**UNIVERSIDADE FEDERAL DO CEARÁ**

**CENTRO DE CIÊNCIAS**

**DEPARTAMENTO DE MATEMÁTICA**

**PROGRAMA DE PÓS-GRADUAÇÃO EM MATEMÁTICA EM REDE NACIONAL**

**AISLAN SIRINO LOPES**

# CRITÉRIO PARA A CONSTRUTIBILIDADE DE POLÍGONOS REGULARES POR RÉGUA E COMPASSO E NÚMEROS CONSTRUTÍVEIS

**JUAZEIRO DO NORTE**

**2014**

**AISLAN SIRINO LOPES**

# CRITÉRIO PARA A CONSTRUTIBILIDADE DE POLÍGONOS REGULARES POR RÉGUA E COMPASSO E NÚMEROS CONSTRUTÍVEIS

Dissertação de Mestrado apresentada ao Programa de Pós-Graduação em Matemática em Rede Nacional da Universidade Federal do Ceará, como requisito parcial para obtenção do Título de Mestre em Matemática. Área de Concentração: Ensino da Matemática.
Orientador: Prof. Ms. Paulo César Cavalcante de Oliveira.

**JUAZEIRO DO NORTE**

**2014**

Dados Internacionais de Catalogação na Publicação
Universidade Federal do Ceará
Biblioteca do Curso de Matemática

L85c Lopes, Aislan Sirino
Critério para a construtibilidade de polígonos regulares por régua e compasso e números construtíveis / Aislan Sirino Lopes. – 2014.
49 f. : il., enc.; 31 cm

Dissertação (mestrado) – Universidade Federal do Ceará, Centro de Ciências, Departamento de Matemática, Programa de Pós-Graduação em Matemática em Rede Nacional, Juazeiro do Norte, 2014.
Área de Concentração: Ensino de Matemática.
Orientação: Prof. Ms. Paulo César Cavalcante de Oliveira.

1. Construções geométricas. 2. Polígonos regulares. 3. Polinômios. I. Título.

CDD 516.13

AISLAN SIRINO LOPES

# CRITÉRIO PARA A CONSTRUTIBILIDADE DE POLÍGONOS REGULARES POR RÉGUA E COMPASSO E NÚMEROS CONSTURÍVEIS

Dissertação de Mestrado apresentada ao Programa de Pós-Graduação em Matemática em Rede Nacional, do Departamento de Matemática da Universidade Federal do Ceará, como requisito parcial para a obtenção do Título de Mestre em Matemática. Área de concentração: Ensino de Matemática.

Aprovada em: 17 / 05 / 2014.

BANCA EXAMINADORA

Prof. Ms. Paulo César Cavalcante de Oliveira (Orientador)
Universidade Federal do Ceará (UFC)

Prof. Ms. Francisco Valdemiro Braga
Universidade Federal do Ceará (UFC)

Prof. Ms. Zelalber Gondim Guimarães
Universidade Regional do Cariri (URCA)

## AGRADECIMENTOS

Aos meus pais e irmãos, pelo apoio de sempre.

À minha esposa, pelo apoio incondicional.

Ao professor Paulo César Cavalcante de Oliveira pela orientação e dedicação.

Àqueles que foram meus professores tanto no ensino básico como no ensino superior, em especial Donatila Luiza Carvalho Coutinho, Mário de Assis Oliveira e Zélalber Gondim Guimarães.

Aos colegas de mestrado, pela amizade e companheirismo ao longo da nossa jornada acadêmica.

À Sociedade Brasileira de Matemática - SBM pela oferta do programa PROFMAT.

À CAPES, pelo apoio financeiro.

Uma verdade matemática não é simples nem complicada por si mesma. É uma verdade. (Emile Lemoine)

## RESUMO

Este trabalho aborda construções geométricas elementares e de polígonos regulares realizadas com régua não graduada e compasso respeitando as regras ou operações elementares usadas na Antiguidade pelos gregos. Tais construções serão inicialmente tratadas de uma forma puramente geométrica e, a fim de encontrar um critério que possa determinar a possibilidade de construção de polígonos regulares, passarão a ser discutidas por um viés algébrico. Este tratamento algébrico evidenciará uma relação entre a geometria e a álgebra, em especial, a relação entre os vértices de um polígono regular e as raízes de polinômios de uma variável com coeficientes racionais. Este tratamento algébrico nos levará naturalmente ao conceito de construtibilidade de números e pontos no plano de um corpo, o que exigirá o uso de extensões algébricas de corpos, e os critérios para a construtibilidade destes nos levará a um critério de construtibilidade dos polígonos pretendidos.



**Palavras-chave:** Construções geométricas. Polígonos regulares. Números construtíveis. Polinômios. Extensões algébricas.

**ABSTRACT**

This work discusses basic geometric constructions and constructions of regular polygons with ruler and compass made respecting the rules or elementary operations used by the ancient Greeks. Such constructs are initially treated in a purely geometric form and, in order to find a criterion that can determine the possibility of construction of regular polygons, will be discussed by an algebraic bias. This algebraic treatment will show a relationship between geometry and algebra, in particular, the relationship between the vertices of a regular polygon and the roots of polynomials in a variable with rational coefficients. This algebraic treatment leads us naturally to the concept of constructibility of numbers and points in a field, which will require the use of algebraic field extensions, and the criteria for the constructibility of these leads to a criterion for constructibility of polygons.

**Keywords:** Geometric constructions. Regular polygons. Constructible numbers. Polynomials. Algebraic fields extensions.

## LISTA DE ILUSTRAÇÕES

**SUMÁRIO**

# 1 INTRODUÇÃO

A matemática da Grécia antiga deve muito do seu desenvolvimentos às construções realizadas com régua não graduada e compasso, que surgem com os pitagóricos, ainda no século V a. C., e cujo ápice dá-se no século III a. C. devido a uma nova forma de resolver problemas algébricos por um viés geométrico. Por exemplo, a existência de um número cujo quadrado resultava em 2 não tinha solução numérica para os gregos, que só admitiam soluções racionais, mas apresentava uma solução geométrica: este número era a medida da diagonal de um quadrado de lado unitário. Tal álgebra tinha um aspecto peculiar em relação à que conhecemos hoje, pois para os gregos, havia a unidade e os números eram formados a partir da unidade, ou seja, os números eram os elementos pertencentes ao conjunto {2, 3, 4, 5, 6, ...}. Mesmo os racionais não eram considerados números, eram razões entre estes.

Alguns problemas problemas clássicos, os quais trataremos no quinto capítulo, resistiram às tentativas dos gregos de resolução com o uso apenas de régua não graduada e compasso, e qualquer resposta definitiva mostrou-se impossível por séculos. Na tentativa de resolver tais problemas, importantes descobertas foram realizadas não só na geometria, mas também na álgebra, fazendo das construções uma fonte bastante frutífera de resultados.

Em contramão com a importância histórica no desenvolvimento da Matemática, além de seu caráter educativo e intrigante, as construções geométricas estão sendo banidas dos currículos escolares da educação básica brasileira e são esquecidas até mesmo nos cursos de licenciatura de Matemática, prejudicando a formação dos futuros professores e restringindo o uso de ferramentas importantes na atuação docente.

Através das construções, pode-se definir conceitos, demonstrar-se propriedades e resolver problemas que contribuirão no desenvolvimento do raciocínio lógico-dedutivo do aluno. A adoção das construções geométricas no ensino básico podem facilitar na compreensão através de uma base mais sólida principalmente da Geometria Euclidiana Plana, mas também de outros componentes curriculares como Geometria Analítica, Conjuntos Numéricos (principalmente na compreensão da existência dos números irracionais), construção de gráficos, entre outros.

Inicialmente a abordagem trará com maior ênfase as construções geométricas como forma de introduzir o assunto e suas justificativas podem ser usadas como objeto de

discussão de temas elementares da geometria euclidiana plana para o ensino básico. A forma como o tema é conduzido até o quarto capítulo destina-o à aplicação no referido nível escolar.

No decurso do trabalho, a abordagem passa a apresentar um aspecto algébrico. Tal aspecto destina-se principalmente ao aperfeiçoamento da formação docente. Analisaremos através da Álgebra a possibilidade ou não da construção de determinados polígonos regulares, o que veremos ser equivalente a construtibilidade ou não dos números como entendidos atualmente.

Para isso, faz-se necessário um estudo de polinômios em uma indeterminada com coeficientes em um determinado corpo e sua irredutibilidade sobre este. Para uma formulação do conceito de construtibilidade de números e pontos em um plano de forma algébrica, trataremos de extensões de corpos dando ênfase às extensões algébricas dos racionais. Enfim, teremos ferramentas que nos dotarão do necessário à encontrar um critério para a não construtibilidade de números e um critério que nos permita decidir a construtibilidade de polígonos regulares.

Espero que este trabalho contribua com o enriquecimento dos conhecimentos dos professores de matemática e permita ao aluno do nível básico adquirir uma visão mais ampla da matemática, formulando conceitos que lhes são indispensáveis.

# 2 CONSTRUÇÕES GEOMÉTRICAS ELEMENTARES COM RÉGUA E COMPASSO

Os gregos antigos conheciam as construções geométricas das quais trataremos aqui. Vale relembrar que estas eram efetuadas com o uso apenas de uma régua não graduada e compasso e são validadas pelos postulados euclidianos.

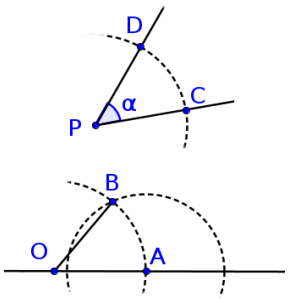
As construções devem seguir algumas regras: conhecendo-se dois pontos distintos, é permitido traçar uma reta com uma régua não graduada; com o compasso, permite-se a construção de uma circunferência desde que tenha centro em um ponto conhecido e que passe em um ponto distinto determinado. A construção de todo e qualquer ponto será resultado do uso de três regras, às quais chamaremos de operações elementares: intersecção de duas retas; intersecção de uma reta e uma circunferência; intersecção de duas circunferências. Diz-se que um ponto é construtível quando este pode ser obtido por um número finito de operações elementares.

Este capítulo apresenta construções elementares de caráter introdutório e que podem ser usadas como pré-requisitos para as construções dos capítulos subsequentes. Consideremos para todos os exemplos estabelecida uma unidade de comprimento.

## 2.1 Construção de um ângulo dada sua medida

Considere uma reta r, um ponto O pertencente a r e um ângulo α dado com vértice em P. Construiremos um ângulo de medida α com vértice em O com um lado sobre r.

Figura 01 – Construção do ângulo α.




Com o compasso centrado no vértice do ângulo α, intersecte os lados do ângulo

nos pontos C e D. Com o compasso centrado em O e preservando a abertura, construa um círculo que intersecte r em A. Meça com o compasso a distância entre C e D e com esta abertura construa um círculo centrado em A intersectando a circunferência de centro em O no ponto B. O ângulo AÔB mede α.

A justificativa da construção é imediata por congruência de triângulos. Por construção, temos que os segmentos CD, PC e PD são congruentes aos segmentos AB, OA e OB, respectivamente. Logo os triângulos PCD e OAB são congruentes, em particular, AÔB mede α.

Figura 02-a – ângulo ângulo α + θ

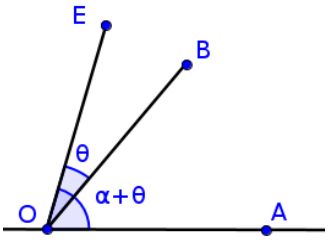
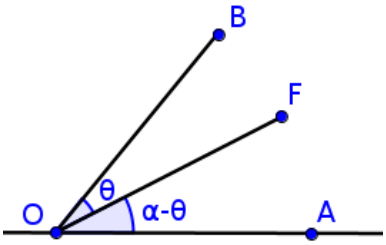


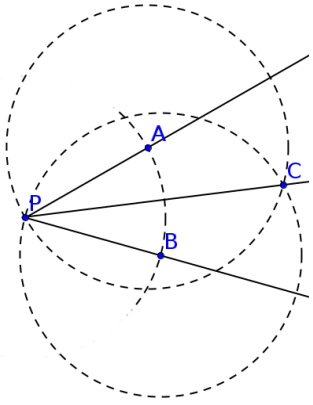

Figura 02-b – ângulo ângulo α - θ




Dado um ângulo θ, o ângulo α + θ com vértice em O pode ser construído realizando a construção de θ sobre a reta suporte de OB. Analogamente, considerando θ < α, ao construir θ com vértice em O sobre a reta suporte de OB, de modo que θ seja interno a α, obtemos um outro ângulo cuja medida é α – θ.

