Universidade Federal do Piauí
Centro de Ciências da Natureza
Pós-Graduação em Matemática
Mestrado em Matemática

Extensões de Corpos e os Três Problemas Clássicos de Construção Matemática

Jeovan Lira dos Santos

Jeovan Lira dos Santos

Dissertação de Mestrado:

Extensões de Corpos e os Três Problemas Clássicos de Construção Matemática

Dissertação submetida à Coordenação do Programa de Pós-Graduação em Matemática, da Universidade Federal do Piauí, como requisito parcial para obtenção do grau de Mestre em Matemática.

Orientador:
Prof. Dr. João Benício de Melo Neto

FICHA CATALOGRÁFICA
Serviço de Processamento Técnico da Universidade Federal do Piauí
Biblioteca Setorial do CCN

S237e Santos, Jeovan Lira dos.
Extensões de corpos e os três problemas clássicos de construção matemática / Jeovan Lira dos Santos. – Teresina, 2017.
67f.: il.

Dissertação (Mestrado) – Universidade Federal do Piauí, Centro de Ciências da Natureza, Pós-Graduação em Matemática, 2017.
Orientador: Prof. Dr. João Benício de Melo Neto

1. Geometria. 2.Construções Geométricas. I. Título

CDD 516.1

PROFMAT

UNIVERSIDADE FEDERAL DO PIAUÍ
CENTRO DE CIÊNCIAS DA NATUREZA
CENTRO DE EDUCAÇÃO ABERTA E À DISTÂNCIA .
MESTRADO PROFISSIONAL EM MATEMÁTICA EM REDE NACIONAL

SBM

Dissertação de Mestrado submetida à coordenação Acadêmica Institucional, na Universidade Federal do Piauí, do Programa de Mestrado Profissional em Matemática em Rede Nacional para obtenção do grau de **mestre em matemática** intitulada: EXTENSÕES DE CORPOS E OS TRÊS PROBLEMAS CLÁSSICOS DE CONSTRUÇÃO MATEMÁTICA, defendida por JEOVAN LIRA DOS SANTOS em 29 / 03 / 2017 e aprovada pela banca constituída pelos professores:

Valmária R. S. Ferraz

Presidente da Banca Examinadora

Examinador

Ítalo Dowell Lima Melo

Examinador Externo

Agradecimentos

Agradeço a Deus por ter me dado a oportunidade de estar sempre nessa infindável busca pelo conhecimento e realizações.

Agradeço a minha esposa Ronayra, pelas críticas construtivas, contribuições, compreensão e companherismo.

Agradeço minha família, em especial minha mãe Maria Dina Lira Luz e meu Pai José Clementino dos Santos, que souberam guiar meus passos para os estudos.

Agradeço o meu orientador, Prof. Dr. João Benício de Melo Neto, pela disponibilidade, apoio, sugestão do tema desse trabalho e contribuições para que o mesmo tornasse possível.

Agradeço aos meus colegas e amigos do mestrado pela ajuda e pelas conversas descontraídas.

Agradeço ao IFPI - Campus Oeiras, pelo apoio e pela liberação de minha carga horária semanal para que eu pudesse me dedicar ao PROFMAT.

Agradeço aos meus professores do mestrado, pela paciência e ensinamentos.

Agradeço ao meu professor do colégio Agrícola de Bom Jesus Prof. Dr. Egnilson Miranda de Moura, por ter me inspirado a estudar matemática.

Agradeço a UFPI, SBM e o IMPA por me proporcionar, nestes dois anos, conhecimento e material suficiente para que eu pudesse fazer este trabalho.

Agradeço a CAPES pelo apoio financeiro.

"*Nós precisamos saber, e nós iremos saber*".

David Hilbert.

Resumo

Durante o desenvolvimento da geometria plana na Grécia antiga, surgiram três problemas que se mostraram sem solução para matemática Grega da época. Esses problemas ficaram conhecidos na literatura como a duplicação do cubo, a quadratura do círculo e a trissecção do ângulo. Os três são problemas de construção geométrica, utilizando apenas régua não graduada e compasso. Apesar do enunciado dos mesmos serem bem simples, eles desafiaram o poder inventivo de inúmeros matemáticos e intelectuais, durante mais de dois mil anos. O presente trabalho tem como objetivo mostrar a impossibilidade de resolução dos três problemas clássicos (também conhecidos como impossibilidade clássica), usando somente régua não graduada e compasso. Dessa forma, fizemos um apanhado sobre trigonometria, números complexos, anel, corpos, homomorfismo, polinômios, extensões algébricas e pontos construtíveis. Fazendo uso do conhecimento supracitado, foi possível enunciar e provar todos os teoremas necessários para alcançarmos o objetivo já mencionado.

Palavras-chave: Geometria, Álgebra, Construções Geométricas, Pontos construtíveis, Impossibilidade.

Abstract

During the development of flat geometry in ancient Greece, three problems emerged which proved to be unsolvable for Greek mathematics at the time. These problems became known in the literature as cube duplication, quadrature of the circle and trisection of the angle. All three are geometric construction problems, using only non-graduated ruler and compass. Although their statement was quite simple, they challenged the inventive power of countless mathematicians and intellectuals for over two thousand years. The present work aims to show the impossibility of solving the three classic problems (also known as classic impossibility), using only a non - graduated ruler and compass. In this way, we have made a survey about trigonometry, complex numbers, ring, bodies, homomorphism, polynomials, algebraic extensions and constructible points. Using the aforementioned knowledge, it was possible to state and prove all the necessary theorems to reach the aforementioned objective.

Keywords: Geometry, Algebra, Geometric Constructions, Constructible Points, Impossibility.

Sumário

Lista de Figuras

Capítulo 1

Introdução

Desde os tempos antigos a matemática vem desafiando os matemáticos e intelectuais, instigando a curosidade dos mesmos a buscar cada vez mais conhecimento nos vários ramos dessa ciência. Os principais ramos da Matemática são: álgebra, análise matemática e geometria, a junção da álgebra, análise e geometria deram origem a outros ramos da matemática, como teoria dos números, geometria diferencial, análise combinatória, topologia Diferencial, topologia algébrica, sistemas dinâmicos, matemática computacional, programação matemática, teoria dos jogos, estatística, probabilidade, entre outros. Na Grécia antiga houve um período bastante produtivo no que diz respeito a matemática, em particular a geometria plana, que se mostrou extremamente importante para o desenvolvimento da humanidade.

Durante o desenvolvimento da geometria plana feita pelos gregos, surgiram três problemas que apesar das inúmeras tentativas dos gregos, os mesmos se mostraram sem solução, são eles: a duplicação do cubo, quadratura do círculo e trissecção do ângulo. Os três problemas clássicos da Geometria grega tratam sobre a impossibilidade de realizar certas construções geométrica usando apenas régua não graduada e compasso, tais problemas levaram mais de dois mil anos para serem provados.

Para que seja comprendido o que venha a ser duplicar um cubo, quadrar um círculo e trissectar um ângulo, primeiramente devemos deixar bem claro quanto ao que é permitido fazer com régua e compasso, para assim compreendermos o porque da impossibilidade de resolver os problemas. Com a régua é permitido traçar uma reta que passe por dois pontos distintos dados, com o compasso é permitido traçar uma circunferência com centro em um ponto dado. Fazendo uso desses dois instrumentos o que é possível de se obter como

resultado no final de cada operação, é a intersecção entre duas retas, interseção entre retas e circunferências ou a interseção entre duas circunferências. De posse dessas informações, os três problemas podem ser entendidos assim:

I. Duplicação do cubo: dado um cubo de aresta x e volume x^3, é impossível se construir a partir desse cubo um novo cubo com volume $2x^3$ utilizando apenas régua e compasso;

II. Quadratura do círculo: dado um círculo de raio r e área πr^2, é impossível se construir a partir desse círculo um quadrado de área πr^2 utilizando apenas régua e compasso;

III. Trissecção do ângulo: dado um ângulo de amplitude β, nem sempre é possível construir a partir desse ângulo dado um novo ângulo de amplitude $\frac{\beta}{3}$ (ou seja, com um terço da amplitude do ângulo dado), utilizando apenas régua e compasso.

Entre os três problemas matemáticos clássicos difundidos antes de Euclides, o problema da duplicação é talvez o mais famoso, inclusive existe uma lenda sobre o mesmo que conta como o problema surgiu.

> ... em 427 a.C. Péricles teria morrido de peste juntamente com um quarto da população de Atenas. Consternados, os atenienses consultaram o oráculo de Apolo, em Delos, para saber como enfrentar a doença. A resposta foi que o altar de Apolo, que possuía o formato de um cubo, deveria ser duplicado. Prontamente, as dimensões do altar foram multiplicadas por 2, mas isso não afastou a peste. O volume havia sido multiplicado por 8, e não por 2. (ROQUE, 2012, p. 155)

Com o objetivo de provar a impossibilidade clássica, foi feito nesse trabalho uma breve explanação sobre alguns tópicos da álgebra e geometria plana. Em seguida usamos essas ferramentas para criarmos o subconjunto $\mathcal{P}_\infty$ de $\mathbb{R}^2$, o qual chamamos de conjunto dos pontos construtíveis. Provamos também que um ponto $(x, y) \in \mathcal{P}_\infty$ é construtível se $(x, 0)$ e $(0, y)$ também são construtíveis. Depois tomamos o conjunto $\mathcal{C}_\mathbb{R} \subset \mathbb{R}$ tal que $\mathcal{C}_\mathbb{R} = \{\alpha \in \mathbb{R} : \alpha \text{ é construtível } \}$ e provamos que o mesmo é um corpo, e em seguinda, enunciamos e provamos o teorema 7.3 que é crucial na demonstração da impossibilidade clássica.

Para a construção do trabalho, foi preciso trabalhar alguns tópicos da matemática elementar, no capítulo 2 foi trabalhado um pouco de plano cartesiano, trigonometria e

números complexos, no capítulo 3 abordamos a definição e exemplos de anel, corpo e homomorfismo de anéis, no capítulo 4 foi estudado os polinômios em uma variável sobre um corpo K, onde tratamos das operações de soma e multiplicação de polinômios, divisão Euclidiana, polinômios irredutíveis, critério de Eisenstein, e finalizamos esse capítulo falando do Teorema fundamental da Álgebra. Já no capítulo 5, retratamos as extensões algébricas, definimos números algébricos e transcedentes, revisamos noções básicas de álgebra linear, para assim termos condições de definirmos o grau de uma extensão. O capítulo 6 foi muito prazeroso, pois nele trabalhamos as construções com régua e compasso, enunciamos e provamos alguns teoremas importantes da geometria plana, como por exemplo, o teorema de Tales e o teorema do Ângulo Inscrito, e finalizamos esse capítulo com a trissecção do ângulo de 90^o.

No capítulo 7 foi juntado todo o conhecimento supracitado para criarmos o conjunto dos pontos construtíveis, usando a geometria e a álgebra. Enunciamos e provamos o teorema 7.3, que é a ferramenta crucial na demonstração da impossibilidade clássica, e finalizamos esse capítulo atingindo o nosso objetivo que foi mostrar a impossibilidade da construção dos três problemas clássicos da matemática Grega: a duplicação do cubo, a quadratura do círculo e a trissecção do ângulo.

O objetivo desse trabalho, foi estudar tópicos de matemática, que foram usados como base para justificar a impossibilidade da duplicação do cubo, quadratura do círculo e a trissecção do ângulo usando apenas régua não graduada e compasso. Os tópicos foram interligados ao longo do texto, buscamos usar uma linguagem simples e de fácil compreenção, para que o leitor tenha um bom entendimento do tema.

Vale resaltar também que todas as figuras foram construidas usando software matemático livre conhecido como **Geogebra**, esse software reúne geometria, álgebra e cálculo, ele foi desenvolvido por Markus Hohenwarter da Universidade de Salzburg para educação matemática nas escolas. O programa permite realizar construções geométricas com a utilização de pontos, retas, segmentos de reta, polígonos, entre outros. O educador interessado em trabalhar com Geogebra, pode baixá-lo gratuitamente no site **www.geogebra.org**.

Capítulo 2

Um Pouco de Trigonometria e Números Complexos

Iniciamos esse trabalho, falando um pouco de plano cartesiano, trigonometria e dos números complexos, pois esses tópicos são muito importante para fundamentar nosso trabalho. Iniciaremos com a definição de plano cartesiano e depois de trigonometria na circunferência, em particular, falaremos de seno e cosseno, com o objetivo de relembrar as fórmulas de adição de arcos, tendo em vista seu uso em algumas partes desse trabalho, como por exemplo na demonstração da impossibilidade do problema da trisecção do ângulo.

O leitor certamente tem uma boa idéia sobre o que venha a ser ponto, reta e plano, portanto vamos deixar claro aqui apenas como será entendida algumas notações. Quando falarmos em reta e ponto, na maiorias das vezes iremos usar letra minúscula para retratar reta(exemplo, $r, s, t, ...$, etc.), e letra maiúscula para retratar ponto(exemplo. $A, B, C, ...$,etc.). Dado os pontos distintos A e B, usaremos AB, para retratar o segmento de origem A e extremidade B, $\overline{AB}$ para representar o tamanho do segmento AB, $\overrightarrow{AB}$ para representar a semirreta de origem A e $\overleftrightarrow{AB}$ para representar a reta que passa por A e B.

2.1 Plano Cartesiano

Consideramos como plano cartesiano, o conjuto denotado por $\mathbb{R}^2$, onde seus elementos são pares ordenado representados por (x, y), onde x é denominado abcissa e y ordenada. Os pares ordenados surgem de forma natural quando se fixa em um plano π e um par de

eixos ortogonais OX e OY, que se intersectam no ponto O, chamado a origem do sistema de cordenadas.

Todo ponto $P \in \pi$ está associado a um par ordenado (x, y), e dizemos que (x, y) é o par ordenado de P. Veja a figura abaixo.

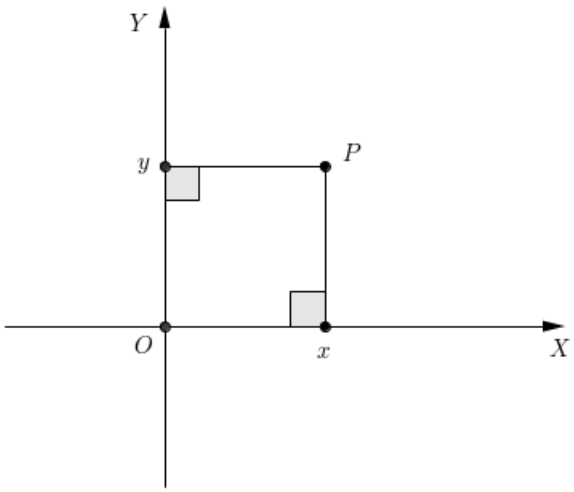

Figura 2.1: Plano cartesiano

Os eixos OX e OY dividem o plano em quatro regiões, chamadas quadrantes, classificados em primeiro, segundo, terceiro e quarto quadrante respectivamente. No primeiro quadrante, tem-se $x \geq 0$ e $y \geq 0$, no segundo $x \leq 0$ e $y \geq 0$, no terceiro $x \leq 0$ e $y \leq 0$, e no quarto $x \geq 0$ e $y \leq 0$.

Vamos entender aqui que o conjunto de pares ordenado $\mathbb{R}^2$, representa o modelo aritmético do plano π, enquanto o plano π representa o modelo geométrico de $\mathbb{R}^2$.

Fazendo uso do famoso Teorema de Pitágoras e da figura 2.2, é fácil concluir que a distância entre dois ponto $A = (x, y)$ e $B = (u, v)$, é dada por $d(A, B) = \sqrt{(x-u)^2 + (y-v)^2}$.

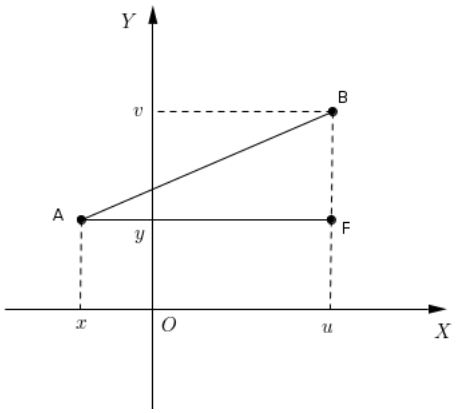

Figura 2.2: Distância entre pontos

2.2 Circunferência e arcos trigonométricos

No plano Cartesiano, a circunferência trigonométrica denotada por λ, é centrada na origem $O = (0, 0)$ e tem raio 1 e comprimento 2π.

