Cyndi Menezes Pimentel

POLÍGONOS CONSTRUTÍVEIS

Ouro Preto - MG, Brasil

24 de abril de 2021

Cyndi Menezes Pimentel

POLÍGONOS CONSTRUTÍVEIS

Monografia apresentada ao Departamento de Matemática da Universidade Federal de Ouro Preto como parte das exigências para obtenção do título de Licenciado em Matemática.

Universidade Federal de Ouro Preto (UFOP)

Instituto de Ciências Exatas e Biológicas (ICEB)

Departamento de Matemática (DEMAT)

Orientador: Sebastião Martins Xavier

Coorientador: Thiago Fontes Santos

Ouro Preto - MG, Brasil

24 de abril de 2021

SISBIN - SISTEMA DE BIBLIOTECAS E INFORMAÇÃO

P644p Pimentel, Cyndi Menezes.
Polígonos construtíveis. [manuscrito] / Cyndi Menezes Pimentel. - 2021.
79 f.

Orientador: Prof. Dr. Sebastião Martins Xavier.
Coorientador: Prof. Dr. Thiago Fontes Santos.
Monografia (Licenciatura). Universidade Federal de Ouro Preto. Instituto de Ciências Exatas e Biológicas. Graduação em Matemática .

1. Geometria. 2. Polígonos regulares. 3. Construções geométricas. 4. Desenho geométrico. I. Santos, Thiago Fontes. II. Xavier, Sebastião Martins. III. Universidade Federal de Ouro Preto. IV. Título.

CDU 514.11

Bibliotecário(a) Responsável: Sione Galvão Rodrigues - CRB6 / 2526

MINISTÉRIO DA EDUCAÇÃO
UNIVERSIDADE FEDERAL DE OURO PRETO
REITORIA
INSTITUTO DE CIENCIAS EXATAS E BIOLOGICAS
COLEGIADO DO CURSO DE LICENCIATURA EM MATEMATICA

FOLHA DE APROVAÇÃO

Cyndi Menezes Pimentel

Polígonos construtíveis

Monografia apresentada ao Curso de Licenciatura em Matemática da Universidade Federal de Ouro Preto como requisito parcial para obtenção do título de Licenciada em Matemática

Aprovada em 14 de abril de 2021

Membros da banca

Dr. Sebastião Martins Xavier - Orientador - Universidade Federal de Ouro Preto
Dr. Edney Augusto Jesus de Oliveira - Universidade Federal de Ouro Preto
Dr. Wanderson Costa e Silva - Universidade Federal de Ouro Preto

Sebastião Martins Xavier, orientador do trabalho, aprovou a versão final e autorizou seu depósito na Biblioteca Digital de Trabalhos de Conclusão de Curso da UFOP em 24/05/2021

Documento assinado eletronicamente por **Sebastiao Martins Xavier**, **PROFESSOR DE MAGISTERIO SUPERIOR**, em 27/05/2021, às 12:29, 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 http://sei.ufop.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0 , informando o código verificador **0174362** e o código CRC **16320C02**.

R. Diogo de Vasconcelos, 122, - Bairro Pilar Ouro Preto/MG, CEP 35400-000
Telefone: (31)3559-1700 - www.ufop.br

Agradecimentos

Agradeço primeiramente a Deus, por trilhar meu caminho sempre com muitas oportunidades.

Aos meus pais Whariston de Paula Pimentel e Érika de Deus Menezes Pimentel, por sempre acreditarem e me darem total apoio em todos meus propósitos, sem vocês nada disso seria possível.

Ao meu irmão Caio Menezes Pimentel por sempre estar do meu lado em todos os momentos que precisei.

Ao meu namorado Jackson por sempre me trazer a tranquilidade nos momentos mais difíceis e por constantemente estar do meu lado vibrando pelas minhas conquistas.

Aos meus amigos Allan Apolinário e Joyce Pedro pelo companheirismo e por sempre me incentivarem a ir mais longe.

Ao meu orientador Sebastião Martins Xavier por toda paciência e dedicação comigo.

Aos meus demais familiares, amigos e professores que de alguma forma contribuíram para o meu desenvolvimento durante o curso.

As leis da natureza não são nada mais que os pensamentos matemáticos de Deus."
Euclides (300 A.C.);

Resumo

Quais polígonos regulares são construtíveis? Este problema foi solucionado pelo matemático Carl Friederich Gauss, ao apresentar um critério geral de construtibilidade dos polígonos regulares. Neste trabalho vamos apresentar uma sequência de resultados que irá nos proporcionar um bom entendimento sobre o estudo que está por trás deste problema cujo o enunciado é tão simples. Sendo assim, este trabalho se inicia com uma introdução, na qual é apresentado uma abordagem histórica, a motivação e o objetivo que se pretende alcançar ao fim deste trabalho. No segundo capítulo são apresentados alguns conceitos básicos de construções geométricas. No terceiro capítulo apresentamos uma ampliação dos conceitos de construções geométricas para os números construtíveis. Em seguida, no quarto e quinto capítulo iniciamos o estudo sobre polinômios e extensões de corpos, em que apresentamos alguns resultados que serão essenciais para o entendimento dos principais resultados deste trabalho. Por fim, no sexto e último capítulo, apresentamos resultados que respondem a pergunta em questão: Quais polígonos regulares são construtíveis?

Palavras-chave: Construções Geométricas; Régua e compasso; Polígonos construtíveis.

Abstract

Which regular polygons are constructible? This problem was solved by the mathematician Carl Friederich Gauss, when he presented a general criterion for the constructibility of regular polygons. In this paper we will present a sequence of results that will provide a good understanding of the study behind this problem whose statement is so simple. Therefore, this paper begins with an introduction, which presents a historical approach, the motivation and the objective that is intended to achieve at the end of this work. In the second chapter some basic concepts of geometric constructions are presented. In the third chapter we present an enlargement of the concepts of geometric constructions to constructible numbers. Then, in the fourth and fifth chapter we begin the study of polynomials and corps extensions, in which we present some results that will be essential for the understanding of the main results of this paper. Finally, in the sixth and last chapter, we present results that answer the question at hand: Which regular polygons are constructible?

Keywords: Geometric Constructions; Ruler and Compass; Constructables Polygons.

Lista de ilustrações

Sumário

1 Introdução

Os problemas de construção geométrica sempre foram assuntos de grandes interesses da geometria, estes desafiam o raciocínio e exigem um bom conhecimento dos teoremas de geometria. Na Grécia antiga, berço das origens da geometria como ciência dedutiva, os matemáticos davam soluções para problemas algébricos, transformando-os em problemas geométricos cujas soluções eram construtivas. Os Gregos eram muitos habilidosos em dar solução a esses tipos de problemas. No entanto, apesar de todo conhecimento e habilidade, haviam problemas geométricos que desafiaram, por séculos, os grandes matemáticos. Problemas estes como a duplicação do cubo, a quadratura do círculo, a trissecção do ângulo e, não menos importante, a construção de polígonos regulares.

Dando destaque ao problema da construção de polígonos regulares, podemos mencionar um grande estudioso que obteve importantes descobertas na matemática, na qual uma delas é o estudo sobre a solubilidade deste problema. Carl Friedrich Gauss $(1777-1855)$, matemático, astrônomo e físico alemão, manifestou aptidão pela matemática desde cedo. Há um relato do início da trajetória escolar de Gauss, em que um de seus professores pediu que os alunos somassem todos os números de 1 a 100, em pouco tempo Gauss apresentou a resposta correta. Certamente, o matemático obteve a soma da progressão aritmética $1+2+3+4+...+99+100$ através da fórmula $\frac{n(n+1)}{2}$. Pouco antes de completar 19 anos, Gauss realizou uma descoberta brilhante sobre a construção de polígonos regulares. Até este momento se sabia construir, com régua e compasso, o triângulo equilátero, o quadrado, o pentágono e os demais polígonos com número de lados múltiplo de 3, 4 e 5, mas nenhum outro polígono com número de lados primo. No entanto, Gauss mostrou que um polígono regular de n lados, é construtível se e somente se, n for da forma $n = 2^b \cdot p_1 \cdot p_2 \cdot p_3 \cdot ... \cdot p_r$, na qual cada p_i é um primo de Fermat.

Portanto, neste trabalho apresentaremos uma sequência lógica que têm como objetivo classificar os polígonos regulares que são construtíveis por meio da régua não graduada e o compasso. Através desta sequência lógica é possível observar que há uma ponte que associa as teorias da álgebra abstrata com a geometria, tornando assim mais palpável alguns resultados que são estudados na área da álgebra. Nosso trabalho expõe resultados e conceitos do mais básico ao mais complexo, que encadeados proporcionará ao leitor um satisfatório entendimento sobre o tema proposto.

2 Construções Geométricas Básicas

Problemas de construções geométricas são estudados desde a Grécia antiga e ainda hoje causa grande fascínio, não somente aos matemáticos como também a diversos estudiosos do assunto. Neste capítulo iremos expor e realizar o passo a passo de algumas construções geométricas básicas, utilizando régua (não graduada) e compasso. O objetivo principal é introduzir o conceito de construções geométricas de um modo geral, com o intuito de facilitar a compreensão dos conceitos que aparecerão a posteriori.

2.1 Retas Paralelas

Duas ou mais retas se dizem paralelas quando estão contidas no mesmo plano e se a interseção entre elas é o conjunto vazio, isto é, elas não possuem um ponto em comum.

Teorema 1 (Construção de retas paralelas)**.** *Dados uma reta r e um ponto P exterior a essa reta r, construir, passando por P uma reta s paralela à reta r .*

A seguir os passos para essa construção:

- Fixando a ponta seca do compasso em P, traçamos uma circunferência com o centro em P e com raio suficientemente grande, de forma que haja a interseção desta circunferência com a reta r, determinando assim dois pontos sobre r. Escolhemos um destes pontos e o denominamos por A. A circunferência formada, denominamos por α.

- Com a ponta seca do compasso em A traçamos outra circunferência (de mesmo raio que a circunferência α). Observe que esta circunferência determina na reta r outros dois pontos, escolhemos um e o denominamos por B. A nova circunferência denominamos por β.

- Novamente, com a ponta seca do compasso em B, traçamos outra circunferência (de mesmo raio que as circunferências α e β), esta nova circunferência denominamos por λ. O ponto de interseção da circunferência α e λ, que se encontra fora da reta r, denominamos por Q.

- Traçamos a reta passando pelos pontos P e Q assim, esta é paralela à reta r.

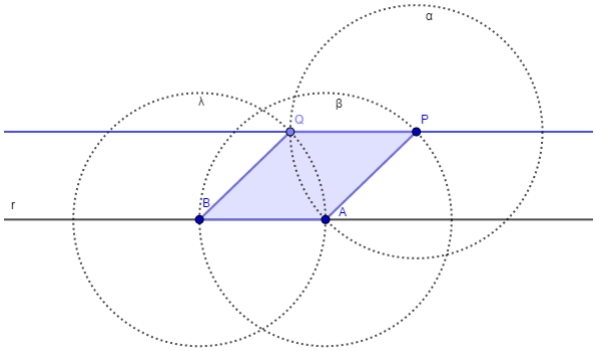

Figura 1 – Retas Paralelas

Fonte: Compilado pelo autor

Demonstração. Considere o quadrilátero $PABQ$. Por construção temos que os segmentos de reta AB, BQ, QP e PA são congruentes e, $PABQ$ possui dois ângulos agudos e dois ângulos obtusos. Logo, $PABQ$ é um losango. Sabemos que o losango é classificado como um paralelogramo, isto é, seus lados são paralelos. Como desejávamos. □

2.2 Retas Perpendiculares

Duas retas são perpendiculares quando ao se interceptarem em um ponto formam um ângulo de 90 graus.

Dados uma reta r e um ponto P exterior à essa reta, construir uma reta s perpendicular à reta r, passando pelo ponto P.
A seguir exibiremos os passos para essa construção:

- Com a ponta seca do compasso em P traçamos uma circunferência de centro P determinando dois pontos na reta r, denominamos estes pontos por A e B respectivamente.
- Sem perda de generalidade, com o centro em A traçamos uma circunferência passando pelo ponto B.
- E, com o centro em B traçamos outra circunferência de mesmo raio que a circunferência anterior, isto é, uma circunferência passando pelo ponto A.
- Observe que a interseção entre as duas últimas circunferências traçadas determinou dois pontos. Sem perda de generalidade, escolhemos o ponto que se encontra no semi-plano oposto ao semi-plano que contém o ponto P, este ponto de interseção denominamos por Q.
- A reta que passa pelos pontos P e Q é a reta perpendicular a reta r.

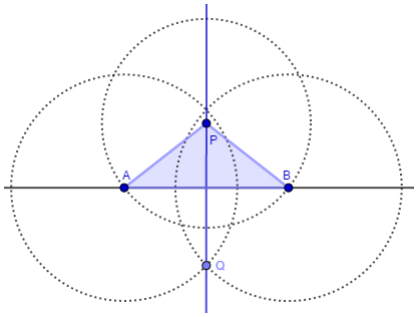

Figura 2 – Retas Perpendiculares

Fonte: Compilado pelo autor

Demonstração. Temos que os triângulos PAQ e PBQ são congruentes, pelo caso LLL, pois $PA = PB$, $QA = QB$ e PQ é lado comum aos dois triângulos. Dessa forma, os ângulos $A\hat{P}Q$ e $Q\hat{P}B$ são iguais. Por outro lado podemos observar que por construção, o triângulo APB é isósceles e como dito anteriormente $A\hat{P}Q = Q\hat{P}B$, isto é, a reta que passa por PQ é a bissetriz do ângulo $A\hat{P}B$. Por propriedades do triângulo isósceles, temos que a bissetriz, a mediatriz e a altura são iguais. Logo, PQ é a altura do triângulo APB, isto é, PQ é perpendicular a reta r. Como desejávamos. □

2.3 Mediatriz

A mediatriz de um segmento é a reta que intercepta perpendicularmente no ponto médio do segmento dado.

Dado AB um segmento de reta qualquer, construiremos sua mediatriz.
Construção:

- Com a ponta seca do compasso em A traçamos uma circunferência de raio maior que $\frac{AB}{2}$ e menor que AB.
- Novamente com o centro em B traçamos outra circunferência com raio de mesma medida que a circunferência anterior.
- A interseção destas duas circunferências determina dois pontos, estes denominamos por P e Q.
- Temos que a reta que passa pelos pontos P e Q, é a mediatriz do segmento AB.

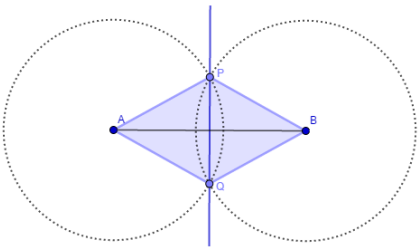

Figura 3 – Mediatriz de um segmento

Fonte: Compilado pelo autor

Demonstração. Observe que temos o quadrilátero $APBQ$ com dois ângulos obtusos e dois ângulos agudos e ainda, temos que $AP = PB = BQ = QA$, isto é, $APBQ$ é um losango. O losango é classificado como um paralelogramo. Portanto, pelas propriedades de paralelogramo temos que, suas diagonais são perpendiculares e se cruzam em seus pontos médios. Como desejávamos. □

2.4 Bissetriz

Dado um ângulo qualquer, a bissetriz desse ângulo é uma semi-reta que tem origem em seu vértice e que o divide em dois ângulos menores de mesma medida.

Dado $A\hat{O}B$ um ângulo arbitrário, construiremos sua bissetriz.
Construção:

- Traçamos uma circunferência de centro O determinando dois pontos nos lados do ângulo $A\hat{O}B$. Estes pontos denominamos por P e Q.
- Em seguida, traçamos duas circunferências de mesmo raio, uma com o centro em P e outra com o centro em Q. Traçamos estas circunferências de maneira que ambas determinem dois pontos ao se interceptarem.
- Um dos pontos determinados pela interseção anterior denominamos por C.
- Por fim, traçamos a semi-reta que tem origem no ponto O e que passa pelo ponto C assim, temos que OC é a bissetriz do ângulo $A\hat{O}C$.

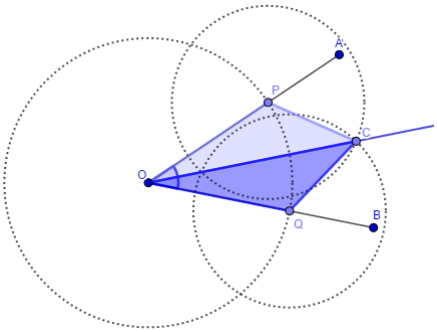

Figura 4 – Bissetriz de um ângulo

Fonte: Compilado pelo autor

Demonstração. Observe que pela construção são formados dois triângulos, OPC e OQC. Observe também que os lados OP e OQ são iguais (pois, é o raio da circunferência de centro O). Temos também que os lados PC e CQ são iguais (pois, por construção traçamos as circunferências de centros P e Q com raios de mesma medida). E, por último temos que OC é um lado comum entre os triângulos OPC e OQC. Logo, pelo caso LLL de congruência temos que os triângulos OPC e OQC são congruentes, com isso, temos que seus ângulos são congruentes também, dessa maneira temos que os ângulos $P\hat{O}C$ e $C\hat{O}Q$ são iguais. Como desejávamos. □

2.5 Triângulo Equilátero

Aqui realizaremos nossa primeira construção de um polígono, o triângulo equilátero. Antes disso, vale a pena relembrarmos a característica principal deste objeto geométrico: um triângulo equilátero é todo triângulo que possui os três lados congruentes.

Seja AB um segmento qualquer. Construiremos um triângulo equilátero cuja a medida dos lados é a medida do segmento AB.
Construção:

- Traçamos uma circunferência de centro em A passando pelo ponto B.
- Traçamos outra circunferência de centro B passando pelo ponto B.
- Observemos que estas duas circunferências determinará dois pontos ao se interceptarem, escolhemos um destes pontos e denominamos por C.
- Por fim, traçamos os segmentos AC e BC. Logo, temos o triângulo equilátero ABC.

Demonstração. Basta observarmos que, por construção, as circunferências de centro A e centro B possuem raio de medida AB, logo $AB = BC = AC$. □

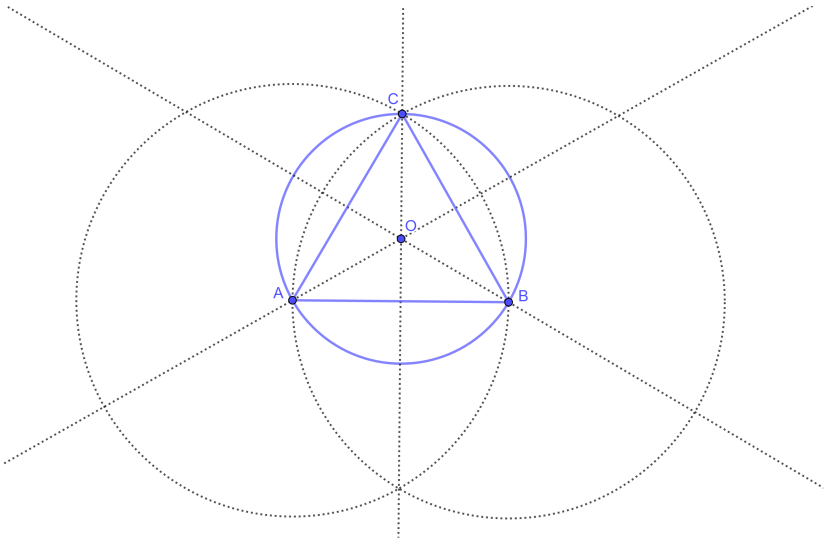

Figura 5 – Triângulo Equilátero

Fonte: Compilado pelo autor

Observe que podemos construir uma circunferência de forma que o triângulo ABC esteja inscrito nela. Para isso, traçamos as alturas do triângulo referentes aos seus respetivos lados. Estas retas irão determinar o ponto central deste triângulo, mais conhecimento como o ortocentro, denominamos este ponto por O. Logo, traçamos uma circunferência de centro O e passando por um dos vértices do triângulo ABC. Assim, teremos o triângulo ABC inscrito numa circunferência.