## 2.2 Bissecção de um ângulo qualquer

Figura 03 – Bissecção de um ângulo.



Seja P o vértice do ângulo, trace um círculo de raio qualquer centrado em P, intersectando os lados dos ângulos em A e B, respectivamente. Trace dois círculos de mesmo raio centrados em A e B de modo que se intersectem em um ponto C. A reta que passa por P e C bissecta o ângulo em questão.

De fato, considere os triângulos PCA e PCB. Por construção, temos que os segmentos PA e PB são congruentes, assim como os segmentos AC e BC, e temos que PC é um segmento em comum. Logo, os triângulos em questão são congruentes, pois têm lados idem. Em particular, os ângulos $A\hat{P}C$ e $B\hat{P}C$ são congruentes.

## 2.3 Perpendicular a uma reta r passando por um ponto P

Figura 04-a – Construção da perpendicular: caso $P \in r$.

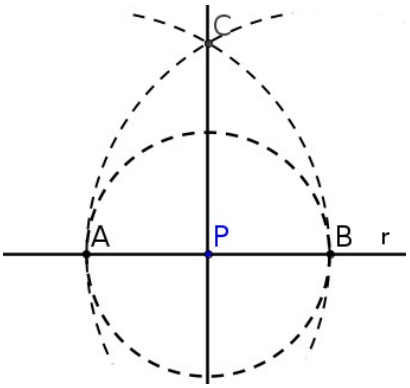
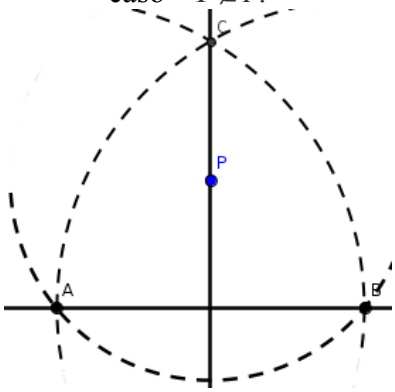



Figura 04-b – Construção da perpendicular: caso $P \notin r$.



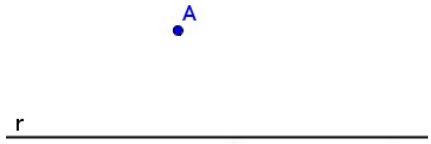

Há dois casos: o ponto P pertence a reta r (Figura 04-a); o ponto P não pertence à reta r (Figura 04-b). Em qualquer deles, trace uma circunferência de centro P que intersecte a reta r em dois pontos distintos A e B. Com centro em A, trace uma semi-circunferência que passe por B. Com centro em B, trace uma semi-circunferência que passe por A. Seja C a intersecção destas semi-circunferências, trace a reta s que passa por C e P. Esta reta é perpendicular a r.

Em ambos os casos, os triângulos ACP e BCP são congruentes. Logo dos ângulos $A\hat{C}P$ e $B\hat{C}P$ são congruentes. Como o triângulo ABC é isósceles, o segmento com extremos em C e na intersecção de r e s é a altura do triângulo ABC e, por conseguinte, a reta s é perpendicular à reta r.

Perceba que se considerarmos o segmento AB, através da construção descrita obtemos seu ponto médio e sua mediatriz.

## 2.4 Reta paralela a uma reta dada

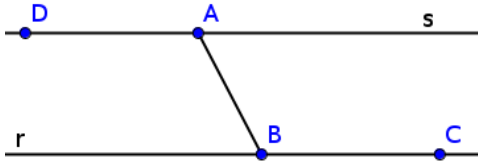
Figura 05 – reta r e ponto A $\notin$ r.




Dados uma reta e um ponto A, construiremos uma reta s, paralela à reta r e passando pelo ponto A.

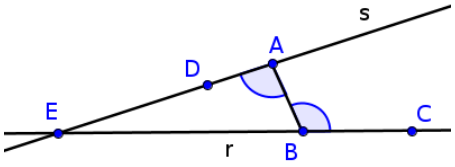
Tomando-se dois pontos sobre a reta r, digamos B e C, una A a B. Construa $B\hat{A}D \equiv A\hat{B}C$ de forma que os pontos C e D estejam em semiplanos opostos em relação à reta que passa por A e B. A reta s que passa por A e D é paralela à reta r.

Figura 06 – reta paralela a uma reta dada.




Suponha por contradição que s não seja paralela a r. Seja E o ponto de intersecção entre r e s. Nos concentremos no caso em que B pertence a CE, pois o segundo caso é análogo. Por construção, temos que $A\hat{B}C = E\hat{A}B = D\hat{A}B$. Mas $A\hat{B}C$ é ângulo externo ao triângulo ABD, logo $A\hat{B}C > E\hat{A}B$, o que é uma contradição. Portanto a suposição é falsa e as retas r e s são, de fato, paralelas.

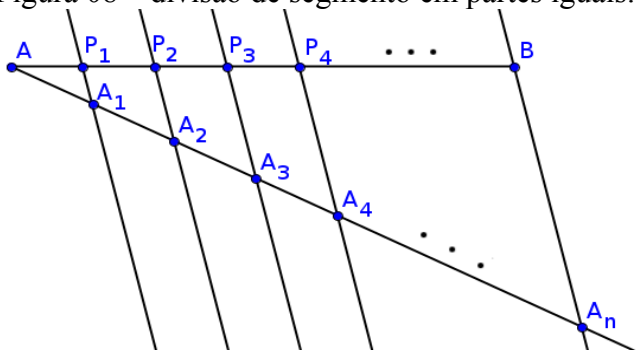
Figura 07 – demonstração do paralelismo.



## 2.5 Divisão de um segmento em partes iguais

Dado um segmento AB, o dividiremos em n segmentos congruentes, $n \in \mathbb{N}$. A partir de A, trace uma reta r concorrente a reta suporte de AB. Marque sobre r um ponto $A_1$ distinto de A. Com o compasso, marque pontos distintos $A_i$ sobre r tais que a distância entre $A_i$ e $A_{i+1}$ é a medida do segmento $AA_1$, i = 1, 2, …, n. Trace a reta s que passa por $A_n$ e B. Construa as retas paralelas a s que passam por cada ponto anteriormente marcado em r. As intersecções $P_i$ das retas paralelas construídas com o segmento AB dividem este segmento em n partes iguais. A aplicação do teorema de Tales valida imediatamente a construção.

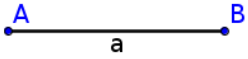
Figura 08 – divisão de segmento em partes iguais.



# 3 NÚMEROS CONSTRUTÍVEIS

**Axioma 3.1.** *A todo segmento corresponde um número maior ou igual a zero; este número é zero se, e somente se, as extremidades coincidem.*

Figura 09 – segmento de medida a.



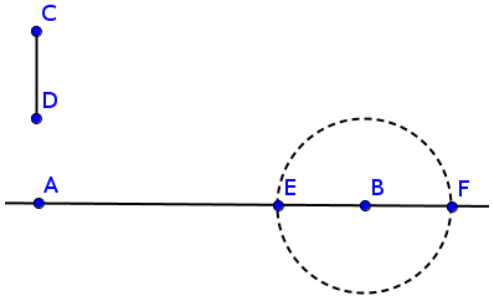

**Axioma 3.2.** *Os pontos de uma reta podem ser sempre colocados em correspondência biunívoca com os números reais, de modo que o módulo da diferença entre estes números seja a distância entre os pontos correspondentes.*

Definimos que um número real x é construtível se x = 0 ou se for possível construir, com régua e compasso, através de um número finito de operações elementares, um segmento de comprimento igual a |x|, a partir de um segmento de reta tomado como unidade.

Seja |x| a medida do segmento AB, x é um número construtível se o segmento AB o for. Para a construção de números negativos deve-se considerar uma reta orientada.

## 3.1 Soma, diferença, produto e razão

Figura 10 – construção da soma e diferença.




**Proposição 3.1.** *Sejam a e b números reais construtíveis, com a > b e b ≠ 0, então são também construtíveis a + b, a – b, ab e a/b.*

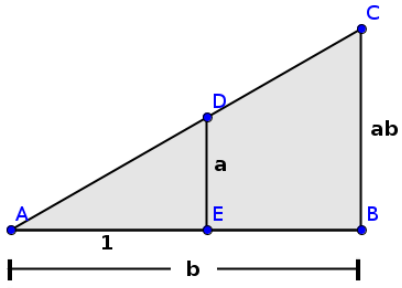
**Demonstração:** Dados segmentos AB e CD de comprimentos *a* e *b*, respectivamente, com

$a > b$. Seja r a reta suporte do segmento AB, com o compasso centrado em B e a abertura medindo $b$, trace uma circunferência intersectando a reta r em E e F. Seja E o ponto mais próximo de A, temos que o segmento AE mede $a - b$; seja F o ponto mais distante de A, temos que o segmento AE mede $a + b$.

Construa um triângulo ADE reto em E cujo lado AE meça a unidade e o lado DE meça a. Sobre a reta que contém AE, encontre B tal que AB meça b. Transporte o ângulo $A\hat{E}D$ para $A\hat{B}C$ sendo C pertencente a reta que contém AD.

Através da semelhança de triângulos verifica-se de imediato que o segmento BC mede ab.

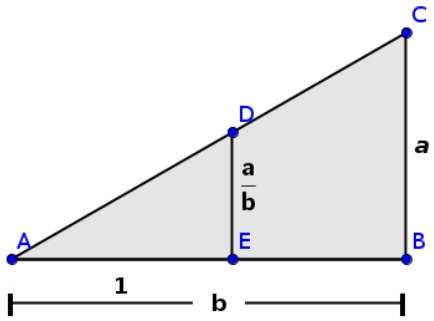
Figura 11 – construção do produto.




Construa um triângulo ABC em que AB meça b e BC meça a. A partir de A, localize o ponto E sobre o segmento AB que meça a unidade. Transporte o ângulo $A\hat{B}C$ para $A\hat{E}D$, sendo D um ponto em AC. Temos que DE mede $\frac{a}{b}$ é novamente verificável através da semelhança de triângulos.

□

Figura 12 – construção da razão.

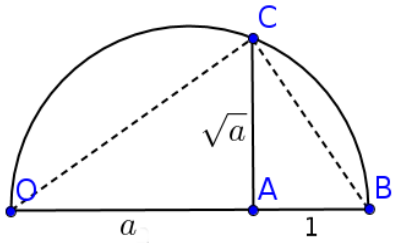



Dado que todo número inteiro é construtível a partir da unidade por um número

finito de passos, o resultado garante que todo número racional pode ser construído.

### 3.2 Construção da raiz quadrada

Figura 13 – construção de $\sqrt{a}$.




**Proposição 3.2.** *Se a é construtível, então* $\sqrt{a}$ *é construtível.*

**Demonstração:** dado um segmento de comprimento *a*, sobre uma reta construa um segmento OA que meça *a* e um segmento AB cuja medida seja a unidade. Construa o semicírculo com diâmetro OB. Construa um segmento AC perpendicular a OB em que C é um ponto do semicírculo. O segmento AC mede $\sqrt{a}$ (figura 09).

Temos que $O\hat{C}B$ é o arco capaz sobre o diâmetro OB, logo é reto. Através da semelhança entre os triângulos ABC e OAC, justifica-se a construção.

Perceba que se considerarmos na construção anterior que OB mede *b*, obtemos a média geométrica entre *a* e *b*.

□

Dados segmentos de medidas *a* e *b* e seja $x=\sqrt{a^2-b^2}$, *x* é um cateto de um triângulo retângulo cuja hipotenusa mede *a* e o outro cateto mede *b* e sua construção é elementar: inicialmente constrói-se uma reta r perpendicular ao segmento AB de comprimento *b* passando por A; centrando o compasso em B e abertura medindo *a*, intersecte a reta r em um ponto C, determinando o segmento AC que mede *x*.