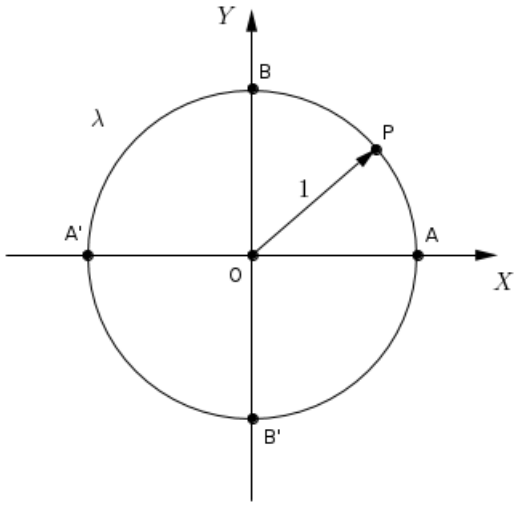

Figura 2.3: Circunferência trigonométrica

Na figura 2.3, é convencionado que o sentido de percurso sobre a circunferência trigonométrica de A para B é anti-horário, e do contrário chamamos de sentido horário. Entendemos também, que um número real positivo x, medido sobre a circunferência λ, a partir do ponto A até um ponto P, representa o comprimento do arco $\overset{\frown}{AP}$. O sentido anti-horário, é entendido na circunferência trigonométrica como positivo e o sentido horário como negativo. Vale lembrar também, que devido a circunferência λ ser de raio 1

o seu comprimento é 2π. Portanto fica fácil representar alguns arcos sobre λ, quando é conhecido o comprimento do mesmo.

Exemplo 1. *Marque sobre a circunferência trigonométrica os arcos de comprimento* $\frac{\pi}{4}$, $\frac{\pi}{2}$, π *e* $-\frac{\pi}{4}$.

Solução. Como toda a circunferência λ a partir do ponto A no sentido anti-horário tem comprimento 2π, temos que a partir de A, o arco de comprimento π está na metade de λ , o de comprimento $\frac{\pi}{2}$ em um quarto de λ, o de comprimento $\frac{\pi}{4}$ em um oitavo de λ e o de $-\frac{\pi}{4}$ em um oitavo de λ no sentido horário a partir de A. A figura 2.4 mostra a representação desses pontos sobre a circunferência λ.

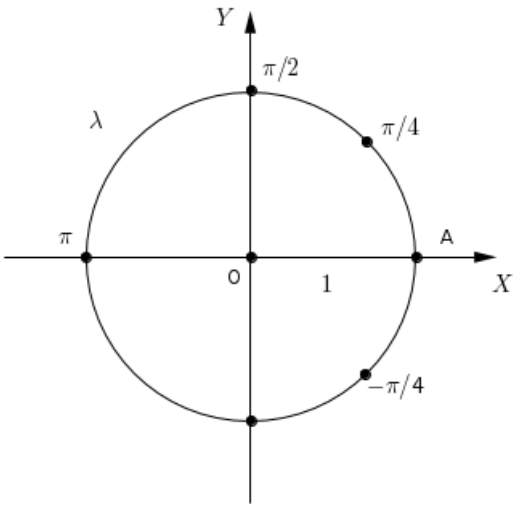

Figura 2.4: Arcos sobre a circunferência trigonométrica

Definição 2.1. *Seja* $c \in \mathbb{R}$ *e* $P \in \lambda$, *com* $P = (x, y)$. *Definimos seno e cosseno do arco* $\overset{\frown}{AP}$, *de medida c, como sendo os números* $cos(c) = x$ *e* $sen(c) = y$.

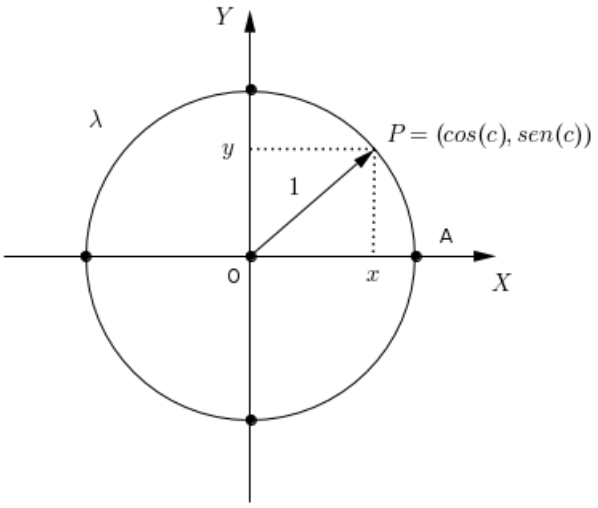

Figura 2.5: Seno e cosseno

Seja P um ponto qualquer de λ , a maior e a menor ordenada de P, está nos pontos de interseção de λ com o eixo OY. Analogamente, a maior e a menor abscissa do ponto P está nos pontos de interseção de λ com o eixo OX. Portanto sendo $c = \overset{\frown}{AP}$, temos:

$$\begin{cases} -1 \leq sen(x) \leq 1 \\ -1 \leq cos(x) \leq 1 \end{cases}$$

Vamos assumir aqui, que já conhecemos o seno e o cosseno dos arcos de medida $0,\ \pi/6,\ \pi/4,\ \pi/3\ e\ \pi/2$, conforme mostra a tabela 2.1.

Tabela 2.1: Arcos notáveis

x	$sen(x)$	$cos(x)$
0	0	1
$\frac{\pi}{6}$	$\frac{1}{2}$	$\frac{\sqrt{3}}{2}$
$\frac{\pi}{4}$	$\frac{\sqrt{2}}{2}$	$\frac{\sqrt{2}}{2}$
$\frac{\pi}{3}$	$\frac{\sqrt{3}}{2}$	$\frac{1}{2}$
$\frac{\pi}{2}$	1	0

Proposição 2.1. *Para todo $c \in \mathbb{R}$, temos que $sen^2(c) + cos^2(c) = 1$.*

Demonstração. Seja $\overset{\frown}{AP} = c$. Note na figura abaixo que $P = (cos(c), sen(c)$ e $O = (0, 0)$, portanto pela seção anterior, temos:

$$d(O, P) = \sqrt{(cos(c) - 0)^2 + (sen(c) - 0)^2} = 1$$

$$\Rightarrow sen^2(c) + cos^2(c) = 1.$$

□

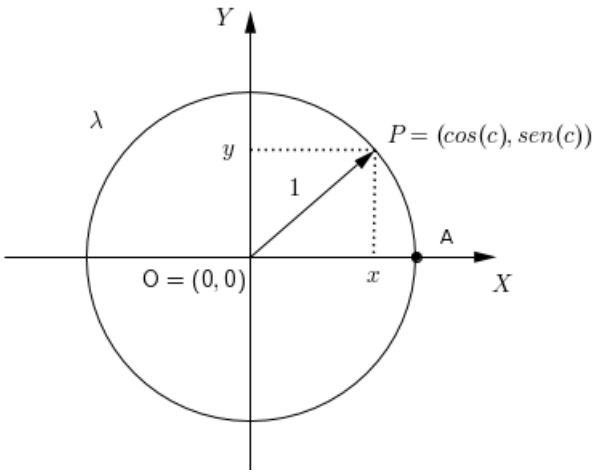

Figura 2.6: Relação fundamental da trigonometria

Finalizamos os conceitos básicos de trigonometria na circunferência λ, falando das fórmulas de adição de arcos para seno e cosseno.

Proposição 2.2. *Para $a, b \in \mathbb{R}$, vale:*

$$\text{a)} \begin{cases} cos(a+b) = cos(a)cos(b) - sen(a)sen(b) \\ cos(a-b) = cos(a)cos(b) + sen(a)sen(b) \end{cases}$$

$$\text{b)} \begin{cases} sen(a+b) = sen(a)cos(b) + cos(a)sen(b) \\ sen(a-b) = sen(a)cos(b) - cos(a)sen(b) \end{cases}$$

Exemplo 2. *Usando a tabela 1.1, temos que :*

$$sen\left(\frac{\pi}{12}\right) = sen\left(\frac{\pi}{4} - \frac{\pi}{6}\right) = sen\left(\frac{\pi}{4}\right)cos\left(\frac{\pi}{6}\right) - cos\left(\frac{\pi}{4}\right)sen\left(\frac{\pi}{6}\right)$$

$$\Rightarrow sen\left(\frac{\pi}{12}\right) = \frac{\sqrt{2}}{2} \cdot \frac{\sqrt{3}}{2} - \frac{\sqrt{2}}{2} \cdot \frac{1}{2}$$

$$\Rightarrow sen\left(\frac{\pi}{12}\right) = \frac{\sqrt{6} - \sqrt{2}}{4}$$

.

2.3 Números Complexos

É do conhecimento de todos, que no conjunto dos números reais a equação dada por $x^2 + 4 = 0$ não possui solução, isso porque nesse conjunto não é possível extrair raiz quadrada de um número negativo. O conjunto dos números complexo nascem mediante essa impossibilidade dos números reais.

Definição 2.2. *Definimos o conjunto* $\mathbb{C} = \{z = a + bi : a, b \in \mathbb{R}\}$, *com* $i = \sqrt{-1}$, *como sendo o conjunto dos números complexos.*

Notemos que a equação $x^2 + 4 = 0$, assume solução em $\mathbb{C}$, pois $x^2 + 4 = 0 \Rightarrow x^2 = -4 \Rightarrow x = \pm\sqrt{-4} = \pm\sqrt{4 \cdot (-1)} = \sqrt{4} \cdot \sqrt{-1} = 2\sqrt{-1} = 2i$. Ou seja, os números $2i$ e $-2i$ são soluções de $x^2 + 4 = 0$ em $\mathbb{C}$.

Da definição 2.2, se $z \in \mathbb{C}$ então z é inscrito na forma $z = a + bi$, onde o número a é chamado de parte real de z e denotamos por $Re(z)$, e b é chamado de parte imaginária de z denotada por $Im(z)$.

Notemos também, que o conjunto dos números reais $\mathbb{R}$ é um subconjunto dos complexos $\mathbb{C}$, pois qualquer $a \in \mathbb{R}$ pode ser inscrito da forma $z = a + 0i = a \in \mathbb{R}$. Portanto $\mathbb{R} \subset \mathbb{C}$.

Um fato muito importante sobre os números complexos, é que podemos ver qualquer complexo $z = a + bi$ como um ponto do plano cartesiano da forma (a, b), para isso basta fazermos a conversão sobre o plano cartesiano XOY, onde o número $a = Re(z)$ fica no eixo OX e o número $b = Im(z)$ fica no eixo OY. Portanto para todo complexo $z = a+bi$, corresponde um único ponto $P = (a, b)$ no plano XOY, tal que OX é dito eixo real e OY eixo imaginário.

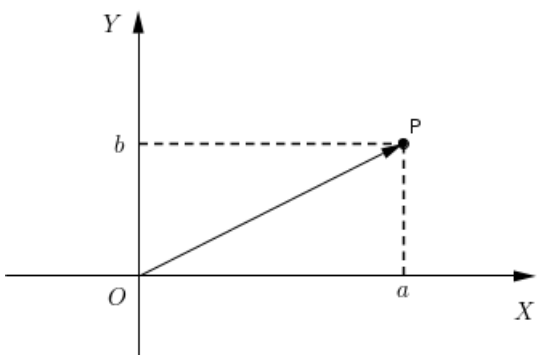

Figura 2.7: Plano complexo

Veremos agora, como se traduz as operações de soma e multiplicação, quando assumimos o número complexo z na sua forma algébrica.

Seja a, b, c e d números reais, tomando os números complexos $a + bi$ e $c + di$, temos que $(a + bi) + (c + di) = (a + c) + (b + d)i$ e $(a + bi) \cdot (c + di) = (ac - bd) + (ad + bc)i)$. Em outras palavras o conjuntos dos números complexos é fechado para as operações de adição e multiplicação.

2.3.1 Módulo e conjugado

Definição 2.3. *Seja $z = a + bi \in \mathbb{C}$, definimos como o conjugado do número complexo z o número $\overline{z} = a - bi$. Definimos também, o módulo do complexo z, como sendo o número real não negativo $|z| = \sqrt{a^2 + b^2}$.*

Olhando para a figura 1.7, podemos notar que geometricamente o número real $|z|$ mede a distância do centro O ao ponto P, ou seja, $d(O, P) = |z|$. É fácil verificar que:

$$z \cdot \overline{z} = (a + bi) \cdot (a - bi) = a^2{}_b{}^2 = |z|^2.$$

O fato mostrado acima, é muito importante quando queremos determinar o número $\frac{1}{z} = \frac{1}{a+bi}$. Podemos obter agora o número $\frac{1}{z}$ em termos de a e b, fazendo:

$$\frac{1}{z} = \frac{\overline{z}}{z\overline{z}} = \frac{\overline{z}}{|z|^2} = \frac{a - bi}{a^2 + b^2} = \frac{a}{a^2 + b^2} - \frac{b}{a^2 + b^2}i.$$

Exemplo 3. *Seja $z = 2 + 5i$, o número $\frac{1}{z}$ é dado por: $\frac{1}{z} = \frac{2}{2^2+5^2} - \frac{5}{2^2+5^2}i = \frac{2}{29} - \frac{5}{29}i$.*

O objetivo da propriedade mostrada acima é ajudar na obtenção do quociente $\frac{z_1}{z_2}$, onde $z_1, z_2 \in \mathbb{C}$, e isso pode ser feito fazendo $\frac{z_1}{z_2} = z_1\left(\frac{1}{z_2}\right)$. No entanto, na prática o cálculo do quociente $\frac{z_1}{z_2}$ é feito multiplicando o numerador e o denominador pelo conjugado de z_2.

Exemplo 4. *Seja $z_1 = 1 + 2i$ e $z_2 = 3 + i$, pelas condições acima temos que:*

$$\frac{z_1}{z_2} = \frac{1 + 2i}{3 + i} = \frac{(1 + 2i)(3 - i)}{(3 + i)(3 - i)} = \frac{5 + 5i}{10} = \frac{1}{2} + \frac{1}{2}i.$$

Proposição 2.3. *Seja $z_1, z_2 \in \mathbb{C}$, então vale:*

i) $(\overline{z_1 z_2}) = \overline{z_1} \cdot \overline{z_2}$;

ii) $(\overline{z_1 + z_2}) = \overline{z_1} + \overline{z_2}$;

iii) $|z_1 z_2| = |z_1||z_2|$.

Demonstração. Sendo $z_1 = a + bi$ e $z_2 = c + di$, fazendo uso da operação multiplicação e da definição de conjugado, temos:

$$\begin{cases} z_1 z_2 = (ac - bd) + (bc + ad)i \\ \overline{z_1 z_2} = (ac - bd) - (bc + ad)i. \end{cases}$$

Como $\overline{z_1} = a - bi$ e $\overline{z_2} = c - di$, temos então, $\overline{z_1} \cdot \overline{z_2} = (a - bi)(c - di) = (ac - bd) - (bc + ad)i = \overline{z_1 z_2}$, portanto $(\overline{z_1 z_2}) = \overline{z_1} \cdot \overline{z_2}$. O que demonstra (i).

ii) Sendo $\overline{z_1} = a - bi$ e $\overline{z_2} = c - di$, pela operação adição, $\overline{z_1} + \overline{z_2} = (a + c) + (-b + (-d))i = (a + c) - (b + d)i = \overline{z_1 + z_2}$.

iii) Notemos que: $|z_1 z_2|^2 = (z_1 z_2)(\overline{z_1 z_2}) = (z_1 \overline{z_1})(z_2 \overline{z_2}) = |z_1|^2 |z_2|^2 = (|z_1||z_2|)^2$. Portanto $|z_1 z_2| = |z_1||z_2|$. □

Observação: Já foi mostrado que $z\overline{z} = |z|^2$.

Capítulo 3

Anel, corpo e Homomorfismo

Nesse capítulo será abordado tópicos fundamentais da álgebra que serviram como base para estudar os três problemas clássicos.

3.1 Anel e corpo

Definição 3.1. *Sejam A um conjunto e $(+)$ e $(\cdot)$ duas operações em A, chamados de adição e multiplicação. A terna $(A, +, \cdot)$ será chamada de anel se as operações definidas em A gozarem das propriedades Abaixo.*

a) Propriedades da adição

(A1) **associativa:** para todos $a, b, c \in A$, tem-se que $(a + b) + c = a + (b + c)$.

(A2) **comutativa:** para todos $a, b \in A$, tem-se que $a + b = b + a$.

(A3) **elemento neutro:** existe $0 \in A$ tal que $0 + x = x$, para todo $x \in A$.

(A4) **simétrico:** para todo $a \in A$, existe $a' \in A$ tal que $a + a' = 0$.

b) Propriedades da multiplicação

(M1) **associativa:** para todo $a, b, c \in A$, tem-se que $(a \cdot b) \cdot c = a \cdot (b \cdot c)$.