2.6 Quadrado

Seja AB um segmento qualquer. Construiremos um quadrado cuja sua diagonal tem medida AB.
Construção:

- Traçamos a mediatriz do segmento AB.
- Marcamos o ponto determinado pela interseção da mediatriz com o segmento AB. Denominamos este ponto por C.
- Com o centro em C e passando pelos pontos A e B, traçamos uma circunferência.
- Marcamos os pontos determinados pela interseção desta circunferência com a mediatriz do segmento AB. Denominamos estes pontos por D e E.
- Traçamos os segmentos AE, EB, BD e DA. Logo, $AEBD$ é o quadrado inscrito na circunferência de diâmetro AB.

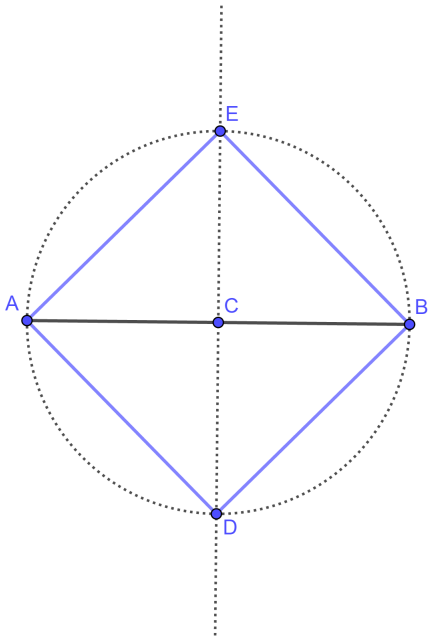

Figura 6 – Quadrado de diagonal AB

Fonte: Compilado pelo autor

Demonstração. Podemos observar que os triângulos AOB, OBC, DBO e ADO são congruentes pelo caso lado, ângulo, lado (LAL). Desta forma, os lados AC, CB, BD e DA são iguais. Podemos observar também que, o ângulo $A\hat{C}B$ é reto, pois é a metade do ângulo central $A\hat{O}B = 180°$. Pensamento análogo para os ângulos $B\hat{A}D$, $A\hat{D}B$ e $D\hat{B}A$. Portanto, $ADBC$ é um quadrado inscrito numa circunferência de diâmetro AB. □

Nos exemplos acima podemos observar que a partir de pontos determinados fomos capazes de construir novos elementos tais como pontos, retas e circunferências, utilizando somente a régua não graduada e o compasso.

Inspirado nessa ideia definimos, no próximo capítulo, o que entendemos por construir com régua e compasso.

3 Números Construtíveis

Este capítulo se inicia com a definição de números construtíveis e a demonstração de algumas propriedades que são satisfeitas por esses números. Veremos que o conjunto dos números construtíveis é um subconjunto dos reais que contem os racionais. Ainda neste capítulo estabelecemos a relação entre números e pontos construtíveis do plano.

3.1 Número real construtível

Dizemos que um número real a é construtível se, tendo uma unidade prefixada, é possível construir segmentos de medida $|a|$ utilizando apenas os instrumentos euclidianos, isto é, a régua não graduada e o compasso.

A proposição a seguir fornece algumas propriedades das quais gozam os números construtíveis.

Proposição 1. *Seja $C_{\mathbb{R}}$ o conjunto dos números construtíveis. Dados $a, b \in C_{\mathbb{R}}$, com $b \neq 0$, temos que:*

1. $a + b \in C_{\mathbb{R}}$;
2. $a - b \in C_{\mathbb{R}}$;
3. $a \cdot b \in C_{\mathbb{R}}$ *e*
4. $\dfrac{a}{b} \in C_{\mathbb{R}}$.

Para demonstração dos quatro itens a seguir, vamos considerar os pontos A e B previamente construídos, a reta r construtível que passa por estes pontos e, assumimos a medida do segmento AB igual a 1.

Demonstração. 1. Se $a, b \in C_{\mathbb{R}}$ então $a + b \in C_{\mathbb{R}}$.

Sejam C e D pontos sobre o segmento AB, de modo que $AC = a$ e $AD = b$. Sem perda de generalidade consideremos $0 < b < a$, vide figura 7. Traçamos uma circunferência com centro em C com raio de medida $AD = b$. Observe que esta, determina em r dois pontos, denominamos estes pontos por E e F. Agora veja que, $AD = EC = CF = b$ e, desta forma $AF = AC + CF = a + b$.

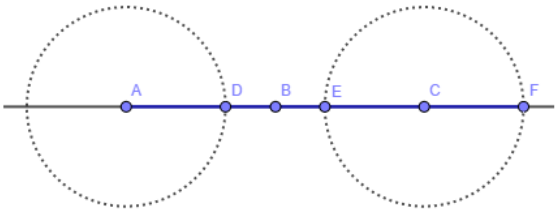

Figura 7 – Propriedade 1

Fonte: Compilado pelo autor

2. Se $a, b \in C_{\mathbb{R}}$ então $a - b \in C_{\mathbb{R}}$

   Essa demonstração segue o mesmo raciocínio da demonstração anterior. Desta maneira, analisando a figura anterior, temos que $AC - EC = a - b = AE$.

3. Se $a, b \in C_{\mathbb{R}}$ então $a \cdot b \in C_{\mathbb{R}}$

   Sendo os segmentos $AC = a$ e $AD = b$, consideremos um ponto P exterior à reta r. Traçamos a reta que passa pelos pontos A e P e em seguida, construamos o triângulo APB. Passando por C traçamos uma reta paralela a reta que passa pelos pontos P e B. Seja P' o ponto determinado pela interseção desta com a reta que passa pelos pontos A e P. Observemos que os triângulos, APB e $AP'C$ são semelhantes, logo, temos que:

   a) $\dfrac{AP}{AP'} = \dfrac{AB}{AC}$

   Analogamente, construamos o triângulo APD e, passando por P' traçamos uma reta paralela ao segmento PD. O ponto determinado pela interseção desta reta paralela com a reta r, denominamos por E. Novamente, observemos que os triângulos APD e $AP'E$ são semelhantes, desta forma temos que:

   a) $\dfrac{AP}{AP'} = \dfrac{AD}{AE}$

   Por (1) e (2), temos que:

   $$\frac{AB}{AC} = \frac{AD}{AE}$$

   Como $AB = 1$, $AC = a$ e $AD = b$, concluímos que,

   $$\frac{1}{a} = \frac{b}{AE} \Leftrightarrow AE = a \cdot b$$

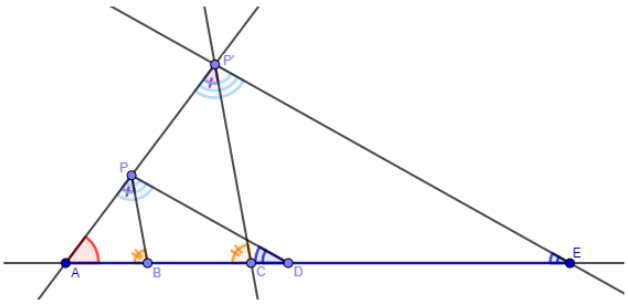

Figura 8 – Propriedade 3

Fonte: Compilado pelo autor

4. Se $a \in C_{\mathbb{R}}$ e $a \neq 0$, então $\dfrac{1}{a} \in C_{\mathbb{R}}$

Neste item, vamos precisar analisar dois possíveis casos, isto é, analisar quando $a > 1$ e $0 < a < 1$. Primeiramente, consideremos $a > 1$.

Seja C um ponto sobre a reta r tal que $AC = a > 1 = AB$. Agora, com a ponta seca do ponta seca do compasso centrado em A, traçamos uma circunferência de raio AC. De modo análogo, com o centro em C, traçamos uma circunferência de raio AC. Observe que estas circunferências se interceptam em dois pontos. Tracemos a reta que passa por estes pontos. Veja que ela interceptará a reta r em um ponto. Denominemos este ponto por M. Note que o ponto M é o ponto médio do segmento AC. Sendo assim, $AM = \dfrac{a}{2}$. Com a ponta seca do compasso fixada em M, traçamos uma circunferência de raio $AM = \dfrac{a}{2}$. Observemos que esta circunferência interceptará a reta r nos pontos A e C, ambos já construídos. Agora, com o centro em A e raio $AB = 1$, construamos outra circunferência. Observemos que esta nova circunferência interceptará a primeira circunferência em dois pontos, escolhemos uma destas interseções e denominamos por P. Feito isso, traçamos uma reta perpendicular a r passando por P, denominamos por Q o ponto de interseção desta com a reta r. Logo, afirmamos que o segmento AQ tem medida igual a $\dfrac{1}{a}$.

Note que, como AC é diâmetro da circunferência centrada em M, assim segue que $\widehat{APC}$ é o arco capaz do ângulo reto $(90°)$, dessa forma $A\hat{P}C = 90°$. Para mais detalhes sobre este assunto, consultar o capítulo 7.

Dessa forma, é possível mostrar que os triângulos APQ e APC são semelhantes. E E pela semelhança de triângulos temos a seguinte relação:

$$\frac{AP}{AQ} = \frac{AC}{AP} \Leftrightarrow AP^2 = AQ \cdot AC$$

como $AP = 1$ e $AC = a$, temos que $AQ = \dfrac{1}{a}$.

Agora consideremos $a \in C_{\mathbb{R}}$ tal que $0 < a < 1$, dessa forma, tome $n \in \mathbb{N}$ de modo que $an > 1$. Assim, como mostramos que se a for maior do que 1 é possível construir o

inverso dele, então basta realizar o pensamento análogo para a construção de an quando $0 < a < 1$. Com isso, mostramos que se a é construtível então seu inverso também é, como desejávamos. □

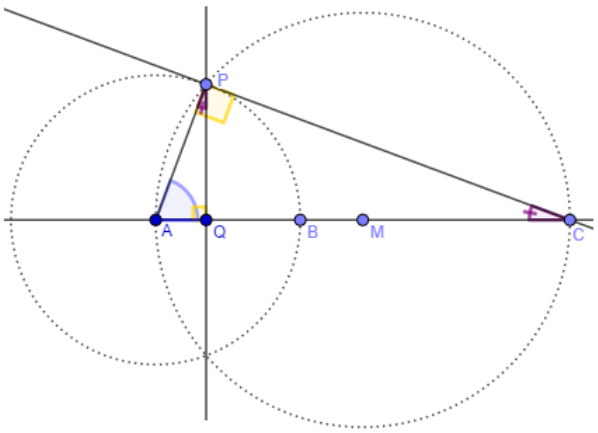

Figura 9 – Propriedade 4

Fonte: Compilado pelo autor

Agora, como mostramos que se $b \in C_{\mathbb{R}}$ segue que $\frac{1}{b} \in C_{\mathbb{R}}$ na qual, $b \neq 0$. E além disso, o produto de números construtíveis resulta em um número construtível, concluímos então que se $a, b \in C_{\mathbb{R}}$ então $\frac{a}{b} = a \cdot \frac{1}{b} \in C_{\mathbb{R}}$.

Observação 1. *Sabemos que o conjunto dos números racionais* $(\mathbb{Q})$ *é fechado para as operações de soma e produto e além disso, possui os elementos inversos multiplicativos. Porém observe que a partir da proposição anterior, mostramos que para quaisquer números construtíveis, a soma, o produto e o inverso de tais números também serão números construtíveis. Dessa forma, como todo número racional* $(\mathbb{Q})$ *pode ser escrito na forma* $\frac{a}{b}$*, concluímos que todo número racional é construtível, isto é, temos que* $\mathbb{Q} \subset C_{\mathbb{R}}$.

Proposição 2. *Se* $a > 0$ *tal que* $a \in C_{\mathbb{R}}$*, então* $\sqrt{a} \in C_{\mathbb{R}}$.

Demonstração. Consideremos sobre a reta r os pontos O, I, M e A de modo que $OI = 1$, $IA = a$ e $OM = \frac{(1+a)}{2}$, vide figura 10. Com a ponta seca do compasso centrada em M, traçamos a circunferência de centro M e raio OM. Esta interceptará a reta r nos pontos O e A, já construídos. Passando pelo ponto I, traçamos uma reta perpendicular a r. Esta interceptará a circunferência em dois pontos, denominamos um destes por P. Agora, traçamos uma circunferência de centro I e raio PI, esta interceptará a reta r em dois pontos, denominamos um destes por P'. Logo, afirmamos que $PI = P'I = \sqrt{a}$.

Temos que qualquer triângulo inscrito em uma semi-circunferência, é retângulo. Dessa forma, PI é altura do triângulo OPA em relação a hipotenusa OA. Segundo as

relações métricas do triângulo retângulo, temos que a altura (relativa a hipotenusa) ao quadrado é igual ao produto das projeções dos catetos. Logo,

$$PI^2 = OI \cdot IA \Rightarrow PI^2 = 1 \cdot a \Rightarrow PI = \sqrt{a}.$$

□

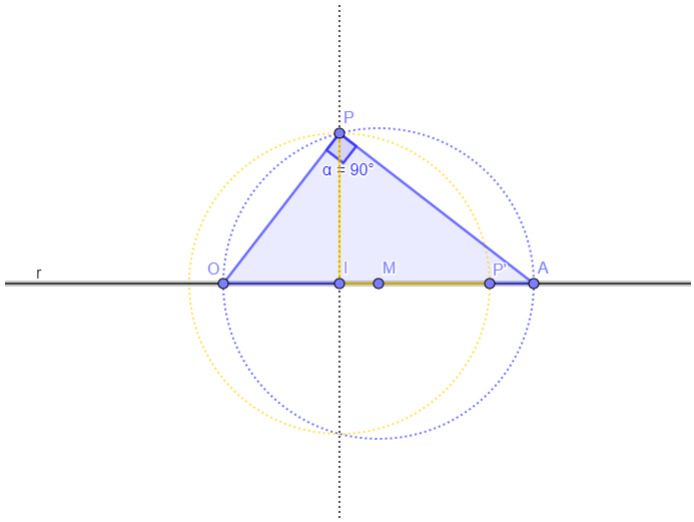

Figura 10 – Construção de $\sqrt{a}$

Fonte: Compilado pelo autor

3.1.1 Pontos Construtíveis no Plano $\mathbb{R}^2$.

Para melhor tratarmos sobre problemas de construção geométrica, precisamos saber quais construções são permitidas utilizando apenas a régua não graduada e o compasso. Utilizando-se apenas esses instrumentos para as construções de novos elementos, devemos partir inicialmente de um conjunto $\mathbb{P} \subset \mathbb{R}^2$ que contenha pelo menos dois pontos. Sejam P_i e P_j pontos quaisquer pertencentes ao conjunto $\mathbb{P}$. Assim, as operações permitidas sobre estes elementos são as seguintes:

- Traçar uma reta que passa por P_i e P_j.
- Traçar uma circunferência com centro em P_i e passando por P_j.
- Se inicialmente são dados certos pontos P_i e P_j, é possível construir outros pontos a partir de uma sequência de interseções entre retas, retas e circunferências e circunferências, que já foram traçadas anteriormente.

Essas operações serão chamadas de **operações elementares** em $\mathbb{P}$.

De um modo geral podemos dizer que a partir de pelo ao menos dois pontos pertencentes a $\mathbb{P}$, pode-se construir, através das operações elementares, novos pontos e, a partir destes pontos construir novas retas e circunferências. Com isso, os elementos construtíveis são os pontos, as retas e as circunferências.

Definição 1. *Dizemos que um ponto $P(a,b) \in \mathbb{R}^2$ é construtível a partir de um dado conjunto $\mathbb{P}$, se puder se obtido por um número finito de operações elementares em $\mathbb{P}$.*

Denotaremos por $< \mathbb{P} >$ o subconjunto dos pontos $P(a,b) \in \mathbb{R}^2$ que são construtíveis a partir de $\mathbb{P}$.

Observemos que todo ponto construtível de $\mathbb{R}^2$ se encontra em um subconjunto que podemos determinar da seguinte forma:

Considere o subconjunto do plano dado por $\mathbb{P}_0 = \{O(0,0), U(1,0)\}$. Seja r a reta que passa pelos pontos O e U. Traçamos a circunferência π_1 de centro O e que passa pelo ponto U. Analogamente, traçamos a circunferência π_2 de centro U e que passa pelo ponto O. Observemos que por operações elementares obtemos os pontos A_1, A_2, A_3 e A_4, como mostra a figura 11. Traçando a reta O_y perpendicular a r passando por O, obtemos um sistema ortogonal de coordenadas, sendo r o eixo das abscissas. Neste sistema, temos que $A_1(-1,0), A_2(2,0), A_3\left(\frac{1}{2}, \frac{\sqrt{3}}{2}\right)$ e $A_4\left(\frac{1}{2}, -\frac{\sqrt{3}}{2}\right)$.

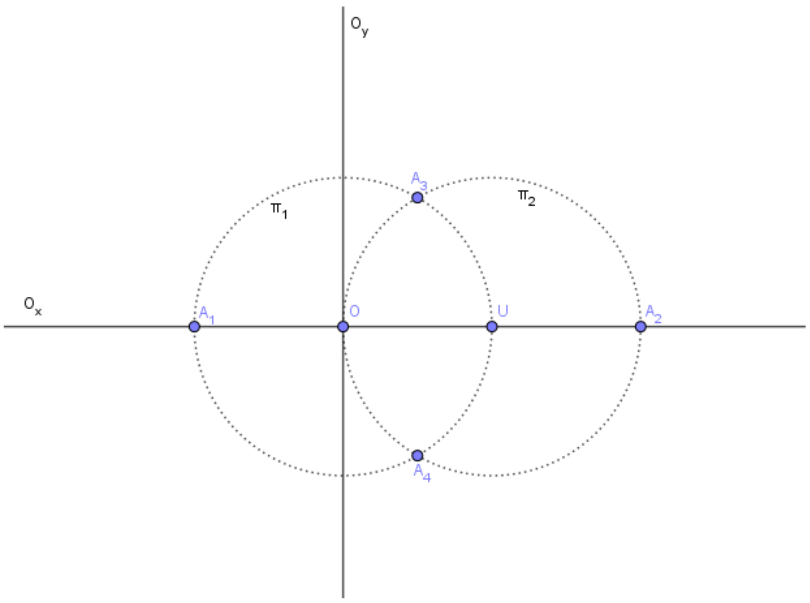

Figura 11 – Pontos contrutíveis

Fonte: Compilado pelo autor

Assim, $< \mathbb{P}_0 >= \{O, U, A_1, A_2, A_3 \text{ e } A_4\}$ é o subconjunto dos pontos do plano que são construtíveis a partir de $\mathbb{P}_0$.

Denotando este subconjunto por $\mathbb{P}_1$, ou seja, $\mathbb{P}_1 =< \mathbb{P}_0 >$, podemos construir outro subconjunto dos pontos do plano que são construtíveis a partir de $\mathbb{P}_1$. Continuando este processo, obtemos a sequência $\{\mathbb{P}_1 =< \mathbb{P}_0 >, \mathbb{P}_2 =< \mathbb{P}_1 >, ..., \mathbb{P}_{n+1} =< \mathbb{P}_n > ..., \forall n \in \mathbb{N}\}$ de modo que,

$$\mathbb{P}_0 \subset \mathbb{P}_1 \subset \mathbb{P}_2 \subset ... \subset \mathbb{P}_n \subset \mathbb{P}_{n+1} \subset \mathbb{R}^2.$$

Denotando por $\mathbb{P}_\infty$ a união de todos esses subconjuntos acima, ou seja, $\mathbb{P}_\infty = \bigcup_{n=0}^{\infty} \mathbb{P}_n$, vemos que $\mathbb{P}_\infty$ é um subconjunto infinito do plano, apesar de cada $\mathbb{P}_n$ ser um subconjunto finito do plano. Desde que $\mathbb{P}_j \subset \mathbb{P}_i \ \forall j < i \in \mathbb{N}$ tem-se que $< \mathbb{P}_\infty >= \mathbb{P}_\infty$ e observe que todo ponto $P(a, b)$ de coordenadas racionais, pertence ao conjunto $\mathbb{P}_\infty$.