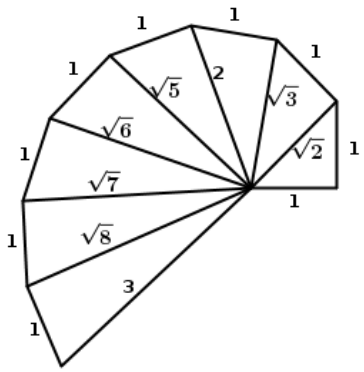
Caso tenhamos $x=\sqrt{a^2+b^2}$, então *x* é a medida da hipotenusa de um triângulo retângulo cujos catetos medem *a* e *b*, o que pode ser facilmente obtido com construções elementares tratadas anteriormente.

Aplicando recursivamente as construções descritas acima, podemos obter expressões da forma $x=\sqrt{a^2+b^2+c^2+\ldots}$, em particular, podemos obter a medida da

diagonal de um paralelepípedo.

Considerando um triângulo retângulo isósceles de catetos medindo *a,* podemos encontrar os números $a\sqrt{2}, a\sqrt{3}, \cdots, a\sqrt{n}$. Por meio do teorema de Pitágoras conclui-se de imediato que a hipotenusa deste triângulo mede $a\sqrt{2};$ tomando-se este lado como cateto e construindo um segmento medindo a unidade perpendicular ao primeiro, chegamos a um novo triângulo retângulo cuja hipotenusa mede $a\sqrt{3};$ repetindo-se os passos uma quantidade finita de vezes, encontramos $a\sqrt{n}$. Em particular, se *a* é a unidade, obteremos a espiral de Teodoro, também conhecida como espiral pitagórica (figura 10).

Figura 14 – espiral de Teodoro.




Obviamente este processo é demasiado lento para valores de n relativamente grandes, o que nos faz procurar meios menos custosos. Por exemplo, basta considerar um triângulo retângulo de catetos medindo 2 e 4 para construirmos $\sqrt{20}$.

Por fim, se pudermos construir *a* e $b\sqrt{n},$ através da construção representada na figura 09 podemos obter $\sqrt{a+b\sqrt{n}}$.

### 3.3 Razão áurea

O número áureo, representado pela letra grega $\Phi$ (phi), é definido da seguinte forma: razão entre os comprimentos de um segmento AB e um segmento AE tal que o ponto E localiza-se entre A e B e $\frac{\overline{AB}}{\overline{AE}} = \frac{\overline{AE}}{\overline{BE}} = \Phi$.

Esta razão foi muito utilizada em construções na Antiguidade, como no templo da

deusa grega Athena Parthenos, o Parthenon, cuja estrutura arquitetônica é atribuída a Phídeas (Φειδίας, em grego), que empresta a inicial de seu nome à razão. A influência arquitetônica perdurou ainda na Idade Média na construção das grandes catedrais.

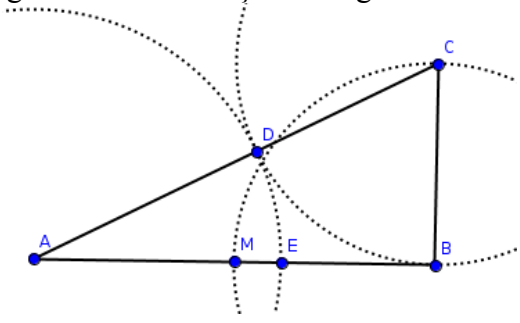
Figura 15 – Segmento áureo.


Sejam x e w os comprimentos dos segmentos AB e AE, respectivamente. Da definição de número áureo, temos $\frac{x}{w}=\frac{w}{x-w}=\Phi$. Segue que $x^2 - wx - w^2 = 0$. Resolvendo a equação quadrática obtida, encontramos a solução $x = w\cdot\left(\frac{1+\sqrt{5}}{2}\right)$.

Resulta que $\Phi=\frac{x}{w}=\frac{w\cdot\left(\frac{1+\sqrt{5}}{2}\right)}{w}=\frac{1+\sqrt{5}}{2}\approx 1{,}618$.

Dado um segmento AB de comprimento x, localize o ponto médio M. Trace um segmento perpendicular a AB de comprimento $\frac{x}{2}$ com extremos em B e C. Trace o segmento AC. Com o compasso em C, localize o ponto D em AC tal que o comprimento de CD seja $\frac{x}{2}$. Com o compasso centrado em A e raio igual ao comprimento do segmento AD, marque o ponto E em AB. O ponto E divide o segmento AB em média e extrema razão, ou seja, $\frac{\overline{AB}}{\overline{AE}}=\frac{\overline{AE}}{\overline{BE}}=\Phi$.

Figura 16 – Construção do segmento áureo.




É fácil verificar que de fato isso ocorre. Fazendo uso do teorema de Pitágoras no

triângulo retângulo ABC, obtém-se que o segmento AC mede $\frac{x\sqrt{5}}{2}$. O segmento AE tem o mesmo comprimento de AD, o que pode ser obtido subtraindo a medida de CD da medida de AC. Chegamos que AE mede $x \cdot \left(\frac{\sqrt{5}-1}{2}\right)$. Calculando a razão das medidas de AE por BE, encontramos $\Phi$.

O retângulo áureo é definido como o retângulo cuja razão das medidas de seu lado maior pelo lado menor é igual a $\Phi$. Seja E o ponto que divide o segmento AB em média e extrema razão, trace por E o segmento EF perpendicular ao segmento AB cuja medida é a mesma de EB. Construa os segmentos FG e AG com as mesmas medidas e perpendiculares a AE e EF, respectivamente. O retângulo AEFG é áureo.

Figura 17 – Retângulo áureo.

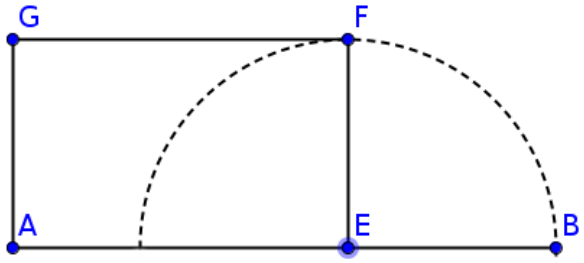
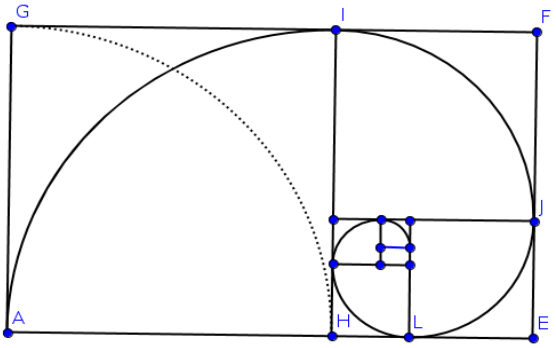



Figura 18 – Espiral áurea.




Construindo internamente ao retângulo AEFG um quadrado AHIG, obtém-se um retângulo EFIG áureo. Este processo pode ser feito recursivamente obtendo-se novos retângulos áureos. Traçando-se arcos com a ajuda do compasso, como mostrados na figura 06, geramos uma bela curva conhecida como espiral áurea.

# 4 CONSTRUÇÕES DE ALGUNS POLÍGONOS REGULARES

Este capítulo tratará das construções de alguns polígonos regulares, fazendo uso de algumas das construções básicas já tratadas e respeitando as regras impostas para tais. Algumas construções impossíveis com estas exigências tornam-se possíveis se utilizada uma régua graduada, por exemplo.

**Definição 4.1.** *Um polígono é dito regular se, e somente se tem todos os seus lados congruentes e todos os seus ângulos internos congruentes.*

**Definição 4.2.** *Referimo-nos como arco de circunferência a cada uma das partes em que esta é dividida por um par de seus pontos.*

**Definição 4.3.** *Denomina-se corda de circunferência a qualquer segmento de reta cujas extremidades sejam pontos sobre ela.*

As construções de polígonos regulares inscritos em circunferências baseiam-se no seguinte teorema.

**Teorema 4.1.** *Dividindo-se uma circunferência em n arcos congruentes com* $(n \geq 3)$, *temos:*

*a) todas as cordas determinadas pelos extremos de um mesmo arco, reunidas, formam um polígono regular de n lados inscrito na circunferência;*

*b) as tangentes à circunferência traçadas pelos extremos dos arcos determinam um polígono regular de n lados circunscritos à circunferência.*

**Demonstração:** Sejam $A_1$ , $A_2$ , $\cdots$ , $A_{n-1}$ , $A_n$ os n pontos extremos dos arcos que dividem a circunferência C de centro O em n arcos, e formam o polígono inscrito $A_1 A_2 \cdots A_{n-1}A_n$. Como temos

$$\text{arco}A_1 A_2 \equiv \text{arco}A_2 A_3 \equiv \cdots \equiv \text{arco}A_{n-1} A_n \equiv \text{arco}A_n A_1 .$$

então

$$A_1 A_2 \equiv A_2 A_3 \equiv \cdots \equiv A_{n-1} A_n \equiv A_n A_1 \ . \qquad (1)$$

Isto é fato, pois arcos congruentes subtendem cordas idem. Considerando os triângulos $OA_{i-1}A_i$, para i = 1, 2, · · · , n, onde $A_0$ coincide com $A_n$, todos estes são congruentes, por conseguinte, $\hat{A}_1, \hat{A}_2, \hat{A}_3, \hat{A}_4, \cdots, \hat{A}_{n-1}, \hat{A}_n$ também são congruentes, pois são ângulos inscritos medindo $\frac{(n-2)\pi}{n}$ radianos. Está provada a primeira parte.

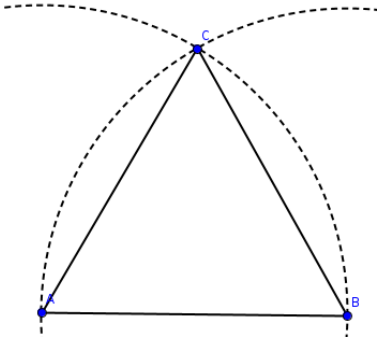
Considere agora as retas tangentes à circunferência C passando pelos pontos $A_i$. Seja $B_i$ cada ponto de intersecção das tangentes que passam por $A_{i-1}$ e $A_i$. São congruentes os triângulos $OA_{i-1}B_i$ e $OA_iB_i$, em particular são congruentes os lados $A_{i-1}B_i$ e $A_iB_i$. A congruência dos ângulos $\hat{B}_i$ verifica-se através dos triângulos $A_{i-1}A_iB_i$.

□

## 4.1 Triângulo equilátero dado o lado

Dado um segmento AB, construa as circunferências de centros A e B, respectivamente, com raio igual a medida do segmento dado. Marque a intersecção C destas circunferências. Trace os segmentos AC e BC.

Figura 19 – Triângulo equilátero.

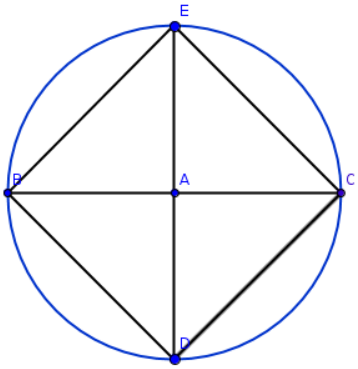



A partir do triângulo equilátero é imediata a construção do hexágono regular.

## 4.2 Quadrado inscrito dada a diagonal

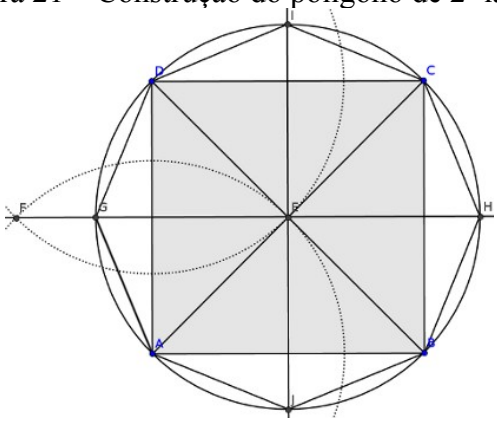
Considere um segmento BC dado. Construa a mediatriz de BC. Seja A o ponto de interseção entre o segmento BC e sua mediatriz, trace uma círculo de centro em A que passe por B e C. Sejam D e E os pontos de interseção da mediatriz de BC com a circunferência, trace os segmentos BD, BE, CD e CE.