(M2) **distributividade a esquerda e a direita** para quaisquer que sejam $a, b, c \in A$, tem-se que $a \cdot (b + c) = a \cdot b + a \cdot c$ e $(a + b) \cdot c = a \cdot c + b \cdot c$.

Se todas as propriedades supracitadas forem satisfeitas, a terna $(A, +, \cdot)$ será chamada de anel não comutativo.

Se o anel $(A, +, \cdot)$ satisfaz:

(M3) **elemento neutro da multiplicação** existe $1 \in A$, tal que $a \cdot 1 = 1 \cdot a = a$. dizemos que $(A, +, \cdot)$ é um anel com unidade.

Se alem disso, for satisfeito a propriedade:

(M4) **comutativa:** para quaisquer que sejam $a, b \in A$, tem-se que $a \cdot b = b \cdot a$. O anel $(A, +, \cdot)$ será chamado de anel comutativo.

(M5) **anel sem divisores de zero:** se $a \cdot b = 0$ então $a = 0$ ou $b = 0$.

Exemplo 5. *Se consideramos o anel* $(\mathbb{Z}_6, +, \cdot)$*, onde* $\mathbb{Z}_6 = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{4}, \overline{5}\}$*, notaremos que* $\overline{2} \cdot \overline{3} = \overline{0}$*, desta forma concluiremos que* $(\mathbb{Z}_6, +, \cdot)$ *é um anel que possui divisores de zero.*

(M6) **inverso multiplicativo:** para todo $a \in A$ com $a \neq 0$, existe $b \in A$ tal que $a \cdot b = 1$.

Vale ressaltar que os elementos neutro da adição e da multiplicação são únicos, pois considerando os elementos neutro $0', 1' \in A$, temos que: $0 = 0 + 0' = 0' + 0 = 0'$ e $1 = 1 \cdot 1' = 1' \cdot 1 = 1'$. Portanto $0 = 0'$ e $1 = 1'$, provando nossa afirmação acima.

Também é fácil provar a unicidade do simétrico, pois se a' e a" são dois simétricos de $a \in A$, pelas propriedades (A2) e (A1) temos que: $a' = 0 + a' = (a" + a) + a' = a" + (a + a') = a" + 0 = a"$.

O simétrico a' de a em relação a adição é geralmente simbolizado por $(-a)$, e durante nossos trabalhos usaremos $a - b$ para representar $a + (-b)$. A operação representa por $-$ é chamada de subtração.

Exemplo 6. *O conjunto* $\mathbb{Z}[i] = \{a + bi | a, b \in \mathbb{Z}\}$*, munido das operações adição(* $+$ *) e multiplicação(* $\cdot$ *) é denominado anel dos inteiros de Gauss, e o mesmo, claramente satisfaz todas as condições de um anel.*

Definição 3.2. *Se a terna* $(A, +, \cdot)$*, é um anel comutativo com unidade e sem divisores de zero então dizemos que* $(A, +, \cdot)$ *é um anel de integridade(ou domínio de integridade).*

Exemplo 7. *Os conjuntos dos números racionais, reais e complexos munidos das operações adição e multiplicação são exemplos de domínios de integridade, e representamos assim:*

$$(\mathbb{Q}, +, \cdot),\ (\mathbb{R}, +, \cdot) \text{ e } (\mathbb{C}, +, \cdot).$$

Exemplo 8. *Seja* A *um domínio de integridade, as únicas soluções da equação* $x^2 = x$*, são* 0 *e* 1*.*

Solução: Seja $x \in A$ tal que $x^2 = x$, assim temos,

$$x^2 - x = x \cdot x - 1 \cdot x = (x-1) \cdot x = 0$$

e daí segue que pela condição M5, que $x - 1 = 0$ ou $x = 0$, isto é, $x = 1$ ou $x = 0$.

Definição 3.3. *Se $(A, +, \cdot)$ for um domínio de integridade e se alem disso satisfazer a propriedade (M6), então $(A, +, \cdot)$ será chamado de corpo.*

Como exemplos de corpos podemos citar as seguintes ternas $(\mathbb{Q}, +, \cdot)$, $(\mathbb{R}, +, \cdot)$ e $(\mathbb{C}, +, \cdot)$. O conjunto dos números racionais definido por $\mathbb{Q} = \{p/q \in \mathbb{Z} \; e \; q \neq 0\}$ é caracterizado como o menor corpo existente.

Definição 3.4. *Seja $(A, +, \cdot)$ um subanel e B um subconjunto não vazio de A, consideremos também que B seja fechado para a operação de adição $(+)$ e multiplicação $(\cdot)$. Se a terna $(B, +, \cdot)$ cumprir com todas as propriedades de um anel a mesma será chamada de um subanel do conjunto A.*

O fato de o conjunto B ser um subconjunto do anel A, ajuda muito a simplificar as operações que verificam se B munido da adição e da multiplicação é ou não um anel. Para isso vamos anunciar abaixo um critério para que um subconjunto de um anel seja um subanel.

Proposição 3.1. *Consideremos o anel $(A, +, \cdot)$ e B um subconjunto de A. O conjunto B será um subanel de A se e somente se as seguintes condições forem satisfeitas:*

(1) O elemento neutro de A em relação a operação adição pertence a B. Ou seja $0 \in B$;

(2) B é fechado para a subtração. Ou seja $x, y \in B \Rightarrow x - y \in B$;

(3) B é fechado para a multiplicação. Ou seja $x, y \in B \Rightarrow x \cdot y \in B$.

Demonstração. Pela definição acima, sendo $(B, +, \cdot)$ subanel de $(A, +\cdot)$ é facil ver que as condições (1), (2) e (3) são cumpridas.

Reciprocamente, seja $B \subset A$, suponhamos válidas as propriedades (1), (2) e (3), daí temos que:

a) Como por (1) $0 \in B$, então $B \neq \varnothing$.

b)Por (1) e (2), temos que: se $(x = 0), y \in B$, então $-y = 0 - y = x - y \in B$.

c) Por (b), (2) e (3), teremos, se $x, y \in B$, então: $\begin{cases} x + y = x - (-y) \in B \\ x \cdot y \in B \end{cases}$, ou seja, B é fechado pra soma e para o produto.

Assim, as oprerações de A estão fechadas em B, e como as propriedades (A1), (A2), (M1) e (M2) são hereditárias, as mesmas valem em B. Portanto $(B, +, \cdot)$ é subanel de $(A, +, \cdot)$. □

Exemplo 9. *O cojunto* $\mathbb{Z}[\sqrt{2}] = \{a + b\sqrt{2}\}$*, munido das operações de adição e multiplicação é um subanel de* $\mathbb{R}$*.*

De fato, sejam $a, b, c, d \in \mathbb{Z}$, então com as operações de adição e multiplicação de números reais temos que:$(a + b\sqrt{2}) + (c + d\sqrt{2}) = (a + c) + (b + d)\sqrt{2}$ e $(a + b\sqrt{2})(c + d\sqrt{2}) = (ac + 3bd) + (ad + bc)\sqrt{2}$, portanto $\mathbb{Z}[\sqrt{2}]$ é fechado para as operações de adição e multiplicação em $\mathbb{R}$. Além disso, $0 = 0 + 0\sqrt{2} \in \mathbb{Z}$ e $-(c + d\sqrt{2}) = (-c) + (-d)\sqrt{2} \in \mathbb{Z} \Rightarrow a + b\sqrt{2} - (c + d\sqrt{2}) = (a - c) + (b - d)\sqrt{2} \in \mathbb{Z}$, assim $(\mathbb{Z}[\sqrt{2}], +, \cdot)$ é um subanel de $\mathbb{R}$.

Definição 3.5. *Se um subanel* $(B, +, \cdot)$ *de um corpo* $(K, +, \cdot)$*, é também um corpo, então* B *é subcorpo de* K*.*

Exemplo 10. *(1)* $\mathbb{Q}$ *é um subcorpo de* $\mathbb{R}$*.*

(2) $\mathbb{R}$ *é um subcorpo de* $\mathbb{C}$*.*

3.2 Homomorfismo de anéis

Nesta seção, vamos descobrir informações sobre um anel, examinando sua interação com outros anéis, isto é feito através dos homomorfismos. Um homomorfismo é uma função que preserva as operações soma e produto entre anéis.

Com o objetivo de simplificar as notações, em alguns casos usaremos A em vez de $(A, +, \cdot)$, alem disso, fica entendido que dado dois anéis A e B o elemento 0 representa elemento neutro de A e $0'$ o elemento neutro de B, se ambos possuem unidade, denotaremos por 1 a unidade de A e por $1'$ a unidade de B.

Definição 3.6. *Uma função* $f : A \longrightarrow B$ *é chamada de um homomorfismo de* A *em* B*, se satisfazer as seguintes condições:*

a) $\forall x, y \in A,\ f(x + y) = f(x) + f(y)$*;*

b) $\forall x, y \in A,\ f(x \cdot y) = f(x) \cdot f(y)$.

Sendo $f : A \longrightarrow B$ um homomorfismo bijetivo, dizemos que f é um **isomorfismo** de A sobre B, e nesse caso A e B são ditos isomorfos e escrevemos $A \simeq B$.

Quando $B = A$, o homomorfismo $f : A \longrightarrow A$ será chamado de **endomorfismo** de A(denotamos por End(A)). Se além disso o endomorfismo de A for um isomorfismo de A, diremos que $f : A \longrightarrow A$ é um **automorfismo** de A (representamos por Aut(A)).

Exemplo 11. *A aplicação de conjugação* $f : \mathbb{C} \longrightarrow \mathbb{C}$ *dada por* $f(a + bi) = a - bi$ *é um endomorfismo, e além disso é claramente um automorfismo.*

Proposição 3.2. *Se* $f : A \longrightarrow B$ *é um homomorfismo, então:*

a) $f(0) = 0'$*;*

b) $f(-a) = -f(a)$ *para todo* $a \in A$*;*

c) Se A *e* B *são anéis de integridade. Então* f *é a função constante zero ou* $f(1) = 1'$.

Demonstração. a) $f(0) = f(0 + 0) = f(0) + f(0) \Rightarrow f(0) = 0'$.

b) Seja $a \in A$, temos:

$$a + (-a) = 0 \Rightarrow f(a + (-a)) = f(a) + f(-a) = f(0) = 0' \Rightarrow f(-a) = -f(a)$$

.

c) $f(1) = f(1 \cdot 1) = f(1) \cdot f(1) \Rightarrow f(1) = f(1)^2$. Pelo exemplo 8, temos que $f(1) = 0'$ ou $f(1) = 1'$, o que conclui nossa demonstração. □

Proposição 3.3. *Seja* $f : A \longrightarrow B$ *é um homomorfismo. Se* L *é um subanel do anel* A*, então* $f(L)$ *é um subanel do anel* B.

Demonstração. Pela proposição 3.2 o elemento neutro de A é o mesmo elemento neuto do subanel L. Ou seja $0 \in L$. Pela proposição 2.2.2 $0' = f(0) \in f(L)$, daí $f(L)$ não é vazio.

Seja $a, b \in L \Rightarrow a - b \in L$ e $a \cdot b \in L$, assim:

$$\begin{cases} f(a) - f(b) = f(a) + f(-b) = f(a + (-b)) = f(a - b) \in f(L) \\ f(a) \cdot f(b) = f(a \cdot b) \in f(L) \end{cases}$$

Portanto, $f(L)$ é um subanel de B. □

Definição 3.7. *Seja* $f : A \longrightarrow B$ *um homomorfismo do anel* A *no anel* B*. Chama-se núcleo de* f *e denota-se por* $N(f)$ *ou* $Ker(f)$ *o seguinte subconjunto de* A.

$$N(f) = \{x \in A : f(x) = 0'\}$$

Para uso no exemplo abaixo, vamos relembrar aqui de um conjunto bem conhecido no meio matemático, que é o conjunto das matrizes de ordem 2 sobre o conjunto dos números reais, representado por $M_{2\times2}(\mathbb{R})$. Ou seja, para todos $a, b, c, d \in \mathbb{R}$:

$$M_{2\times2}(\mathbb{R}) = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

Tomando que para todos $a, b, c, d, e, f, g, h \in \mathbb{R}$ temos, $\begin{pmatrix} a & b \\ c & d \end{pmatrix} + \begin{pmatrix} e & f \\ g & h \end{pmatrix} = \begin{pmatrix} a+e & b+f \\ c+g & d+h \end{pmatrix}$ e $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot \begin{pmatrix} e & f \\ g & h \end{pmatrix} = \begin{pmatrix} ae+bg & af+bh \\ ce+dg & cf+dh \end{pmatrix}$. Claramente $(M_{2\times2}(\mathbb{R}), +, \cdot)$ é um anel, e o seu elemento neutro é $\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$.

Exemplo 12. *Seja $f : \mathbb{C} \longrightarrow M_{2\times2}(\mathbb{R})$, definido por:*

$$f(x+iy) = \begin{pmatrix} x & y \\ -y & x \end{pmatrix}$$

um homomorfismo do corpo $\mathbb{C}$ no anel $B = M_{2\times2}(\mathbb{R})$.

Pela definição acima $N(f) = \{x + iy \in \mathbb{C} : f(x+iy) = 0'\}$. Assim sendo, temos:

$$f(x+iy) = 0' \Rightarrow \begin{pmatrix} x & y \\ -y & x \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} \Rightarrow x = y = 0$$

.

Capítulo 4

Noções Básicas de Polinômios

Nesse capítulo trabalharemos com polinômios sobre um corpo K, em particular no corpo K contido nos complexos. Falaremos sobre igualdade de polinômios, adição e multiplicação de polinômios, grau do polinômio, algoritmo da divisão, corpo algebricamente fechado, irredutibilidade, e para finalizar citaremos o teorema fundamental da álgebra.

4.1 Polinômios

Definição 4.1. *Consideremos o corpo $(K, +, \cdot)$. Definimos o polinômio p sobre o corpo $(K, +, \cdot)$ em uma varável x, a seguinte igualdade*

$$p(x) = a_0 + a_1x^1 + a_2x^2 + a_3x^3 + \dots a_nx^n$$

onde cada elemento $a_i \in K$, para todo $i \in \mathbb{N}$ e são chamados de coeficientes, além disso, existe $n \in \mathbb{N}$ tal que $a_i = 0$ para todo $i > n$.

Também poderiamos representar o polinômio $p(x)$ da seguinte forma:

$$p(x) = a_0 + a_1x^1 + a_2x^2 + a_3x^3 + \dots a_nx^n = \sum_{i=1}^{n} a_ix^i$$

pois, pelas condições acima $a_{n+i} = 0$ para todo $i \in \{1, 2, 3, \dots\}$.

Exemplo 13. *As seguintes aplicações abaixo são polinômios:*

(1) $p(x) = 7 + 4x - x^2 + x^3$ *onde* $a_0 = 7, a_1 = 4, a_3 = -1$ *e* $a_4 = 1$*;*

(2) $p(x) = 1 - 10x^5$ *onde* $a_0 = 1, a_1 = a_2 = a_3 = a_4 = 0$ *e* $a_5 = -10$.

A título de exemplo definimos abaixo os polinômios:

(1) **Polinômio identicamente nulo:** $p(x) = 0 + 0x^1 + 0x^2 + \ldots + 0x^n = 0$;

(2) **Polinômio constante:** $p(x) = a + 0x + 0x^2 + \ldots + 0x^n = a$.

Pela definição acima, existe um número $n \in \mathbb{N}$ tal que $a_n \neq 0$ e $a_i = 0$ para todo $i > n$. O número n será definido abaixo com grau do polinômio $p(x)$, a_n será chamado de coeficiente líder de $p(x)$ e quando $a_n = 1$, $p(x)$ será classificado com polinômio mônico.

Definição 4.2. *Seja $p(x) = a_0 + a_1x^1 + a_2x^2 + a_3x^3 + \ldots a_nx^n$ um polinômio não nulo. Definimos como grau do polinômio $p(x)$ o número natural n e escrevemos $\partial p(x) = n$, se e somente se $a_n \neq 0$ e $a_j = 0$ para todo $j > n$.*

Exemplo 14. *(1)* $p(x) = 8 - 2x^6 \Rightarrow \partial p(x) = 6$;

(2) $p(x) = 5x^3 + x^2 \Rightarrow \partial p(x) = 3$.

Observação: Vale lembrar que não se define grau para polinômio nulo.

Definição 4.3. *Dois polinômios $p(x) = a_0 + a_1x^1 + a_2x^2 + a_3x^3 + \ldots a_nx^n$ e $q(x) = b_0 + b_1x^1 + b_2x^2 + b_3x^3 + \ldots b_nx^m$ sobre o corpo $(K, +, \cdot)$ são iguais se, e semente se são identicamente nulos ou tenham o mesmo grau e $a_i = b_i$ em K para todo $i \in \{0, 1, 2, \ldots\}$.*

Seja $p(x)$ um polinômio sobre o corpo K. Para um valor dado x_0, definimos o valor $p(x_0)$ como raiz de $p(x)$ se $p(x_0) = 0$.