Dessa forma podemos caracterizar os elementos construtíveis da seguinte maneira:

Definição 2. *1. Um ponto $P(a, b)$ do plano é dito construtível se $P \in \mathbb{P}_\infty$;*

2. Uma reta é construtível, se pelo ao menos dois de seus pontos pertencem a $\mathbb{P}_\infty$. E uma circunferência é construtível, se seu centro e um de seus pontos pertencem a $\mathbb{P}_\infty$;

3. Um número real a diz-se construtível se $P(a, 0) \in \mathbb{P}_\infty$.

A proposição a seguir mostra que o conhecimento dos números construtíveis é suficiente para determinar os pontos construtíveis.

Proposição 3. *Um ponto $P(a, b)$ do plano é construtível se e somente se, suas coordenadas $a, b \in \mathbb{R}$ são números construtíveis, ou seja, $A(a, 0) \in \mathbb{P}_\infty$ e $B(b, 0) \in \mathbb{P}_\infty$.*

Demonstração. ($\Rightarrow$) Suponhamos que o ponto $P(a, b) \in \mathbb{P}_\infty$. Então traçamos por este ponto uma reta s perpendicular ao eixo das abscissas e uma reta r perpendicular ao eixo das ordenadas, através do tópico 2.2 vimos que tais construções são possíveis. As intersecções dessas retas com os eixos coordenados nos fornece os pontos $A(a, 0)$ e $B_0(0, b)$, veja Figura 12. Com o compasso centrado na origem do sistema, traçamos um círculo de raio $|b|$. Este círculo encontra o eixo das abscissas no ponto $B(b, 0)$. Portanto, $B(b, 0) \in \mathbb{P}_\infty$ e de modo similar, $A(a, 0) \in \mathbb{P}_\infty$.

($\Leftarrow$) Reciprocamente, suponhamos que a e b sejam números construtíveis, isto é, $A(a, 0) \in \mathbb{P}_\infty$ e $B(b, 0) \in \mathbb{P}_\infty$. Com a ponta seca o compasso centrado na origem, traçamos o círculo de raio $|b|$. Esse círculo determina sobre o eixo das ordenadas o ponto $B_0(0, b)$. A reta passando por $B_0(0, b)$, perpendicular ao eixo das ordenadas, intersecta a reta que passa por $A(a, 0)$, perpendicular ao eixo das abscissas, no ponto $P(a, b)$. Portanto, $P(a, b) \in \mathbb{P}_\infty$. □

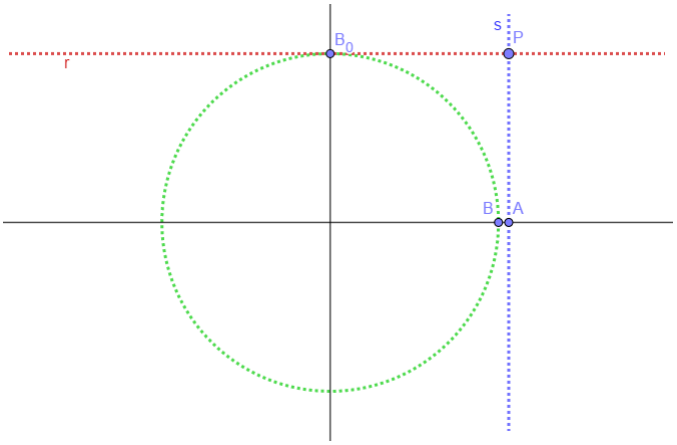

Figura 12 – Ponto construtível

Fonte: Compilado pelo autor

A partir destes conceitos, foi possível obtermos uma ideia de quais objetos geométricos são construtíveis e como podemos construí-los. No capítulo posterior começaremos a estudar alguns conceitos ,que nos darão base para compreender como é a estrutura do conjunto dos números construtíveis ($C_{\mathbb{R}}$).

4 Polinômios

Neste capítulo exibiremos alguns resultados mais técnicos cujo objetivo é fornecer ferramentas necessárias para a compreensão do resultado principal desta monografia que consiste na caracterização dos polígonos que são construtíveis por régua e compasso. Desta forma, alguns detalhes de provas mais robustas serão omitidos.

4.1 Anéis

Seja A um conjunto não vazio onde esteja definido duas operações, soma e produto, na qual denotaremos por $(+)$ e $(\cdot)$, respectivamente. Essas operações são definidas da seguinte forma:

$+ : A \times A \to A$
$(a, b) \mapsto a + b$
e,
$\cdot : A \times A \to A$
$(a, b) \mapsto a \cdot b$

Dado um conjunto A e elementos a, b, c pertencentes a A, nos interessamos pelas seguintes propriedades:

A1) $(a + b) + c = a + (b + c)$ - *Associatividade em relação a soma*;

A2) $\exists 0 \in A$ tal que $a + 0 = 0 + a$ - *Elemento neutro da soma*;

A3) $a + b = b + a$ - *Comutatividade em relação a soma*;

A4) $\forall a \in A$ existe um único elemento $b \in A$ da forma $b = -a$, tal que, $a + b = b + a = 0$ - *Existência do inverso aditivo*;

M1) $(a \cdot b) \cdot c = a \cdot (b \cdot c)$ - *Associatividade em relação ao produto*;

M2) $a \cdot b = b \cdot a$ - *Comutatividade em relação ao produto*;

M3) $\exists\ 1 \in A$ tal que $a \cdot 1 = 1 \cdot a = a, \forall a \in A$ - *Elemento neutro do produto*;

D1) $(a + b) \cdot c = a \cdot c + b \cdot c$; $a \cdot (b + c) = a \cdot b + a \cdot c$ - *Distributividade em relação à soma*;

D2) $a \cdot b \Rightarrow a = 0$ ou b=0 - *Sem divisores de zero*;

D3) $\forall a \in A$ com $a \neq 0, \exists$ b $\in A$, tal que, $a \cdot b = b \cdot a = 1$ - *Existência do inverso multiplicativo.*

A partir destas propriedades e utilizando $(A, +, \cdot)$ como notação para o conjunto cujo as operações soma e produto estão bem definidas. Temos que,

1. Se $(A, +, \cdot)$ satisfaz as propriedades A_1, A_2, A_3, A_4, M_1 e D_1, então dizemos que $(A, +, \cdot)$ é um anel.
2. Se $(A, +, \cdot)$ satisfaz as propriedades citadas anteriormente e M_2, então dizemos que $(A, +, \cdot)$ é um anel comutativo.
3. Se $(A, +, \cdot)$ satisfaz as propriedades que citamos em 1) e a propriedade M_3, então dizemos que $(A, +, \cdot)$ é um anel com unidade.
4. Se $(A, +, \cdot)$ satisfaz as 9 primeiras propriedades, ou seja, de $A_1 ... D_2$, então dizemos que $(A, +, \cdot)$ é um domínio de integridade.

A definição que mais nos interessa é:

Definição 3 (Corpo)**.** *Um corpo é domínio de integridade* $(A, +, \cdot)$ *que satifaz a condição* D_3*.*

Definição 4 (Subcorpo)**.** *Seja* $(A, +, \cdot)$ *um corpo e* B *um subconjunto não vazio de* A*. Se* B *for corpo com as operações de* A*, isto é,* $(B, +, \cdot)$*, dizemos que* B *é subcorpo de* A*.*

Proposição 4. *Seja* $(A, +, \cdot)$ *um anel e seja* B *um subconjunto de* A*. Então,* B *é um subcorpo de* A *se e somente se as seguintes condições são verificadas:*

1. $0 \in B$ *(o elemento neutro de* A *pertence a* B*)*
2. $x, y \in B \Rightarrow x - y \in B$ *(*B *é fechado para a diferença)*
3. $x, y \in B \Rightarrow x \cdot y \in B$ *(*B *é fechado para o produto)*

Demonstração. ($\Rightarrow$) Se B é subcorpo, então temos pela definição 4 que os itens 1, 2 e 3 são satisfeitos.
($\Leftarrow$) Agora, precisamos mostrar que B é subcorpo de A, isto é, B é não vazio, é fechado para a soma e para o produto.
Assim, observe que o elemento neutro $0'$, em relação a soma, de B é o mesmo elemento neutro 0 de A, pois $0' = b + (-b) = 0$.
Suponhamos que $B \subset A$ e que as os itens 1, 2 e 3 são satisfeitos. Dessa forma, por 1 segue que $B \neq \varnothing$ e novamente, por 1 e 2 temos: se

$$y \in B \Rightarrow -y = 0 - y \in B \tag{4.1}$$

Contudo, por 2 e por 4.1, temos que se $x, y \in B$ então $x + y = x - (-y) \in B$, isto é, B é fechado para a soma. E por 3, B é fechado para o produto. □

Exemplo 1. *São exemplos de corpos os seguintes conjuntos* $\mathbb{Q}, \mathbb{R}, \mathbb{C}, \mathbb{Z}_p$ *com* $p \geq 2$ *primo e* $\mathbb{Q}[\sqrt{p}] = \{a + b\sqrt{p} \, : \, a, b \in \mathbb{Q}, p \text{ primo}\}$.

Teorema 2. $C_{\mathbb{R}} = \{\alpha \in \mathbb{R} : \alpha \text{ é construtível } \}$ *é um subcorpo de* $\mathbb{R}$ *contendo* $\mathbb{Q}$.

Demonstração. Precisamos mostrar duas coisas, primeiro que $\mathbb{Q} \subset C_{\mathbb{R}}$ e segundo que $C_{\mathbb{R}}$ é subcorpo de $\mathbb{R}$.
Observe que pela proposição 1 do capítulo anterior, concluímos na observação 1 que $\mathbb{Q} \subset C_{\mathbb{R}}$. Portanto a primeira parte da demonstração está feita.
Agora, para mostrar que $C_{\mathbb{R}}$ é subcorpo de $\mathbb{R}$, precisamos mostrar que pela proposição 4 que são válidas as seguintes propriedades:

1. $0 \in C_{\mathbb{R}}$;
2. $\alpha, \beta \in C_{\mathbb{R}} \Rightarrow \beta - \alpha \in C_{\mathbb{R}}$;
3. $\alpha, \beta \in C_{\mathbb{R}} \Rightarrow \beta \cdot \alpha \in C_{\mathbb{R}}$.

Seja α um número construtível, assim temos que $0 = \alpha - \alpha$, logo $0 \in C_{\mathbb{R}}$ e o item 1 está provado. Agora, observe que os itens 2 e 3 foram demonstrados na Proposição 1 do capítulo anterior. Dessa maneira, temos que $C_{\mathbb{R}}$ é subcorpo de $\mathbb{R}$. □

Definição 5. *Seja* K *um corpo qualquer, chamamos de um polinômio sobre* K *em uma indeterminada* x *a expressão* $p(x) = a_0 + a_1x + ... + a_nx^n + ...$, *onde* $a_i \in K, \forall i \in \mathbb{N}$ *e* $\exists m \in \mathbb{N}$ *tal que* $a_j = 0 \ \forall j > m$.

A partir desta definição podemos ressaltar algumas observações sobre polinômios:

- Dizemos que dois polinômios, $p(x) = a_0 + a_1x + ... + a_nx^n + ...$ e $q(x) = b_0 + b_1x + ... + b_mx^m + ...$ em K são iguais se e somente se, $a_i = b_i$, $\forall i \in \mathbb{N}$.
- Dizemos que o polinômio $p(x)$ é identicamente nulo se e somente se $a_i = 0 \ \forall i \in \mathbb{N}$.
- Se $a \in K$, consideremos o polinômio $p(x) = a$ tal que, $a = a_0$ e $a_i = 0 \ \forall i \geq 1$, então chamamos $p(x)$ de polinômio constante a.
- Se $p(x) = a_0 + a_1x + ... + a_nx^n + ...$ é um polinômio tal que $a_n \neq 0$ e $a_j = 0$ $\forall j > n$, dizemos que n é o grau do polinômio $p(x)$ e nesse caso, escrevemos $p(x) = a_0 + a_1x + ... + a_nx^n$ e o grau de $p(x)$ denotamos por $\partial p(x) = n$.

Podemos observar que o grau do polinômio nulo não está definido, e ∂ pode ser interpretado como uma função do conjunto de todos os polinômios em $(K[x])$ não nulos para o conjunto $\mathbb{N}$. Isto é:

$$\partial : K[x] - \{0\} \to \mathbb{N}$$
$$p(x) \mapsto \partial p(x)$$

Denotaremos por $K[x]$ o conjunto de todos os polinômios, sobre K em uma indeterminada x. Agora, iremos definir as operações, soma e produto no conjunto $K[x]$.

Definição 6. *Sejam* $p(x) = a_0 + a_1x + ... + a_nx^n + ...$ *e* $q(x) = b_0 + b_1x + ... + b_mx^m + ...$ *polinômios do conjunto* $K[x]$.
As operações de soma e de produto de polinômios é definido por:
$+ : p(x) + q(x) = c_0 + c_1x + ... + c_kx^k + ...,$ *onde* $c_i = (a_i + b_i) \in K$, $\forall i \in \mathbb{N}$.
e
$\cdot : p(x) \cdot q(x) = c_0 + c_1x + ... + c_kx^k + ...,$ *com* $c_k \in K$, $\forall k \in \mathbb{N}$ *dado por:*
$c_0 = a_0b_0, c_1 = a_0b_1 + a_1b_0, c_2 = a_0b_2 + a_1b_1 + a_2b_0, ..., c_k = \sum_{j=0}^{k} a_jb_{k-j}$.

Desta forma temos que as operações de soma e produto estão bem definidas sobre o conjunto $K[x]$. Observemos que se identificarmos os elementos $a \in K$ como os polinômios $p(x) = a \in K[x]$ podemos pensar em $K[x]$ contendo o corpo K.

Como dito anteriormente, o grau (∂) de um polinômio pode ser interpretado como uma função, e esta possui as seguintes propriedades:

1. $\partial(p(x)+q(x)) \leq$ máx $\{\partial p(x), \partial q(x)\}$, quaisquer que sejam os polinômios $p(x), q(x) \in K[x]$, na qual, $p(x) + q(x) \neq 0$.

2. $\partial(p(x) \cdot q(x)) = \partial p(x) + \partial q(x)$, quaisquer que sejam os polinômios não nulos.

Suponhamos que um polinômio $p(x) \neq 0$ possui um elemento inverso multiplicativo em $K[x]$, então existe $q(x) \in K[x] - \{0\}$ tal que $p(x) \cdot q(x) = 1$. Pela Propriedade 2 acima segue que $p(x) = a \neq 0$ (polinômio constante). De fato, como $p(x) \neq 0$, suponhamos que $\partial p(x) = n$, assim pela Propriedade 2, temos que $\partial(p(x) \cdot q(x)) = \partial p(x) + \partial q(x) = 1$. Porém, como $p(x), q(x)$ são não nulos e $\partial(p(x) \cdot q(x)) = \partial p(x) + \partial q(x) = 1$, segue que $p(x)$ é o polinômio constante.

4.2 Algoritmo da divisão

Teorema 3. *(Algoritmo da divisão): Sejam* $f(x), g(x) \in K[x]$ *e* $g(x) \neq 0$. *Então existem únicos* $q(x), r(x) \in K[x]$ *tais que:*

$$f(x) = g(x) \cdot q(x) + r(x),$$
$$\text{em que } r(x) = 0 \text{ ou } \partial r(x) < \partial g(x)$$

Demonstração. Sejam

$$f(x) = a_n x^n + ... + a_1 x + a_0$$

e

$$g(x) = b_m x^m + ... + b_1 x + b_0$$

Primeiro, iremos provar que existem polinômios $q(x)$ e $r(x) \in K[x]$ tais que é válida a expressão referida no enunciado do teorema.

Antes disso, observemos que se $f(x) = 0$, isto é, o polinômio nulo, basta tomarmos $q(x) = r(x) = 0$, e assim está provada a existência destes polinômios. Desta forma, assumimos $f(x)$ não nulo com $\partial f(x) = n$ e, prosseguiremos a demonstração por indução sobre $\partial f(x) = n$.

Assim, se $\partial f(x) = n < m = \partial g(x)$, basta tomarmos $q(x) = 0$ e $r(x) = f(x)$ e novamente, a existência de tais polinômios está provada. Por estes fatos, assumimos $\partial f(x) = n \geq m = \partial g(x)$.

Seja $f_1(x)$ o polinômio definido da seguinte forma:

$$f(x) = a_n b_m^{-1} x^{n-m} \cdot g(x) + f_1(x) \tag{4.2}$$

Notemos que o $\partial f_1(x) < \partial f(x)$, pois da equação 4.2 temos:

$$\begin{aligned} f_1(x) &= f(x) - a_n b_m^{-1} x^{n-m} \cdot g(x) \\ &= f(x) - a_n b_m^{-1} x^{n-m} \cdot (b_m x^m + b_{m-1} x^{m-1} + ... + b_1 x + b_0) \\ &= f(x) - (a_n x^n + a_n b_{m-1} b_m^{-1} x^{n-1} + ... + a_n b_0 b_m^{-1} x^{n-m}) \\ &= (a_n x^n + a_{n-1} x^{n-1} + ... + a_1 x + a_0) - (a_n x^n + a_n b_{m-1} b_m^{-1} x^{n-1} + ... + a_n b_0 b_m^{-1} x^{n-m}) \\ &= (a_{n-1} + a_n b_{m-1} b_m^{-1}) x^{n-1} + ... + a_0 \end{aligned}$$

Ou seja, $\partial f_1(x) = n - 1 < n = \partial f(x)$.

Observação 2. *A hipótese de indução é, qualquer polinômio cujo o seu grau é menor que $\partial f(x) = n$, pode ser escrito na forma que fora enunciada no teorema.*

Assim, se $n = 0$ e $n \geq m$ temos automaticamente que $m = 0$. Portanto os polinômios f e g são da forma $f(x) = a_0 \neq 0$ e $g(x) = b_0 \neq 0$, isto é, constantes. Dessa maneira, podemos escrever o polinômio f como $f(x) = a_0 b_0^{-1} \cdot g(x)$. A partir daí, basta tomarmos os polinômios $q(x), r(x) \in K[x]$ como sendo $q(x) = a_0 b_0^{-1}$ e $r(x) = 0$ e assim, a hipótese de indução é válida.

Vimos anteriormente que $f_1(x)$ é definido da seguinte forma:

$$f_1(x) = f(x) - a_n b_n^{-1} x^{n-m} \cdot g(x). \tag{4.3}$$

na qual $\partial f_1(x) = n - 1 < n = \partial f(x)$.

Desta forma, como $\partial f_1(x) = n - 1$, temos por hipótese de indução que existem polinômios $q_1(x), r_1(x) \in K[x]$ tais que

$$f_1(x) = q_1(x) \cdot g(x) + r_1(x). \tag{4.4}$$

Logo, pelas equações 4.3 e 4.4 temos:

$$f(x) - a_n b_m^{-1} x^{n-m} \cdot g(x) = q_1(x) \cdot g(x) + r_1(x)$$

$$f(x) = [a_n b_m^{-1} x^{n-m} + q_1(x)] \cdot g(x) + r_1(x).$$

E deste modo, tomando $q(x) = a_n b_m^{-1} x^{n-m} + q_1(x)$ e $r(x) = r_1(x)$, provamos a existência dos polinômios $q(x)$ e $r(x)$ tais que $f(x) = q(x) \cdot g(x) + r(x)$, onde $r(x) = 0$ ou $\partial r(x) < \partial g(x)$.