Figura 20 – Quadrado inscrito.




## 4.3 Construção de polígono de $2^n$ lados

Figura 21 – Construção do polígono de $2^n$ lados.



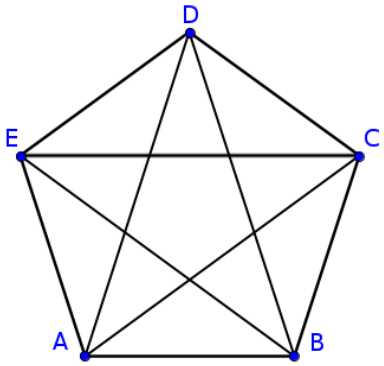

Descreveremos como proceder na construção de um polígono regular de $2^n$ lados, com $n \in \mathbb{N}$ e $n \geq 3$. Construa um quadrado ABCD e trace suas diagonais. Com o compasso centrado na intersecção das diagonais E, trace uma circunferência de raio igual a distância

entre E e os vértices do quadrado. Bissecte os ângulos AÊD, BÊC, CÊD e AÊB, e marque as intersecção das bissetrizes com a circunferência, respectivamente, G, H I e J. Trace os segmentos AJ, BJ, BH, CH, CI, DI, AG e DG. Obtemos assim um octágono. Aplicando a bissecção nos ângulos internos recursivamente podemos construir o polígono de $2^n$ lados desejado.

Perceba que se um determinado polígonos regular de m lados é construtível, obviamente m sendo um número natural, então pode-se construir um polígono regular de $m.2^n$ lados através da bissecção de seus ângulos internos. Por exemplo, construindo-se um triângulo equilátero, pode-se obter um hexágono e, através de uma nova bissecção, um dodecágono.

### 4.4 Pentágono e decágono regulares a partir da razão áurea

Figura 22 – pentágono regular e pentagrama.




Imagine que o pentágono regular ABCDE esteja construído. Trace suas diagonais. Sejam $x$ e $y$ as medidas do lado do pentágono e de sua diagonal, respectivamente. Nos concentrando no triângulo ABC, pela lei dos senos, temos que

$$\frac{x}{\operatorname{sen}\left(\frac{\pi}{5}\right)} = \frac{y}{\operatorname{sen}\left(\frac{3\pi}{5}\right)}. \qquad (1)$$

Através das fórmulas de adição de arcos, encontramos que para um determinado ângulo θ, que $\cos(2\theta) = 2\cos^2(\theta) - 1$. Usando este fato, encontramos que

$$\operatorname{sen}\left(\frac{3\pi}{5}\right)=\operatorname{sen}\left(\frac{\pi}{5}\right)\left(4\cos^2\left(\frac{\pi}{5}\right)-1\right) \quad (2)$$

Substituindo (2) em (1), chegamos a

$$\frac{y}{x}=4\cos^2\left(\frac{\pi}{5}\right)-1 \quad (3)$$

Usando os fatos de sen(2θ) = 2sen(θ)cos(θ) e $\operatorname{sen}\left(\frac{3\pi}{5}\right)=\operatorname{sen}\left(\frac{2\pi}{5}\right)$ e substituindo na expressão (1) encontramos que

$$\frac{y}{x}=2\cos\left(\frac{\pi}{5}\right) \quad (4)$$

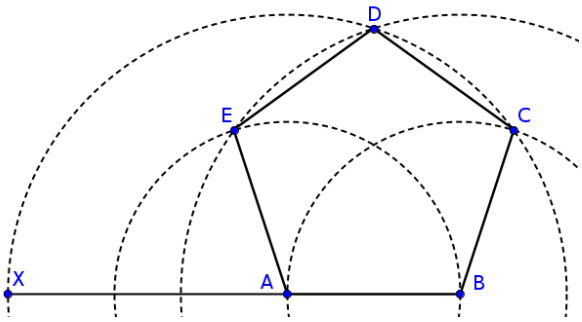
De (3) e (4) resulta a equação

$$4\cos^2\left(\frac{\pi}{5}\right)-2\cos\left(\frac{\pi}{5}\right)-1=0$$

Daí encontramos que $\cos\left(\frac{\pi}{5}\right)=\frac{1+\sqrt{5}}{4}$ e, de (4) $\frac{y}{x}=\Phi$.

Logo podemos construir o pentágono regular a partir do segmento áureo.

Figura 23 – construção do pentágono.




Seja XB um segmento e A o ponto que o divide na proporção áurea. Considere que $XA > AB$. Com o compasso centrado em A, construa a circunferência $C_1$ que passa por X. Conserve a abertura e construa uma nova circunferência $C_2$ de centro B. Marque o ponto D de intersecção entre estas circunferências. O triângulo ABD é um triângulo áureo. Com o compasso centrado em A, construa uma circunferência que passe por B e marque a intersecção E com $C_2$. Centrado em B, construa uma circunferência que passe por A e marque a intersecção C com $C_1$. Trace os segmentos AB, BC, CD, DE e AE.

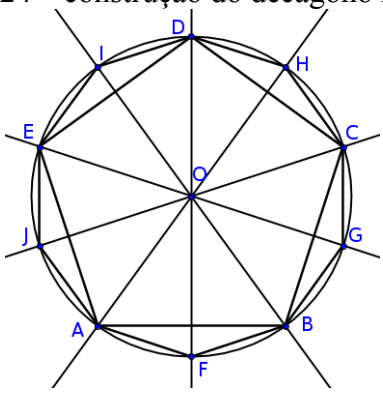
Facilmente se verifica que o polígono ABCDE é um pentágono regular.

O decágono pode ser obtido a partir do pentágono. Construa as mediatrizes dos lados do pentágono. Todas intersectam-se no mesmo ponto O. Construa a circunferência de centro em O e que passe pelos vértices do pentágono. As intersecções das mediatrizes com a

circunferência juntamente com os vértices do pentágono são vértices do decágono regular.

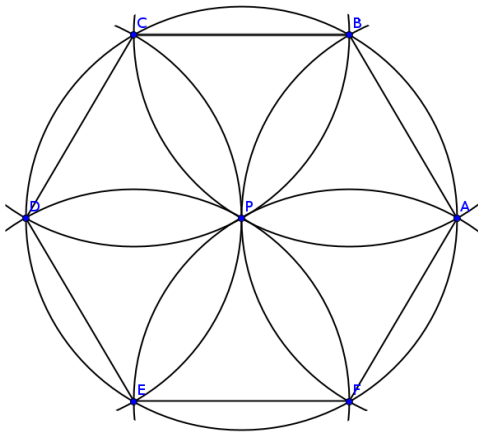
Na verdade, poderíamos ter construído antes o decágono a partir de um triângulo áureo. O pentágono pode ser obtido tomando-se vértices do decágono alternadamente.

Figura 24 – construção do decágono regular.




## 4.5 Hexágono inscrito em círculo de raio dado

Figura 25 – construção de um hexágono regular inscrito.

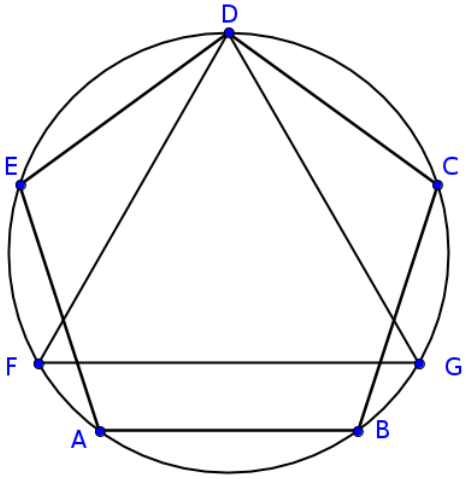



Dado uma circunferência $C_r$ de centro P e raio r, construa uma segunda circunferência de raio r e centro A, sendo A pertencente à primeira circunferência, e marque o ponto B de interseção entre ambas. Com centro em B, construa outra circunferência de raio r e marque a intersectando $C_r$ num ponto C. Aplicando o mesmo processo recursivamente, marque os pontos D, E e F. Trace os segmentos AB, BC, CD, DE, EF e AF.

## 4.6 Pentadecágono regular

Sejam ABCDE e DFG, respectivamente um pentágono e um triângulo regulares inscritos em uma mesma circunferência de raio r. Obviamente, o arco de extremos D e G representa um terço da circunferência, enquanto o arco de extremos D e B representa um quinto da mesma. Calculando a diferença, obtemos que o arco de extremos B e G representa uma décima quinta parte da circunferência, ou seja, o segmento BG tem a medida de um lado do pentadecágono regular inscrito na circunferência de raio r.

Figura 26 – construção do pentadecágono regular.

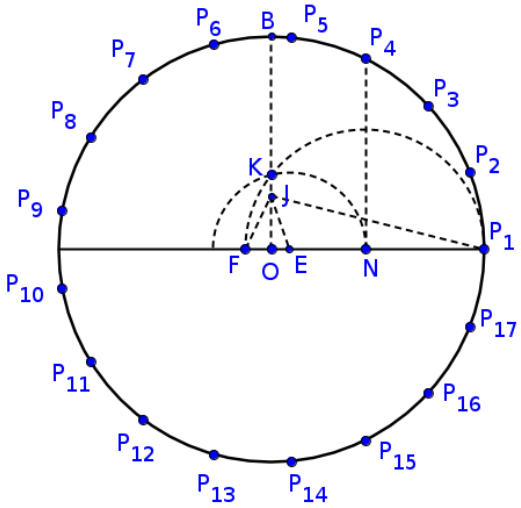



Com a abertura do compasso igual a distância entre B e G, marque os demais vértices do pentadecágono sobre a circunferência. Concluída a construção, podemos obter facilmente os polígonos regulares cujo número de lados é o produto de 15 por uma potência de 2.

## 4.7 Heptadecágono regular

Em 1796, aos 19 anos, o matemático alemão Gauss demonstrou algebricamente a possibilidade de construção do heptadecágono regular, embora não o tenha construído. A primeira construção foi realizada pelo matemático Johannes Erchinger. A construção a seguir é de H. W. Richmond, datada de 1893.

Figura 27 – construção do heptadecágono regular.



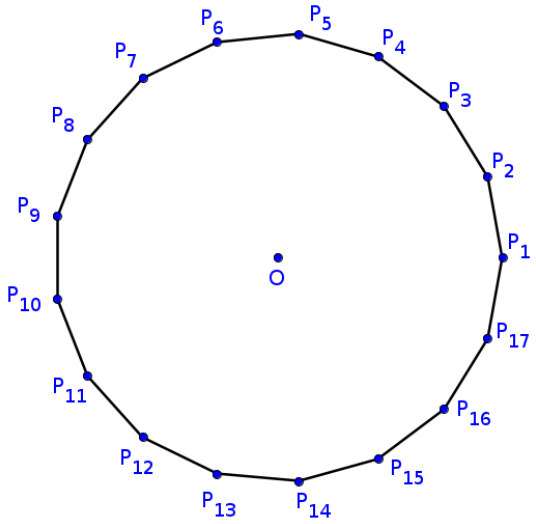

Construa uma circunferência de raio R e centro O e trace seu diâmetro (figura 23). Seja $P_1$ um dos pontos de intersecção do diâmetro com a circunferência, construa um segmento OB perpendicular a $OP_1$. Marque o ponto J sobre OB de tal forma que OJ seja $\frac{1}{4}$ da medida de OB, o que pode ser feito através da construção da mediatriz recursivamente. Trace o segmento $JP_1$. Encontre o ponto E pertencente a $OP_1$ tal que $O\hat{J}E$ meça $\frac{1}{4}$ da medida de $O\hat{J}P_1$. Encontre o ponto F sobre o diâmetro tal que $E\hat{J}F$ meça $\frac{\pi}{4}$ radianos ($E\hat{J}O$ deve ser interno a $E\hat{J}F$). Construa o semicírculo com diâmetro FP1, marcando seu ponto de intersecção K com o segmento OB. Construa o semicírculo com centro em E e raio igual a medida de EK, marcando o ponto de intersecção N deste com $OP_1$. Trace a perpendicular a $OP_1$ por N, marcando seu ponto de intersecção $P_4$ com a circunferência. $P_1$ e $P_4$ são vértices do heptadecágono. Com o compasso, meça a distância entre $P_1$ e $P_4$ e encontre sobre a circunferência os pontos $P_7$, $P_{10}$, $P_{13}$ e $P_{16}$. Conservando a abertura, encontre $P_2$, $P_5$, $P_8$, $P_{11}$, $P_{14}$ e $P_{17}$. Finalmente, com a abertura preservada e a partir de $P_{17}$, marque $P_3$, $P_6$, $P_9$, $P_{12}$, $P_{15}$ e $P_1$. Cada $P_i$, com i = 1, 2, 3, …, 17, é um vértice do heptadecágono.