Definição 4.4. *Consideremos os polinômios*

$$p(x) = a_0 + a_1x^1 + a_2x^2 + a_3x^3 + \ldots a_mx^m + \ldots = \sum_{i=1}^{m} a_ix^i$$

com $a_m \neq 0$ e $a_j = 0, \forall j > m$

e

$$q(x) = b_0 + b_1x^1 + b_2x^2 + b_3x^3 + \ldots b_nx^n + \ldots = \sum_{i=1}^{n} b_ix^i$$

com $a_n \neq 0$ e $a_j = 0, \forall j > n$

Definimos:

a) Adição

$$p(x) + q(x) = (p + q)(x) = c_0 + c_1x + c_2x^2 + \ldots + c_kx^k + \ldots = \sum_{i=0}^{k} c_ix^i$$

onde $c_i = (a_i + b_i) \in C$ *e* $c_j = 0, \forall j > k$.

b) Multiplicação

$$p(x) \cdot q(x) = (pq)(x) = c_0 + c_1x + c_2x^2 + \ldots + c_kx^k + \ldots$$

$$= \sum_{i=0}^{m+n} c_ix^i$$

onde $c_j = 0, \forall j > m+n$ *e*

$c_0 = a_0b_0, c_1 = a_0b_1 + a_1b_0, c_2 = a_0b_2 + a_1b_1 + a_2b_0, \ldots, c_{m+n} = a_0b_{m+n} + a_1b_{m+n-1} + \ldots + a_{m+n-1}b_1 + a_{m+n}b_0 = a_m \cdot b_n$ *e* $k \in \mathbb{N}$.

Fica definido de agora em diante que $K[x]$ representa o conjunto de todos os polinômios sobre K, em uma variável x.

Teorema 4.1. *Seja* $p,\ q \in K[x]$, *polinômios não nulos, então:*

a) $\partial(p+q) \leq max\{\partial p, \partial q\}$.

b) $\partial(pq) = \partial p + \partial q$

Demonstração. Seja $p(x) = \sum_{i=0}^{m} a_ix^i$ e $q(x) = \sum_{i=0}^{n} b_ix^i$ com $a_m \neq 0$, $b_n \neq 0$, $\partial p = m$ e $\partial q = n$. Pela propriedade da tricotomia $m = n$ ou $m < n$ ou $m > n$.

a) Se $m = n$, temos que $max\{m, n\} = m$ e por definição:

$$c_i = a_i + b_i = 0 + 0 = 0, \forall i > n$$

como $c_n = a_n + b_n$ pode ser zero, concluimos que $\partial(p+q) \leq max\{\partial p, \partial q\}$.

No caso de $m < n$, temos:

$$c_n = a_n + b_n = 0 + b_n \text{ e } c_i = a_i + b_i = 0 + 0 = 0, \forall i > n$$

portanto $\partial(p+q) = m = max\{\partial p, \partial q\}$.

Para o caso de $m > n$ se prova de forma análoga.

b) Claramente o coeficiente $c_{m+n} = a_m + b_n$ é lider, e portanto $\partial(p \cdot q) = \partial p + \partial q$. □

Proposição 4.1. *A adição e a multiplicação em* $K[x]$ *têm as seguintes propriedades, para quaisquer* $p(x), q(x) e h(x)$ *em* $K[x]$*:*

$$\textbf{\textit{Associativa :}} \begin{cases} (p(x) + q(x)) + h(x) = p(x) + (q(x) + h(x)), \\ (p(x) \cdot q(x)) \cdot h(x) = p(x) \cdot (q(x) \cdot h(x)) \end{cases} ;$$

Comutativa : $\begin{cases} p(x)+q(x)=q(x)+p(x), \\ p(x)\cdot q(x)=q(x)\cdot p(x) \end{cases}$;

Distributiva : $p(x)\cdot(q(x)+h(x))=p(x)\cdot q(x)+p(x)\cdot h(x)$;

Existência de elemento neutro aditivo : *O polinômio nulo é o elemento neutro, ou seja,* $p(x)=0+p(x)$ *para todo* $p(x)\in K[x]$;

Existência de simétrico : *Dado* $p(x)=a_0+a_1x+\ldots+a_nx^n$, *o simétrico de* $p(x)$ *é o polinômio* $-p(x)=(-a_0)+(-a_1)x+\ldots+(-a^n)x^n$;

Existência de elemento neutro multiplicativo: *O polinômio constante* $p(x)=1$ *é tal que* $1\cdot p(x)=p(x)$, *para todo* $f(x)\in K[x]$.

4.2 Divisão Euclidiana para Polinômios

Introduziremos nesse tópico os conceitos de divisibilidade de polinômios em um corpo K, em particular $K=\mathbb{C}$.

Teorema 4.2. *(Algoritmo da Divisão). Seja* $p(x),h(x)\in(\mathbb{C},+,\cdot)$ *e* $h(x)\neq 0$. *Então existe e são únicos,* $q(x),r(x)\in\mathbb{C}[x]$ *tal que:*

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

onde $0\leq\partial r(x)<\partial h(x)$.

Demonstração. Seja $p(x)=a_0+a_1x+\ldots+a_nx^n$ e $h(x)=b_0+b_1+\ldots+b_mx^m$, onde $\partial p(x)=n$ e $\partial h(x)=m$.

Para o caso de $p(x)$ ser um polinômio nulo, ou seja, $p(x)=o$, para provarmos o teorema tomamos $q(x)=r(x)=0$.

Se $p(x)\neq 0$ e como $\partial p(x)=n$ e $\partial h(x)=m$, temos que, $n<m$ ou $n\geq m$. Se acontecer de $n<m$, basta tomarmos $q(x)=0$ e $r(x)=p(x)$.

A demonstração para o caso de $n\geq m$ será feita por indução sobre $n=\partial p(x)$. Portanto se $n=0$, então $0=\partial p(x)\geq m=\partial h(x)$, ou seja $m=0$, essim $p(x)=a_0\neq 0$(lembre que tamos considerando $p(x)$ não nulo) e $h(x)=b_0$. Como $\mathbb{C}$ é um corpo e $b_0\in\mathbb{C}$, temos que $b^{-1}\in\mathbb{C}$, assim fazendo uso da propriedade associativa: $p(x)=a_0=a_0\cdot(b_o^{-1}\cdot b_0)=(a_0\cdot b_0{-}1)\cdot b_0=(a_0\cdot b_0{-}1)\cdot h(x)$, e portanto $q(x)=a_0b_0^{-1}$ e $r(x)=0$. Logo é verdadeiro para $n=0$.

Supondo o resultado válido para todo os polinômios com grau menor do que $n = \partial p(x)$, queremos provar que também que vale para $p(x)$, para isso definimos um polinômio $r_1(x) = p(x) - a_n b_m^{-1} x^{m-n} h(x)$. Como o polinômio $a_n b_m^{-1} x^{m-n} h(x)$ tem coeficiente lider a_n e grau n, que cancela o termo $a_n x^n$ em $p(x)$, então $\partial r_1(x) < \partial p(x)$. Desta forma pela hipótese de indução, existe $q_1(x)$ e $r'(x)$ tal que: $r_1(x) = q_1(x).h(x) + r'(x)$, onde $0 \leq \partial r'(x) < \partial h(x)$.

Como $r_1(x) = p(x) - a_n b_m^{-1} x^{n-m} h(x)$, temos que:

$$p(x) = a_n b_m^{-1} x^{n-m} h(x) + r_1(x)$$

$$= a_n b_m^{-1} x^{n-m} h(x) + (q_1(x).h(x) + r'(x))$$

$$= (a_n b_m^{-1} x^{n-m} + q_1(x))h(x) + r'(x).$$

Tomando $q(x) = a_n b_m^{-1} x^{n-m} + q_1(x)$ e $r(x) = r'(x)$, chegamos ao fato de que $p(x) = q(x) \cdot h(x) + r(x)$. Logo por indução, a propriedade vale para todo n natural.

Unicidade

Vamos mostra a unicidade por contradição. Para isso, consideremos $q'(x), q"(x), r'(x)$ e $r"(x)$ tais que:

$$p(x) = q'(x) \cdot h(x) + r'(x) = q"(x) \cdot h(x) + r"(x)$$

$$\Leftrightarrow (q'(x) - q"(x))h(x) = r"(x) - r'(x)$$

onde $0 \leq \partial r'(x) < \partial h(x)$ e $0 \leq \partial r"(x) < \partial h(x)$.

Supondo $q'(x) - q"(x) \neq 0$. Sendo assim $r"(x) - r'(x) \neq 0$, pois, $h(0)$ é um polinômio não nulo. Pelo teorema 4.1, $\partial(r"(x) + r'(x)) \leq max\{\partial r'(x), \partial r"(x)\}$ e $\partial(q'(x) - q"(x)) \cdot h(x) = \partial(q'(x) - q"(x) + \partial h(x)$, como $0 \leq \partial r'(x) < \partial h(x)$ e $0 \leq \partial r"(x) < \partial h(x)$, temos $\partial(q'(x) - q"(x))h(x) \geq \partial h(x) > max\{\partial r'(x), \partial r"(x)\} \geq \partial(r"(x) + (-r'(x))$ o que é um absurdo. Portanto temos que ter $q'(x) - q"(x) = 0$, e assim $q'(x) = q"(x)$, e consequentimente $r'(x) = r"(x)$. □

O fato de estarmos trabalhando com corpos é fundamental para garantir várias propriedades dos polinômios, pois se considerarmos um corpo $(K, +, \cdot)$ e um polinômio $p(x) \in K[x]$ de grau n, então o número de raízes de $p(x)$ em K é no máximo igual a $n = \partial p(x)$. Esse fato não pode ser garantido caso $(K, +, \cdot)$ seja um anel qualquer, como exemplo dessa afirmação, se tomarmos o polinômio $p(x) = x^2 - x$ sobre o anel $(\mathbb{Z}_6, +, \cdot)$, onde $\mathbb{Z}_6 = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{4}, \overline{5}\}$ veremos que $p(x)$ possui quatro raízes, são elas: $\overline{0}, \overline{1}, \overline{3}$ e $\overline{4}$.

4.3 Polinômios Irredutíveis e o Critério de Eisenstein

Nessa seção falaremos dos polinômios com Coeficientes Inteiros, definiremos polinômios irredutíveis e finalizaremos falando do critério de Eisenstein.

Definição 4.5. *Um polinômio* $p(x) = a_0 + a_1x + \ldots + a_nx^n$, *com* $a_0, a_1, \ldots, a_n \in \mathbb{Z}$ *é chamado de polinômios com coeficientes inteiros de grau* n.

Dados os elementos $a, b \in \mathbb{Z}$, usaremos aqui a notação $a|b$, para dizer que a divide b, e quando a não dividir b representaremos por $a \nmid b$. Por definição a divide b quando existe $q \in \mathbb{Z}$ tal que $b = q \cdot a$.

Definida essas notações, podemos fazer a demonstração do teorema abaixo que será usado na demonstração do teorema 4.4.

Teorema 4.3. *Sejam* $a, b, c \in \mathbb{Z}$ *tal que* $a|(b+c)$ *e* $a|b$, *então* $a|c$.

Demonstração: Ddo que $a|(b+c)$ e $a|b$, pelo o que acabamos de definir, existe $q, r \in \mathbb{Z}$ tal que $b + c = q \cdot a$ e $b = r \cdot a$. Juntando essas duas igualdades, temos:

$$b + c = q \cdot a \Rightarrow r \cdot a + c = q \cdot a \Rightarrow c = (q - r) \cdot a$$

portanto concluimos que $a|c$.

Definição 4.6. *Seja* K *um corpo e* $p(x) \in K[x]$ *um polinômio tal que* $\partial p(x) \geq 1$. *Dizemos que* $p(x)$ *é um polinômio irredutivel sobre* K *se toda vez que* $p(x) = q(x).h(x)$, $q(x), h(x) \in K[x]$ *então* $q(x)$ *ou* $h(x)$ *é um polinômio constante em* K.

Também podemos definir que o polinômio $p(x) \in K[x]$ é irredutivel sobre K se for impossível expressar $p(x)$ como um produto de dois polinômios $q(x)$ e $h(x)$ de $K[x]$, com $\partial q(x) \geq 1$ e $\partial h(x) \geq 1$.

Definição 4.7. *Se* $p(x)$ *for não irredutível sobre* K, *dizemos que* $p(x)$ *é redutível sobre* K.

Exemplo 15. *Notemos que o polinômio* $p(x) = x^2 + 2$ *é irredutível sobre* $\mathbb{R}$. *No entanto* $p(x)$ *é redutível sobre* $\mathbb{C}$, *pois,* $p(x) = x^2 + 2 = (x + \sqrt{2}i) \cdot (x - \sqrt{2}i)$.

Portanto só faz sentido dizer que um polinômio $p(x)$ é irredutivel se for dito qual corpo estamos trabalhando.

4.3.1 Critério de Eisentein

Em geral a verificação de irredutibilidade de um polinômio sobre um corpo é um problema muito difícil. Nesta subseção vamos ver um teorema que nos dá condições suficiente para que um polinômio $p(x) \in \mathbb{Z}[x]$ seja irredutível sobre $\mathbb{Q}$.

Antes de enuciarmos a proposição abaixo conhecida como lema de Gauss, notemos que se dado $p(x) = \frac{a_0}{b_0} + \frac{a_1}{b_1}x + \ldots + \frac{a_n}{b_n}x^n \in \mathbb{Q}[x]$ e $m = M.M.C(b_0, b_1, \ldots, b_n)$, então $m \cdot p(x) \in \mathbb{Z}[x]$.

Proposição 4.2. *Se $p(x) \in \mathbb{Z}[x]$ irredutível sobre $\mathbb{Z}$, então $p(x)$ é irredutível sobre $\mathbb{Q}$.*

Teorema 4.4. *(Critério de Eisenstein) Dado o polinômio $f(x) = a_0 + a_1x + \ldots + a_nx^n \in \mathbb{Z}[x]$. Se existir um número primo p tal que $p^2 \nmid a_0, p|a_1, p|a_2, \ldots p|a_{n-1}$ e $p \nmid a_n$. Então, $f(x)$ é irredutível em $\mathbb{Q}$.*

Demonstração. Pela proposição 4.2, basta provarmos que $f(x)$ é irredutivel sobre $\mathbb{Z}$. Supondo por contradição que,

$$f(x) = q(x) \cdot h(x) = (b_0 + b_1x + \ldots + b_mx^m) \cdot (c_0 + c_1x + \ldots + c_rx^r)$$

onde $1 \leq \partial q(x) = m < \partial f(x) = n, 1 \leq \partial h(x) = r < n$ e $n = m + r$.

Pela definição 4.4 parte (b) $a_0 = b_0 \cdot c_0$. Como por hipótese $p|a_0$, temos que $p|b_0$ ou $p|c_0$, mas não ambos, pois $p^2 \nmid a_0$. Sem perda alguma podemos tomar:

$$p|b_0 \text{ e } p \nmid c_0 \qquad (*)$$

Novamente pela definição 4.4 parte b), temos:

- $a_1 = b_0 \cdot c_1 + b_1 \cdot c_0$, como por hipótese $p|a_1$ segue de $(*)$ e do teorema 4.3 que $p|b_1$;
- $a_2 = b_0 \cdot c_2 + b_1 \cdot c_1 + b_2 \cdot c_0$, como por hipótese $p|a_2$ e pelo caso anterior $p|b_1$, segue de $(*)$ e pelo teorema 4.3 que $p|b_2$.

Proseguindo com isso, demonstramos que $p|b_j$ para cada $j \in \{0, 1, 2, \ldots, m\}$. Como $a_n = b_m \cdot c_r$ e $p|b_m$, temos que $p|a_n$, o que é uma contradição, pois por hipótese $p \nmid a_n$. □

Exemplo 16. *O polinômio $f(x) = x^4 + 3x^3 - 6x^2 + 12x + 4$ é irredutivel sobre $\mathbb{Q}$. Poís o critério de Einsenstein se aplica para o primo $p = 3$.*

4.4 Teorema Fundamental da Álgebra

O famoso Teorema Fundamental da Álgebra (TFA) garante que o corpo dos complexos $\mathbb{C}$ é algebricamente fechado. Este Teorema possui uma longa história e muitas demonstrações, mais nenhuma delas se faz com métodos puramente algébricos, devendo-se sempre usar métodos da análise matemática. Nesse seção citamos o TFA sem fazer sua demonstração.