Agora, mostraremos a unicidade dos polinômios $q(x)$ e $r(x)$.

Suponhamos que existam $q_1(x), q_2(x), r_1(x), r_2(x) \in K[x]$ tais que:

$$f(x) = q_1(x) \cdot g(x) + r_1(x) = q_2(x) \cdot g(x) + r_2(x) \tag{4.5}$$

na qual, $r_i(x) = 0$ ou $\partial r_i < \partial g(x), i = 1, 2$.

Assim temos:

$$[q_1(x) - q_2(x)] \cdot g(x) = r_2(x) - r_1(x). \tag{4.6}$$

Por um lado, se $q_1(x) \neq q_2(x)$ temos que o grau do polinômio a esquerda da igualdade acima é maior ou igual a $m = \partial g(x)$. Por outro lado, temos que o grau do polinômio a direita desta igualdade é estritamente menor que $m = \partial g(x)$, o que é contradição. Contradição vinda da suposição de que existem polinômios $q_1(x)$ e $q_2(x)$ diferentes tais que satisfazem a igualdade 4.5. Portanto, $q_1(x) = q_2(x)$.

Agora, pela expressão 4.6 temos:

$$0 = r_2(x) - r_1(x) \Rightarrow r_1(x) = r_2(x).$$

Como queríamos demonstrar. □

Proposição 5. *Seja K um corpo e seja $f(x) = a_0 + a_1 x + ... + a_n x^n$ um polinômio não nulo em $K[x]$ de grau n, então, o número de raízes de $f(x)$ em K é no máximo igual a $\partial f(x) = n$.*

Demonstração. Se $f(x)$ não possui raízes em K, então não há o que demonstrar.

Suponhamos que $\alpha \in K$ seja uma raiz de $f(x)$. Considerando $g(x) = (x - \alpha) \in K[x]$ temos, pelo algoritmo da divisão, que existem $q(x), r(x) \in K[x]$ de modo que:

$$f(x) = (x - \alpha) \cdot q(x) + r(x)$$

na qual, $r(x) = 0$ ou $\partial r(x) < \partial g(x)$.

Como $\partial g(x) = 1$, então $r(x) = b_0$ (polinômio constante) e assim, $f(x) = (x - \alpha) \cdot q(x) + b_0$. Como α é raiz de $f(x)$, temos que $f(\alpha) = 0 \cdot q(x) + b_0 = 0$, ou seja, $r(x) = b_0 = 0$. Dessa forma,

$$f(x) = (x - \alpha) \cdot q(x)$$

e $\partial f(x) = \partial(x - \alpha) + \partial q(x)$, isto é, $\partial q(x) = \partial f(x) - \partial(x - \alpha) = n - 1$.

Agora, se $\beta \in K$ é uma raiz qualquer de $f(x)$ então, $f(\beta) = (\beta - \alpha) \cdot q(\beta) = 0$, e como em um corpo não há divisores de zero segue que, ou $\beta = \alpha$ ou β é raiz do polinômio $q(x) \in K$. Dessa maneira, temos que as raízes de $f(x)$ são α e as raízes de $q(x)$. Faremos a prova por indução sobre o grau de $f(x)$, $\partial f(x) = n$. Se $n = 0$, isto é $f(x)$ é polinômio constante, então $f(x)$ não possui raízes em K e nesse caso, não há o que demonstrar. Seja $n > 0$ e suponhamos que todo polinômio $q(x)$ em $K[x]$ de grau menor que n possui no máximo $\partial q(x) = n - 1$ raízes em K. Porém, como as possíveis raízes de $f(x)$ são α e as raízes do polinômio $q(x)$ então concluímos que $f(x)$ possui no máximo n raízes. □

4.3 Polinômios irredutíveis

Seja K um corpo e seja $K[x]$ o domínio dos polinômios sobre K.

Definição 7. *Um polinômio $p(x) \in K[x]$ é dito ser irredutível, se for de grau maior ou igual que 1 e se for dada uma fatoração $p(x) = f(x) \cdot g(x)$ então $\partial f(x)$ ou $\partial g(x)$ é igual a 0, ou seja, $f(x)$ ou $g(x)$ é um polinômio constante.*

Como exemplo, podemos ver que o polinômio $x^2 + 1$ é irredutível sobre o corpo $\mathbb{R}$ porém é redutível sobre $\mathbb{C} \supset \mathbb{R}$, ou seja, um polinômio pode ser irredutível sobre um corpo K, porém pode ser redutível sobre um corpo "maior"que contém K. (Numa extensão de K.)

Teorema 4. *(Fatoração única) Seja K um corpo. Então todo polinômio $f(x) \in K[x] - \{0\}$ pode ser escrito na forma $f(x) = u \cdot p_1(x) \cdot \ldots \cdot p_m(x)$ onde $u \in K - \{0\}$ e $p_1(x), p_2(x), ..., p_m(x)$ são polinômios irredutíveis sobre K (não necessariamente distintos).*

Mais ainda, essa expressão é única a menos da constante u e da ordem dos polinômios $p_1(x), p_2(x), ..., p_m(x)$.

Demonstração. Sejam $f(x) \in K[x] - \{0\}$ e $u \in K - \{0\}$. Primeiramente, queremos mostrar que existem polinômios $p_1(x), ..., p_m(x) \in K[x]$ irredutíveis tais que $f(x)$ é escrito como enunciado no teorema. Para isso, utilizaremos indução sobre $\partial f(x) = n$.

Observemos que, se $n = 0$ então $f(x) = u \in K - \{0\}$. Ainda, se $n = 1$, então $f(x) = u \cdot p_1(x)$, na qual $u \in K - \{0\}$ e $p_1(x) \in K[x] - \{0\}$, e temos que todo polinômio

de grau igual a 1 sobre um corpo é irredutível sobre este corpo. Desta forma, assumimos $\partial f(x) = n > 1$.

Seja $f(x)$ um polinômio qualquer de grau n. Se $f(x)$ for irredutível, então a demonstração está finalizada. Agora, se $f(x)$ for redutível, então $f(x)$ pode ser escrito como produto de polinômios $g(x), h(x)$, tal que $1 \leq \partial g(x), \partial h(x) < n$.

É importante observarmos que $g(x)$ e $h(x)$ não podem ser, simultaneamente, polinômios de grau igual a 1, pois assim teríamos que $g(x)$ e $h(x)$ seriam polinômios irredutíveis sobre K e estaríamos utilizando um fato que estamos querendo demonstrar.

Assim suponhamos, por hipótese de indução, que todo polinômio não nulo de grau menor que n pode ser escrito como o produto de polinômios irredutíveis. Então, como $1 \leq \partial g(x), \partial h(x) < n$, temos que:

$$g(x) = a \cdot p_1(x) \cdot ... \cdot p_r(x)$$

na qual, $a \in K - \{0\}$ e $p_1(x), ..., p_r(x)$ são polinômios irredutíveis sobre K. E analogamente,

$$h(x) = b \cdot p_{r+1}(x) \cdot ... \cdot p_m(x)$$

na qual, $b \in K - \{0\}$ e $p_{r+1}(x), ..., p_m(x)$ são polinômios irredutíveis sobre K.

Consequentemente,

$$f(x) = u \cdot p_1(x) \cdot ... \cdot p_r(x) \cdot p_{r+1}(x) \cdot ... \cdot p_m(x)$$

na qual, $u = a \cdot b \in K - \{0\}$ e $p_1(x), ..., p_m(x) \in K[x] - \{0\}$ são polinômios irredutíveis sobre K. Contradição! Uma vez que supomos que $f(x)$ não poderia ser escrito como produto de polinômios irredutíveis. Portanto, concluímos que $f(x)$ pode ser escrito da forma desejada.

Desta forma, provamos a existência dos polinômios $p_1(x), ..., p_m(x)$ irredutíveis tais que

$$f(x) = u \cdot p_1(x) \cdot ... \cdot p_m(x)$$

Agora, provaremos que estes polinômios são únicos.

Para a unicidade, suponha que exista duas expressões para $f(x)$, ou seja

$$f(x) = up_1(x)...p_m(x) = u'p'_1(x)...p'_s(x)$$

Como os polinômios p_k são todos irredutíveis então cada p_j com $j \in \{1, 2, \cdots, m\}$ divide o produto $p'_1(x)...p'_s(x)$. Neste caso, existe algum índice $i \in \{1, 2, \cdots, s\}$ de modo que $p_1(x)$ divide $p'_i(x)$, ou seja, $p'_i(x) = u'_i.p_1(x)$. Claro que se m= 1 e $p_1(x)$ é irredutível, então s=1. Suponha o resultado válido para todo natural até $m - 1$. Então

$$up_1(x)...p_m(x) = u'p'_1(x)...p'_s(x) \Rightarrow u\frac{p'_i(x)}{u'_i}...p_m(x) =$$
$$u'p'_1(x)...\cdot p'_{i-1}(x)\cdot p'_i(x)\cdot p'_{i+1}(x)...p'_s(x) \Rightarrow up_2(x)...p_m(x) = u'p'_1(x)...\cdot p'_{i-1}(x)\cdot p'_{i+1}(x)...p'_s(x).$$

Portanto, $m-1 = s-1$ por indução, e segue o resultado.

□

Proposição 6. *(Gauss). Seja $f(x) \in \mathbb{Z}[x]$ tal que $f(x)$ é irredutível sobre $\mathbb{Z}$, então $f(x)$ é irredutível sobre $\mathbb{Q}$.*

Demonstração. Suponhamos que $f(x)$ seja irredutível sobre $\mathbb{Z}$ mas redutível sobre $\mathbb{Q}$, ou seja,

$$f(x) = g(x) \cdot h(x),$$

na qual, $g(x), h(x) \in \mathbb{Q}$ e $1 \leq \partial g(x), h(x) < \partial f(x)$.

Seja $m = mmc$ dos denominadores dos coeficientes racionais de $g(x) \cdot h(x)$. Sendo assim, é possível encontrarmos $g_1(x), h_1(x) \in \mathbb{Z}[x]$ tais que

$$m \cdot f(x) = g_1(x) \cdot h_1(x) \tag{4.7}$$

Desta forma, consideremos:

$$g_1(x) = a_0 + a_1x + ... + a_rx^r,$$

na qual $a_i \in \mathbb{Z}$, $\forall\ i \in \{1, ..., r\}$. E,

$$h_1(x) = b_0 + b_1x + ... + b_sx^s$$

na qual, $b_j \in \mathbb{Z}$, $\forall\ j \in \{1, ..., s\}$.

Agora suponhamos que $p|m$, em que p é primo. Provaremos que $p|a_i\ \forall\ i \in \{1, ..., r\}$ ou $p|b_j\ \forall\ j \in \{1, ..., s\}$.

Caso exista $i \in \{1, ..., r\}$ e $j \in \{1, ..., s\}$ tal que $p \nmid a_i$ e $p \nmid b_j$, suponhamos que estes índices sejam os menores possíveis tais que esta propriedade é válida, ou seja, qualquer coeficiente a_k ou b_k tal que $k > i$ ou $k > j$, temos que a_k ou b_k será divisível por p.

Como $p|m$, temos que p divide o polinômio $m \cdot f(x) = g_1(x) \cdot h_1(x)$, isto é,

$$p|\sum_{k=0}^{i+j} b_k \cdot a_{i+j-k}$$

Pelo fato de termos escolhido i e j menores possíveis tais que $p \nmid a_i$ e $p \nmid b_j$, temos que p divide cada parcela da soma acima, exceto a parcela $b_j \cdot a_i$. Porém, p divide o polinômio $m \cdot f(x)$, logo p divide toda a expressão acima, então necessariamente p deve dividir cada coeficiente de x^{i+j}, inclusive $b_j \cdot a_i$.

Como p é primo, tem-se que $p|a_i$ e/ou $p|b_j$, o que é uma contradição, vinda do absurdo de supormos que existem coeficientes a_i e b_j são tais que p não divide. Portanto $p|a_i$ ou $p|b_j$ se, e somente se, p é primo e $p|m$ $\forall i \in \{1, ..., r\}$ ou $\forall j \in \{1, ..., s\}$.

Sem perda de generalidade, suponhamos que $p|a_i$ $\forall$ $i \in \{1, ..., r\}$.

Desta forma, como $p|g_1(x)$ segue que $g_1(x) = p \cdot g_2(x)$, na qual $g_2(x) \in \mathbb{Z}$ e, como $p|m$ tem-se $m = p \cdot m_1$. Então por 4.7 temos,

$$p \cdot m_1 \cdot f(x) = p \cdot g_2(x) \cdot h_1(x) \Rightarrow m_1 \cdot f(x) = g_2(x) \cdot h_1(x).$$

Como o número de fatores primos de m é finito e prosseguindo com o argumento acima, chegaremos em:

$$f(x) = g_*(x) \cdot h_*(x) \tag{4.8}$$

na qual, $g_*(x), h_*(x) \in \mathbb{Z}[x]$ e, $g_*(x), h_*(x)$ são múltiplos racionais de $g(x), h(x)$ respectivamente, ou seja,

$$g_*(x) = \frac{1}{m} \cdot g(x)$$

$$h_*(x) = \frac{1}{m} \cdot h(x).$$

Por (4.8), concluímos que $f(x)$ é redutível sobre $\mathbb{Z}$, o que é uma contradição, já que inicialmente supomos $f(x)$ irredutível sobre $\mathbb{Z}$, contradição esta, vinda do absurdo de supormos que $f(x)$ é redutível sobre $\mathbb{Q}$. Portanto, concluímos que $f(x)$ é irredutível sobre $\mathbb{Q}$. Como queríamos demonstrar. □

4.3.1 Critério de Eisenstein

Agora enunciaremos um critério que verifica a irredutibilidade de um polinômio sobre o corpo $\mathbb{Q}$.

Teorema 5. *Seja $p(x) = a_0 + a_1x + ... + a_nx^n$ um polinômio em $\mathbb{Z}$. Suponhamos que exista um inteiro primo p tal que:*

1. $p \nmid a_n$;
2. $p|a_0, a_1, ..., a_{n-1}$;
3. $p^2 \nmid a_0$.

Então $p(x)$ é irredutível sobre $\mathbb{Q}$.

Demonstração. Pela proposição anterior, vimos que basta provarmos que $f(x)$ é irredutível sobre $\mathbb{Z}$. Desta forma, suponhamos que $f(x)$ é redutível em $\mathbb{Z}$, ou seja

$$f(x) = g(x) \cdot h(x)$$

tais que $g(x), h(x) \in \mathbb{Z}$ e, $1 \leq \partial g(x), \partial h(x) < \partial f(x) = n$.

Sejam,

$$g(x) = b_0 + b_1 x + ... + b_r x^r \in \mathbb{Z}[x], \partial g(x) = r,$$

$$h(x) = c_0 + c_1 x + ... + c_s x^s \in \mathbb{Z}[x], \partial h(x) = s.$$

Assim, $n = r + s$.

Primeiro, analisaremos os termos independentes do polinômio $g(x) \cdot h(x)$.

Sabemos que, $b_0 \cdot c_0 = a_0$ e pela hipótese 2 do teorema, temos que $p|a_0$, desta forma, $p|b_0 \cdot c_0$. Pelo fato de p ser primo e pela hipótese 3, temos que p deve dividir apenas um fator do produto $b_0 \cdot c_0$, pois se p dividir as duas parcelas, teremos que tanto b_0 quanto c_0 serão múltiplos de p. Ambos sendo múltiplos de p, o produto $b_0 \cdot c_0$ terá como fator p^2, o que torna a_0 sendo um múltiplo de p^2, o que é um absurdo pois contradiz uma das hipóteses do teorema.

Desta forma, vamos admitir sem perda de generalidade que $p|b_0$ e $p \nmid c_0$.

Agora, analisaremos os coeficientes dos termos dominantes. Sabemos que $a_n = b_r + c_s$ é o coeficiente do termo $x^n = x^{r+s}$ e por hipótese temos que $p \nmid a_n$, ou seja, $p \nmid b_r$ e $p \nmid c_s$. Mas vimos anteriormente que $p \mid b_0$. Sendo assim, seja b_i o primeiro coeficiente de $g(x)$ tal que $p \nmid b_i$.

Observemos que os coeficientes do polinômio $f(x)$ é da seguinte forma:

$$a_i = \sum_{k=0}^{i} b_k \cdot c_{i-k}.$$

Pelo fato de termos pego i como sendo o menor índice tal que $p \nmid b_i$, temos que $p|b_0, ..., b_{i-1}$. Daí, como temos que $p \nmid b_i$, $p \nmid c_0$ e como $b_i \cdot c_0$ é a última parcela do somatório acima, concluímos que $p \nmid a_i$. Pela hipótese 1 do teorema, este fato implica que $i = n$, o que é um absurdo já que, $1 \leq i \leq r < n$. Absurdo vindo da suposição de que o polinômio $f(x)$ é redutível sobre $\mathbb{Z}$. Desta forma, temos que $f(x)$ é irredutível sobre $\mathbb{Z}$ o que é equivalente a $f(x)$ ser irredutível sobre $\mathbb{Q}$. Como queríamos demonstrar. □

A seguir podemos ver alguns exemplos em que os teoremas citados anteriormente podem ser aplicados:

Exemplo 2. *Seja* $p(x) = x^3 + 3x^2 - 9x + 6$. *O Critério de Eisenstein se aplica para o primo* $p = 3$, *pois*

1. $3 \nmid 1$;

2. $3|6$, $3|(-9)$ e $3|3$;

3. $3^2 \nmid 6$.

Portanto, $f(x)$ é irredutível sobre $\mathbb{Q}$.

Exemplo 3. *Seja p um número primo qualquer e seja $f(x) = x^n - p$ um polinômio de grau maior ou igual a 1 sobre $\mathbb{Q}$.*

Neste caso, podemos observar que o próprio primo p se aplica no critério de Eisenstein, e portanto $f(x)$ é irredutível sobre $\mathbb{Q}$.

5 Extensões de Corpos

Neste capítulo tal como no anterior teremos mais resultados que nos ajudará numa melhor compreensão dos números construtíveis. Aqui abordaremos superficialmente a teoria de extensão de corpos, que nos permitirá enxergar o conjunto dos números construtíveis ($C_{\mathbb{R}}$) como sendo uma extensão algébrica de grau igual a uma potência de dois (2^n) dos números racionais.

5.1 Extensão de Corpos

Definição 8. *Seja L um corpo. Dizemos que L é uma extensão de um corpo K se $L \supset K$ e se as operações de L restritas a K coincidem com as operações de K.*

Exemplo 4. *O corpo $\mathbb{C}$ é uma extensão do corpo $\mathbb{R}$ e este é uma extensão do corpo $\mathbb{Q}$.*

Uma observação a ser feita é que se um corpo L é uma extensão de um corpo K, então L é um espaço vetorial sobre o K.

Definição 9. *Dizemos que $L \supset K$ é uma extensão finita se L tem dimensão finita como espaço vetorial sobre K e definimos o grau da extensão como sendo $[L : K] = dim_K L$. Se L como espaço vetorial sobre K não possui dimensão finita então dizemos que L é uma extensão infinita.*

A seguir mais um exemplo de extensão do corpo $\mathbb{Q}$:

Exemplo 5. *Seja $L = \mathbb{Q}[i] = \{a + bi \mid a, b \in \mathbb{Q}\}$. Se olharmos para L como sendo um espaço vetorial sobre $\mathbb{Q}$, temos que uma base deste espaço é o conjunto $B = \{1, i\}$. Dessa forma, temos que L é uma extensão finita de $\mathbb{Q}$, na qual o grau de tal extensão é $[L : \mathbb{Q}] = 2$*

Proposição 7. *Sejam K um corpo e $c > 0$ tal que $c \in K$ e $\sqrt{c} \notin K$. Então*

$$K[\sqrt{c}] := \{a + b\sqrt{c} \mid a, b \in K\}$$

é um corpo.

