2+v^2);
> subst(g,u,d/2,v,-((-m2+md-n2)/(2n)));
0
```

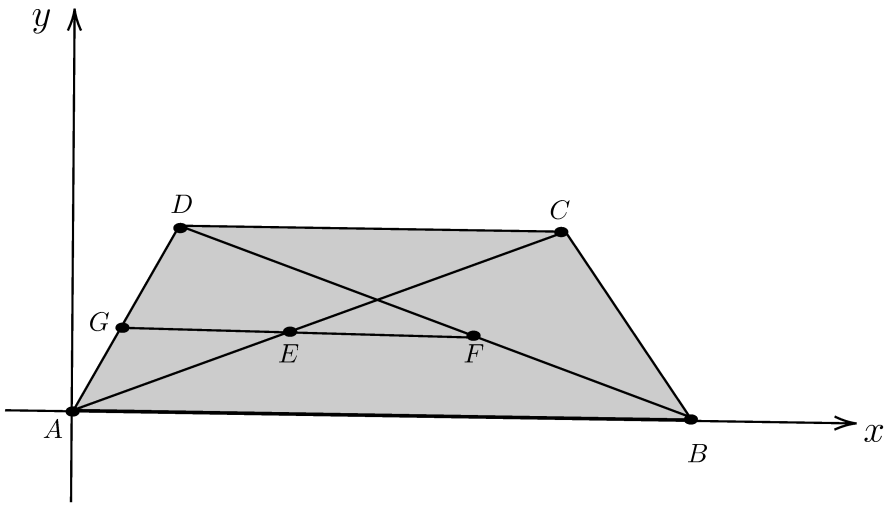
Quando a tese é definida somente por um polinômio, podemos usar `poly` ou `ideal`. Se a tese for definida por mais do que um polinômio, melhor usar `ideal`, pois em um ideal podemos ter vários polinômios como seus geradores, e daí usa-se o comando `subst` uma única vez.

5.6 Teorema: Diagonais de um trapézio e o ponto médio dos lados não paralelos

Teorema 10. *A reta que passa pelos pontos médios das diagonais de um trapézio divide os lados que não são paralelos ao meio.*

Demonstração:

Considere o trapézio $ABCD$, com os lados AB e CD paralelos. Utilizando o sistema de coordenadas cartesianas, podemos supor que A coincida com a origem do sistema e que o lado AB esteja sobre o eixo x, conforme ilustrado na figura abaixo.



Sejam $A(0,0)$, $B(x_3,0)$, $C(x_2,y_1)$ e $D(x_1,y_1)$ os vértices do trapézio $ABCD$.

Se E for o ponto médio da diagonal AC e F for o ponto médio da diagonal BD, então:

$$E\left(\frac{0+x_2}{2},\frac{0+y_1}{2}\right)=E\left(\frac{x_2}{2},\frac{y_1}{2}\right).$$

$$F\left(\frac{x_3+x_1}{2},\frac{0+y_1}{2}\right)=F\left(\frac{x_3+x_1}{2},\frac{y_1}{2}\right).$$

Queremos mostrar que a reta r que passa por E e F corta o lado AD em $G\left(\frac{x_1}{2},\frac{y_1}{2}\right)$ que é o ponto médio de AD.

Note que os pontos E,F e G, têm a mesma ordenada, o que já é suficiente para provar o teorema. Apesar disso vamos utilizar equações polinomiais para provar o teorema.

Chamando de $M(u,v)$ o ponto em que a reta r intersecta o lado AD, temos duas equações que formam as hipóteses.

A primeira hipótese h_1 é que os pontos M,E,F são colineares, logo:

$$h_1 : \begin{vmatrix} u & v & 1 \\ \frac{x_2}{2} & \frac{y_1}{2} & 1 \\ \frac{x_3+x_1}{2} & \frac{y_1}{2} & 1 \end{vmatrix} = \frac{uy_1}{2} + \frac{vx_3 + vx_1}{2} + \frac{x_2y_1}{4} - \frac{x_3y_1}{4} - \frac{x_1y_1}{4} - \frac{uy_1}{2} - \frac{vx_2}{2} = 0$$

$$h_1 : 2vx_3 + 2vx_1 + y_1x_2 - y_1x_3 - y_1x_1 - 2vx_2 = 0.$$

A segunda hipótese h_2 é que os pontos M, A, D são colineares, logo:

$$h_2 : \begin{vmatrix} u & v & 1 \\ 0 & 0 & 1 \\ x_1 & y_1 & 1 \end{vmatrix} = 0 + vx_1 + 0 - 0 - uy_1 - 0 = 0$$

$$h_2 : vx_1 - uy_1 = 0.$$

Vamos utilizar as equações h_1 e h_2 para mostrar que os pontos G e M são iguais, isto é, precisamos mostrar que g_1 (igualdade das abscissas) e g_2 (igualdade das ordenadas) se verificam, onde:

$$\begin{array}{ll} g_1 : \frac{x_1}{2} = u & g_2 : \frac{y_1}{2} = v \\ g_1 : 2u - x_1 = 0 & g_2 : 2v - y_1 = 0. \end{array}$$

Resolvendo o sistema abaixo com as variáveis x_1, x_2, x_3, y_1 sendo independentes, os pontos médios M, E, F são dependentes dos vértices A, B, C, D, isto é, u e v são dependentes de x_1, x_2, x_3 e y_1.