Definição 4.8. *Dizemos que um corpo K é algebricamente fechado se todo polinômio não constante $p(x) \in K[x]$ tem pelo menos uma raiz em K.*

Corolário 4.1. *Seja K um corpo algebricamente fechado e seja ainda $p(x) \in K[x] \setminus K$. Se $\partial p(x) = n > 0$, então existe $\alpha_1, \alpha_2, \ldots, \alpha_n \in K$ e $a \in K$ tal que*

$$p(x) = a \cdot (x - \alpha_1) \cdot (x - \alpha_2) \cdot \ldots \cdot (x - \alpha_n)$$

A prova desse colorário pode ser feita por indução sobre n, levando em consideração que se α é raiz de $p(x)$, então $x - \alpha$ divide $p(x)$ e assim $p(x) = (x - \alpha) \cdot q(x)$, onde $0 \leq \partial q(x) < \partial p(x)$.

Exemplo 17. *O corpo $\mathbb{R}$ não é algebricamente fechado, pois o polinômio $p(x) = x^2 + 2 \in \mathbb{R}[x]$ não possui raiz em $\mathbb{R}$.*

Teorema 4.5 (Teorema Fundamental da Álgebra)**.** *Seja $p(x) \in \mathbb{C}[x] \setminus \mathbb{C}$. O polinômio $p(x)$ admite pelo menos uma raiz em $\mathbb{C}$.*

De posse do TFA e do corolário 4.1, podemos afirmar que qualquer polinômio $p(x) \in \mathbb{C}[x]$ pode ser representado da forma

$$p(x) = a \cdot (x - \alpha_1) \cdot (x - \alpha_2) \cdot \ldots \cdot (x - \alpha_n)$$

onde $\alpha_1, \alpha_2, \ldots, \alpha_n \in \mathbb{C}$ são raízes e $a \in \mathbb{C}$.

A representação $a \cdot (x - \alpha_1) \cdot (x - \alpha_2) \cdot \ldots \cdot (x - \alpha_n)$ é chamada forma fatorada de $p(x)$. Caso a raiz $\alpha_i \in \mathbb{C}$ com $i \in \{1, 2, \ldots, n\}$ apareça apenas uma vez na forma fatorada de $p(x)$, dizemos que α_i é uma raiz simples. Se α_i aparecer $m \in \mathbb{N}$ vezes na fatoração, dizemos que α_i é uma raiz múltipla de multiplicidade m.

Exemplo 18. *É fácil ver que $p(x) = x^4 + 7x^3 + 18x^2 + 20x + 8 = (x + 1) \cdot (x + 2)^3$, logo $\alpha_1 = -1$ é uma raiz simples e $\alpha_2 = -2$ é uma raiz múltipla de multiplicidade 3.*

Capítulo 5

Extensões Algébricas e Grau de uma Extensão

Neste capítulo, estabelecemos a definição de números algébricos, números transcendentes, extensão de corpos e grau de uma extensão, os quais são fundamentais para atingirmos nossos objetivos.

5.1 Números Algébricos e Transcendente

Definição 5.1. *Seja K um corpo. Um número α é dito algébrico sobre K se existir $p(x) \in K[x]\backslash\{0\}$, tal que $p(\alpha) = 0$. Do contrário dizemos que α é transcendente sobre K.*

Quando um número α é algébrico sobre $\mathbb{Q}$, dizemos apenas que α é algébrico. Se for transcendente sobre $\mathbb{Q}$, dizemos que α é transcendente.

Exemplo 19. *O número $\sqrt{2}$ é algébrico, pois $\sqrt{2}$ é raiz do polinômio $p(x) = x^2 - 2$. Já os números irracionais π e e são transcendente sobre $\mathbb{Q}$, pois $p(\pi) \neq 0$ e $p(e) \neq 0$ para todo $p(x) \in \mathbb{Q}[x]$.*

As demonstrações da transcedência de π e e, foge dos nossos objetivos, pois necessitam do conhecimento de análise infinitesimal, e portanto, vamos aceitar aqui sem demonstração a transcedência dos dois. No entanto, claramente se ver que que π e e, são algébricos sobre o conjunto dos números reais.

Definição 5.2. *Definimos que um corpo L é uma extensão do corpo K, se K for um subcorpo de L.*

Definição 5.3. *Seja $K \subset L$, onde K é um corpo. Se para todo $\alpha \in L$, α é algébrico sobre K então L é uma extensão algébrica.*

Exemplo 20. *O corpo $\mathbb{R}$ é uma extensão do corpo $\mathbb{Q}$, no entanto pela definição anterior $\mathbb{R}$ não é uma extensão algébrica, pois o número transcedente π não pertence ao conjunto $\mathbb{Q}$. Por outro lado, π é algébrico em $\mathbb{R}$, pois é raiz do polinômio $p(x) = x - \pi \in \mathbb{R}[x]$.*

Teorema 5.1. *Todo corpo K é algébrico sobre si mesmo.*

Demonstração. Notamos que para todo $\alpha \in K$, o polinômio $p(x) = x - \alpha \in K[x]$, tem α como raiz. □

Agora vamos tomar $\alpha \in L \supset K$, e com isso definirmos o conjunto $K[\alpha] = \{p(\alpha) : p(x) \in K[x]\}$. No caso de α ser um elemento algébrico sobre K, o conjunto $K[\alpha]$ é um subcorpo de L, pois sendo α algébrico sobre K implica por definição que existe $p(x) \in K[x]$ tal que $p(\alpha) = 0$, e alem disso, dado $p(x), q(x) \in K[x]$ temos que $p(\alpha), q(\alpha), -q(\alpha) \in K[\alpha]$ e assim $p(\alpha) - q(\alpha) \in K[\alpha]$ e $p(\alpha) \cdot q(\alpha) \in K[\alpha]$.

Definição 5.4. *Seja a extensão $L \supset K$, e S um subconjunto de L. Definimos $K[S]$ como sendo uma extensão de K gerada por S, onde $K[S]$ é o menor subcorpo de L contendo $K \cup S$.*

Na definição acima, claramente se ver que $K[S]$ é uma extensão sobre K contida no corpo L, e assim quando for dado $S = \{\alpha_0, \alpha_1, \ldots, \alpha_r\}$, escrevemos $K[S] = K[\alpha_0, \alpha_1, \ldots, \alpha_r]$.

Definição 5.5. *Uma extensão L sobre K diz-se simples, se existe α pertencente a L tal que $L = K[\alpha]$.*

Exemplo 21. *Dado a extensão $L = \mathbb{R} \supset \mathbb{Q}$, e o número $\alpha = \sqrt{2} \in \mathbb{R}$, então $\mathbb{Q}[\sqrt{2}] = \{a + b\sqrt{2} : a, b \in \mathbb{Q}\}$.*

De fato, pela condição acima $\mathbb{Q}[\sqrt{2}] = \{p(\sqrt{2}) : p(x) \in \mathbb{Q}[x]\}$. Pelo o algoritmo da divisão, se $p(x) \in \mathbb{Q}$ então existe $q(x), r(x) \in \mathbb{Q}[x]$ tal que $p(x) = q(x) \cdot (x^2 - 2) + r(x)$, onde $r(x) = a + bx$, com $a, b \in \mathbb{Q}$.

Tomando $x = \sqrt{2}$, temos:

$$p(\sqrt{2}) = q(\sqrt{2}) \cdot ((\sqrt{2})^2 - 2) + r(\sqrt{2}) \Rightarrow p(\sqrt{2}) = q(\sqrt{2}) \cdot (2 - 2) + r(\sqrt{2})$$

$$\Rightarrow p(\sqrt{2}) = q(\sqrt{2}) \cdot 0 + r(\sqrt{2})$$

$$\Rightarrow p(\sqrt{2}) = r(\sqrt{2})$$

.

Como $r(x) = a + b\sqrt{2}$, temos então $p(\sqrt{2}) = r(\sqrt{2}) = a + b\sqrt{2}$. Portanto $\mathbb{Q}[\sqrt{2}] = \{a + b\sqrt{2} : a, b \in \mathbb{Q}\}$.

É possível provar que, se $\alpha \in L \supset K$ é um elemento algébrico sobre K, então $K[\alpha]$ é um subcorpo de L. Em particular no exemplo acima $\mathbb{Q}[\sqrt{2}]$ é um corpo.

5.2 Noções Básicas de Álgebra Linear

Nessa seção, vamos fazer um estudo das noções básicas da álgebra linear, como espaço vetorial, base e dimensão. Essas ferramentas, serão necessárias para a definição do grau de uma extensão.

Definição 5.6. *Seja K um corpo qualquer, e V um conjunto não vazio onde está definida as operações de adição e multiplicação por um número de K, conforme abaixo.*

$$\begin{cases} + : V \times V \to V \\ (u, v) \rightsquigarrow u + v \end{cases} \quad e \quad \begin{cases} \cdot : K \times V \to V \\ (\lambda, v) \rightsquigarrow \lambda \cdot v \end{cases}$$

O conjunto V munido dessas operações acima é dito um espaço vetorial sobre o corpo K, se as propriedades abaixo forem verificadas para quaisquer que sejam os elementos $u, v, w \in V$ e $\alpha, \beta \in K$.

A) ***Adição:***

A_1) Comutatividade: $u + v = v + u$

A_2) associatividade: $(u + v) + w = u + (v + w)$

A_3) Existência do elemento neutro: $\exists 0 \in V$ tal que $u + 0 = 0 + u = u$

A_4) Existência de inverso: $\forall x \in V \exists y \in V$ tal que $x + y = y + x = 0$

M) ***Multiplicação:***

M_1 Associatividade : $(\alpha \cdot \beta) \cdot u = \alpha \cdot (\beta \cdot u)$

M_2 Distributividade : $\begin{cases} (\alpha + \beta) \cdot u = \alpha \cdot u + \beta \cdot u \\ \alpha \cdot (u + v) = \alpha \cdot u + \alpha \cdot v \end{cases}$

M_3 Multiplicação por 1: $1 \cdot u = u$

Exemplo 22. *Sendo S um conjunto não vazio e K um corpo. O símbolo $\mathcal{F}(S, K)$ representa o conjunto de todas as funções $f, g : S \to K$. Ele se torna um espaço vetorial sobre*

o corpo K, quando se define a soma $f+g$ de duas funções e o produto $\alpha \cdot f$ do número $\alpha \in K$ pela função f da maneira natural:

$$(f+g)(x) = f(x) + g(x) \ \forall x \in S$$

$$(\alpha f)(x) = \alpha \cdot f(x) \ \forall x \in S$$

Do exemplo acima temos em particular que se $K = \mathbb{R}$ então $\mathcal{F}(S, K = \mathbb{R})$ é dito um espaço vetorial sobre $\mathbb{R}$. Notemos tambem que variando o conjunto S, obtêm-se diversos exemplos de espaços da forma $\mathcal{F}(S, \mathbb{R})$. Como exemplo temos $\mathcal{F}([0,1], \mathbb{R})$ e $\mathcal{F}(\{1, 2 \ldots, n\}, \mathbb{R}) = \mathbb{R}^n$, onde $\mathbb{R}^n$ representa o espaço vetorial euclidiano n-dimensional.

Notemos que as operações de soma e multiplicação dadas por:

$$\begin{cases} L \times L \to L \\ (u, v) \rightsquigarrow u + v \end{cases} \quad \text{e} \quad \begin{cases} K \times L \to L \\ (\lambda, v) \rightsquigarrow \lambda \cdot v \end{cases}$$

já existem de forma natural em uma extensão algébrica L sobre o corpo K e alem disso cumpre com todas as propriedades de um espaço vetorial, e portanto, pode ser chamado de um espaço vetorial sobre K.

Definição 5.7. *Seja V um espaço vetorial e K um corpo. Um subconjunto não vazio W de V é dito subespaço vetorial de V se as seguintes condições forem satisfeitas:*

(1) $0 \in W$;

(2) Se $u, v \in W$ então $u + v \in W$;

(3) Se $u \in W$ então, para todo $\alpha \in K$, temos $\alpha \cdot u \in W$.

Definição 5.8. *Sejam $A = \{v_1, v_2, \ldots, v_n\} \subset V$ e os elementos $a_1, a_2, \ldots a_n$ pertencente ao corpo K. Qualquer vetor $v \in V$ escrito da forma:*

$$v = a_1 v_1 + a_2 v_2 + \ldots + a_n v_n$$

é uma combinação linear dos vetores $v_1, v_2, \ldots v_n$.

Definição 5.9. *Consideremos o espaço vetorial V, o corpo K e $A = \{v_1, v_2, \ldots, v_n\} \subset V$. Dizemos que A é linearmente independente (e simbolicamente representamos por LI) se a equação vetorial $\sum_{i=1}^{n} \alpha_i v_i = 0$, $\alpha_i \in K$ admite apenas a solução trivial $\alpha_1 = \alpha_2 = \ldots = \alpha_n = 0$. Do contrário dizemos que A é linearmente dependente (e simbolicamente representamos por LD).*

Exemplo 23. *O conjunto W de todos os vetores de V que são combinações lineares dos vetores de A é um subespaço vetorial de V.*

De fato, se:

$$\begin{cases} u = a_1v_1 + a_2v_2 + \ldots + a_nv_n \\ w = b_1v_1 + b_2v_2 + \ldots + b_nv_n \end{cases}$$

são dois vetores de W. Temos que:

(1) $0 = 0v_1 + 0v_2 + \ldots + 0v_n \in W$

(2) $u + w = (a_1 + b_1)v_1 + (a_2 + b_2)v_2 + \ldots (a_n + b_n)v_n \in W$

(3) $\alpha u = (\alpha a_1)v_1 + (\alpha a_2)v_2 + \ldots + (\alpha a_n)v_n \in W$

Quando todos os vetores do espaço vetorial V são combinações lineares dos vetores de A, dizemos que V é gerado por A. E alem disso se A for LI, dizemos que A é uma base do espaço vetorial V.

Definição 5.10. *Todo espaço vetorial V sobre um corpo K possui uma base. Alem disso se uma base de V tem n elementos, então toda base de V possui n elementos. O número n de elementos de uma base chamamos de dimensão do espaço vetorial V sobre o corpo K e simbolicamente representamos por $[V : K] = n$.*

5.3 Grau de uma Extensão

Claramente uma extensão $L \supset K$ é um espaço vetorial sobre o corpo K. A dimensão do espaço vetorial L sobre K é dada por $[L : K]$. Chamamos $[L : K]$ de grau da extensão L sobre K. Desta forma dizemos que uma extensão $L \supset K$ é finita se a dimensão $[L : K] < \infty$. Caso contrário $L \supset K$ diz-se uma extensão infinita.

Exemplo 24. *Dado o conjunto $Q[\sqrt{2}] = \{a + b\sqrt{2}, a, b \in \mathbb{Q}\}$ é uma extensão de $\mathbb{Q}$ com $[Q[\sqrt{2}] : \mathbb{Q}] = 2$.*

Exemplo 25. *$\mathbb{R}$ é uma extensão de $\mathbb{Q}$ de grau infinito. Isso é equivalente dizer que π é transcedente.*

Já sabemos que todo número $c \in \mathbb{C}$ pode ser escrito da forma $c = a+bi$, onde $a, b \in \mathbb{R}$. Isso nos garante que o conjunto $\{1, i\}$ é uma base do espaço vetorial $\mathbb{C}$ sobre $\mathbb{R}$. Então pelas condições acima a extensão $\mathbb{C} \supset \mathbb{R}$ tem grau $[\mathbb{C} : \mathbb{R}] = 2$.

Antes de anunciarmos o próximo teorema vejamos a seguinte definição.

Definição 5.11. *Dado $\alpha \in L$ algébrico sobre K. O polinômio não nulo, mônico e de menor grau $p(x) \in K[x]$, tal que $p(\alpha) = 0$. É chamado de polinômio minimal de α sobre K. Simbolicamente representaremos tal polinômio como $p(x) = irr(\alpha, K)$.*

O fato de α ser algébrico sobre o corpo K garante que $irr(\alpha, K)$ existe e além disso é irredutível. De fato sendo α algébrico sobre K, por definição existe $p(x) \in K[x]\backslash\{0\}$ tal que $p(\alpha) = 0$. Supondo que $irr(\alpha, K) = p(x) = q(x) \cdot h(x)$ com $\partial q(x) \geq 0$ e $\partial h(x) \geq 0$, então α será raiz de $q(x)$ ou $h(x)$, onde ambos tem grau menor que o grau de $p(x)$. Como $q(x)$ e $h(x)$ podem ser polinômios mônicos, caimos em um absurdo, pois $p(x) = irr(\alpha, K)$.