Demonstração. Seja $x = a + b\sqrt{c} \neq 0$. inverso de x é dado por

$$x^{-1} = \frac{1}{a + b\sqrt{c}} = \frac{1}{a + b\sqrt{c}} \cdot \frac{a - b\sqrt{c}}{a - b\sqrt{c}} = \left(\frac{a}{a^2 - b^2 c}\right) + \left(\frac{-b}{a^2 + b^2 c}\sqrt{c}\right) = a_1 + b_1\sqrt{c} \in K.$$

As demais condições são facilmente verificadas. □

Definição 10. *Dados o corpo K, $c > 0$, tal que $c \in K$ e $\sqrt{c} \notin K$, chamaremos de* ***extensão quadrática*** *de K o corpo*

$$K(\sqrt{c}) := \{a + b\sqrt{c} \mid a, b \in K\}.$$

A seguir um exemplo de extensão quadrática do corpo $\mathbb{Q}$:

Exemplo 6. *Seja $\mathbb{Q}[\sqrt{2}] = \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}$. Temos que $\mathbb{Q}[\sqrt{2}]$ é uma extensão quadrática de $\mathbb{Q}$, na qual $B = \{1, \sqrt{2}\}$ é uma base do espaço vetorial $\mathbb{Q}[\sqrt{2}]$ sobre $\mathbb{Q}$ e $[\mathbb{Q}[\sqrt{2}] : \mathbb{Q}] = 2$.*

Definição 11. *Dado um corpo K, chamamos de $K[x]$ o conjunto de todos os polinômios na variável x e que possuem coeficientes em K.*

Definição 12. *Seja L uma extensão de K. Dizemos que um elemento $\alpha \in L$ é algébrico sobre K se existe um polinômio não nulo $p(x) \in K[x] - \{0\}$ tal que $p(\alpha) = 0$, isto é, se α satisfaz a uma equação polinomial $a_n x^n + ... + a_1 x + a_0 = 0$ que possui coeficientes em K nem todos nulo. Se $\alpha \in L$ não for algébrico sobre K, dizemos que α é transcendente sobre K.*

Definição 13 (Extensão Algébrica)**.** *Seja L uma extensão de um corpo K. Dizemos que L é uma extensão algébrica de K se todo $\alpha \in L$ é algébrico sobre K.*

Exemplo 7. *O número $\sqrt{7} \in \mathbb{R}$, é algébrico sobre $\mathbb{Q}$, pois $\sqrt{7}$ é raiz do polinômio $f(x) = x^2 - 7 \in \mathbb{Q}[x]$. No entanto, o número π não é algébrico sobre $\mathbb{Q}$, pois não existe $q(x) \in \mathbb{Q}[x]$ tal que $q(\pi) = 0$.*

Definição 14. *Seja $\alpha \in L$ algébrico sobre K. Definimos o polinômio mínimo de α sobre K como sendo o polinômio $p(x) \in K[x]$, mônico, ou seja, com coeficiente dominante $a_n = 1$ e de menor grau tal que $p(\alpha) = 0$.*

Um fato que podemos observar é que o polinômio mínimo $p(x)$ é o único. Denotaremos este polinômio por $p(x) = irr(\alpha, K)$.

Exemplo 8. *O número $\sqrt{3}$ é algébrico sobre $\mathbb{Q}$, cujo polinômio mínimo é $p(x) = x^2 - 3$.*

Sejam $\alpha \in L \supset K$ e $f(x) \in K[x]$, definimos $K[\alpha] = \{f(\alpha) : f(x) \in K[x]\}$.

Exemplo 9. *Mostraremos que $\mathbb{Q}[\sqrt{3}] = \{a + b\sqrt{3} \mid a, b \in \mathbb{Q}\}$.*

De fato, $\mathbb{Q}[\sqrt{3}] = \{f(\sqrt{3}) : f(x) \in \mathbb{Q}[x]\}$. Pelo algoritmo da divisão existem $q(x)$ e $r(x) \in \mathbb{Q}[x]$ tais que $f(x) = (x^2 - 3) \cdot q(x) + r(x)$, na qual $r(x) = 0$ ou $r(x) = ax + b$. Observemos que, no exemplo anterior, o polinômio mínimo de $\alpha = \sqrt{3}$ é o polinômio $p(x) = x^2 - 3$, ou seja, $p(x)$ é o polinômio de menor grau em $\mathbb{Q}[x]$ que se anula em

$\alpha = \sqrt{3}$. Desta forma, como $r(x) \in \mathbb{Q}[x]$, temos que $r(\sqrt{3}) \neq 0$ logo, $r(x) = a + bx$. Daí, $f(\sqrt{3}) = 0 \cdot q(\sqrt{3}) + r(\sqrt{3}) = a + b\sqrt{3} : a, b \in \mathbb{Q}$.

Proposição 8. *Seja $L \supset K, \alpha \in L$ algébrico sobre K. Se o grau do polinômio $irr(\alpha, K)$ é n, então:*

1. *$\forall f(x) \in K[x], f(\alpha)$ pode ser expresso de modo único na forma $f(\alpha) = a_0 + a_1\alpha + ... + a_{n-1}\alpha^{n-1}$, onde $a_i \in K$.*
2. *$K[\alpha] = \{a_0 + a_1\alpha + ... + a_{n-1}\alpha^{n-1} : a_i \in K\}$ é um subcorpo de L que contém K.*

Faremos a demonstração apenas do primeiro item desta Proposição.

Demonstração. Consideramos $p(x) = irr(\alpha, K)$. Pelo algoritmo da divisão, para todo $f(x) \in K[x]$ existem $q(x), r(x) \in K[x]$ tais que,

$$f(x) = p(x) \cdot q(x) + r(x)$$

com $r(x) = 0$ ou $\partial r(x) < \partial p(x) = n$. Como $p(x) = irr(\alpha, K)$, temos que $p(\alpha) = 0$ assim pela expressão anterior,

$$f(\alpha) = r(\alpha) = a_0 + a_1\alpha + ... + a_{n-1}\alpha^{n-1}$$

na qual $a_i \in K$.

Agora, suponhamos que

$$f(\alpha) = a_0 + a_1\alpha + ... + a_{n-1}\alpha^{n-1} = b_0 + b_1\alpha + ... + b_{n-1}\alpha^{n-1}.$$

Consideremos $g(x) = \sum_{i=0}^{n-1}(a_i - b_i)x^i$. Pela forma como $g(x)$ foi definido, $g(x)$ é um polinômio de grau menor que n que se anula em α, logo devemos ter que $g(x)$ é o polinômio nulo, isto é, $g(x) = 0$. De fato, se $g(x)$ for um polinômio irredutível então contradizemos a hipótese de $p(x)$ ser o polinômio mínimo. Portanto $g(x) = 0$ e $a_i = b_i, \forall\ i \in \{0, 1, ..., n-1\}$, como desejávamos.

□

Proposição 9. *Seja K um corpo e $L \supset K$ uma extensão de K. Então,*

1. *se $L \supset K$ é finita então $L \supset K$ é algébrica.*
2. *se $\alpha \in L \supset K$ é um elemento algébrico sobre K e grau de $irr(\alpha, K)$ é igual a n então $1, \alpha, ..., \alpha^{n-1}$ é um base do espaço vetorial $K[\alpha]$ sobre K e $[K[\alpha] : K] = n$.*
3. *Se α é um elemento transcendente sobre K então $K[\alpha] \supset K$ é uma extensão infinita.*

Demonstração. Suponhamos que $L \supset K$ seja uma extensão finita, cujo grau $[L : K] = n$. Seja α um elemento qualquer de L, mostraremos que α é algébrico sobre K. E assim, a extensão $L \supset K$ será algébrica.

Como $[L : K] = n$, temos que o conjunto $\{1, \alpha, \alpha^2, ..., \alpha^n\}$ com $n + 1$ elementos é linearmente dependente. Logo, existem escalares $a_0, a_1, a_2, ..., a_n \in K$ não todos nulos tais que

$$a_0 + a_1\alpha + a_2\alpha^2 + ... + a_n\alpha^n = 0.$$

Observemos que a expressão acima é um polinômio pertencente a $K[x]$, de coeficientes não todos nulos, que aplicado em α resulta em zero. Mas esta é justamente a definição de α ser algébrico sobre K. Como desejávamos.

Pelo primeiro item da Proposição 8 temos que, para todo α algébrico sobre K tal que o grau do $irr(\alpha, K) = n$, os elementos de $K[\alpha]$ são escritos de modo único como combinação linear de $B = \{1, \alpha, \alpha^2, ..., \alpha^{n-1}\}$, isto é, o conjunto B gera o espaço $K[\alpha]$. Agora, sejam $b_0, b_1, b_2, ..., b_{n-1} \in K$, tais que

$$b_0 + b_1\alpha + b_2\alpha^2 + ... + b_{n-1}\alpha^{n-1} = 0$$

como o grau de $irr(\alpha, K)$ é n, temos que $b_0 = b_1 = b_2 = ... = b_{n-1} = 0$, ou seja, B é linearmente independente. Portanto, $B = \{1, \alpha, \alpha^2, ..., \alpha^{n-1}\}$ é uma base de $K[\alpha]$ e $[K[\alpha] : K] = n$, o que prova o segundo item .

O último é obvio, pois se a extensão $K[\alpha] \supset K$ fosse finita, então pelo primeiro item seria algébrica.

□

Proposição 10. *Sejam L, F e K corpos de modo que $L \supset F \supset K$. Suponhamos que $[L : F] = m$ e $[F : K] = n$. Então $[L : K] = m \cdot n$.*

Demonstração. Sejam $B_L = \{l_1, l_2, \cdots, l_m\}$ base de L sobre F e $B_F = \{f_1, f_2, \cdots, f_n\}$ base de F sobre K. Dado $l \in L$ temos que

$$l = a_1l_1 + a_2l_2 + \cdots a_ml_m$$

com $a_i \in F$ para todo $i \in \{1, 2, \cdots, m\}$.

Para cada $i \in \{1, 2, \cdots, m\}$ temos que

$$a_i = b_{i1}f_1 + b_{i2}f_2 + \cdots b_{in}f_n,$$

com $b_{ij} \in K$ para todo $j \in \{1, 2, \cdots, n\}$. Assim

$$l = \sum_{i=1}^{m}\sum_{j=1}^{n} b_{ij}l_if_j.$$

Como o conjunto de vetores $\{l_i f_j\}$ com $(i,j) \in \{1,2,\cdots,m\} \times \{1,2,\cdots,n\}$ gera o espaço L sobre K, resta mostrar que este conjunto é linearmente independente. De fato, considere a combinação linear nula $\sum_{i=1}^{m}\sum_{j=1}^{n} b_{ij} l_i f_j = 0$. Para cada j fixado, temos que $\sum_{i=1}^{m} b_{ij} l_i = 0$, pois o único vetor f_j é L.I. Da mesma forma, $b_{ij} = 0$ para cada $i \in \{1,2,\cdots,m\}$. Portanto, $\{l_i f_j\}$ com $(i,j) \in \{1,2,\cdots,m\} \times \{1,2,\cdots,n\}$ é uma base para L sobre K com $m \cdots n$ elementos. Isso prova a proposição. □

Definição 15. *Seja $c_1 \in \mathbb{Q} = K_0$ de modo que $\sqrt{c_1} \notin \mathbb{Q}$ defina $K_1 = \mathbb{Q}[\sqrt{c_1}]$. De modo recorrente, para todo natural $i > 1$, tome $c_i \in K_{i-1}$tal que $\sqrt{c_i} \notin K_{i-1}$ e defina $K_i = K_{i-1}[\sqrt{c_i}]$.*

Observação 3. *Observamos que para cada i, K_i é uma extensão quadrática de K_{i-1} e todos eles são extensões quadráticas iteradas de $\mathbb{Q}$, isto é, K_i é da forma $K_i = \mathbb{Q}(\sqrt{c_1}, \sqrt{c_2}, \cdots, \sqrt{c_i})$.*

Observação 4. *Observe que a dimensão de K_j como espaço vetorial sobre $\mathbb{Q}$ é igual a 2^j. De fato, como a dimensão de K_j sobre K_{j-1} é igual a 2, o resultado segue por indução com o uso da Proposição 10.*

Definição 16. *Para cada racional $c_i \in \mathbb{Q}$ definimos $\mathbb{T}_{c_i} = \bigcup_{j=1}^{\infty} K_j$, sendo*

$$K_j = \mathbb{Q}\left(\sqrt{(c_i)_1}, \sqrt{(c_i)_2}, \cdots, \sqrt{(c_i)_j}\right)$$

uma extensão quadrática iterada de $\mathbb{Q}$.

Proposição 11. *Seja $\mathbb{T}$ a união todas as suas extensões quadráticas, ou seja, $\mathbb{T} = \bigcup_{i\in\mathbb{N}} \mathbb{T}_{c_i}$. Um número α é construtível se e somente se $\alpha \in \mathbb{T}$.*

Demonstração. É claro que se $\alpha \in \mathbb{T}$, então α é construtível. Por outro lado, temos que se α for um número construtível, então $P(\alpha, 0) \in \mathbb{P}_\infty$, ou seja, $P(\alpha, 0)$ pode se obtido por um número finito de operações elementares que consistem de interseções de duas retas, reta e circunferência ou duas circunferências. Em qualquer dos casos acima, as equações algébricas envolvidas necessitam apenas das quatro operações fundamentais e da extração da raiz quadrada para serem resolvidas. Portanto, a solução estará em alguma extensão quadrática dos racionais. □

A partir desta proposição podemos concluir que o conjunto dos números construtíveis ($C_\mathbb{R}$) é o conjunto da união de todas as extensões quadráticas, isto é, $C_\mathbb{R} = \mathbb{T}$.

A prova do teorema a seguir decorre das proposições e observações acima.

Teorema 6. *O conjunto dos números construtíveis $C_{\mathbb{R}}$ é uma extensão algébrica dos racionais tal que para todo $\alpha \in C_{\mathbb{R}}$ temos que o grau da extensão $\mathbb{Q}[\alpha]$ é uma potência de 2, ou seja, $[\mathbb{Q}[\alpha] : \mathbb{Q}] = 2^r$*

Demonstração. Seja $\alpha \in \mathbb{C}_{\mathbb{R}}$. Pela Proposição 11 temos que $\alpha \in \mathbb{T}$. Assim, $\alpha \in \mathbb{Q} \cup K_j$ para algum $j \in \mathbb{N}$. Logo, $\mathbb{Q}[\sqrt{\alpha}] = K_{j+1}$ com $\sqrt{\alpha} \notin K_j$. Portanto, pela Observação 4, temos que $[\mathbb{Q}[\alpha] : \mathbb{Q}] = 2^{j+1}$.

□

Proposição 12. *Se n é um número ímpar ≥ 3 e p um número primo ≥ 2 então $\sqrt[n]{p}$ não é construtível.*

Demonstração. Seja $\alpha = \sqrt[n]{p}$ tal que n é um número ímpar ≥ 3 e p é um número primo maior ou igual 2, então $irr(\alpha, \mathbb{Q}[\alpha]) = x^n - p$. Assim, pela Proposição 9 segue que $[\mathbb{Q}[\alpha] : \mathbb{Q}] = n$ ímpar, ou seja, $[\mathbb{Q}[\alpha] : \mathbb{Q}] \neq 2^r$. Portanto, $\alpha = \sqrt[n]{p}$ não é construtível. □

Em particular $\sqrt[3]{2}$ não é construtível.

Relembraremos agora o teorema que nos fornece condições necessárias e suficientes para que um polinômio possua raiz racional.

Teorema 7 (Teorema das Raízes Racionais)**.** *Seja $f(x) = a_n x^n + a_{n-1}x^{n-1} + ... + a_1 x + a_0$ com coeficientes nem todos nulos e $a_i \in \mathbb{Z}$. Se $\alpha = \dfrac{p}{q} \in \mathbb{Q}$, no qual $mdc(p, q) = 1$, é raiz de $f(x)$, então $p|a_0$ e $q|a_n$.*

Demonstração. Seja $\alpha = \dfrac{p}{q}$ raiz do polinômio $f(x) = a_n x^n + a_{n-1}x^{n-1} + ... + a_1 x + a_0$. Dessa forma,

$$f\left(\frac{p}{q}\right) = a_n \frac{p^n}{q^n} + a_{n-1}\frac{p^{n-1}}{q^{n-1}} + ... + a_1 \frac{p}{q} + a_0 = 0.$$

Multiplicando a equação acima por q^n obtêm-se:

$$a_n p^n + a_{n-1}p^{n-1}q + ... + a_1 pq^{n-1} + a_0 q^n = 0$$

Analisando a equação acima, p divide suas n primeiras parcelas, isto é, p divide $a_n p^n, ..., a_1 pq^{n-1}$. Sendo assim, p deve dividir a parcela $a_0 q^n$, porém p e q são coprimos, portanto $p|a_0$.

De modo similar, q divide as n últimas parcelas do polinômio anterior, ou seja, q divide $a_{n-1}p^{n-1}q, ..., a_o q^{n-1}$. Dessa forma, q deve dividir a parcela $a_n p^n$, porém como p e q são coprimos tem-se que $q|a_n$. Como desejávamos. □

A proposição a seguir nos fornece uma condição para que as raízes de um polinômio de grau 3 com coeficientes racionais seja construtível.

Proposição 13. *Seja* $f(x) = x^3 + bx^2 + cx + d$, $b, c, d \in \mathbb{Q}$. *As raízes de* $f(x)$ *são construtíveis se, e somente se, pelo menos uma delas é racional.*

Demonstração. ($\Rightarrow$) Seja α uma raiz qualquer de $f(x)$. Por hipótese temos que α é construtível, e pela Proposição 11 α pertence a $\mathbb{T}$, isto é, α pertence a alguma extensão quadrática $K_i = \mathbb{Q}(\sqrt{c_1}, \sqrt{c_2}, \cdots, \sqrt{c_i})$.

Suponhamos que $f(x)$ seja irredutível sobre $\mathbb{Q}$, assim tem-se que $irr(\alpha, \mathbb{Q}) = f(x)$ e, observe que grau de $irr(\alpha, \mathbb{Q})$ é igual a 3. Segue pela Proposição 9 e pelo Teorema 6 que as raízes de $f(x)$ não são construtíveis, contradizendo a hipótese desta Proposição. Dessa forma $f(x)$ é redutível sobre $\mathbb{Q}$, isto é, $f(x) = (x - \alpha)p(x)$, na qual $\alpha \in \mathbb{Q}$ e $p(x) \in \mathbb{Q}[x]$. Como queríamos demonstrar.

($\Leftarrow$) Agora, seja α raiz racional de $f(x)$, existe $p(x) \in \mathbb{Q}[x]$ tal que

$$f(x) = (x - \alpha)p(x).$$

Observe que, se $p(x)$ for redutível sobre $\mathbb{Q}$ então as raízes de $p(x)$ serão racionais e portanto construtíveis.

Assim, suponhamos $p(x)$ irredutível sobre $\mathbb{Q}$. Observe que, como $f(x) = (x-\alpha)p(x)$ e $p(x)$ é irredutível em $\mathbb{Q}$, segue que o grau de $p(x)$ é igual a 2. De fato, observe que se β for raiz de $p(x)$, isto é, $p(\beta) = 0$, então $[\mathbb{Q}[\beta] : \mathbb{Q}] = 2$, pois o polinômio mínimo de β sobre $\mathbb{Q}$ é $p(x)$, e grau de $p(x)$ é 2. Logo, pelo Teorema 6, β é construtível. □

6 Polígonos

Neste capítulo estudamos alguns conceitos básicos sobre polígonos, damos uma breve introdução sobre os números complexos e apresentamos alguns critérios para a construtibilidade dos polígonos regulares.