Em seu livro, Disquisitiones Arithmeticae, Gauss prova que são construtíveis os polígonos regulares de n lados (n < 300), para os seguintes valores de n: 2, 3, 4, 5, 6, 8, 10, 12, 15, 16, 17, 20, 24, 30, 32, 34, 40, 48, 51, 60, 64, 68, 80, 85, 96, 102, 120, 128, 136, 160, 170, 192, 204, 240, 255, 256, 257, 272.

A partir das construções de polígonos regulares tratadas até aqui e fazendo uso das

construções elementares do capítulo 2, é possível construir, com exceção de n = 257, todos os polígonos para os demais valores de n. Por exemplo, para encontrar a medida do lado do polígono regular de 51 lados inscrito em uma circunferência de raio r, pode-se fazê-lo de modo análogo à construção do pentadecágono, usando um triângulo e um heptadecágono regulares inscritos.

Figura 28 – heptadecágono regular.



# 5 TRATAMENTO ALGÉBRICO PARA A CONSTRUTIBILIDADE

Discutiremos sobre um critério para determinar se um número é ou não construtível, o que veremos estar relacionado diretamente a construtibilidade de polígonos regulares. Para tanto, precisamos de algumas definições e resultados.

**Definição 5.1.** *Uma operação binária definida em um conjunto A é uma aplicação*

$$\begin{aligned} *: A \times A &\to A \\ (a, b) &\to a * b \end{aligned}$$

**Definição 5.2.** *Um anel (*A, +, ·*) é um conjunto* A *com as operações binárias + e · definidas, as quais chamaremos soma e produto, e que possui as seguintes propriedades para todo a, b, c* $\in$ A*:*

1. *(a + b) + c = a + (b + c) (associatividade da soma);*
2. $\exists 0 \in A$ *tal que a + 0 = 0 + a = a (existência de elemento neutro da soma);*
3. $\forall\, a \in A$ *existe um único* $x \in A$ *denotado por* $x = -a$*, tal que a + x = x + a = 0. (existência de inverso aditivo);*
4. *a + b = b + a (comutatividade da soma);*
5. *(a·b)·c = a·(b·c) (associatividade do produto);*
6. *a·(b + c) = a·b + a·c; (a + b)·c = a·c + b·c (distributividade à esquerda e à direita).*

**Definição 5.3.** *Um corpo (*A, +, ·*) é um anel que satisfaz as seguintes propriedades para todo a, b* $\in$ A*:*

1. $\exists 1 \in A, 0 \neq 1$*, tal que a·1 = 1·a = a (é um anel com unidade);*
2. *a·b = b·a (é um anel comutativo);*
3. *a·b = 0* $\Rightarrow$ *a = 0 ou b = 0 (anel sem divisores de zero);*
4. $\forall\, a \neq 0, \exists x \in A$ *denotado por* $a^{-1}$ *tal que a·x = x·a = 1.*

Um anel que satisfaz as três primeiras propriedades da definição 5.3 é um domínio de integridade.

Um subconjunto B $\subset$ A será chamado subcorpo de A se ainda é um corpo munido

das operações de A.

Chamamos de polinômio sobre o corpo A em uma variável (ou indeterminada) x à expressão $a(x)=\sum_{i=0}^{n} a_i x^i$, onde $a_i \in A, \forall\, i \in \mathbb{N}$. Analogamente, podemos entender a(x) como uplas $(a_0,a_1,a_2,a_3,...,a_n,...)$ tal que $\exists n \in \mathbb{N}$ tal que $a_j=0, \forall\, j \geq n$. O índice n é o grau do polinômio e denotaremos por $gr(a(x)) = n$. Se $a_n=1$, diremos que o polinômio é mônico. Se o grau do polinômio é zero, diremos que ele é constante.

Um polinômio será dito identicamente nulo se $a_i=0 \in A, \forall\, i \in \mathbb{N}$. Dois polinômios a(x) = $(a_0,a_1,a_2,a_3,...)$ e b(x) = $(b_0,b_1,b_2,b_3,...)$ serão iguais se, e somente se, $a_i=b_i$ em A para todo $i \in \mathbb{N}$. O grau do polinômio nulo é indefinido.

Da adição de $(a_0,a_1,a_2,a_3,...)$ e $(b_0,b_1,b_2,b_3,...)$ obtemos como resultado a soma $c(x)=(c_0,c_1,c_2,c_3,...)$ onde $c_i=a_i+b_i$.

A multiplicação entre os polinômios $(a_0,a_1,a_2,a_3,...)$ e $(b_0,b_1,b_2,b_3,...)$ resulta no produto $(c_0,c_1,c_2,c_3,...)$ tal que $c_k=a_0 b_k+a_1 b_{k-1}+\cdots+a_{k-1} b_1+a_k b_0$ para todo índice k. O grau de c(x) é o produto dos graus de a(x) e b(x).

Um elemento $\alpha \in A$ tal que $p(\alpha)=0$ é chamado raiz do polinômio p(x).

Denotaremos por A[x] o conjunto de todos os polinômios sobre o corpo A, em uma indeterminada x.

**Teorema 5.1 (Algoritmo da divisão).** *Sejam a(x), b(x)* $\in$ A[x] *e b(x)* $\neq$ *0, então existem únicos q(x), r(x)* $\in$ A[x] *tais que*

$$a(x)=b(x).q(x)+r(x)$$

*onde* r(x) = 0 *ou* $gr(r(x))<gr(b(x))$.

**Demonstração:** sejam os polinômios em A[x] $a(x)=a_0+a_1 x+\cdots+a_m x^m$ e $b(x)=b_0+b_1 x+\cdots+b_n x^n$ com $b_n \neq 0$. Vamos demostrar a existência.

Se $a(x)$ é nulo, basta tomar $q(x) = r(x) = 0$. Se $a(x)$ é não nulo e m < n, basta que $q(x) = 0$ e $r(x) = a(x)$. Vamos ao caso em que $a(x)$ é não nulo e m $\geq$ n.

Seja $f_1(x)$ o polinômio tal que

$$f(x) = a_m b_n^{-1} x^{m-n} b(x)+f_1(x)$$

Perceba que gr($f_1$) < gr(f). Usaremos indução sobre m.

Se m = 0, de m $\geq$ n obtemos que n = 0, de forma que $a(x)=a_0$ e $b(x)=b_0$, daí podemos escrever $f(x) = a_0 b_0^{-1} b(x)$, bastando tomar $q(x) = a_0 b_0^{-1}$ e $r(x) = 0$.

Reorganizando os termos, podemos escrever $f_1(x) = f(x)-a_m b_n^{-1} x^{m-n} b(x)$ com $gr(f_1)<gr(a)$. Pela hipótese de indução, existem $q_1(x)$ e $r_1(x)$ com $r_1(x)$ nulo ou $gr(r_1(x))<g(b(x))$ tais que

$$f_1(x) = b(x)q_1(x)+r_1(x).$$

Destas duas últimas igualdades, encontramos que

$$f(x) = b(x)\left(q_1(x)+a_n b_m^{-1} x^{m-n}\right)+r_1(x).$$

Assim, basta tomar $q(x) = (q_1(x)+a_n b_m^{-1} x^{m-n})$ e $r(x) = r_1(x)$.

Devemos ainda demonstrar a unicidade de $q(x)$ e $r(x)$. Sejam $q_1(x), q_2(x), r_1(x)$ e $r_2(x)$ com $r_j(x) = 0$ ou $gr(r_j(x))<gr(b(x))$ para j = 1, 2 tais que

$$f(x) = b(x)q_1(x)+r_1(x) = b(x)q_2(x)+r_2(x)$$

Então temos que $b(x)(q_1(x)-q_2(x)) = r_1-r_2(x)$. Se tivermos $q_1(x)\neq q_2(x)$, então o grau do polinômio do lado esquerdo da última igualdade será maior do que ou igual a $gr(b(x))$, enquanto que o grau do polinômio resultante do lado direito é menor que $gr(b(x))$, o que é absurdo. Então $q_1(x) = q_2(x)$ que implica em $r_1 = r_2(x)$.

□

Como consequência do algoritmo da divisão, $x-\alpha$ divide a(x) se, e somente se, $\alpha$ é raiz de a(x). De fato, se $\alpha$ é raiz, pelo algoritmo da divisão existe b(x) tal que $a(x)=b(x).(x-\alpha)+r(x)$ com $gr(r(x))<gr(x-\alpha)=1$. Assim, $r(x) = r$ e aplicando $\alpha$ temos que $0 = a(\alpha)=b(\alpha).(\alpha-\alpha)+r=r$, logo $x-\alpha$ divide a(x). Se $x-\alpha$ divide a(x), então $a(x)=b(x).(x-\alpha)$ e obviamente $a(\alpha) = 0$.

Diremos que d(x) é um mdc (máximo divisor comum) dos polinômios a(x) e b(x) se divide a ambos e tem grau máximo entre todos os divisores de a(x) e b(x). Denotaremos por d(x) = MDC(a(x), b(x)).

A expressão um mdc deve-se à possibilidade de existência de mais de um polinômio que atenda à definição. Por exemplo, sejam os polinômios $a(x)=10x^2-20x+10$ e

$b(x)=5x^2-5$, os polinômios $x-1$ e $5x-5$ podem ser vistos como MDC(a(x), b(x)).

**Teorema 5.2 (Bézout).** *Seja* A *um corpo e a(x), b(x)* $\in$ A[x]*, existem polinômios g(x), h(x)* $\in$ A[x] *tais que* $a(x)g(x)+b(x)h(x)=\text{MDC}(a(x),b(x))$.

**Demonstração:** sejam os conjuntos $S=\{a(x)m(x)+b(x)n(x);m(x),n(x)\in A[x]\}$ e $G=\{gr(p(x));\ p(x)\in S\}$. Claro que o conjunto G tem um menor elemento. Seja $d(x)\in S$ tal que $gr(d(x))$ é o menor elemento de G. Para mostrar que $d(x)$ é um mdc de $a(x)$ e $b(x)$, antes mostraremos que $d(x)$ é divisor comum de ambos.

Como $d(x)\in S$, então existem $g(x),h(x)\in A[x]$ tais que

$$d(x)=a(x)g(x)+b(x)h(x) \qquad (1)$$

Pelo algoritmo de Euclides, existem $q(x),r(x)\in A[x]$ com $gr(r(x))<gr(d(x))$ ou $r(x)$ nulo tais que

$$a(x)=d(x)q(x)+r(x)$$

Substituindo (1) nesta última igualdade e isolando $r(x)$obtemos que

$$r(x)=a(x)(1-g(x)q(x))-b(x)h(x)q(x)$$

Se $r(x)\in S$, então não deve ser nulo, mas o fato de $gr(r(x))<gr(d(x))$ contraria a minimalidade de $d(x)$. Portanto $r(x)$ é nulo e $d(x)$ divide $a(x)$. Analogamente se mostra que $d(x)$ divide $b(x)$.

Agora basta mostrar que qualquer divisor de $a(x)$ e $b(x)$ divide $d(x)$. Seja $d'(x)$ outro divisor comum de $a(x)$ e $b(x)$. Então $a(x)=d'(x)u(x)$ e $b(x)=d'(x)v(x)$ para certos $u(x)$ e $v(x)$ em A[x]. Substituindo em $d(x)=a(x)g(x)+b(x)h(x)$ encontramos

$$d(x)=d'(x)u(x)g(x)+d'(x)v(x)h(x)=d'(x)(u(x)g(x)+v(x)h(x))$$

Portanto, $d'(x)$ divide $d(x)$.