Teorema 5.2. *Seja $L \supset K$, α algébrico sobre K. Se o grau do polinômio $irr(\alpha, K)$ é n, então para todo $p(x) \in K[x]$, $p(\alpha)$ pode ser expresso de modo único na forma $p(\alpha) = a_0 + a_1\alpha + a_2\alpha^2 + \ldots + a_{n-1}\alpha^{n-1}$, onde $a_i \in K$, $\forall i \in \{o, 1, \ldots, n\}$.*

Demonstração. Seja $f(x) = irr(\alpha, K)$. Pela hipótese $\partial f(x) = n$. Tomando $p(x) \in K[x]$, pelo algoritmo da divisão (teorema 4.2) $\exists q(x), r(x) \in K[x]$ tal que $p(x) = q(x) \cdot f(x) + r(x)$, onde $0 \leq \partial r(x) < \partial f(x)$. Assim o polinômio $r(x)$, é algo do tipo $r(x) = a_0 + a_1x + a_2x^2 + \ldots + a_{n-1}x^{n-1}$, com $a_i \in K$, e $i \in \{0, 1, 2, \ldots, n-1\}$.

Tomando $x = \alpha$, temos:

$$p(\alpha) = q(\alpha) \cdot f(\alpha) + r(\alpha).$$

Como por hipótese α é algébrico sobre K, temos então $f(\alpha) = 0$, e assim:

$$p(\alpha) = q(\alpha) \cdot f(\alpha) + r(\alpha) \Rightarrow p(\alpha) = r(\alpha)$$

e portanto $p(\alpha) = r(\alpha) = a_0 + a_1\alpha + a_2\alpha^2 + \ldots + a_{n-1}\alpha^{n-1}$.

Para provarmos a unicidade vamos supor $p(\alpha) = a_0 + a_1\alpha + a_2\alpha^2 + \ldots + a_{n-1}\alpha^{n-1}$ e $p(\alpha) = b_0 + b_1\alpha + b_2\alpha^2 + \ldots + b_{n-1}\alpha^{n-1}$, temos daí que, $(a_0 - b_0) + (a_1 - b_1)\alpha + (a_2 - b_2)\alpha^2 + \ldots + (a_{n-1} - b_{n-1})\alpha^{n-1} = 0$. Seja $t(x) \in K[x]$, tal que $t(x) = (a_0 - b_0) + (a_1 - b_1)x + (a_2 - b_2)x^2 + \ldots + (a_{n-1} - b_{n-1})x^{n-1}$. Como $t(\alpha) = 0$ e $\partial t(x) \leq n - 1 < n = irr(\alpha, K)$, temos que $t(x) = o$ (ou seja é o polinômio nulo), e assim $a_0 - b_0 = 0, a_1 - b_1 = 0, a_2 - b_2 = 0, \ldots, a_{n-1} - b_{n-1} = 0$. Assim concluimos que $a_i = b_i, \forall i \in \{0, 1, \ldots, n-1\}$. O que prova a unicidade. □

Exemplo 26. *O número real $\sqrt[3]{5}$ é claramente algébrico sobre $\mathbb{Q}$, e $irr(\sqrt[3]{5}, \mathbb{Q}) = x^3 - 5 \Rightarrow \partial irr(\sqrt[3]{5}, \mathbb{Q}) = 3$. Tomando o polinômio $p(x) \in \mathbb{Q}$, onde $p(x) = x^4 - 2x^3 - x^2 + x - 6$, temos que $p(\sqrt[3]{5}) = (\sqrt[3]{5})^4 - 2(\sqrt[3]{5})^3 - (\sqrt[3]{5})^2 + \sqrt[3]{5} - 6 = -16 + 6(\sqrt[3]{5})^1 - 1(\sqrt[3]{5})^2$.*

Teorema 5.3. *Seja K um corpo e $L \supset K$ uma extensão de K. Então,*

i) se $L \supset K$ é finita, então $L \supset K$ é algébrica;

ii) se $\alpha \in L \supset K$ é um elemento algébrico sobre K e grau $irr(\alpha, K)$ é igual a n então $1, \alpha, \ldots, \alpha^{n-1}$ é uma base do espaço vetorial $K[\alpha]$ sobre K e $[K[\alpha] : K] = n < \infty$.

iii) se $\alpha \in L \supset K$ é um elemento transcedente sobre K então $[K] \supset K$ é uma extensão infinita.

Demonstração. i) Supondo que $[L : k] = n < \infty$. Para $\alpha \in L$, o conjunto $\{1, \alpha, \alpha^2, \ldots, \alpha^n\}$ é linearmente dependente (LD) em L sobre K (pois tem $n+1$ elementos). Portanto existem $a_0, a_1, a_2, \ldots, a_n \in K$, não todos nulos, tais que:

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

Claramente o polinômio $p(x) = a_0 + a_1x + a_2x^2 + \ldots + a_nx^n \in K[x]$ tem α como raiz. Logo α é algébrico sobre K.

ii) Seja $\alpha \in L \supset K$ um elemento algébrico sobre K e $\partial irr(\alpha, K) = n$. Pelo teorema 5.2 todo elemento de $K[\alpha]$ pode ser escrito de modo único como combinação linear dos elementos do conjunto $\{1, \alpha, \alpha^2, \ldots, \alpha^{n-1}\}$ sobre K. Assim pela definição 5.10, o conjunto $\{1, \alpha, \alpha^2, \ldots, \alpha^{n-1}\}$ é uma base de $K[\alpha]$ sobre K. Portanto $[K[\alpha] : K] = n$.

iii) Note que, se a extensão $K[\alpha] \supset K$ fosse finita, pelo item (i) seria algébrica. Portanto $K[\alpha] \supset K$ é infinita. □

Decorre imediatamente do teorema 5.3 que se $\alpha \in L \supset K$ é algébrico sobre K, então $K[\alpha]$ é uma extensão algébrica finita de K.

5.4 Teorema da Torre

O próximo teorema, nos garante uma facilidade maior no cálculo do grau de determinadas extensões, uma vez que, permite usar outras com grau já conhecidos.

Teorema 5.4. *Sejam $M \supset L \supset K$ corpos tais que $[M : L]$ e $[L : K]$ são finitos então $[M : K]$ é finito e $[M : K] = [M : L] \cdot [L : K]$.*

Consideramos a baixo os conjunto I e J, onde $I = \{1, 2, \ldots, r\}$ e $J = \{1, 2, \ldots, s\}$.

Demonstração. Seja $(v_i)_{i \in I}$ uma base para o espaço vetorial de M sobre L e $(u_j)_{j \in J}$ uma base do espaço vetorial L sobre K. Vamos provar que $(v_i \cdot u_j)_{i \in I, j \in J}$ é uma base do espaço

vetorial de M sobre K e isto pela definição 5.10 demonstra a proposição. Para mostrarmos que $(v_i \cdot u_j)_{i\in I, j\in J}$ é uma base, devemos primeiramente provar que este conjunto é LI em M sobre K. Para isto, tomemos,

$$\sum_{i,\ j} \alpha_{ij} v_i u_j = 0$$

onde $\alpha_{ij} \in K, 1 \leq i \leq r$ e $1 \leq j \leq s$.

Podemos reescrever a equação acima do seguinte modo:

$$(\alpha_{11}u_1 + \alpha_{12}u_2 + \ldots + \alpha_{1s}u_s)v_1 + \ldots + (\alpha_{r1}u_1 + \alpha_{r2}u_2 + \ldots + \alpha_{rs}u_s)v_r = 0$$

Como os elementos u_j estão em L e $(v_i)_{i\in I}$ uma base para o espaço vetorial de M sobre L. Segue pela independência linear do conjunto $(v_i)_{i\in I}$ em M sobre L, que:

$$\begin{cases} \alpha_{11}u_1 + \alpha_{12}u_2 + \ldots + \alpha_{1s}u_s = 0 \\ \vdots \ \vdots \ \vdots \ \vdots \ \vdots \ \vdots \ \vdots \ \vdots \ \vdots \ \vdots \ \vdots \\ \alpha_{r1}u_1 + \alpha_{r2}u_2 + \ldots + \alpha_{rs}u_s = 0 \end{cases}$$

Ora, como $\alpha_{ij} \in K$ e $(u_j)_{j\in J}$ uma base do espaço vetorial L sobre K. Pela dependência linear $\alpha_{ij} = 0$ para todos $i \in I$ e $j \in J$. Assim $(v_i \cdot u_j)_{i\in I, j\in J}$ é LI de M sobre K.

Resta mostrar que todo y pertencente ao espaço vetorial M sobre K, pode ser escrito como combinação linear de $(v_i \cdot u_j)_{i\in I, j\in J}$. Ou seja, $(v_i \cdot u_j)_{i\in I, j\in J}$ gera M sobre K. Começamos no fato de $(v_i)_{i\in I}$ ser uma base para o espaço vetorial de M sobre L e assim existe $\lambda_i \in L$ com $i \in I$ tal que:

$$y = \sum_{i=1}^{r} \lambda_i v_i \quad \rightsquigarrow \ (*)$$

Como $\lambda_i \in L$ e $(u_j)_{j\in J}$ uma base do espaço vetorial L sobre K, podemos escrever λ_i como combinação linerar de $\{u_1, u_2, \ldots, u_s\}$. Ou seja, existe $\alpha_{i,j} \in K$ tal que:

$$\lambda_1 = \sum_{j=1}^{s} \alpha_{1j}u_j, \ \lambda_2 = \sum_{j=1}^{s} \alpha_{2j}u_j, \ \ldots, \lambda_i = \sum_{j=1}^{s} \alpha_{ij}u_j, \ \ldots, \ \lambda_r = \sum_{j=1}^{s} \alpha_{rj}u_j$$

Substituindo esses resultados em $(*)$. Segue que:

$$y = \sum_{i=1}^{r} \alpha_{i,j} v_i u_j$$

onde $\alpha_{i,j} \in K$.

Portanto $(v_i \cdot u_j)_{i\in I, j\in J}$ é uma base para o espaço vetorial de M sobre K, e sua dimensão é $r \cdot s = [M : k] = [M : L] \cdot [L : K]$. □

Exemplo 27. *Já sabemos pelo exemplo 24 que* $[\mathbb{Q}[\sqrt{2}] : \mathbb{Q}] = 2$. *Dado o conjunto* $\big(\mathbb{Q}[\sqrt{2}]\big)[\sqrt{3}] = \{a + b\sqrt{3} : a, b \in \mathbb{Q}[\sqrt{2}]\}$, *visivelmente o conjunto* $\{1, \sqrt{3}\}$ *é uma base para o espaço vetorial* $\big(\mathbb{Q}[\sqrt{2}]\big)[\sqrt{3}]$ *sobre* $\mathbb{Q}[\sqrt{2}]$, *e assim* $[\big(\mathbb{Q}[\sqrt{2}]\big)[\sqrt{3}] : \mathbb{Q}[\sqrt{2}]] = 2$. *Como* $\big(\mathbb{Q}[\sqrt{2}]\big)[\sqrt{3}] \supset \mathbb{Q}[\sqrt{2}] \supset \mathbb{Q}$, *pelo teorema 5.4, temos que:*

$$[\big(\mathbb{Q}[\sqrt{2}]\big)[\sqrt{3}] : \mathbb{Q}] = [\big(\mathbb{Q}[\sqrt{2}]\big)[\sqrt{3}] : \mathbb{Q}[\sqrt{2}]] \cdot [\mathbb{Q}[\sqrt{2}] : \mathbb{Q}] = 2 \cdot 2 = 4$$

.

Notemos que, o conjunto $\{1, \sqrt{2}, \sqrt{3}, \sqrt{6}\}$ é uma base do espaço vetorial $\big(\mathbb{Q}[\sqrt{2}]\big)[\sqrt{3}]$ sobre $\mathbb{Q}$.

Corolário 5.1. *Se* $K_n \supset \ldots \supset K_1 \supset K_0$ *são corpos tais que* $[K_n : K_{n-1}]$, $[K_{n-1} : K_{n-2}]$, $\ldots, [K_1 : K_0]$ *são finitos, então*

$[K_n : K_0] = [K_n : K_{n-1}] \cdot [K_{n-1} : K_{n-2}] \cdot \ldots \cdot [K_1 : K_0]$.

Exemplo 28. *Consideremos os conjuntos* $\big(\big(\mathbb{Q}[\sqrt{2}]\big)[\sqrt{3}]\big)[\sqrt{5}] = \{a + b\sqrt{5} : a, b \in \big(\mathbb{Q}[\sqrt{2}]\big)[\sqrt{3}]\}$. *É fácil ver que o conjunto* $\{1, \sqrt{5}\}$ *é uma base do espaço vetorial* $\big(\big(\mathbb{Q}[\sqrt{2}]\big)[\sqrt{3}]\big)[\sqrt{5}]$ *sobre* $\big(\mathbb{Q}[\sqrt{2}]\big)[\sqrt{3}]$ *e assim* $[\big(\big(\mathbb{Q}[\sqrt{2}]\big)[\sqrt{3}]\big)[\sqrt{5}] : \big(\mathbb{Q}[\sqrt{2}]\big)[\sqrt{3}]]$. *Como* $\big(\big(\mathbb{Q}[\sqrt{2}]\big)[\sqrt{3}]\big)[\sqrt{5}] \supset \big(\mathbb{Q}[\sqrt{2}]\big)[\sqrt{3}] \supset \mathbb{Q}[\sqrt{2}] \supset \mathbb{Q}$, *temos pelo teorema 5.4 que:* $[\big(\big(\mathbb{Q}[\sqrt{2}]\big)[\sqrt{3}]\big)[\sqrt{5}] : \mathbb{Q}] = [\big(\big(\mathbb{Q}[\sqrt{2}]\big)[\sqrt{3}]\big)[\sqrt{5}] : \big(\mathbb{Q}[\sqrt{2}]\big)[\sqrt{3}]] \cdot [\big(\mathbb{Q}[\sqrt{2}]\big)[\sqrt{3}] : \mathbb{Q}[\sqrt{2}]] \cdot [\mathbb{Q}[\sqrt{2}] : \mathbb{Q}] = 2 \cdot 2 \cdot 2 = 8$.

Capítulo 6

Construção por meio de Régua e Compasso

O objetivo desse capítulo, é fazer com que o leitor tenha noção sobre as construções geométricas fundamentais de desenho geométrico, para que assim tenha um bom entendimento do próximo capítulo.

6.1 Construções Elementares

6.1.1 Uso da Régua e Compasso

Vamos começar as construções geométricas, definindo as regras básicas para a utilização da rágua e compasso.

Definição 6.1. *a) Com uma régua não graduada, conhecendo dois pontos distintos em um plano é possível traçar uma única reta que passa por esses dois pontos.*

b) Com um compasso, é possivel tracar uma circunferência com centro em um dado ponto e que passa por um segundo ponto conhecido.

6.1.2 Retas Perpendiculares

1º Caso:

Dado um ponto A e uma reta r passando por A. Trace um reta t perpendicular a reta r que passa por A.

Passos

(1) Com o compasso centrado em A e abertura qualquer, tracemos uma circunferência λ cortando a reta r em dois pontos B e C;

(2) Com o centro em B e abertura do compasso maior que o raio da circunferência λ, trace uma nova circunferência λ_1. Mantendo a abertura façamos o mesmo procedimento com o compasso centrado em C, obtendo assim a circunferência λ_2 e os pontos D, E $\in \lambda_1 \cap \lambda_2$;

(3) Com a régua ligue os pontos D e C, gerando assim a reta t perpendicular a r.

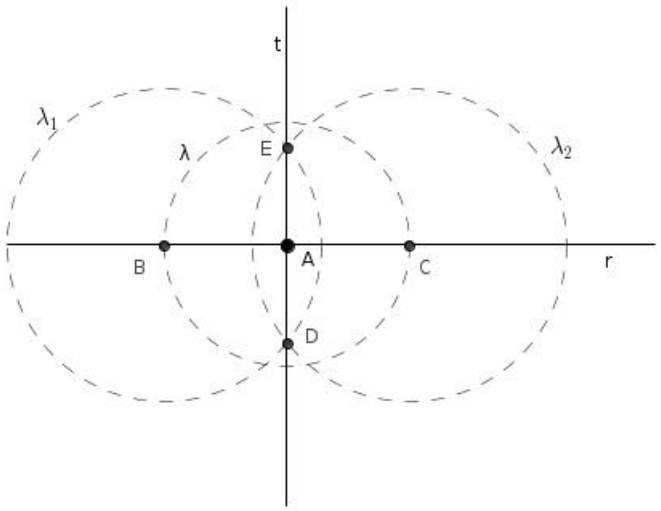

Figura 6.1: Retas Perpendiculares 1

2º Caso:

Dado um ponto A fora da reta r. Trace uma reta t perpendicular a r e que passe pelo ponto A.

Passos

(1) Com o compasso centrado em A e abertura maior que a distância de A até a reta r, tracemos uma circunferência λ tocando a reta r em dois pontos B e C;

(2) Com o centro em B e com abertura do compasso maior que a metade de $\overline{BC}$, tracemos uma circunferência λ_1. Mantendo a mesma abertura do compasso façamos o mesmo procedimento com o compasso centrado em C, obtemos assim a circunferência λ_2 e os pontos D, $E \in \lambda_1 \cap \lambda_2$;

(3) Tracemos uma reta t ligando os pontos D e E. Notemos que $A \in t$ e $t \perp$ r.