Definição 17 (Polígono)**.** *Figura plana limitada por segmentos de retas que se intersectam exatamente em dois outros extremos de segmentos. Esses segmentos são denominados lados do polígono e seus extremos são os vértices.*

Definição 18 (Polígono Convexo)**.** *Dizemos que um polígono é convexo quando qualquer segmento de reta que possui extremidades em seu interior está inteiramente contido no polígono.*

Definição 19 (Polígono Regular)**.** *Se um polígono convexo possui todos os lados e ângulos internos congruentes, então o polígono é dito regular.*

Definição 20. *Um polígono é construtível se todos os seus vértices são pontos construtíveis do plano.*

A seguir relembraremos um pouco sobre os números complexos e notaremos que os vértices de um polígono regular de n lados está relacionado com as raízes da unidade.

6.1 Números complexos

Um número complexo $z = a + bi$ pode ser representado como um ponto no plano de coordenadas (a, b) ou como um vetor $\overrightarrow{Oz}$ de origem O e extremidade z. Porém, esta representação dá ênfase somente às coordenadas do ponto z. Uma representação que dá ênfase aos elementos geométricos do número complexo $z = a + bi$ é sua a representação na forma polar. Sendo $a = r\cos\theta$ e $b = rsen\theta$, a forma polar do número $z = a + bi$ é

$$z = |z|(\cos\theta + isen\theta)$$

na qual, $r = |z|$ é o comprimento de Oz e θ é o ângulo formado pelo eixo x e o vetor Oz, chamado de argumento de z.

Proposição 14 (Primeira Fórmula de De Moivre)**.** *Dado um número complexo não nulo $z = r(\cos\theta + isen\theta)$, então para cada número inteiro positivo n, tem-se que*

$$z^n = r^n(\cos(n\theta) + isen(n\theta))$$

Demonstração. Seja $z = r(\cos\theta + isen\theta)$ um número complexo não nulo. Faremos a demonstração por indução sobre n.

Se $n = 1$ então $z^1 = r^1(\cos(\theta) + isen(\theta))$ e a expressão é válida, pois é o número complexo z escrito na forma polar. Agora, suponhamos que a seguinte expressão é verdadeira:

$$z^n = r^n(\cos(n\theta) + isen(n\theta)).$$

Assim, queremos mostrar que é válido a seguinte expressão

$$z^{n+1} = r^{n+1}(\cos((n+1)\theta) + isen((n+1)\theta)).$$

Desse modo,

$$\begin{aligned} z^{n+1} = z^n \cdot z &= r^n(\cos(n\theta) + isen(n\theta)) \cdot r(\cos\theta + isen\theta) \\ &= r^n \cdot r(\cos(n\theta) + isen(n\theta)) \cdot (\cos\theta + isen\theta) \\ &= r^n \cdot r(\cos(n\theta)\cos\theta - sen(n\theta)sen\theta) \\ &+ i(\cos(n\theta)sen\theta + sen(n\theta)\cos\theta)) \\ &= r^{n+1}(\cos(n\theta+\theta) + isen(n\theta+\theta)) \\ &= r^{n+1}(\cos((n+1)\theta) + isen((n+1)\theta)) \end{aligned}$$

Logo, concluímos que dado um número complexo $z = r(\cos\theta + isen\theta)$, para cada número inteiro positivo n é possível obter $z^n = r^n(\cos(n\theta) + i\,\mathrm{sen}(n\theta))$. Como desejávamos.

□

Definição 21. *Dizemos que um número z é raiz enésima de um dado número complexo w, se $z^n = w$.*

Exemplo 10 (Segunda Fórmula de De Moivre)**.** *Determine todas as raízes complexas da equação $z^n = w$, sendo $w \in \mathbb{C}$ e $n \geq 2$.*

Solução: Se $w = 0$, a única solução é $z = 0$. Assim, consideremos $w \neq 0$ e escrevemos $z = r(\cos(\theta) + isen(\theta))$ e $w = \rho(\cos(\phi) + isen(\phi))$. Pela fórmula de De Moivre temos que a equação $z^n = w$ pode ser escrita:

$$r^n(\cos(n\theta) + isen(n\theta)) = \rho(\cos(\phi) + isen(\phi))$$

Sabe-se que a igualdade de números complexos requer a igualdade das partes reais e imaginárias separadamente. Assim,

$$r^n\cos(n\theta) = \rho\cos(\phi) \text{ e } r^n sen(n\theta) = \rho sen(\phi)$$

Isto é,

$$r = \sqrt[n]{\rho} \text{ e } \theta = \frac{\phi + 2k\pi}{n}, \text{ para } k = 1, 2, ..., n-1.$$

Observe que para $k \geq n$, obtêm-se as raízes anteriores.

Portanto tem-se que r é uma raiz enésima positiva de ρ e,

$$z_k = \sqrt[n]{w} = \sqrt[n]{\rho}\left(\cos\frac{\phi + 2k\pi}{n} + isen\frac{\phi + 2k\pi}{n}\right), \text{ para } k = 0, 1, 2, ..., n-1.$$

são as raízes enésimas de w.
Como curiosidade, pode-se observar que a equação acima é intitulada como a Segunda Fórmula de De Moivre. Fica como sugestão ao leitor, realizar uma pesquisa a cerca do assunto.

6.1.1 Raízes da unidade

Um caso interessante é quando $w = 1$. Neste caso teremos que as raízes enésimas da unidade serão os números $z_k = cos\left(\frac{2k\pi}{n}\right) + isen\left(\frac{2k\pi}{n}\right)$, para $k = 0, 1, \cdots, n-1$. Observe que se $z_1 = cos\left(\frac{2\pi}{n}\right) + isen\left(\frac{2\pi}{n}\right)$ é raiz da unidade então todas as raízes da unidade são os números $\{1, z_1, z_1^2, z_1^3, \cdots, z_1^{n-1}\}$.

Ao representarmos graficamente esses números, obteremos um **polígono regular de n** lados inscrito no círculo de raio 1.

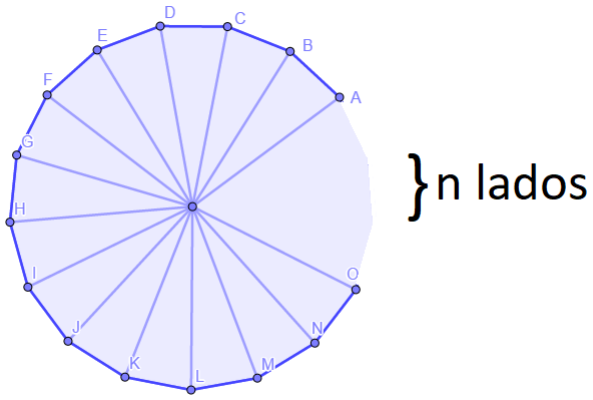

Figura 13 – Polígono de n lados

Fonte: Compilado pelo autor

Exemplo 11. *Determine as raízes da equação $z^5 = 1$. Em seguida represente estas raízes no plano complexo.*

Neste exemplo queremos encontrar cinco números complexos que ao serem elevados a quinta potência, resulte no número 1.

Observe que o comprimento(r) *do número 1 é* $r = 1$ *e o ângulo*(θ) *que este número faz com o eixo* x *é* $\theta = 0$. *Sendo assim, pela fórmula de De Moivre tem-se que as raízes complexas do número 1 são:*

$$\begin{aligned}
z_1 &= cos\left(\frac{2\pi}{5}\right) + isen\left(\frac{2\pi}{5}\right);\\
z_2 &= cos\left(\frac{4\pi}{5}\right) + isen\left(\frac{4\pi}{5}\right);\\
z_3 &= cos\left(\frac{6\pi}{5}\right) + isen\left(\frac{6\pi}{5}\right);\\
z_4 &= cos\left(\frac{8\pi}{5}\right) + isen\left(\frac{8\pi}{5}\right);\\
z_5 &= cos\left(\frac{10\pi}{5}\right) + isen\left(\frac{10\pi}{5}\right)\\
&= cos(2\pi) + isen(2\pi) = 1 + 0i = 1.
\end{aligned}$$

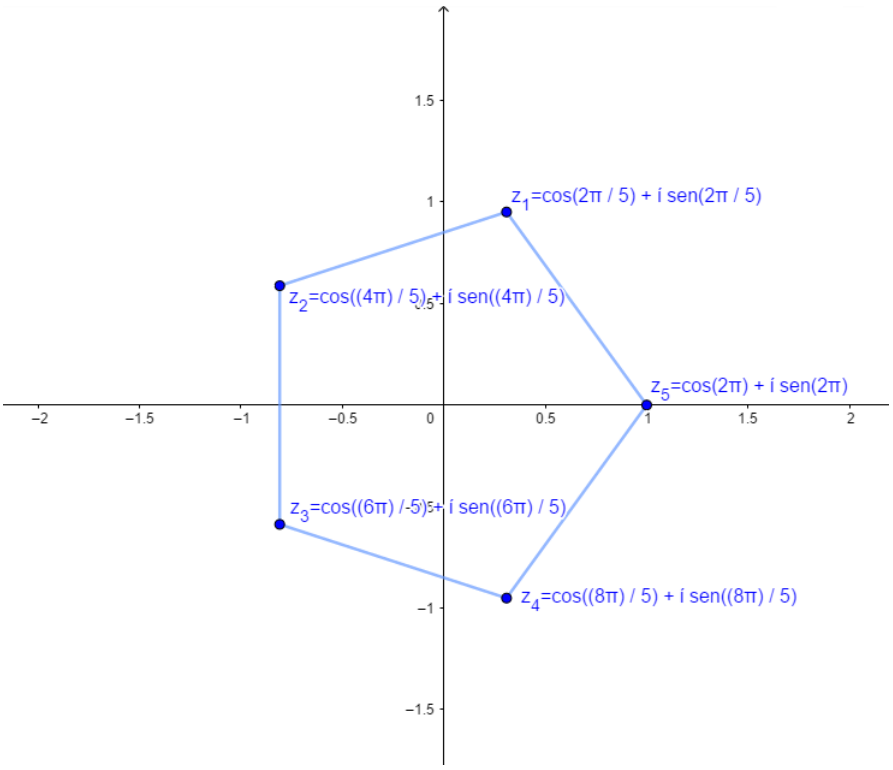

Figura 14 – Pentágono Regular

Fonte: Compilado pelo autor

O exemplo mostra que as raízes de $z^5 = 1$ formam os vértices de um pentágono regular. Na sequência justificaremos porque o pentagono regular é construtível.

Antes, lembramos que um polígono é construtível se seus vértices são construtíveis. Como os vértíces de um polígono regular são as raízes da unidade, então este polígono só

será construtível se o número complexo que representa a raiz da unidade for construtível, ou seja, se $z_k = cos\left(\frac{2k\pi}{n}\right) + isen\left(\frac{2k\pi}{n}\right)$, para $k = 0, 1, \cdots, n-1$ for construtível. Isto equivale a dizer que $cos\left(\frac{2k\pi}{n}\right)$ é construtível, como também é equivalente dizer que $2cos\left(\frac{2k\pi}{n}\right) = z_k + \frac{1}{z_k}$ é construtível.

Demonstraremos esta última igualdade.

Lema 1. *Seja* $z_k = cos\left(\frac{2k\pi}{n}\right) + isen\left(\frac{2k\pi}{n}\right)$, *então* $2cos\left(\frac{2k\pi}{n}\right) = z_k + \frac{1}{z_k}$.

Demonstração. Temos que

$$\begin{aligned}
\left(z_k + \frac{1}{z_k}\right) &= cos\left(\frac{2k\pi}{n}\right) + isen\left(\frac{2k\pi}{n}\right) + \frac{1}{cos\left(\frac{2k\pi}{n}\right) + isen\left(\frac{2k\pi}{n}\right)} \\
&= \frac{cos\left(\frac{2k\pi}{n}\right)\left[cos\left(\frac{2k\pi}{n}\right) + isen\left(\frac{2k\pi}{n}\right)\right] + isen\left(\frac{2k\pi}{n}\right)\left[cos\left(\frac{2k\pi}{n}\right) + isen\left(\frac{2k\pi}{n}\right)\right] + 1}{cos\left(\frac{2k\pi}{n}\right) + isen\left(\frac{2k\pi}{n}\right)} \\
&= \frac{cos^2\left(\frac{2k\pi}{n}\right) - sen^2\left(\frac{2k\pi}{n}\right) + 2icos\left(\frac{2k\pi}{n}\right)sen\left(\frac{2k\pi}{n}\right) + 1}{cos\left(\frac{2k\pi}{n}\right) + isen\left(\frac{2k\pi}{n}\right)}
\end{aligned}$$

Utilizando que, $cos^2\left(\frac{2k\pi}{n}\right) + sen^2\left(\frac{2k\pi}{n}\right) = 1$, teremos:

$$\begin{aligned}
\left(z_k + \frac{1}{z_k}\right) &= \frac{cos^2\left(\frac{2k\pi}{n}\right) - sen^2\left(\frac{2k\pi}{n}\right) + 2icos\left(\frac{2k\pi}{n}\right)sen\left(\frac{2k\pi}{n}\right) + cos^2\left(\frac{2k\pi}{n}\right) + sen^2\left(\frac{2k\pi}{n}\right)}{cos\left(\frac{2k\pi}{n}\right) + isen\left(\frac{2k\pi}{n}\right)} \\
&= \frac{2cos^2\left(\frac{2k\pi}{n}\right) + 2icos\left(\frac{2k\pi}{n}\right)sen\left(\frac{2k\pi}{n}\right)}{cos\left(\frac{2k\pi}{n}\right) + isen\left(\frac{2k\pi}{n}\right)} \\
&= 2cos\left(\frac{2k\pi}{n}\right)\left[\frac{cos(\frac{2k\pi}{n}) + isen(\frac{2k\pi}{n})}{cos(\frac{2k\pi}{n}) + isen(\frac{2k\pi}{n})}\right] \\
&= 2cos\left(\frac{2k\pi}{n}\right).
\end{aligned}$$

□

Dessa forma, para verificarmos se as raízes da equação $z^n = 1$ são construtíveis, basta verificar se o número $2cos\left(\frac{2k\pi}{n}\right)$ é construtível.

Em resumo, estamos obtendo que o polígono regular de n lados é construtível se e somente se, e as raízes da equação

$$(z-1)(z^{n-1} + z^{n-2} + \cdots + 1) = 0$$

são construtíveis. A seguir utilizaremos este critério para mostrar se alguns polígonos são ou não construtíveis:

Triângulo Equilátero

O problema de verificar se o triângulo equilátero é construtível ou não é equivalente ao problema de verificar se é possível construir as raízes da equação $z^3 = 1$ ou não. Para tal verificação, neste caso, por ser uma equação do terceiro grau, ou podemos utilizar o critério mencionado acima ou podemos apenas encontrar as raízes z_1, z_2 e z_3 que satisfazem tal equação.

Sendo assim,

$$z^3 - 1 = 0 \Rightarrow (z-1)(z^2 + z + 1) = 0$$

$$\Rightarrow z - 1 = 0 \text{ e } z^2 + z + 1 = 0.$$

Utilizando Bháskara, tem-se que as raízes cúbicas da unidade são: $z_0 = 1, z_1 = \dfrac{-1 + \sqrt{3}i}{2}$ e $z_2 = \dfrac{-1 - \sqrt{3}i}{2}$.

Observe que estas raízes quando colocadas no plano complexo são exatamente os pontos $(1, 0), \left(\dfrac{-1}{2}, \dfrac{\sqrt{3}}{2}\right), \left(\dfrac{-1}{2}, \dfrac{-\sqrt{3}}{2}\right)$, na qual, pela Proposição 1 são coordenadas construtíveis, logo são pontos construtíveis e consequentemente, o triângulo equilátero é construtível.

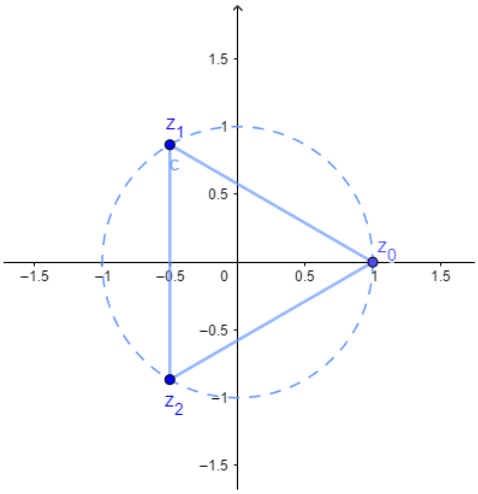

Figura 15 – Triângulo Equilátero

Fonte: Compilado pelo autor

Pentágono Regular

Para descobrir se o pentágono regular é construtível, basta utilizarmos o critério mencionado anteriormente, isto é, basta descobrir se as raízes da equação $z^5 - 1 = 0$ são construtíveis. Para isso,

$$z^5 - 1 = 0 \Rightarrow (z-1)(z^4 + z^3 + z^2 + z + 1) = 0$$

$$\Rightarrow z - 1 = 0 \text{ e } z^4 + z^3 + z^2 + z + 1 = 0$$

Sabendo-se que 1 é raiz da equação acima, agora precisamos encontrar as demais raízes z_k que satisfazem a equação $z_k^4 + z_k^3 + z_k^2 + z_k + 1 = 0$, tal que $z_k + \dfrac{1}{z_k} = 2cos\left(\dfrac{2k\pi}{5}\right)$.

Dividindo a equação $z_k^4 + z_k^3 + z_k^2 + z_k + 1 = 0$ por z_k^2 tem-se:

$$z_k^2 + z_k + 1 + \frac{1}{z_k} + \frac{1}{z_k^2} = 0.$$

Reorganizando a equação

$$\left(z_k + \frac{1}{z_k}\right) + \left(z_k^2 + \frac{1}{z_k^2}\right) + 1 = 0.$$

Agora, chamando $z_k + \dfrac{1}{z_k} = a$, temos que a equação acima pode ser reescrita numa nova variável:

$$a + a^2 - 2 + 1 = 0 \Rightarrow a^2 + a - 1 = 0.$$

Utilizando Bháskara, encontramos que as raízes do polinômio acima são $a = \dfrac{-1 \pm \sqrt{5}}{2}$. Observe que, pelas Proposições 1 e 2 ambas são números construtíveis.

Portanto, como $z_k + \dfrac{1}{z_k} = 2cos\left(\dfrac{2k\pi}{5}\right)$, temos que $2cos\left(\dfrac{2k\pi}{5}\right)$ é construtível e consequentemente, o pentágono é construtível.