$$\begin{cases} h_1 : \ 2vx_3 + 2vx_1 + y_1x_2 - y_1x_3 - y_1x_1 - 2vx_2 = 0 \\ \\ h_2 : \ vx_1 - uy_1 = 0. \end{cases}$$

Em h_1, isolando v teremos:

$$2v(x_3 + x_1 - x_2) = -y_1x_2 + y_1x_3 + y_1x_1$$

$$v = \frac{y_1(x_1 - x_2 + x_3)}{2(x_1 - x_2 + x_3)}$$

$$v = \frac{y_1}{2}.$$

Note que $x_2 \neq x_1 + x_3$, senão teríamos um paralelogramo. Substituindo v em h_2 teremos:

$$u = \frac{vx_1}{y_1}$$

$$u = \frac{y_1}{2}\frac{x_1}{y_1}$$

$$u = \frac{x_1}{2}.$$

Substituindo u e v em g_1 e g_2, temos:

$$\begin{array}{lrcrcl} g_1: & 2u & - & x_1 & = & 0 \\ g_1: & 2\frac{x_1}{2} & - & x_1 & = & 0 \\ g_1: & 0 & & & = & 0 \end{array} \quad \text{e} \quad \begin{array}{lrcrcl} g_2: & 2v & - & y_1 & = & 0 \\ g_2: & 2\frac{y_1}{2} & - & y_1 & = & 0 \\ g_2: & 0 & & & = & 0. \end{array}$$

Logo, a reta r bissecta o lado AD. Analogamente, a mesma reta r bissecta o lado BC do trapézio. Portanto, concluímos que a reta que une os pontos médios das diagonais de um trapézio bissecta os lados que não são paralelos.

□

Resolvendo este problema via Singular

No singular entre com os seguintes comandos:

```
> ring r= (0,x1,x2,x3,y1),(u,v),lp;
> option(redSB);
> ideal I=2*v*x3+2*v*x1+y1*x2-y1*x3-y1*x1-2*v*x2,v*x1-u*y1;
> ideal J=std(I);
> simplify(J,1);
_[1]=v+(-y1)/2
_[2]=u+(-x1)/2
>
```

Note que o resultado do último comando traduz facilmente os valores de u e v.

Usando o comando `subst`, podemos constatar o anulamento da tese.

```
> ideal g = 2*u-x1,2*v-y1;
> subst(g,u,x1/2,v,y1/2);
_[1]=0
_[2]=0
>
```

Como a tese é definida por mais de um polinômio, é melhor usar `ideal`, pois em um ideal podemos ter vários polinômios como seus geradores.

O comando `subst(g,f1,g1,f2,g2,...,fn,gn)`, significa que vamos substituir o objeto `fi` por `gi` no objeto `g`. Substituímos u por $x_1/2$ e v por $y_1/2$ nos polinômios g_1 e g_2.

6. Considerações finais

Este trabalho possibilitou aprimorar os conceitos de anéis de polinômios de várias variáveis, ordens monomiais, conjuntos algébricos afins, algoritmo da divisão, além de introduzir o uso do sistema algébrico computacional Singular. Foram muitas as aprendizagens com o desenvolvimento desse trabalho, trazendo muitas contribuições para a minha prática no cotidiano escolar.

Os problemas de geometria euclidiana plana apresentados neste trabalho foram demonstrados com enfoque em conhecimentos adquiridos ao longo do ensino médio.

Utilizando os axiomas da geometria euclidiana plana e introduzindo as coordenadas cartesianas no plano, foram desenvolvidas as hipóteses e as conclusões por meio de equações polinomiais dos teoremas apresentados no Capítulo 5.

Os problemas foram provados resolvendo sistemas de equações polinomias formados pelas hipóteses e conclusões, buscando uma estratégia de ensino que facilite o processo de aprendizagem, estimulando o raciocínio lógico, melhorando a interpretação e ampliando os conhecimentos e conceitos que precisam ser consolidados.

Utilizamos o Singular para agilizar as resoluções de alguns dos problemas apresentados.

Apesar de parte dos conceitos estudados aqui não serem ensinados com detalhes e demonstrações no ensino básico, exemplificamos a demonstração do algoritmo da divisão de polinômio que é um procedimento aplicado desde o ensino fundamental.

Por fim, esperamos que este trabalho possa trazer contribuições para alunos e professores que buscam aprimorar e enriquecer seus conhecimentos em resolução de problemas da Geometria, Álgebra de polinômios e seus diversos desdobramentos.

Referências Bibliográficas

[1] Coutinho, S. C.: *Polinômios e Computação Algébrica.* Instituto Nacional de Matemática Pura e Aplicada - IMPA - Coleção Matemática e Aplicações, 2012.

[2] Cox, D., Little, J. e O´Shea, D.: *Ideals, Varieties, and Algorithms.* Springer-Verlag, Berlin-Heidelberg-New York, 2nd ed., 1997. https://doi.org/10.1007/978-1-4757-2693-0.

[3] Gonçalves, A.: *Introdução à Álgebra.* Projeto Euclides - Rio de Janeiro: SBM, 6ª ed., 2017.

[4] Greuel, G. M. e Pfister, G.: *A Singular Introduction to Commutative Algebra.* Cambridge Studies in Advanced Mathematics, 2002. https://doi.org/10.1007/978-3-662-04963-1.

[5] Greuel, G. M., Pfister, G. e Schönemann, H.: *Singular Reference Manual.* Reports On Computer Algebra Number 12, Centre for Computer Algebra, University of Kaiserslautern, 1997. https://www.singular.uni-kl.de.

[6] Greuel, G. M., Pfister, G. e Schönemann, H.: Singular*: A Computer Algebra System for Polynomial Computations.* Centre for Computer Algebra, University of Kaiserslautern, free software under the GNU General Public Licence, 2007. https://www.singular.uni-kl.de.