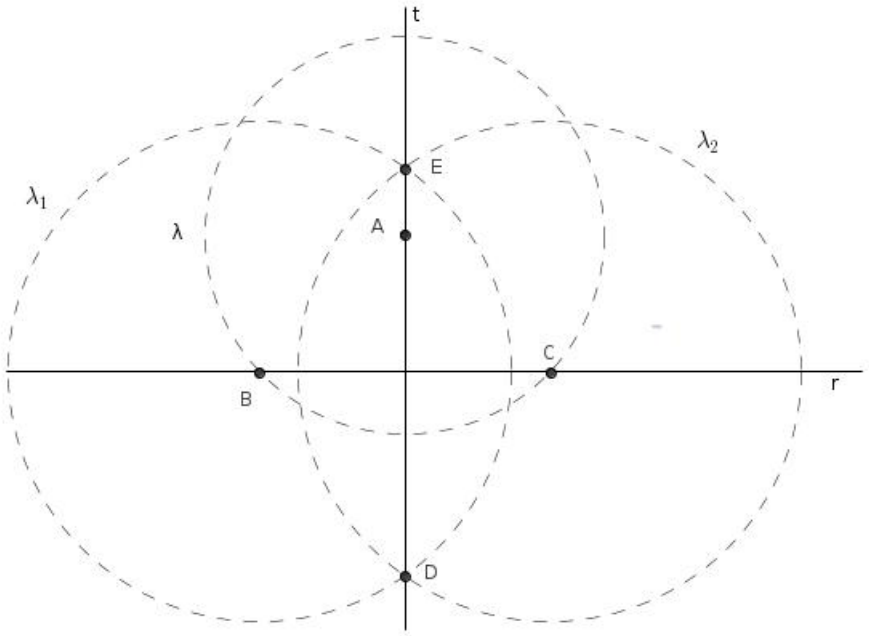

Figura 6.2: Retas Perpendiculares 2

6.1.3 Retas Paralelas

Dado uma reta r e um ponto A fora dela, traçar uma reta paralela a r passando por A.

Passos

(1) Tome o compasso com uma abertura maior do que a distância do ponto A a reta r, e com centro em A desenhe uma circunferência λ intersectando a reta r em dois pontos B e C.

(2) Tome um desses pontos, digamos, C. Com a mesma abertura e com centro em C, desenhe a circunferência λ_1 intersectando r nos pontos D e E.

(3) Depois, com a mesma abertura e centro em E, desenhe a circunferência λ intersectando a primeira em F.

(4) Tracemos a reta t ligando os pontos A e F. Notemos que $A \in t$ e t é paralela a r.

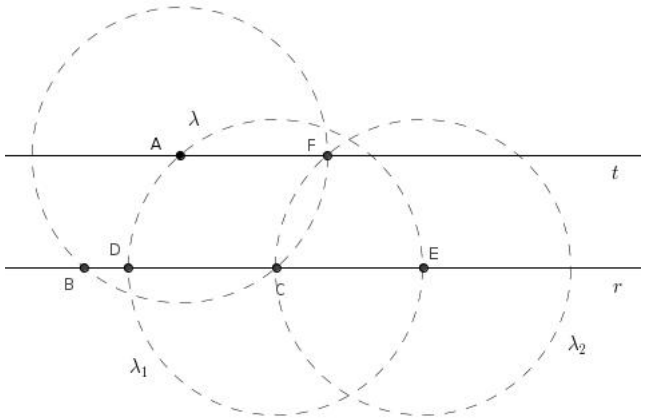

Figura 6.3: Retas Paralelas

Vale lembra que por definição duas retas são paralelas quando são coplanares e não se intersectam.

6.1.4 Mediatriz

A mediatriz t de um segmento qualquer AB, é perpendicular a esse segmento e passa pelo seu ponto médio.

Passos

(1) Tome o compasso centrado no ponto A, e com abertura maior do que a metade de $\overline{AB}$, trace uma circunferência λ_1.

(2) Depois, com o compasso centrado em B e mesma abertura, trace outra circunferência λ_2 intersectando a primeira em dois pontos, digamos, C e D.

(3) Depois é só ligar os pontos C e D com uma régua. Portanto, a reta t que passa por C e D é a mediatriz de AB.

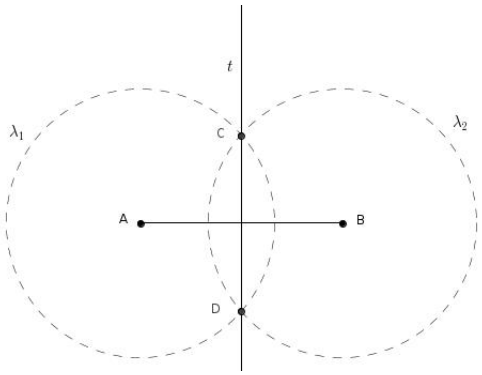

Figura 6.4: Mediatriz do Segmento

Ressaltamos que a mediatriz de um segmento é o conjunto de todos os pontos equidistantes dos extremos desse segmento.

6.1.5 Bissetriz

Dizemos que bissetriz de um ângulo é a semirreta que o divide em dois ângulos iguais. Para entendermos melhor consideremos o seguinte problema.

Dado um ângulo qualquer de vértice no ponto A, traçar a sua bissetriz do ângulo $\angle BAC$.

Passos

(1) Tome o compasso centrado no vértice do ângulo (ponto A) e, com uma abertura qualquer, trace uma circunferência λ_1, intersectando os lados do ângulo em dois pontos, digamos B e C.

(2) Em seguida, com mesma abertura, centro em B e depois centro em C, trace as circunferências λ_2 e λ_3, cujas uma das intersecções é o ponto D

(3) Ligue os pontos A e D com uma régua. Temos assim que $\overrightarrow{AD}$ é a bissetriz do ângulo $\angle BAC$.

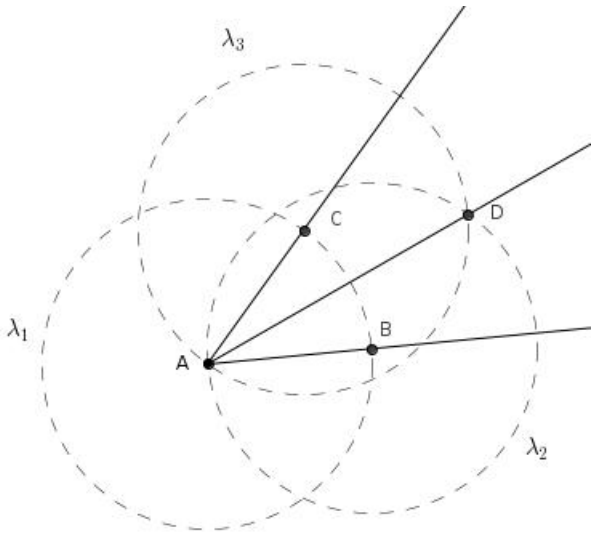

Figura 6.5: Bissetriz do Ângulo

6.1.6 Utilizando o Teorema de Tales

Segundo o Teorema de Tales, um feixe de retas paralelas determina sobre duas retas transversais quaisquer, segmentos correspondentes proporcionais. O Teorema de Tales

é tido como um dos resultados fundamentais da Geometria Euclidiana plana, e será de grande importância para justificar a construção da quarta proporcional, e também será usado na demonstração de teoremas no capítulo 7.

Teorema 6.1. *(Teorema Tales) Sejam r, s, t retas paralelas. Dados os pontos $A, A' \in r$, $B, B' \in s$ e $C, C' \in t$, de modo que A, B, C e A', B', C' sejam dois ternos de pontos colineares (veja a figura). Então*

$$\frac{\overline{AB}}{\overline{A'B'}} = \frac{\overline{BC}}{\overline{B'C'}} = \frac{\overline{AC}}{\overline{A'C'}}.$$

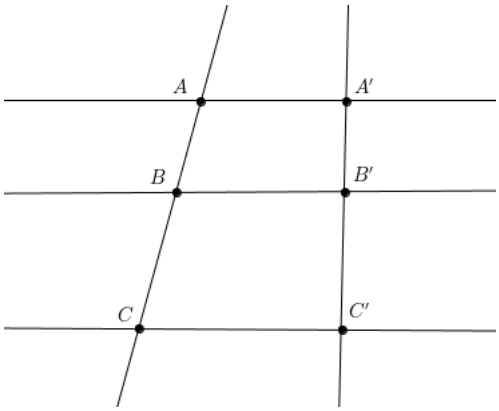

Figura 6.6: Teorema de Tales

O leitor interessado em mais detalhes sobre esse teorema pode consultar as referências [2] e [6].

Definição 6.2. *Seja a, b e c números reais positivos, vamos dizer que o número real também positivo x é a quarta proporcional de a, b e c nessa ordem, se*

$$\frac{a}{b} = \frac{c}{x}.$$

Caso a, b e c sejam comprimento de três segmentos, o segmento de comprimento x que satisfaz a igualdade acima é a quarta poporcional dos segmentos a, b e c nessa ordem. No caso de $b = c$ o elemento x será denominado de terceira proporcional.

Exemplo 29. *Descreva os passos da construção com régua e compasso da quarta proporcional x, supondo que seja dado os segmentos a, b e c.*

Passos

(1) Trace duas retas r e s, concorrentes no ponto A;

(2) Marque sobre a reta r os segmentos AB e BC tais que $\overline{AB} = a$ e $\overline{BC} = c$;

(3) Marque sobre a reta s os segmentos AD tal que $\overline{AD} = b$;

(3) Trace usando os procedimentos da subceção 6.3.3, a paralela a reta $\overleftrightarrow{BD}$, a qual intersecta a reta s no ponto E. Pelo teorema de Thales, temos $\frac{a}{b} = \frac{c}{x} \Rightarrow x = \frac{bc}{a}$.

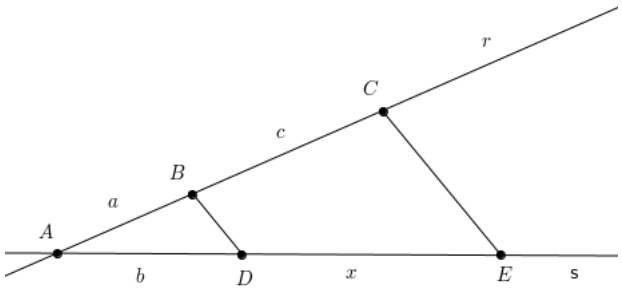

Figura 6.7: Quarta proporcional

6.1.7 Triângulo equilátero

Definição 6.3. *Triângulo equilátero é todo triângulo em que os três lados são iguais.*

Para contruirmos um triângulo equilátero com régua e compasso basta seguir os passos abaixo.

(1) tome um segmento AB;

(2) Com centro em A e raio $\overline{AB}$, fazer uma circunferência λ_1;

(3) Com centro em B e raio $\overline{BA}$, fazer uma circunferência λ_2;

(4) O ponto de encontro entre λ_1 e λ_2 é C e D;

(5) Os triângulos ABC e ABD são equilátero.

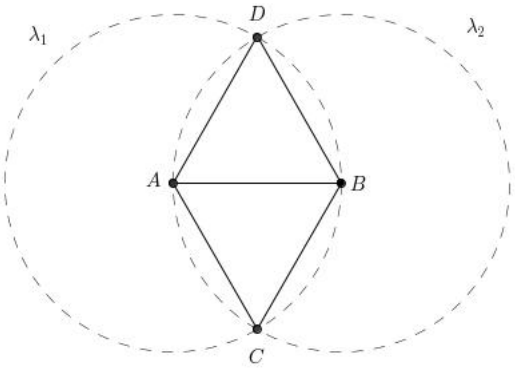

Figura 6.8: Triângulo equilátero

Em um triângulo ABC, a altura relativa ao lado BC é um segmento que têm uma extremidade no vértice A(oposto ao lado BC) e a outra extremidade, digamos H está no segmento BC de tal forma que BC e AH sejam ortogonais(ou seja formam um ângulo de 90^o). A mediana relativa a BC é o segmento que tem uma extemidade no vértice A e a outra no ponto médio M do lado BC. O triângulo ABC é dito isósceles de base BC quando $\overline{AB} = \overline{AC}$.

Teorema 6.2. *Se ABC é um triângulo isósceles de base BC, então $A\widehat{B}C = A\widehat{C}B$ e a bissetriz interna, mediana e altura relativas ao lado BC coincidem.*

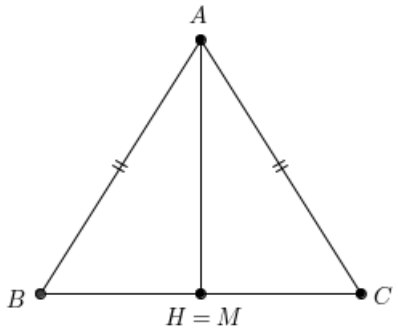

Figura 6.9: Tiângulo isósceles

Corolário 6.1. *Os ângulos internos de um triângulo equilátero são todos iguais.*

Demonstração. Basta observar que todos os lados do triângulo equilátero podem ser vistos como base, e assim aplicar as condições do teorema 6.2. □

Para nos ajudar no entendimento da próxima definição vamos enunciar e provar o teorema do ângulo inscrito.

Teorema 6.3. *Se AB e AC são cordas de uma circunferência λ de centro O, então a medida do ângulo inscrito $\angle BAC$ é igual à metade da medida do ângulo central $\angle BOC$ correspondente.*

Demonstração. Para essa demonstração, devemos tomar três casos separadamente. O caso em que o ângulo $\angle BAC$ contém o centro O, o caso em que o ângulo $\angle BAC$ não contém o centro O e o caso em que o centro O está sobre um lado do ângulo $\angle BAC$.

Vamos provar aqui apenas o caso em que o ângulo $\angle BAC$ contém o centro O em seu interior. Note que os triângulos OAC e OAB são isósceles de bases $\overline{AC}$ e $\overline{AB}$

respectivamente. Desta forma $O\widehat{A}C = O\widehat{C}A = x$ e $O\widehat{A}B = O\widehat{B}A = y$. Portanto $A\widehat{O}C = 180^o - 2x$,$A\widehat{O}B = 180^o - 2y$ e $B\widehat{A}C = O\widehat{A}C + O\widehat{A}B = x + y$. Tomando $B\widehat{O}C = \alpha$, temos $A\widehat{O}C + A\widehat{O}B + B\widehat{O}C = 360 \Rightarrow 180^o - 2x + 180 - 2y + \alpha = 360 \Rightarrow -2x - 2y + \alpha = 0 \Rightarrow x + y = \frac{\alpha}{2} \Rightarrow O\widehat{A}B = \frac{\alpha}{2}$. □

A demonstração mais completa desse teorema pode ser visto na referência [10] páginas 107 e 108.

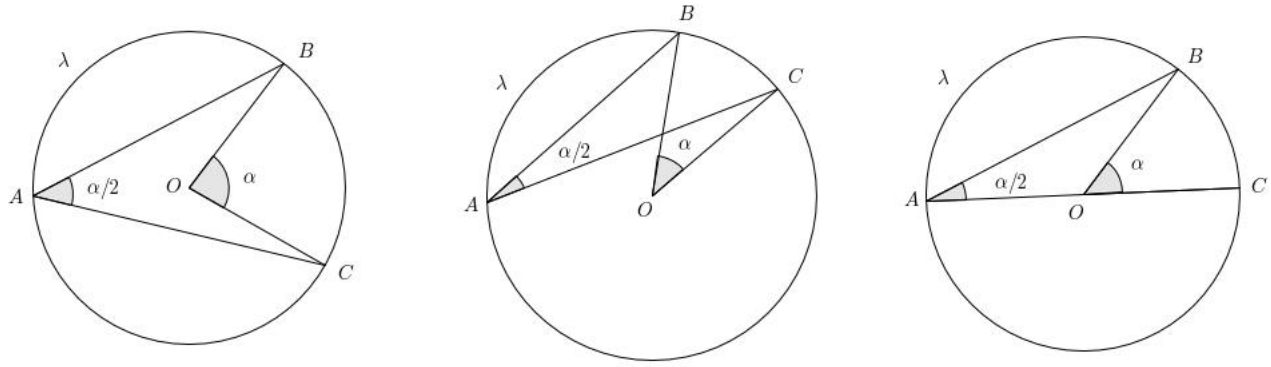

Figura 6.10: Ângulo inscrito

6.1.8 Arco capaz

Definição 6.4. *Dado numa circunferência λ, uma corda AB e um ponto P pertencente ao arco $\widehat{AB}$. O ângulo $\alpha = A\widehat{P}B$ é constante para todo $P \in \widehat{AB}$. E o arco $\widehat{AB}$ é chamado de Arco capaz.*

Para uma melhor compreensão dessa definição vejamos a figura abaixo.