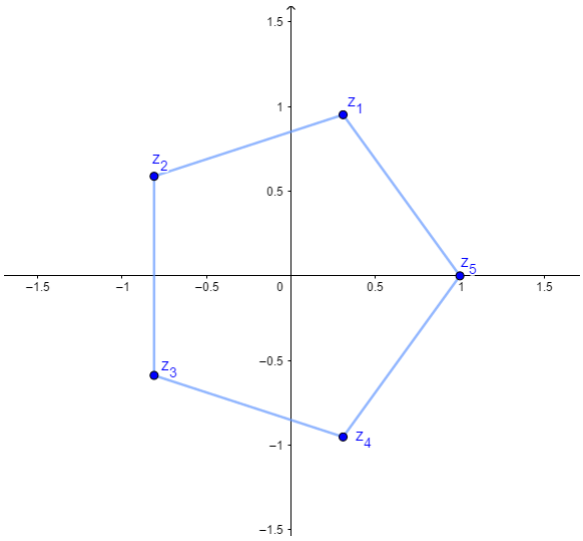

Figura 16 – Pentágono Regular

Fonte: Compilado pelo autor

Heptágono Regular

Como no exemplo anterior, para descobrimos se o heptágono é construtível, basta descobrirmos se as raízes da equação $z^7 - 1 = 0$ são construtíveis. Assim,

$$z^7 - 1 = 0 \Rightarrow (z-1)(z^6 + z^5 + z^4 + z^3 + z^2 + z + 1) = 0$$

$$\Rightarrow z - 1 = 0 \text{ e } z^6 + z^5 + z^4 + z^3 + z^2 + z + 1 = 0.$$

Como anteriormente, sabemos que 1 é raiz da equação acima, porém além desta, queremos encontrar as demais raízes z_k que satisfazem a equação $z_k^6 + z_k^5 + z_k^4 + z_k^3 + z_k^2 + z_k + 1 = 0$ e que $z_k + \dfrac{1}{z_k} = 2cos\left(\dfrac{2k\pi}{7}\right)$. Dessa forma, dividindo a equação anterior por z_k^3 tem-se:

$$z_k^3 + z_k^2 + z_k + 1 + \frac{1}{z_k} + \frac{1}{z_k^2} + \frac{1}{z_k^3} = 0.$$

Reorganizando a equação anterior:

$$\left(z_k^3 + \frac{1}{z_k^3}\right) + \left(z_k^2 + \frac{1}{z_k^2}\right) + \left(z_k + \frac{1}{z_k}\right) + 1 = 0.$$

Chamando $z_k + \dfrac{1}{z_k} = a$, temos que a equação anterior pode ser reescrita na nova variável a:

$$(a^3 - 3a) - (a^2 - 2) + a + 1 = 0 \Rightarrow a^3 + a^2 - 2a - 1 = 0.$$

De acordo com o Teorema 7 tem-se que, uma possível raiz do polinômio acima são 1 ou -1. Considerando $p(a) = a^3 + a^2 - 2a - 1$, observe que $p(1) = -1$ e $p(-1) = 1$, isto é, 1 e

-1 não são raízes do polinômio $p(a)$. Dessa forma, pela Proposição 13 segue que $p(a)$ não possui raízes racionais, consequentemente as raízes de $p(a)$ não são construtíveis. Logo, não é possível construir o Heptágono.

Eneágono Regular

Com o raciocínio análogo, para descobrir se o eneágono é construtível, descobriremos se as raízes da equação $z^9 - 1 = 0$ são números construtíveis. Dessa forma,

$$z^9 - 1 = 0 \Rightarrow (z-1)(z^8 + z^7 + z^6 + z^5 + z^4 + z^3 + z^2 + z + 1) = 0$$

$$\Rightarrow z - 1 = 0 \text{ e } z^8 + z^7 + z^6 + z^5 + z^4 + z^3 + z^2 + z + 1 = 0.$$

Como nos casos anteriores, sabemos que 1 é raíz da equação acima, porém além desta, queremos encontrar as demais raízes z_k que satisfazem a equação $z_k^8 + z_k^7 + z_k^6 + z_k^5 + z_k^4 + z_k^3 + z_k^2 + z_k + 1 = 0$ e que $z_k + \dfrac{1}{z_k} = 2cos\left(\dfrac{2k\pi}{9}\right)$. Sendo assim, dividindo a equação anterior por z_k^4 tem-se:

$$z_k^4 + z_k^3 + z_k^2 + z_k + 1 + \frac{1}{z_k} + \frac{1}{z_k^2} + \frac{1}{z_k^3} + \frac{1}{z_k^4} = 0.$$

Reorganizando seus termos:

$$\left(z_k^4 + \frac{1}{z_k^4}\right) + \left(z_k^3 + \frac{1}{z_k^3}\right) + \left(z_k^2 + \frac{1}{z_k^2}\right) + \left(z_k + \frac{1}{z_k}\right) + 1 = 0.$$

Agora, chamando $z_k + \dfrac{1}{z_k} = a$, podemos reescrever a equação anterior em função da variável a:

$$(a^4 - 4a^2 + 2) + (a^3 - 3a) + (a^2 - 2) + a + 1 = 0$$

$$\Rightarrow a^4 + a^3 - 3a^2 - 2a + 1 = 0.$$

Observe que o polinômio acima pode ser fatorado da seguinte maneira

$$(a+1)(a^3 - 3a + 1) = 0.$$

Agora, analisando o polinômio $q(a) = a^3 - 3a + 1$, tem-se pelo Teorema 7 que uma possível raiz deste polinômio são 1 ou -1. Porém, observe que $q(1) = -1$ e $q(-1) = 3$. Portanto, pela Proposição 13 conclui-se que $q(a)$ não possui raízes racionais, logo suas raízes não são construtíveis e consequentemente, o eneágono não é construtível.

Proposição 15. *Sejam m e n primos entre si. O polígono $P_{m\cdot n}$ de $m\cdot n$ lados é construtível se, e somente se, os polígonos de m e n lados, P_m e P_n, respectivamente são construtíveis.*

Demonstração. Por um lado, seja P_{mn} o polígono de mn lados construtível. Assim, tem-se na circunferência mn pontos equidistantes. Para obter o polígono P_m de m lados, basta ligar os m pontos existentes na circunferência anterior, de forma que estes sejam pontos equidistantes entre si. Da mesma forma, para obter o polígono P_n de n lados, basta unir os n pontos da circunferência de maneira que estes também sejam equidistantes entre si. Assim, teremos construídos os polígonos P_m e P_n.

Por outro lado, sejam P_m e P_n polígonos construtíveis de m e n lados respectivamente. Assim, é possível construir os ângulos centrais $\frac{2\pi}{m}$ e $\frac{2\pi}{n}$, e é desejável mostrar que é possível construir o ângulo central $\frac{2\pi}{mn}$.

Antes de prosseguir com a demonstração desta proposição, é necessário relembrar o Teorema de Bachet Bézout que diz:

$$\textit{Dados } a, b \in \mathbb{Z}\textit{, então existem } x, y \in \mathbb{Z} \textit{ tais que } ax + by = mdc(a, b).$$

Agora, por hipótese tem-se que m, n são primos entre si, isto é, $mdc(m, n) = 1$. Dessa forma, pelo teorema enunciado acima, existem $x, y \in \mathbb{Z}$ tais que:

$$mx + by = 1$$

Daí, multiplicando a equação acima por 2π e dividindo-a por mn tem-se:

$$\frac{2\pi mx}{mn} + \frac{2\pi ny}{mn} = \frac{2\pi}{mn} \Rightarrow \frac{2\pi x}{n} + \frac{2\pi y}{m} = \frac{2\pi}{mn}.$$

Note que, do lado esquerdo da igualdade tem-se a soma de dois números construtíveis, que são os ângulos centrais dos polígonos P_n e P_m respectivamente. E, do lado direito da igualdade, tem-se o resultado da soma de dois números construtíveis, logo, este também será um número construtível, e novamente, observe que este é o ângulo central do polígono P_{mn} de mn lados. Portanto, P_{mn} é construtível, pois se os ângulos centrais são construtíveis então o polígono é construtível. Como desejávamos. □

6.1.2 Critério geral de construtibilidade

Nesta seção enunciaremos o teorema que estabelece condições sobre n para que o polígono regular de n lados seja construtível.

A prova deste teorema reúne alguns elementos que não estudamos neste texto. De qualquer forma, por se tratar de um belo teorema que encerra satisfatoriamente este trabalho, enunciamos alguns resultados, que encadeados corretamente, permite ao leitor um bom entendimento da demonstração.

O teorema o qual referimos diz:

Se o polígono regular de n lados for construtível, então n se fatora na forma $n = 2^b \cdot p_1 \cdot p_2 \cdots p_r$, *sendo* p_i *primos de Fermat distintos.*

Os resultados que seguem, fornecerão as ideias para a demonstração do teorema citado.

Lema 2. *Considere o inteiro positivo* $p = 2^r + 1$ *com* $r > 0$. *Se p for um número primo, então* $r = 2^k$, $k \in \mathbb{N}$.

Demonstração. Suponhamos que $r \neq 2^k$. Portanto, podemos escrever que $r = 2^t \cdot s$ com $t, s \in \mathbb{N}$ e s um número ímpar diferente de 1. Assim:

$$p = 2^r + 1 = 2^{2^{t} \cdot s} + 1 = (2^{2^t})^s + 1 = (2^{2^t} + 1) \cdot [(2^{2^t})^{s-1} - (2^{2^t})^{s-2} + \cdots \pm 1]$$

Isto mostra que p é composto, o que contradiz a hipótese. Portanto, $r = 2^k$. □

Primos dessa forma são denominados primos de Fermat. A recíproca da proposição é falsa! (k=5).

Definição 22. *A função* ϕ *de Euler associa a cada inteiro positivo n a quantidade de inteiros positivos menores que n que são coprimos com n*

$$\phi(n) := \sharp\{a \in \mathbb{N} \colon \text{mdc}(a, n) = 1 \text{ e } 1 \leq a \leq n\}.$$

Observação 5. *Se* a, b *são primos entre si então* $\phi(ab) = \phi(a) \cdot \phi(b)$.

Pelo princípio da inclusão e exclusão é possível provar o teorema abaixo:

Teorema 8. *O valor de* $\phi(m)$ *é dado por:*

$$\phi(m) = m\left(1 - \frac{1}{p_1}\right) \cdot \left(1 - \frac{1}{p_2}\right) \cdots \left(1 - \frac{1}{p_r}\right)$$

sendo $p_1, p_2, \cdots, p_r$ *os divisores primos de m.*

Demonstração. Vide Introdução a Análise Combinatória (SANTOS; MELLO; MURARI, 2007), de José Plínio de Oliveira Santos . □

Proposição 16. *Se* $\phi(m) = 2^b$, *então* $m = 2^a \cdot p_1 \cdot p_2 \cdots p_s$, *sendo* $p_i = 2^{b_i} + 1$ *primos de Fermat.*

Demonstração. Por hipótese, temos que $\phi(m) = 2^b$ e utilizando o Teorema 8 podemos escrever a seguinte igualdade

$$\begin{aligned} \phi(m) &= m\left(1 - \frac{1}{p_1}\right) \cdot \left(1 - \frac{1}{p_2}\right) \cdot \ldots \cdot \left(1 - \frac{1}{p_r}\right) = 2^b \\ \Rightarrow \phi(m) &= m\left(\frac{p_1 - 1}{p_1}\right) \cdot \left(\frac{p_2 - 1}{p_2}\right) \cdot \ldots \cdot \left(\frac{p_r - 1}{p_r}\right) = 2^b \end{aligned}$$

na qual cada $p_i's$ são fatores primos de m distintos entre si. Assim, seja a seguinte decomposição de m em fatores primos

$$m = 2^{\alpha_0} \cdot p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot ... \cdot p_r^{\alpha_r}, \text{ com } \alpha_0 \neq 0.$$

Dessa forma,

$$2^{\alpha_0} \cdot p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot ... \cdot p_r^{\alpha_r} \cdot \left(\frac{p_1 - 1}{p_1}\right) \cdot \left(\frac{p_2 - 1}{p_2}\right) \cdot ... \cdot \left(\frac{p_r - 1}{p_r}\right) = 2^b$$

$$\Rightarrow 2^{\alpha_0} \cdot p_1^{\alpha_1 - 1} \cdot p_2^{\alpha_2 - 1} \cdot ... \cdot p_r^{\alpha_r - 1} \cdot (p_1 - 1) \cdot (p_2 - 1) \cdot ... \cdot (p_r - 1) = 2^b \tag{6.1}$$

Agora analisando a igualdade acima (equação 6.1, do lado direito há apenas o termo 2^b e cada $p_i's$, do lado esquerdo, são distintos entre si e diferentes de 2, logo, segue que cada $\alpha_i - 1 = 0$, ou seja, $\alpha_i = 1$. Com isso, tem-se que

$$m = 2^{\alpha_0} \cdot p_1 \cdot p_2 \cdot ... \cdot p_r$$

como é desejado.

Novamente, como do lado direito da igualdade (equação 6.1) há apenas potência de 2, é necessário que cada $p_i - 1$ também seja potência de 2, ou seja, $p_i - 1 = 2^{b_i}$ para algum $b_i \in \mathbb{N}$. Nessa condição, temos que cada $p_i = 2^{b_i} + 1$, que é um primo de Fermat. Como queríamos demonstrar. □

Definição 23 (Raiz primitiva)**.** *Chama-se raiz $n-$ésima primitiva da unidade qualquer raiz $n-$ésima $z \neq 1$ tal que n é o menor inteiro positivo tal que $z^n = 1$.*

Abaixo exemplificamos os conceitos de raiz n-ésima da unidade e raiz primitiva da unidade.

Exemplo 12. *Encontre as raízes primitivas da equação $z^6 = 1$.*

Sabemos que as raízes da unidade de $z^6 = 1$ são

$$\begin{aligned}
z_1 &= cos\left(\frac{2\pi}{6}\right) + isen\left(\frac{2\pi}{6}\right) = \frac{1}{2} + \frac{\sqrt{3}}{2}i; \\
z_2 &= cos\left(\frac{4\pi}{6}\right) + isen\left(\frac{4\pi}{6}\right) = -\frac{1}{2} + \frac{\sqrt{3}}{2}i; \\
z_3 &= cos\left(\frac{6\pi}{6}\right) + isen\left(\frac{6\pi}{6}\right) = -1; \\
z_4 &= cos\left(\frac{8\pi}{6}\right) + isen\left(\frac{8\pi}{6}\right) = -\frac{1}{2} - \frac{\sqrt{3}}{2}i; \\
z_5 &= cos\left(\frac{10\pi}{6}\right) + isen\left(\frac{10\pi}{6}\right) = \frac{1}{2} - \frac{\sqrt{3}}{2}i; \\
z_6 &= cos\left(\frac{12\pi}{6}\right) + isen\left(\frac{12\pi}{6}\right) = 1.
\end{aligned}$$

No entanto, observe que as raízes da unidade da equação $w^3 = 1$ *são*

$$\begin{aligned} w_1 &= cos\left(\frac{2\pi}{3}\right) + isen\left(\frac{2\pi}{3}\right) = -\frac{1}{2} + \frac{\sqrt{3}}{2}i; \\ w_2 &= cos\left(\frac{4\pi}{3}\right) + isen\left(\frac{4\pi}{3}\right) = -\frac{1}{2} - \frac{\sqrt{3}}{2}i; \\ w_3 &= cos\left(\frac{6\pi}{3}\right) + isen\left(\frac{6\pi}{3}\right) = 1. \end{aligned}$$

Desta forma, temos que as raízes w_1, w_2 *e* w_3 *são iguais as raízes* z_2, z_4 *e* z_6 *respectivamente, logo estas não são as raízes primitivas da equação* $z^6 = 1$*, pois existe* $n = 3$ *tal que* $z_i^3 = 1$ *para* $i = 2, 4, 6$*. E observe que* $z_3 = -1$ *e* $z_6 = 1$ *também não são raízes primitivas, pois existe* $m, p < 6$ *tal que* $z^m = 1$ *e* $z^p = -1$*. Agora, a cargo do leitor, pode-se verificar que não existe* n *com* $3 < n < 6$ *tal que* $z_1^n = 1$ *ou* $z_5^n = 1$*. Portanto, concluímos que as raízes primitivas de* $z^6 = 1$ *são* z_1, z_5*.*

Proposição 17. *Se* z *é uma raiz enésima primitiva da unidade então as raízes enésimas primitivas da unidade são as raízes* z^i*, na qual* $i < n$ *e* $mdc(i, n) = 1$*.*

Demonstração. De fato, tomamos m como sendo o menor inteiro positivo tal que $(z^i)^m = z^{im} = 1$. Pelo algoritmo da divisão existem q e r, em que $im = qn + r$ e $0 \leq r < n$. Assim, $z^r = z^{im} \cdot z^{-qn} = 1 \cdot 1 = 1$. Pela definição da raiz enésima primitiva, temos que n é o menor inteiro com a propriedade qie $z^n = 1$. Portanto, $r = 0$, ou seja, $im = nq$. Logo, n é um inteiro que divide o produto im, porém como $mdc(i, n) = 1$, temos que n divide m. O fato de que $m \leq n$ implica que $n = m$. □

Observação 6. *Observe que de acordo com a Proposição 17, a quantidade de raízes enésimas primitivas da equação* $z^n = 1$ *é exatamente* $\phi(n)$*.*

Vimos no início do subcapítulo de Raízes da Unidade (Subcapítulo 6.1.1), que se $z_1 = cos\left(\frac{2\pi}{n}\right) + isen\left(\frac{2\pi}{n}\right)$ é raiz da unidade então as outras raízes são dadas por $w_k = z_1^k$, na qual $k = 0, 1, ..., n-1$.

O conjunto das enésimas raízes da unidade $U_n = \{z_1, z_2, ..., z_n^{n-1}, z_n^n = 1\}$ é o grupo cíclico das enésimas raízes da unidade. Um gerador ψ para este grupo é uma raiz enésima primitiva da unidade.

Na página 278 do livro do Serg-Lang (Referência (LANG et al., 2002)), temos a prova do seguinte teorema:

Teorema 9. *Seja* ψ *uma raiz enésima primitiva da unidade, então* $[\mathbb{Q}[\psi] : \mathbb{Q}] = \phi(n)$*, na qual* ϕ *é a função de Euler.*

A partir destes resultados conseguimos obter as ideias principais que nos auxiliará na construção da demonstração do teorema abaixo.

Teorema 10. *Se o polígono regular de n lados for construtível, então n se fatora na forma* $n = 2^b \cdot p_1 \cdot p_2 \cdots p_r$*, sendo* p_i *primos de Fermat distintos.*

Demonstração. Seja P_n um polígono regular de n lados construtível, assim os $z_i's$ vértices desse polígono são raízes da unidade da equação $z^n = 1$. Além disso, como cada z_i é um ponto construtível do plano, temos pelo teorema 6 que o grau da extensão $\mathbb{Q}[z_i]$ é uma potência de 2, ou seja, $[\mathbb{Q}[z_i] : \mathbb{Q}] = 2^j$ para algum $j \in \mathbb{N}$.

Por outro lado, para cada w_i, segue pelo teorema 9 que $\phi(n) = [\mathbb{Q}[w_i] : \mathbb{Q}]$. Logo, $\phi(n) = 2^j$. E portanto pela proposição 16, $n = 2^a \cdot p_1 \cdot p_2 \cdot ... \cdot p_s$ na qual cada p_i é um primo de Fermat, como desejávamos.

□

7 Apêndice I

7.1 O arco capaz

Neste subcapítulo vamos definir o que é O Arco Capaz e faremos a sua construção. Mas antes disso, devemos aprender, a partir da construção geométrica, como transportar um ângulo de um lugar para o outro. Lembrando que nossas construções só são feitas com régua e compasso, logo, não podemos usar transferidor ou qualquer outra ferramenta diferente das que citamos acima para obtermos estes ângulos.
Então seja β o ângulo dado, de vértice O, e suponhamos que desejamos construir o ângulo B$\hat{A}$X=β. Para isso, seguiremos os seguintes passos:

- De centro no vértice O do ângulo β, traçamos uma circunferência de raio qualquer. Percebemos que a circunferência intercepta os lados do ângulo β em dois pontos, estas interseções as denominamos por P e Q.
- Com o raio de mesma medida, traçamos outra circunferência de centro A, percebemos que a circunferência interceptará na semi-reta AB, este ponto denominaremos por P'.
- Logo, tracemos uma circunferência de centro P' e raio PQ. Observe que haverá duas intercessões entre as duas circunferências traçadas, escolhemos uma interseção e denominamos por Q'.
  Assim temos que, B$\hat{A}$X = P'$\hat{A}$Q'= β.