□

**Proposição 5.1.** *Sejam* A *um domínio de integridade e* a(x) $\in$ A[x]\{0}. *Se* a(x) *tem grau n, então* a(x) *tem no máximo n raízes em* A.

**Demonstração:** usaremos indução. Para n = 0, é óbvio: a(x) será um polinômio constante não-nulo, logo não possuirá raiz em A. Suponhamos, por hipótese de indução, que vale para um n qualquer. Considere a(x) um polinômio em A[x] com grau n + 1. Não haveria nada a provar se a(x) não tivesse raízes, o que nos leva a considerar o caso em que o polinômio tenha pelo menos uma raiz $\alpha$. Neste caso, podemos escrever $a(x)=b(x).(x-\alpha)$ com $gr(b(x))=n$, o que implica que toda raiz de b(x) é raiz de a(x). Por hipótese, b(x) tem no máximo n raízes, que juntamente a $\alpha$, resulta que a(x) tem no máximo n + 1 raízes.

□

Diremos que a(x) é irredutível em A[x] se não é constante e inexistem $b(x),c(x) \in A[x]$ tais que $gr(b(x)),\ gr(c(x)) < gr(a(x))$ e $a(x) = b(x).c(x)$.

**Proposição 5.2 (Gauss).** *Seja* $a(x) \in \mathbb{Z}[x]$ *um polinômio irredutível sobre* $\mathbb{Z}$*, então* a(x) *é também irredutível sobre* $\mathbb{Q}$.

**Demonstração:** antes um resultado auxiliar. Um polinômio $a(x) \in \mathbb{Z}[x]$ é dito primitivo se o mdc (máximo divisor comum) dos seus coeficientes é igual a 1. Mostraremos que se a(x) e b(x) são primitivos, então o produto a(x)b(x) é primitivo. Suponha, por absurdo, o contrário, o que significa que existe um número primo p que divide todos os coeficientes de a(x)b(x). Tomando os coeficientes de a(x)b(x) módulo p, temos que a(x)b(x) = 0 em $\mathbb{Z}_p[x]$. Daí, ainda em $\mathbb{Z}_p[x]$, a(x) = 0 ou b(x) = 0 ou seja, ou os coeficientes de a(x) são múltiplos de p ou o são os coeficientes de b(x), o que contraria a hipótese. Conclui-se então que o produto de polinômios primitivos é ainda primitivo.

Provaremos agora o resultado principal. Suponha que a(x) pode ser fatorado sobre $\mathbb{Q}$, com $a(x)=b(x).c(x)$. Sejam $m_1$ e $m_2$ o mmc (mínimo múltiplo comum) dos denominadores dos coeficientes de b(x) e c(x), respectivamente. Temos que $m_1 b(x)$ e $m_2 c(x)$ são primitivos. Então

$$m_1 m_2 a(x)=m_1 b(x).m_2 c(x)$$

Como o lado direito da última igualdade é primitivo, o lado esquerdo também o é, o que obriga a termos $m_1=\pm 1$ e $m_2=\pm 1$, ou seja, nossa fatoração inicial já era sobre $\mathbb{Z}$.

□

**Teorema 5.3 (Critério de Eisenstein).** *Seja* $a(x)=a_0+a_1x+\cdots+a_nx^n \in \mathbb{Z}[x]$ *um polinômio de grau n . Caso exista um número primo p tal que* $a_n \not\equiv 0 \pmod p$, $a_i \equiv 0 \pmod p$ *para* $0 \le i \le n-1$ *e* $a_0 \not\equiv 0 \pmod{p^2}$, *então a(x) é irredutível sobre* $\mathbb{Q}$.

**Demonstração:** pela proposição anterior, basta mostrar a irredutibilidade de a(x) sobre $\mathbb{Z}$. Suponha, por contradição, que $a(x)=b(x).c(x)$, com $b(x),c(x)\in\mathbb{Z}$ e $1 \le gr(g(x)), gr(h(x)) < gr(a(x)) = n$. Sejam ainda $b(x)=b_0+b_1x+\cdots+b_rx^r$, gr(b(x)) = r, $c(x)=c_0+c_1x+\cdots+c_sx^s$ e gr(c(x)) = s. Deste modo, n = r + s.

Temos $a_0=b_0.c_0$, o que implica que p divide $b_0$ ou p divide $c_0$, mas não a ambos, pois $p^2$ não divide $a_0$. Admitamos, sem perda de generalidade que p divide $b_0$, logo não divide $c_0$.

Como $a_n=b_r.c_s$ e p não divide $a_n$, então p não divide $b_r$. Seja $b_i$ o primeiro coeficiente de b(x) tal que p não divide $b_i$. Temos

$$a_i = b_0c_i + \cdots + b_{i-1}c_1 + b_ic_0$$

Como p divide $b_0, b_1, \cdots, b_{i-1}$ e não divide $b_ic_0$, então p não divide $a_i$. Logo, por hipótese, i = n > r, o que evidentemente é um absurdo.

□

Seja $n \ge 2$ inteiro, denotaremos por $\bar{a}$ a classe de equivalência de $a\in\mathbb{Z}$ na congruência módulo n. O conjunto quociente de $\mathbb{Z}$ pela congruência módulo n será representado por $\mathbb{Z}_n$. Assim,

$$\mathbb{Z}_n = \{\bar{0}, \bar{1}, ..., \overline{n-1}\}.$$

**Proposição 5.3.** *Seja p primo e* $a(x)=a_0+a_1x+\cdots+a_nx^n\in\mathbb{Z}[x]$. *Seja o polinômio* $\bar{a}(x)=\overline{a_0}+\overline{a_1}x+\cdots+\overline{a_n}x^n\in\mathbb{Z}_p[x]$. *Se* $p\nmid a_n$ *e* $\bar{a}(x)$ *é irredutível em* $\mathbb{Z}_p$, *então a(x) é irredutível em* $\mathbb{Q}$.

**Demonstração:** seja $a(x)=a_0+a_1x+\cdots+a_nx^n\in\mathbb{Z}[x]$ e p primo tal que $p\nmid a_n$. Suponha que $a(x)$ seja redutível em $\mathbb{Z}[x]$. Pela proposição 5.2, existem polinômios $b(x)=b_0+b_1x+\cdots+b_rx^r$ e $c(x)=c_0+c_1x+\cdots+c_sx^s$ com coeficientes em $\mathbb{Z}[x]$ tais que $1 \le gr(b(x)) = r < n$ e $1 \le gr(c(x)) = s < n$ e

$$a(x)=b(x)c(x)$$

Então também existem $\bar{b}(x)$ e $\bar{c}(x)$ tais que $\bar{a}(x)=\bar{b}(x)\bar{c}(x)$. Como p não divide $a_n=b_r c_s$, então p não divide $b_r$ e p não divide $c_s$. Logo $gr(\bar{b}(x)) = r$ e $gr(\bar{c}(x)) = s$, o que significa que $\bar{a}(x)$ é redutível. Isto demonstra.

□

## 5.1 Extensões de corpos

Sejam A e B dois corpos, diremos que B é um subcorpo de A ou que A é uma extensão de B se $B \subset A$ e as operações de adição e multiplicação de A restringem-se às correspondentes em B. Simbolizamos por A|B.

O fato de A ser um corpo nos garante que a adição em A é comutativa, associativa, tem elemento neutro e todo elemento possui simétrico. Juntamente a isto, para $\alpha, \beta \in A$, as seguintes propriedades fazem de A um B-espaço vetorial :

1. $(a+b)\alpha=a\alpha+b\alpha$
2. $a(\alpha+\beta)=a\alpha+a\beta$
3. $a(b\alpha)=(ab)\alpha$
4. $1\alpha=\alpha$

Definimos o grau da extensão A|B, denotado por $[A:B]$, como a dimensão do espaço vetorial A sobre B. Se existe $n \in \mathbb{N}$ tal que $n = [A:B]$, diremos que a extensão é finita; será infinita, caso contrário. Exceto se especificado, nos deteremos em extensões finitas.

Se $\alpha \in A$, diremos que $\alpha$ é algébrico sobre B se $\alpha$ é raiz de um polinômio b(x) não nulo em B[x]; caso não exista b(x) nestas condições tal que $b(\alpha) = 0$, então $\alpha$ será dito transcendente.

Por exemplo, consideremos a extensão $\mathbb{C}|\mathbb{R}$. Já que $\mathbb{C}=\{a+bi;\ a,b \in \mathbb{R}\}$, e {1,i} é uma base de $\mathbb{C}$, logo $[\mathbb{C}:\mathbb{R}]=2$. Além disso, $\pm i$ são raízes de $p(x)=x^2+1$ que é um polinômio (não nulo) em R(x), logo $\pm i$ são algébricos em $\mathbb{R}$.

Considerando A uma extensão de B e $S \subseteq A$. Denotamos por B(S) ao menor subcorpo contido em A tal que $B \cup S \subset A$. O subcorpo B(S) é claramente uma extensão de B

contida em A. Se $S=\{\alpha_1,\alpha_2,\alpha_3,\cdots,\alpha_n\}$ ou $S=\{\alpha\}$, representaremos por $B(\alpha_1,\alpha_2,\alpha_3,\cdots,\alpha_n)$ ou $B(\alpha)$. Considerando o último caso, $B(\alpha)$ é uma extensão simples de B, ou uma adjunção de $\alpha$ a B.

Seja A|B uma extensão, e $\alpha\in A$ algébrico sobre B, definimos o polinômio mínimo de $\alpha$ sobre B como o polinômio mônico de menor grau com coeficientes em B que tenha $\alpha$ como raiz.

**Proposição 5.4.** *Sejam A|B uma extensão,* $\alpha\in A$ *e b(x) um polinômio mônico com coeficientes em B, tal que* $b(\alpha) = 0$. *São equivalentes:*

(1) *b(x) é o polinômio mínimo de* $\alpha$;

(2) *se* $c(x)\in B[x]$ *é tal que* $c(\alpha) = 0$, *então b(x) divide c(x);*

*(3) b(x) é irredutível.*

**Demonstração:** mostraremos inicialmente que (1) implica (2).

Seja b(x) o polinômio mínimo de $\alpha$ sobre B. Considere $c(x)\in B[x]$ um polinômio tal que $c(\alpha) = 0$. Pela divisão euclidiana, existem $q(x), r(x) \in A[x]$ com $gr(r(x))<gr(b(x))$ ou $r(x)$ nulo tais que

$$c(x) = b(x)q(x)+r(x)$$

Avaliando em $\alpha$ temos

$$0 = c(\alpha) = b(\alpha)q(\alpha)+r(\alpha) = r(\alpha)$$

Logo $b(x)$ divide $c(x)$.

É evidente que (2) implica (3). Se m(x) e n(x) são polinômios com coeficientes em B e b(x) divide $m(x)n(x)$, então existe p(x) tal que b(x)p(x) = m(x)n(x). Avaliando em $\alpha$, temos que $0 = b(\alpha)p(\alpha) = m(\alpha)n(\alpha)\in A$. Logo $m(\alpha) = 0$ ou $n(\alpha) = 0$, o que significa que b(x) divide m(x) ou b(x) divide n(x).

O fato de (3) implica (1) decorre direto das definições de polinômio mínimo e polinômio irredutível.

□

**Proposição 5.5.** *Sejam a extensão* A|B *com* $\alpha\in A$ *algébrico sobre* B *e* n *o grau do polinômio mínimo de* $\alpha$ *sobre* B, *então* $[A:B] = n$ *e* $\{1,\alpha,\alpha^2,\ldots,\alpha^{n-1}\}$ *é uma base de* $B(\alpha)$ *sobre B.*

**Demonstração:** seja b(x) o polinômio mínimo de $B(\alpha)$. Seja ainda $\beta \in B(\alpha)$, então existem f(x), g(x) $\in B[x]$ tais que $\beta = \frac{f(\alpha)}{g(\alpha)}$ com $g(\alpha) \neq 0$. Por termos $g(\alpha)$ não nulo, b(x) não divide g(x), e por b(x) ser irredutível, $MDC(b(x), g(x)) = 1$. Daí existem, pelo Teorema de Bézout, r(x) e s(x) $\in B[x]$ tais que

$$1 = b(x)r(x) + g(x)s(x)$$

Aplicando $\alpha$ na última igualdade, obtemos que $\frac{1}{g(\alpha)} = s(\alpha)$ e $\beta = f(\alpha)s(\alpha)$.