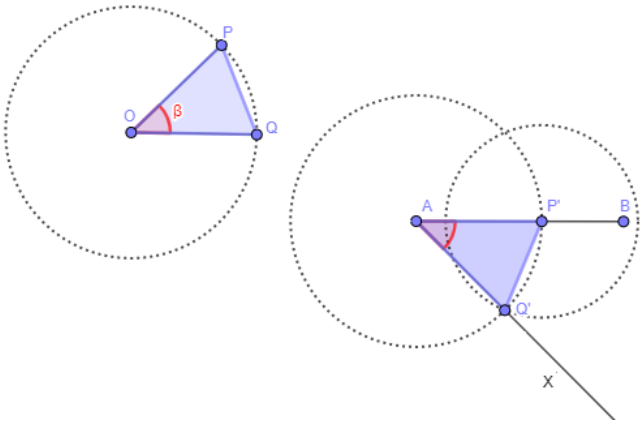

Figura 17 – Transporte de um ângulo

Fonte: Compilado pelo autor

Demonstração. Sejam, POQ e $P'AQ'$ triângulos, por construção sabemos que os lados PQ e $P'Q'$ possuem mesmas medidas. Sabemos também por construção que, $OP = OQ$, $AP' = AQ'$ e que $OP = AP'$(pois, por construção OP e AP' são raios de mesmo tamanho de circunferências distintas), logo temos que $OP = OQ = AP' = AQ'$. Sendo assim, temos que os triângulos POQ e $P'AQ'$ são congruentes, logo, seus ângulos internos são iguais. □

Agora que já sabemos como transportar um ângulo, vamos conhecer um pouco mais sobre O Arco Capaz. Sejam dois pontos A e B pertencentes a circunferência. Para todo ponto O' sobre um dos arcos da circunferência, temos que o ângulo $A\hat{O}'B = \beta$ é sempre constante. Chama-se $\widehat{AO'B}$ de o arco capaz do ângulo β sobre o segmento AB. Observação: Se existir um ponto E pertencente a outro arco da circunferência, o ângulo AÊB também será constante e igual a $180 - \beta$. Caso AB seja diâmetro da circunferência, temos que $\beta = 90°$.

- Sejam A e B dois pontos sobre a circunferência e seja AB o segmento de reta. Traçamos a mediatriz de AB e o ângulo BÂX= β (dado). O ponto de interseção da mediatriz com o segmento AB denominamos por C.
- Feito isso traçamos a perpendicular à reta AX, passando pelo ponto A.
- Com isso, observe que a perpendicular interceptará a mediatriz em um ponto, este ponto denominamos por O. Dessa forma, o arco de centro O e extremidades A e B, situado no semi plano oposto ao ponto X (referente ao segmento de reta AB), é o arco capaz do ângulo β sobre AB.

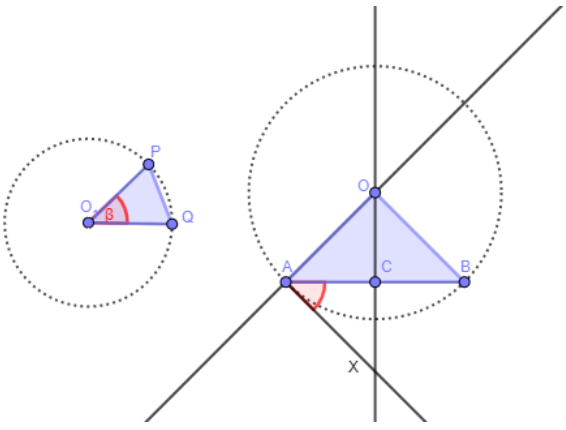

Figura 18 – O arco capaz

Fonte: Compilado pelo autor

Demonstração. Observando o triângulo AOC temos que $\widehat{C} = 90°$, pois a mediatriz (reta que passa por OC) do segmento AB é a reta que passa pelo ponto médio do segmento, formando um ângulo de 90°. Temos também que O$\hat{A}$C $= 90 - \beta$, logo $A\hat{O}C = \beta$. Se $A\hat{O}C = \beta$ então $A\hat{O}B = 2\beta$.

Sabemos que A$\hat{O}$B é o ângulo central e que todo ângulo inscrito em um círculo mede metade do ângulo central, portanto para qualquer ponto O' sobre o arco $\widehat{AB}$ (oposto ao segmento de reta AB), $\hat{O}' = \beta$. □

7.2 Divisão de um segmento em partes iguais

Seja AB um segmento de reta qualquer, na qual queremos dividi-lo em 3 partes iguais.

- Traçamos uma semi-reta AX e, sobre ela construímos 3 segmentos de medidas iguais. Para isso, trace uma circunferência de centro A e raio arbitrário, esta interceptará a reta AX em um ponto, denomine este ponto por A_1. Novamente, trace uma circunferência de centro A_1 e raio com mesma medida da circunferência traçada anteriormente, o ponto de interseção com a reta AX, denomine por A_2. De forma análoga, realize estes passos até obter os três segmentos de medidas iguais (vide Figura 19).
  Observação: Se quiséssemos dividir o segmento AB em 4 partes iguais, construiríamos sobre a semi-reta 4 segmentos iguais, pensamento análogo se quisermos dividir o segmento AB em n partes iguais, onde n $\in \mathbb{N}$.

- Os pontos de interseção da semi-reta com os segmentos que acabamos de construir denominamos por A_1, A_2 e A_3 respectivamente.

- Traçamos o segmento de reta A_3B.

- Feito isso, traçamos retas paralelas a A_3B, uma passando pelo ponto A_2 e outra passando pelo ponto A_1. Estas retas determinaram em AB os pontos B_1 e B_2 que o dividiram em 3 partes iguais.

Demonstração. Analisando os triângulos ABA_3, AB_2A_2 e AB_1A_1 (vide Figura 19), podemos dizer que os ângulos correspondentes $\widehat{B}, \widehat{B_2}$ e $\widehat{B_1}$ possuem mesma medida, pois as retas $\overleftrightarrow{BA_3}, \overleftrightarrow{B_2A_2}$ e $\overleftrightarrow{B_1A_1}$ são paralelas e estão cortadas pela reta $\overleftrightarrow{BA}$ transversal, logo os ângulos correspondentes determinados são congruentes. De maneira análoga, os ângulos $\widehat{A_3}, \widehat{A_2}$ e $\widehat{A_1}$ também possuem a mesma medida. Dessa forma, pelo caso de semelhança Ângulo Ângulo (AA), concluímos que os triângulos ABA_3, AB_2A_2 e AB_1A_1 são semelhantes, e consequentemente seus lados homólogos são proporcionais, isto é, os lados dos triângulos que estão opostos aos ângulos de mesma medida são proporcionais. Sem perda

de generalidade, observemos os triângulos AB_2A_2 e AB_1A_1, por serem semelhantes, então é válida a seguinte igualdade:

$$\frac{AA_2}{AA_1} = \frac{AB_2}{AB_1}. \tag{7.1}$$

Porém anteriormente, construímos os segmentos AA_1, A_1A_2 e A_2A_3 com medidas iguais, logo segue que $AA_2 = 2AA_1$ e pela equação 7.1 tem-se

$$\frac{2AA_1}{AA_1} = \frac{AB_2}{AB_1} \Rightarrow \frac{AB_2}{AB_1} = 2 \Rightarrow AB_2 = 2AB_1.$$

No entanto $AB_2 = AB_1 + B_1B_2$, então □

$$AB_2 = 2AB_1 \Rightarrow AB_1 + B_1B_2 = AB_1 + AB_1 \Rightarrow B_1B_2 = AB_1$$

ou seja, concluímos que os segmentos de reta B_1B_2 e AB_1, que foram construídos, são iguais. Da mesma maneira, mostramos que os segmentos B_2B e B_1B_2 também possuem mesma medida, como desejávamos.

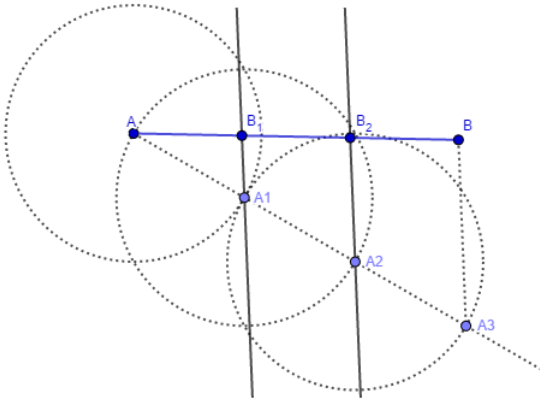

Figura 19 – Divisão de segmentos em partes iguais

Fonte: Compilado pelo autor

7.3 Traçado das tangentes a um círculo

Neste subcapítulo, iremos apresentar dois possíveis casos de construção das retas tangentes a um círculo. Lembrando que, a condição de existência da reta tangente a uma circunferência é que ela seja perpendicular ao raio desta circunferência.

Caso 1: Ponto P pertencente a circunferência.

Dado a circunferência λ e um ponto P sobre ela, queremos traçar a reta tangente a esta circunferência passando pelo ponto P. Desta forma, seja C o centro desta circunferência e seja r o seu raio.

- Tracemos uma semirreta que tem origem no ponto C e passa pelo ponto P.

- tracemos uma reta perpendicular a esta semirreta passando por P, esta reta, denominamos por reta s.

Assim, temos que a reta s é a reta tangente à circunferência λ.

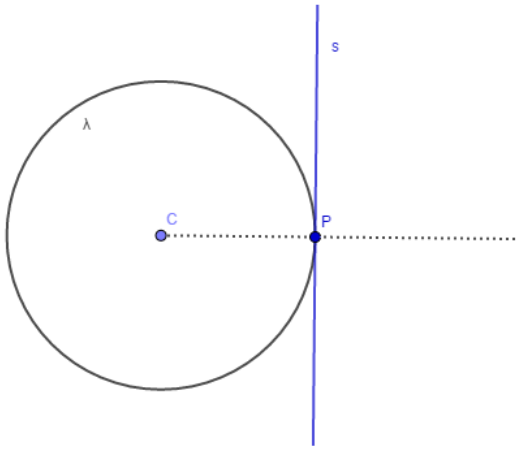

Figura 20 – Traçado da tangente pelo ponto pertencente à circunferência

Fonte: Compilado pelo autor

Demonstração. Observemos que a semirreta que passa por CP contém o raio da circunferência λ e posteriormente traçamos uma reta perpendicular a essa semireta, dessa forma, temos que esta reta também é perpendicular ao raio r de λ. Pela condição de existência da reta tangente, temos que ela sempre será perpendicular ao raio no seu ponto de tangência. □

Caso 2: Ponto P exterior a circunferência.

Dado a circunferência α de centro O e um ponto P exterior a ela, queremos traçar a reta tangente a esta circunferência passando pelo ponto P.

- Traçamos o segmento PO e em seguida determinamos o ponto médio deste segmento. Denominamos este ponto por M.
- Com o centro M e raio MO, traçamos a circunferência β. Observe que as circunferências β e α se interceptam em dois pontos, estes denominamos por A e A'.

Logo, temos que as retas $\overleftrightarrow{PA}$ e $\overleftrightarrow{PA'}$ são tangentes a circunferência α passando pelo ponto P.

Demonstração. Com relação a circunferência β, observe que $\widehat{PAO}$ é um ângulo inscrito na circunferência β sobre o diâmetro PO, logo $\widehat{PAO} = 90°$. Sendo assim, tem-se que a

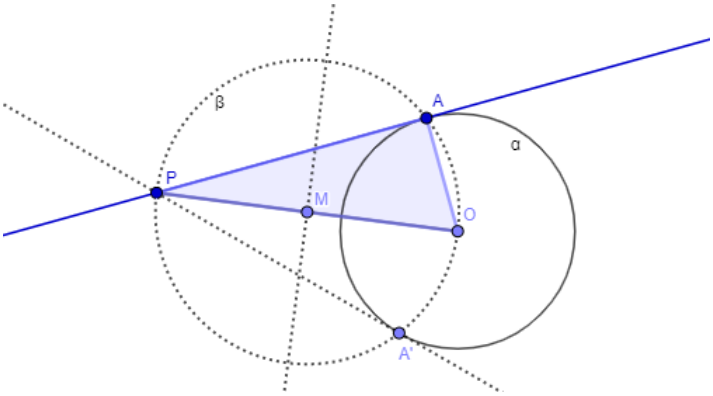

Figura 21 – Traçado da tangente pelo ponto exterior à circunferência

Fonte: Compilado pelo autor

reta PA é perpendicular ao raio AO da circunferência α, com outras palavras, PA é a reta tangente a circunferência α. Análogo para o ponto A'.

□

8 Apêndice II

Neste apêndice abordaremos de forma bastante sucinta sobre Os Três Problemas Clássicos da Geometria que são, a Duplicação do Cubo, a Quadratura do Círculo e a Trissecção do Ângulo. Falaremos sobre do que se trata cada problema, traremos algumas lendas que foram associadas a eles e também exporemos a impossibilidade de solução destes problemas.

8.1 Duplicação do cubo

Segundo Eduardo Wagner (WAGNER; CARNEIRO, 2007), reza a lenda que, em 429 a.C, os atenienses dirigiram-se para o memorável oráculo de Apolo na ilha de Delos, suplicando a graça de cessar uma peste que então devastava a sua cidade. Sendo assim, o Oráculo respondeu que a peste seria dizimada caso fosse feito a construção de um outro altar no templo da divindade, cujo o seu volume fosse o dobro do que lá existia. Os atenienses então construíram o novo altar dobrando a aresta do antigo, que havia forma de um cubo. Certamente, este novo templo foi construído de forma que seu volume fosse oito vezes maior do que o volume do antigo. E claro, a nova aresta deveria medir $\sqrt[3]{2}$ vezes a anterior. Devido a esta falha, a peste dizimou um grande número de atenienses. Com isso, o problema de "duplicar o cubo"ficou conhecido como o "problema de Delos". A partir deste apanhado histórico analisaremos o porquê, na linguagem matemática, o problema da duplicação do cubo é insolúvel.

Dado o cubo de aresta a, na qual seu volume é a^3, é desejado construir um novo cubo de aresta l, cujo seu volume seja dado por $l^3 = 2a^3$, ou seja, o novo cubo deve ter o dobro do volume do cubo anterior. Relacionando esta equação ao polinômio $f(x) = x^3 - 2a^3$, temos que $\alpha = a\sqrt[3]{2}$ é raiz de $f(x)$. Porém, note que $f(x)$ é mônico, irredutível e se anula em $\alpha = a\sqrt[3]{2}$, logo $irr(\alpha, \mathbb{Q}) = f(x)$ e, grau de $irr(\alpha, \mathbb{Q})$ é igual a 3. Assim, pela Proposição 9 segue que $[\mathbb{Q}[\alpha] : \mathbb{Q}] = 3$, que não é uma potência de 2. Portanto, pelo Teorema 6, α não é construtível.

8.2 Quadratura do círculo

Este problema pode ser ditado da seguinte forma: Dado um círculo, construa um quadrado de mesma área. Calcular áreas faziam parte do cotidiano das civilizações antigas, como exemplo, o cálculo da área de terras. De forma intuitiva, o quadrado se tornou a figura mais simples de calcular a área, sendo assim, para calcular as áreas de outras figuras, como o retângulo, o triângulo e entre outros polígonos, essas eram relacionadas com o

quadrado. A partir desta ideia que surge a expressão "quadratura", na qual é construir um quadrado equivalente a figura geométrica dada utilizando apenas a régua não graduada e o compasso.

Após o surgimento da ideia de quadrar polígonos, surge também a questão de quadrar figuras não poligonais (regiões curvas), na qual, junto vem as dificuldades de resolver este problema. O problema de quadrar o círculo fascinou vários geômetras gregos que por muito tempo se dedicaram para demonstrá-lo usando apenas os instrumentos euclidianos que são a régua não graduada e o compasso.

A partir desta pequena introdução do problema, como na duplicação do cubo, mostraremos o porquê, na linguagem matemática, o problema da quadratura do círculo não possui solução. Dessa forma, dado um círculo C de raio r, tem-se que sua área é dada por $A_c = \pi r^2$. Agora, queremos construir um quadrado de lado l cuja sua área seja igual a área do círculo citado anteriormente, ou seja, precisamos construir um quadrado de lado $l = r\sqrt{\pi}$.

Observe que pelo Teorema 6, $C_{\mathbb{R}}$ é uma extensão algébrica dos racionais, e pela definição de extensão algébrica (Definição 13), tem-se que π é um número transcendente, isto é, não existe um polinômio de coeficientes racionais tal que π seja raiz. Portanto π não pertence ao conjunto dos números construtíveis $C_{\mathbb{R}}$ e consequentemente $\sqrt{\pi}$ também não, logo não é possível construir o quadrado de lado $l = r\sqrt{\pi}$.

8.3 Trissecção do ângulo

Trissectar um ângulo qualquer significa dividi-lo em três ângulos menores de mesma medida. Em pelo menos dois aspectos este problema grego se difere dos outros dois que comentamos anteriormente. Um dos aspectos é que não existe alguma lenda associada a este problema e o outro é que, diferente da duplicação do cubo e da quadratura do círculo, é possível trisseccionar alguns ângulos utilizando apenas a régua não graduada e o compasso.

Como este problema consiste em trisseccionar qualquer ângulo, para mostrar a sua insolubilidade, exporemos um contra exemplo, isto é, mostraremos que não é possível trissectar o ângulo $\theta = \dfrac{2\pi}{18}$, daí

$$\theta = \frac{\pi}{9} \Rightarrow 3\theta = \frac{\pi}{3} \Rightarrow \cos(3\theta) = \cos\left(\frac{\pi}{3}\right).$$

A cargo do leitor fica para verificação que a seguinte relação é válida

$$cos(3\theta) = 4cos^3(\theta) - 3cos(\theta).$$

Assim,

$$\begin{aligned} \cos(3\theta) &= \cos\left(\frac{2\pi}{6}\right) \\ \Rightarrow 4\cos^3(\theta) - 3\cos(\theta) &= \frac{1}{2} \\ \Rightarrow 8\cos^3(\theta) - 6\cos(\theta) &= 1 \\ \Rightarrow 8\cos^3(\theta) - 6\cos(\theta) - 1 &= 0. \end{aligned}$$

Para melhor visualização, faremos uma mudança de variável na equação acima, seja $u = \cos(\theta)$, assim

$$p(u) = 8u^3 - 6u - 1 = 0.$$

Observe que, pelo Teorema 7 as possíveis raízes racionais de $p(u)$ são -1 e 1. Porém, $p(1) = 1$ e $p(-1) = -3$, sendo assim, $p(u)$ não possui raiz racional. Portanto, pela Proposição 13 concluímos que as raízes de $p(u) = 8u^3 - 6u - 1 = 0$ não são construtíveis. E consequentemente, não é possível trissectar o ângulo $\theta = \frac{\pi}{9}$.

Referências

ÁVILA, G. *Variáveis complexas e aplicações*. [S.l.]: LTC, 2008. Nenhuma citação no texto.

BOYER, C. B.; MERZBACH, U. C. *História da matemática*. [S.l.]: Editora Blucher, 2019. Nenhuma citação no texto.

BRAITT, M. dos S.; WHITLEY, W. G. Geometria iii. Nenhuma citação no texto.

EVES, H. W. *Introdução à história da matemática*. [S.l.]: Unicamp, 1995. Nenhuma citação no texto.

GONÇALVES, A. *Introdução à álgebra*. [S.l.]: Impa, 1979. Nenhuma citação no texto.

HEFEZ, A.; VILLELA, M. L. T. *Polinômios e equações algébricas*. [S.l.]: Sociedade Brasileira de Matemática, 2012. Nenhuma citação no texto.

LANG, S. et al. *Algebra*. [S.l.]: Springer New York, 2002. Citado na página 67.

SALDANHA, N. *Polígonos construtíveis por régua e compasso: Uma apresentação para professores da Educação Básica*. Tese (Doutorado) — PUC-Rio, 2015. Nenhuma citação no texto.

SANTOS, J. P. de O.; MELLO, M. P.; MURARI, I. T. C. *Introdução à análise combinatória*. [S.l.]: Ed. Ciencia Moderna, 2007. Citado na página 65.

WAGNER, E.; CARNEIRO, J. P. Q. *Construções geométricas*. [S.l.]: Sociedade Brasileira de Matemática, 2007. Citado na página 75.