Pelo teorema 5.5, existem q(x), r(x) $\in B[x]$ tais que f(x)s(x) = b(x)q(x) + r(x), com $0 \leq gr(r(x)) < gr(b(x)) = n$ ou r(x) nulo. Aplicando novamente $\alpha$ nesta última igualdade obtemos que $\beta = f(\alpha)s(\alpha) = r(\alpha)$.

Tomando $r(x) = r_0 + r_1 x + \cdots + r_{n-1} x^{n-1}$ um polinômio com coeficientes em B, temos $\beta = r(\alpha) = r_0 + r_1 \alpha + \cdots + r_{n-1} \alpha^{n-1}$. Então $\{1, \alpha, \alpha^2, \cdots, \alpha^{n-1}\}$ gera $B(\alpha)$. Mais do que isso, encontramos uma base para $B(\alpha)$, pois se existissem $t_0, t_1, \cdots, t_{n-1} \in B$ não todos nulos tais que $t_0 + t_1 \alpha + \cdots + t_{n-1} \alpha^{n-1} = 0$, existiria t(x) em B[x] com $\alpha$ como raiz, contradizendo a minimalidade de b(x).

□

**Teorema 5.4 (Teorema da torre).** *Sejam* $A \supseteq B \supseteq C$ *extensões sucessivas de um corpo* C. *Então* $[A:C] = [A:B] \cdot [B:C]$.

**Demonstração:** Seja v um vetor de A, escreva $v = \sum_j b_j v_j$, com $b_j \in B$ para cada j = 1, 2, $\cdots$, n. Expressando $b_j$ em termos da base de B sobre C, façamos $b_j = \sum_i a_{ij} u_i$, com $a_{ij} \in C$ para i = 1, 2, $\cdots$, m. Daí temos que

$v = \sum_j (\sum_i a_{ij} u_i) v_j = \sum_{i,j} a_{ij} u_i v_j$.

Os mn elementos $u_i v_j$ geram, portanto, o espaço vetorial A. Agora basta mostrar que estes elementos são linearmente independentes. Considerando $a_{ij} \in C$, temos que

$$0 = \sum_{i,j} a_{ij} u_i v_j \Leftrightarrow$$
$$0 = \sum_j (\sum_i a_{ij} u_i) v_j \Leftrightarrow$$

$$0 = \sum_i a_{ij} u_i, \text{ para } j = 1, 2, , m \Leftrightarrow$$
$$0 = a_{ij}, \text{ para } i = 1, 2, \cdots, m; \quad j = 1, 2, \cdots, n$$

□

## 5.2 Critério para não construtibilidade

Considere $\mathscr{P}$ como um subconjunto de $\mathbb{R}^2$ com pelo menos dois pontos distintos. É conveniente considerar que $\{0, U\} \subset \mathscr{P}$ onde 0 = (0, 0) e U = (1, 0).

Diremos que uma reta r de $\mathbb{R}^2$ é uma reta em $\mathscr{P}$ se contém dois pontos distintos de $\mathscr{P}$; uma circunferência c de $\mathbb{R}^2$ é uma circunferência em $\mathscr{P}$ se o centro e um ponto de c pertencem ao conjunto $\mathscr{P}$.

Um ponto qualquer em $\mathbb{R}^2$ será dito construtível se pode ser obtido a partir dos pontos de $\mathscr{P}$ com o uso das operações elementares mencionadas no capítulo 2. Denotaremos por $\mathscr{C}_{\mathbb{R}}$ ao conjunto de todos os pontos construtíveis a partir de $\mathscr{P}$.

**Teorema 5.5.** *$\mathscr{C}_{\mathbb{R}}$ é um subcorpo de $\mathbb{R}$, com $\mathbb{Q} \subset \mathscr{C}_{\mathbb{R}}$.*

Basta verificar que $\mathscr{C}_{\mathbb{R}}$ tem a estrutura necessária para ser um corpo. As construções do capítulo 3 são suficientes para mostrar que $\mathbb{Q} \subset \mathscr{C}_{\mathbb{R}}$.

Seja $\mathscr{P} = \mathscr{P}_0$, denotaremos por $\mathscr{P}_i$ ao conjunto formado pelos pontos de $\mathscr{P}_{i-1}$ e pelos pontos construtíveis a partir de $\mathscr{P}_{i-1}$, com i = 1, 2, ···, n, para $n \in \mathbb{N}$.

Por exemplo, considerando $\mathscr{P}_0 = \{0, U\}$ como descrito anteriormente, podemos determinar os pontos $P_1 = (-1, 0)$, $P_2 = (2, 0)$, $P_3 = (1/2, \sqrt{3}/2)$, $P_4 = (1/2, -\sqrt{3}/2)$ a partir de retas e circunferências em $\mathscr{P}_0$ fazendo uso das operações elementares. Assim, temos que $\mathscr{P}_1 = \{0, U, P_1, P_2, P_3, P_4\}$. Segue que

$$\mathscr{P}_0 \subset \mathscr{P}_1 \subset \mathscr{P} - 2 \subset \cdots \subset \mathscr{P}_n \subset \mathscr{P}_{n+1} \subset \cdots \subset \mathbb{R}^2.$$

Um ponto P será construtível se $P \in \mathscr{P}_n$ para algum $n \in \mathbb{N}$; uma reta ou circunferência será construtível se é uma reta ou circunferência em algum $\mathscr{P}_n$,

respectivamente.

É imediato que um ponto é construtível se, e somente se suas coordenadas são números construtíveis.

Seja $P = (x_n, y_n) \in \mathscr{P}_n$, chamaremos $x_n$ e $y_n$ de coordenadas de $\mathscr{P}_n$. O conjunto de todas as coordenadas de $\mathscr{P}_n$ será denotado por $\mathscr{A}_n$. É claro que $\mathscr{A}_n \subset \mathscr{C}_{\mathbb{R}} \; \forall \, n \in \mathbb{N}$.

Tomando $K_0 = \mathbb{Q}$, $K_1 = \mathbb{Q}(\mathscr{A}_1)$, ⋯, $K_n = \mathbb{Q}(\mathscr{A}_n)$, como consequência teremos

$$\mathbb{Q} = K_0 \subset K_1 \subset K_2 \subset \cdots \subset K_n \subset K_{n+1} \subset \cdots \subset \mathscr{C}_{\mathbb{R}}.$$

**Definição 5.4.** *Seja* A *um corpo, um plano de* A *é o conjunto de pares ordenados* $(a, b)$ *com* $a, b \in A$.

**Lema 5.1.** *Os números reais* $x_i$ e $y_i$, *coordenadas de* $\mathscr{P}_i$, *são raízes em* $K_i$ *de um polinômios de coeficientes em* $K_{i-1}$ *de grau 1 ou 2; em particular,* $[K_i : K_{i-1}] \in \{1, 2, 4\}$.

**Demonstração:** Considerando que $a_1, b_1, c_1, a_2, b_2, c_2 \in K_{i-1}$, o caso da intersecção de duas retas de $K_i$ equivale à solução do sistema de equações

$$\begin{aligned} a_1 x + b_1 y + c_1 &= 0 \\ a_2 x + b_2 y + c_2 &= 0 \end{aligned}$$

Como a resolução do sistema envolve apenas operações racionais, suas soluções também pertencem a $K_{i-1}$. Logo $[K_i : K_{i-1}] = 1$.

O caso da interseção de uma reta com uma circunferência, considerando $a_1, b_1, c_1, a_2, b_2, c_2 \in K_{i-1}$, reduz-se à solução do sistema

$$\begin{aligned} a_1 x + b_1 y + c_1 &= 0 \\ x^2 + y^2 + a_2 x + b_2 y + c_2 &= 0 \end{aligned}$$

Na impossibilidade de termos $a_1$ e $b_1$ simultaneamente nulos, podemos resolver a primeira equação em ordem a qualquer das variáveis. Sem perda de generalidade, resolvendo a equação em y teremos

$$y = -\frac{c_1}{a_1} - \frac{c_1}{a_1} x$$

Realizando a substituição na segunda equação, obtemos uma equação do segundo

grau em x com coeficientes em $K_{i-1}$. Resolvendo-a, encontraremos soluções do tipo $x_i = A \pm B\sqrt{\Delta}$ com $A, B, \Delta \in K_{i-1}$. Substituindo estas soluções na primeira equação, encontraremos soluções do tipo $A' \pm B'\sqrt{\Delta}$ com $A', B' \in K_{i-1}$. Assim $x_i$ e $y_i$ são raízes de polinômios de grau 2.

O caso da interseção de duas circunferências leva-nos ao sistema

$$x^2 + y^2 + a_1 x + b_1 y + c_1 = 0$$
$$x^2 + y^2 + a_2 x + b_2 y + c_2 = 0$$

Subtraindo-se uma das equações da outra, obtém-se uma equação linear com coeficientes em A. Com esta última equação juntamente a uma equação de uma das circunferências, reduz-se este ao segundo caso.

Em qualquer dos casos, temos $[K_{i-1}(x_i) : K_{i-1}], [K_{i-1}(y_i) : K_{i-1}] \in \{1, 2\}$. Também que

$$[K_{i-1}(x_i, y_i) : K_{i-1}(x_i)] \leq [K_{i-1}(y_i) : K_{i-1}].$$

Daí, $[K_{i-1}(x_i, y_i) : K_{i-1}(x_i)]$ também só pode assumir os valores 1 ou 2. Consequentemente,

$$[K_i : K_{i-1}] = [K_{i-1}(x_i, y_i) : K_{i-1}(x_i)][K_{i-1}(x_i) : K_{i-1}] \in \{1, 2, 4\}.$$

□

**Teorema 5.6.** *$\mathscr{C}_{\mathbb{R}}$ é uma extensão algébrica de $\mathbb{Q}$, tal que $\forall\, \alpha \in \mathscr{C}_{\mathbb{R}}$, $[\mathbb{Q}(\alpha) : \mathbb{Q}]$ é potência de 2.*

**Demonstração:** seja $\alpha \in \mathscr{C}_{\mathbb{R}} = \bigcup_{n=0}^{\infty} K_n$. Então $\exists\, n \in \mathbb{N}$ tal que $\alpha \in K_n = \mathbb{Q}(\mathscr{A}_n)$. Pelo teorema da torre, temos que $[\mathbb{Q}(\alpha) : \mathbb{Q}]$ divide $[K_n : \mathbb{Q}]$, bastando, pois, provar que para algum $s \in \mathbb{N}$, $[K_n : \mathbb{Q}] = 2^s$.

Usaremos indução sobre n. Para n = 0, $K_0 = \mathbb{Q}$ e segue da definição que $[K_0 : \mathbb{Q}] = 1$ corroborando a validade do teorema. O mesmo vale para n = 1, pois teremos $K_1 = \mathbb{Q}(\sqrt{3})$ que resulta em $[K_1 : \mathbb{Q}] = 2$.

Suponhamos que $[K_i : \mathbb{Q}]$ é potência de 2 $\forall\ 0 \leq i < n$. Provaremos que isto também ocorre com $[K_n : \mathbb{Q}]$.

Novamente pelo teorema 5.4, o fato de $K_{n-1}$ ser um subconjunto de $K_n$ aliado à $[K_n:\mathbb{Q}]$, será o bastante provar que $[K_n:K_{n-1}]$ é potência de 2, o que o lema anterior já nos garante.

□

O teorema 5.6 nos garante que se $\alpha$ é construtível, então $[\mathbb{Q}(\alpha):\mathbb{Q}]$ é potência de 2; se tivermos $[\mathbb{Q}(\alpha):\mathbb{Q}]$ como potência de 2, não temos a garantia de $\alpha$ ser construtível.

Um polígono será construtível se os seus vértices são pontos construtíveis de $\mathbb{R}^2$. Logo, um polígono regular de n lados é construtível se o ponto $A_n = \left(\cos\frac{2\pi}{n}, \text{sen}\frac{2\pi}{n}\right)$ é construtível. Isto sugere que a construção de polígonos regulares de n lados pode ser realizada no plano complexo, identificando os vértices $\left(\cos\frac{2\pi}{k}, \text{sen}\frac{2\pi}{k}\right)$ como $\cos\frac{2\pi}{k} + i\,\text{sen}\frac{2\pi}{k}$ para $k = 1, 2, \cdots, n$ e $i = \sqrt{-1}$.

O polinômio $x^n - 1$ tem n raízes complexas distintas que podem ser vistas como vértices de um polígono regular de n lados inscrito na circunferência de centro (0, 0) e raio 1. Temos que

$$x^n - 1 = (x-1)(x^{n-1} + x^{n-2} + \cdots + x + 1).$$

Como os pontos (0, 0) e (0, 1) são dados, interessa descobrir os pontos $z \in \mathbb{C}$ tais que $z^{n-1} + z^{n-2} + \cdots + z + 1 = 0$.

## 5.3 Critério para construtibilidade de polígonos regulares

**Proposição 5.6.** *Se* $p \geq 3$ *é um número primo, e um polígono de p lados é construtível, então* $p = 2^{2^s} + 1$ *para algum* $s \in \mathbb{N}$.

**Demonstração:** como, por hipótese, o polígono regular de p lados é construtível, então é construtível o ponto $\left(\cos\frac{2\pi}{p}, \text{sen}\frac{2\pi}{p}\right)$. Pelo teorema 5.6, temos para algum m natural

$[\mathbb{Q}(\alpha,\beta):\mathbb{Q}] = 2^m$, com $\alpha = \cos\frac{2\pi}{p}$ e $\beta = \operatorname{sen}\frac{2\pi}{p}$.

Seja $i = \sqrt{-1}$, a extensão $\mathbb{Q}(\alpha,\beta,i)\subset\mathbb{C}$ tem $[\mathbb{Q}(\alpha,\beta,i):\mathbb{Q}] = 2^{m+1}$.

Considere $\zeta = \cos\frac{2\pi}{p} + i\operatorname{sen}\frac{2\pi}{p} = \alpha + i\beta \in \mathbb{Q}(\alpha,\beta,i)$ uma raiz p-ésima da unidade. Como $\mathbb{Q}(\zeta)\subset\mathbb{Q}(\alpha,\beta,i)$, então $[\mathbb{Q}(\zeta):\mathbb{Q}] = 2^r$ para algum r natural.

O polinômio mínimo de $\zeta$ sobre $\mathbb{Q}$ é $x^{p-1}+x^{p-2}+\cdots+x+1$, e pela proposição 5.4, $p-1 = [\mathbb{Q}(\zeta):\mathbb{Q}] = 2^r$. Assim temos $p = 2^r+1$.

Falta mostrar que $r = 2^s$. Suponha, por absurdo, que r tenha um fator ímpar $t>1$, de modo que $r = vt$. Daí temos

$$p = (2^v)^t+1 = (2^v+1)((2^v)^{t-1}-(2^v)^{t-2}+(2^v)^{t-3}- \cdots \pm 1).$$

Absurdo, pois p é primo.

□

**Proposição 5.7.** *Seja $n = n_1 n_2$, com $n_1, n_2 \in \mathbb{N}$ primos entre si e maiores que 2. O polígono regular de n lados é construtível se, e somente se são construtíveis os polígonos regulares de $n_1$ e $n_2$ lados.*

**Demonstração:** sejam $n_1$ e $n_2$ divisores de $n$. Se o polígono regular de n lados é construtível, basta traçar convenientemente $n_1$ diagonais tomando os vértices $n_2$ a $n_2$ para obter um polígono regular de $n_1$ lados; de modo análogo se obtém um polígono regular de $n_2$ lados.

Se os polígonos regulares de $n_1$ e $n_2$ lados são construtíveis, pelo fato de $n_1$ e $n_2$ serem primos entre si, temos que existem números inteiros $a$ e $b$ tais que $a n_1 + b n_2 = 1$. Portanto

$$\frac{a}{n_2} + \frac{b}{n_1} = \frac{1}{n_1 n_2} = \frac{1}{n}$$

A partir dos ângulos $\frac{2\pi}{n_1}$ e $\frac{2\pi}{n_2}$ podemos construir $\frac{2\pi}{n_1 n_2}$ e daí obter o polígono de n lados.

□

**Lema 5.2.** *Se p é primo e* $\zeta$ *é uma* $p^n$*-ésima raiz primitiva da unidade em* $\mathbb{C}$*, então o polinômio mínimo de* $\zeta$ *sobre* $\mathbb{Q}$ *é*

$$a(x)=1+x^p+x^{2p}+\ldots+x^{p^n-p}$$

**Demonstração:** perceba que $a(x)=\frac{x^{p^n}-1}{x^p-1}$. Temos que $\zeta^{p^n}-1=0$ e $\zeta^p-1\neq 0$. Logo $a(\zeta)=0$. Agora é suficiente mostrar que $a(x)$ é irredutível sobre $\mathbb{Q}$.

Observando que $a(x)=b(x)c(x)$ se, e somente se $a(x+1)=b(x+1)c(x+1)$ para $b(x),c(x)\in\mathbb{Q}[x]$, é suficiente, por sua vez, concluir a irredutibilidade de $a(x+1)$ sobre $\mathbb{Q}$. Escrevamos

$$a(x+1)=\frac{(x+1)^{p^n}-1}{(x+1)^p-1}$$

Considerando $a(x+1)$ módulo p, do desenvolvimento binomial das potências resulta que

$$\bar{a}(x+1)=x^{p^n-p}$$

Como o polinômio $\bar{a}(x+1)$ é irredutível módulo p, a(x) é irredutível em $\mathbb{Q}$.

□

Em 1796, Gauss descobriu uma construção de um polígono regular de 17 lados, e uma condição suficiente para a construtibilidade do polígono regular de n lados, afirmando que o critério era também necessário, porém a demonstração só foi publicada em um artigo de Wantzel em 1837.

**Teorema 5.7 (Gauss-Wantzel).** *O polígono regular de* n *lados é construtível se, e somente se* $n = 2^r p_1 p_2 \ldots p_k$ *para* $p_i=2^{2^s}+1$ *com r, s* $\in \mathbb{N}$ *e* $1\leq i\leq k$.

**Demonstração:** pelas proposições 5.6 e 5.7, se $n = 2^r p_1 p_2 \ldots p_k$ para $p_i=2^{2^s}+1$ com r, s $\in \mathbb{N}$ e $1\leq i\leq k$, então o polígono regular de n lados é construtível, pois sabemos serem construtíveis também polígonos regulares de $2^r$ lados com $r\in\mathbb{N}$.

Por outro lado, considere construtível um polinômio regular de n lados. Sejam $p_1, p_2, \cdots, p_k$ fatores primos ímpares, teremos para determinados $r, \alpha_1, \alpha_2, \cdots, \alpha_k \in \mathbb{N}$.

$$n = 2^r p_1^{\alpha_1} p_2^{\alpha_2} \ \ldots \ p_k^{\alpha_k}.$$

Pela proposição 5.7, o polígono regular de $p_i^{\alpha_i}$ lados é construtível para todo $1 \leq i \leq k$. Suponha por absurdo que $\alpha_i \geq 2$. O grau do polinômio mínimo da $p_i^{\alpha_i}$-ésima raiz primitiva da unidade sobre $\mathbb{Q}$ é uma potência de 2. Pelo lema 5.2, o grau deste polinômio é $p^{\alpha_i} - p = p(p^{\alpha_i - 1} - p)$ que não pode ser potência de 2, pois p é ímpar. Então $\alpha_i = 1$ e o polígono de $p_i$ lados é construtível. Como $p_i$ é primo, pela proposição 5.6, $p_i = 2^{2^s} + 1$ para algum $s \in \mathbb{N}$.

□

## 5.4 Aplicação na solução de problemas clássicos gregos

A matemática grega deve muito do seu desenvolvimento às construções realizadas apenas com a régua não graduada e compasso, mas alguns problemas resistiram às tentativas de resolução utilizando apenas estes recursos, de forma que grandes descobertas foram realizadas na busca de suas soluções. São eles:

1. *A trissecção do ângulo;*
2. *A duplicação do cubo;*
3. *A quadratura do círculo.*

De fato, é impossível realizar tais feitos, como veremos.

Alguns ângulos podem ser trissectados com o uso de régua não graduada e compasso, por exemplo o ângulo reto, mas em geral a trissecção de um ângulo qualquer torna-se impossível.

Resolveremos para o caso da trissecção do ângulo $\pi/3$ radianos. Usando as fórmulas de adição de arcos, encontramos que para um dado ângulo $\theta$, $\cos(3\theta) = 4\cos^3(\theta) - 3\cos(\theta)$. Em particular, considerando $3\theta = \pi/3$ cujo valor do cosseno é conhecido, obtemos que $8\cos^3(\theta) - 6\cos(\theta) - 1 = 0$, o que significa que $\cos(\theta)$ é raiz do polinômio $a(x) = 8\cos^3(\theta) - 6\cos(\theta) - 1$ irredutível sobre $\mathbb{Q}$, ou seja, não é construtível.

De outro modo, trissectar o ângulo de $\pi/3$ radianos equivale à construção do

eneágono, o que o teorema 5.7 garante que não pode ser realizado.

A duplicação do cubo consiste em construir um cubo cujo volume seja o dobro do volume de um dado cubo, o que equivale a construção do número $\sqrt[3]{2}$. O polinômio mínimo sobre $\mathbb{Q}$ associado é $x^3 - 2$, daí $[\mathbb{Q}(\sqrt[3]{2}):\mathbb{Q}] = 3$ e, pelo teorema 5.6, não é construtível.

A quadratura do círculo consiste em construir um quadrado com a mesma área de um dado círculo. Seja r o raio do círculo, o lado de um quadrado de mesma área é dada por $r\sqrt{\pi}$. Ocorre que $\pi$ é transcendente, o que foi demonstrado por Lindemann em 1882, portanto tal construção é impossível.

# 6 CONCLUSÃO

As construções geométricas com régua não graduada e compasso foram a fonte de importantes resultados da matemática grega e posterior, rendendo descobertas que expandiram não apenas a geometria, mas também a álgebra. A fascinante relação entre a álgebra e a geometria corrobora a tese de que a matemática é uma construção contínua, posto que é fruto de investigações que atravessaram séculos. Tais avanços permitiram a compreensão de uma estruturação da própria matemática.

Em contrapartida, as dificuldades apresentadas pelos alunos do ensino básico no nosso país, em especial das escolas públicas, demonstram uma construção deficiente do conceito de número e de seus principais conjuntos, perpetuando uma visão mecanicista da matemática como um conjunto de regras e fórmulas a serem memorizadas sem um entendimento claro do que se está fazendo.

Considerando isso, as construções geométricas aliadas à álgebra permitem ao aluno do nível básico adquirir uma visão mais ampla da matemática como uma ciência solidamente estruturada. Para isso, é necessário criar atividades que permitam a exploração e por vezes descobertas por conta própria.

Vários componentes curriculares do ensino básico podem ser explorados com o uso dos métodos de construções, entre os quais estão a geometria euclidiana plana, geometria analítica, conjuntos numéricos (como facilitador na compreensão da existência dos números irracionais, por exemplo), construção de gráficos, entre outros.

Como o ensino não é como uma ciência exata, cabe ao professor ponderar o que é apropriado para aquele nível escolar, incentivando a abstração e a construção dos conceitos necessários a uma compreensão adequada dos assuntos abordados.

## REFERÊNCIAS


GONÇALVES, Adilson. *Introdução à álgebra*. 5. ed. Rio de Janeiro: Impa, 2008.

PICADO, Jorge. *Apontamentos de álgebra ii*. , 2006. Disponível em: <http://www.mat.uc.pt/~picado/algebraII/apontamentos/sebenta.pdf>. Acesso em: 19 mar. 2014.

STEWART, Ian. *Galois Theory*, 3. ed. Boca Haton, Chapman & Hall/CRC Press, 2004.

WAGNER, E.,*Construções Geométricas*. Rio de Janeiro: SBM, 2007. (Coleção do Professor de Matemática)

WAGNER, E. . O símbolo da RPM. *Revista do Professor de Matemática*, v. 20, p. 11-14, 1992.