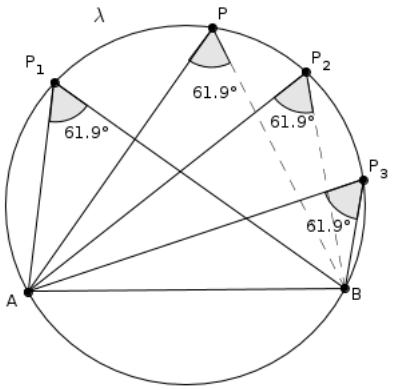

Figura 6.11: Arco capaz

O que diz a definição acima é justificado pelo teorema 6.3. Portanto dado uma circunferência λ de centro O e um corda AB de λ, destacamos um caso particular importante da teorema 6.3 que é aquele em que AB é um diâmetro de λ . Sendo P um ponto de λ distinto de A e B, segue do referido teorema que $A\widehat{P}B = \frac{1}{2} \cdot 180^o = 90^o$.

A prova do teorema supracitado, de certa forma nos ensina como construir os arcos capazes de um ângulo α sobre o segmento AB, quando $0^o < \alpha \leq 90^o$. No caso de $\alpha = 90^o$, temos somente de construir uma circunferência de diâmetro AB. Devido a essa afirmação, não será mostrado a construção do arco capaz de um ângulo α, pois as ferramentas de construção geométrica citada acima são suficientes apenas para construir o arco capaz quando $\alpha = 90^o$.

Vejamos como é ilustrado na figura abaixo.

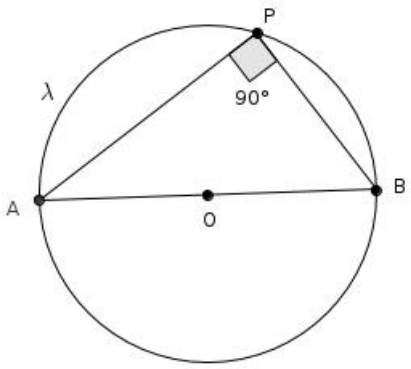

Figura 6.12: Ângulo inscrito em uma semicircunferência

Para a construção da figura acima com régua e compasso é só traçar a mediatriz do segmento AB. O ponto de interseção da mediatriz com o segmento AB é o centro da circunferência λ.

6.2 Média Geométrica ou Média Proporcional

Para desenvolvermos essa seção vamos precisar relembrar algumas propriedades sobre os triângulos retângulo.

6.2.1 Relações Métricas no Triângulo Retângulo

Seja ABC um triângulo retângulo em A, utilizando de nosso estudo de retas perpendiculares caso 2, é possível tracar o segmento $\overline{AH}$ perpendicular à hipotenusa, obtendo

assim novos elementos nesse triângulo. Vejamos abaixo.

Figura 6.13: Relações métricas no triângulo retãngulo

Dados:

(i) $a = m + n$;

(ii) Altura relativa a hipotenusa: $\overline{AH} = h$;

(iii) projeção do cateto $\overline{AB}$ sobre a hipotenusa: $\overline{BH} = m$;

(iv) projeção do cateto $\overline{AC}$ sobre a hipotenusa: $\overline{CH} = n$.

É fácil mostrar que sobre o triângulo retângulo acima vale as relações abaixo.

(1) $b^2 = a \cdot n$

(2) $c^2 = a \cdot m$

(3) $h^2 = m \cdot n$

Pelas condições acima temos que:

$$b^2 + c^2 = a \cdot n + a \cdot m = a \cdot (n + m) = a \cdot a = a^2$$

$$\Rightarrow b^2 + c^2 = a^2$$

Essa igualdade é conhecida na matemática como Teorema de Pitágoras.

Definição 6.5. *(Média Geométrica) Chama-se média geométrica entre dois segmentos* $\overline{AB}$ *e* $\overline{CD}$*, o segmento* x *tal que* $x^2 = \overline{AB} \cdot \overline{CD}$.

Notemos que as as igualdades (1), (2) e (3) representam médias geométricas.

Para a construção da raiz quadrada de um número, podemos levar em conta a média geométrica das projeções dos catetos de um triângulo retângulo sobre a hipotenusa. Usando a forma das relações métricas (1), (2) e (3), tem-se:

(1') $b = \sqrt{a \cdot n}$

(2') $c = \sqrt{a \cdot m}$

(3') $h = \sqrt{m \cdot n}$

No próximo capítulo vamos ver que um número real positivo é chamado de construtível se for possível usar apenas um compasso e uma régua não graduada para construir com um número finito de passos um segmento de reta cujo o comprimento seja a, a partir de um segmento tomado como unidade. Destacamos também que números construtíveis são números algébricos cujo grau é uma potência de 2.

Vale antecipar que se a e b são números construtíveis, então $a + b$, $a - b$, $a \cdot b$, $\frac{a}{b}$ e $\sqrt{a}$ são números construtíveis.

6.2.2 Construindo raiz quadrado com régua e compasso

Dado um segmento $\overline{AB}$ de comprimento a onde a é um número construtível. Vamos construir com régua e compasso o segmento $x = \sqrt{a}$.

Passos

Usando as ferramentas mencionadas anteriormente e fixando uma dada unidade 1:

(1) Tracemos o segmento $\overline{AB}$ de comprimento $a > 1$;

(2) construimos uma semicircunferência λ com centro no ponto médio do segmento $\overline{AB}$;

(3) Tracemos uma perpendicular passando pelo ponto D em $\overline{AB}$ com distância de A até D igual a 1;

(4) Marcamos o ponto C de interseção entre a perpendicular e a semicircunferência.

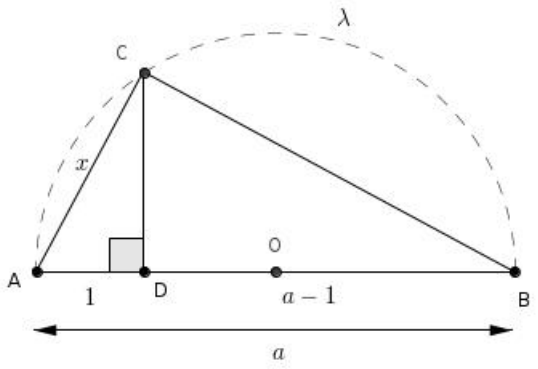

Figura 6.14: Raiz quadrada

A justificativa é simples, basta usarmos a propriedade (2') acima para concluir que $x = \sqrt{a \cdot 1} = \sqrt{a}$.

Para construir uma raiz cujo índice seja uma potência de 2, basta aplicarmos sucessivamente as construções acima, gerando irracionais algébricos.

Exemplo 30. *Os números a seguir, são números construtíveis gerados a partir de número algébricos pela relação (3'):*

* *se* $m = 2, n = 1$ *então* $h^2 = 2 \cdot 1 \Rightarrow h = \sqrt{2}$;
* *se* $m = \sqrt{2}, n = 1$ *então* $h^2 = \sqrt{2} \cdot 1 \Rightarrow h = \sqrt[4]{2}$;
* *se* $m = \sqrt{2}, n = \sqrt{3}$ *então* $h^2 = \sqrt{2} \cdot \sqrt{3} \Rightarrow h = \sqrt[4]{6}$.

6.3 Duplicação do cubo, Quadratura do círculo e a Trisecção do ângulo

Os problemas de construções geométricas na maioria das vezes são complicados e em alguns casos até impossíveis, com é o caso da duplicação do cubo, a quadratura do círculo e a trisecção do ângulo, já mencionados na introdução desse trabalho.

6.3.1 Duplicação do cubo

Como já sabemos o problema da duplicação do cubo(também chamado de problema de Delos) consiste em construir usando régua e compasso um de aresta b cujo o volume seja o dobro do volume de um cubo dado de aresta a.

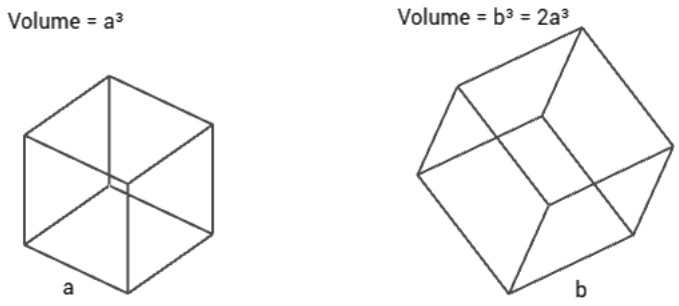

Figura 6.15: Duplicação do cubo

De forma algebrica, dado o cubo de aresta a e volume a^3, queremos obter um novo cubo de aresta b e volume b^3 onde $b^3 = 2a^3$, mas para isso, temos que obter usando apenas

régua não graduada e compasso o segmento $b = a\sqrt[3]{2}$, no entanto o número real $\sqrt[3]{2}$ não é construtível, como veremos mais adiante, e por isso o problema da duplicação do cubo com régua não graduada e compasso se torna impossível.

6.3.2 Quadratura do círculo

Este problema consiste em construir um quadrado cuja área seja igual à área de um círculo dado, utilizando apenas régua e compasso.

De modo mais formal, vamos considerar um número construtível r e um círculo Γ de raio r com área πr^2. Queremos encontrar o lado x de um quadrado, tal que $x^2 = r\sqrt{\pi}$. Ou seja:

$$x = r\sqrt{\pi}$$

.

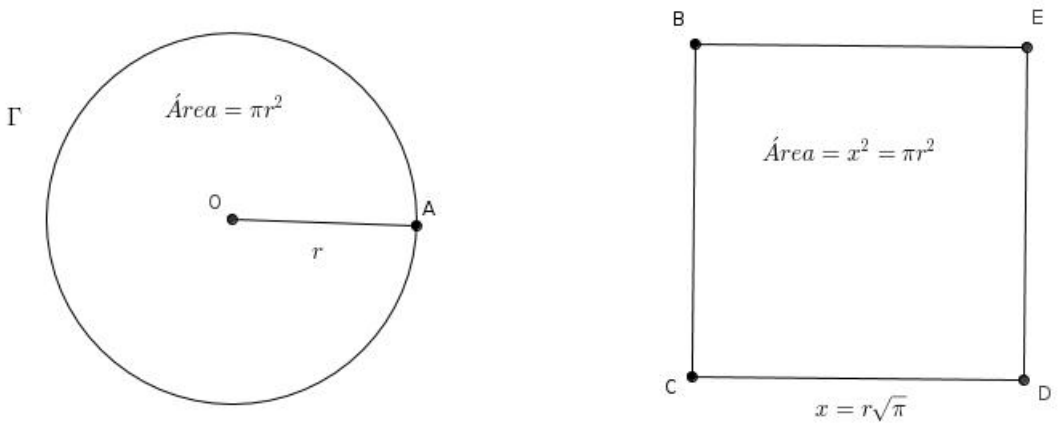

Figura 6.16: Quadratura do círculo

Como r é construtível o problema agora consiste em construir um segmento de medida $\sqrt{\pi}$. Já sabemos que π é um número transcedente e nos próximos capítulos veremos que todo número transcedente é não construtível, e portanto o número $\sqrt{\pi}$ é também não construtível, logo o problema da quadratura do círculo é impossível.

6.3.3 Trissecção do ângulo

Para começar nossos estudos, vale apenas resaltar que a trissecção de um ângulo qualquer difere dos outros dois problemas clássicos. Afirmamos isso porque existem certos

ângulos que podem ser trissectados por régua não marcada e compasso, enquanto os outros dois problemas clássicos não permitem nenhum exemplo de cubo duplicável ou círculo que possua quadratura conhecida através de uma construção que utiliza somente régua não marcada e compasso. Um exemplo de ângulo que pode ser trissectado é o ângulo de 90^o, como veremos mais a frente.

A trissecção do ângulo consiste em dividir em três partes iguais um ângulo dado. Veremos no próximo capítulo que isso é impossível por exemplo para o ângulo de 60^o.

Antes de passarmos para o próximo capítulo, vamos mostrar como é feita a trissecção do ângulo de 90^o. Para fazermos essa trisecção, primeiro consideramos no plano o ângulo $\angle AOB$ (figura 6.17) medindo 90^o, depois construímos um triângulo equilátero sobre o segmento OB dividindo o ângulo $\angle AOB$ em dois ângulos, um de 30^o e o outro de 60^o(colorário 6.1). Para finalizar é só fazermos a bissetriz do ângulo de 60^o usando os procedimentos de construção da bissetriz mencionados na subseção 6.3.3.

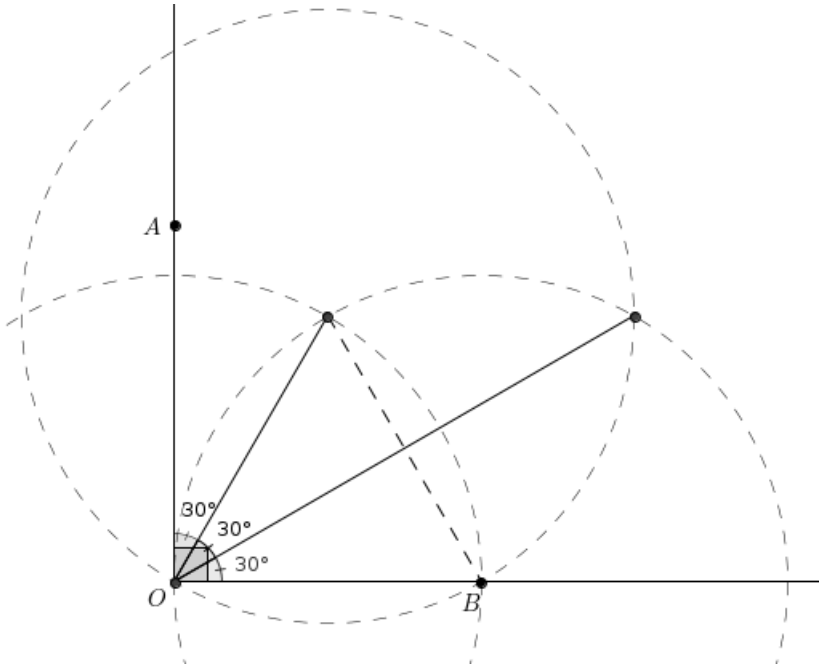

Figura 6.17: Trissecção do ângulo de 90^o

Capítulo 7

Pontos Construtíveis

7.1 Regras impostas ao compasso e a régua

Devemos ser bem claros quanto ao que é permitido fazer com régua e compasso, para assim compreendermos o porque da impossibilidade de resolver os problemas clássicos, com a régua é permitido traçar uma reta que passe por dois pontos distintos dados. Com o compasso é permitido traçar uma circunferência com centro em um ponto dado.

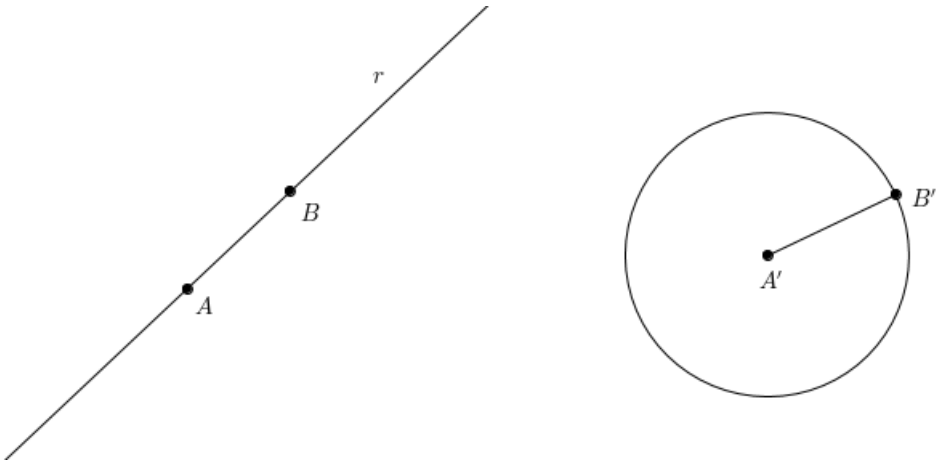

Figura 7.1: Descrição das regras impostas a régua e compasso

Vale ressaltar que a régua não possui marcação ou escalas, e o compasso usado pelos Gregos desmontava-se quando era levantado um dos seus braços, diferindo assim do compasso de hoje, que pode ser usado, por exemplo, como transferidor.

Notemos que usando o compasso dos tempos de hoje, dado um segmento $\overline{AB}$ conforme a figura acima, é possível colocar a ponta seca do compasso no ponto A e a outra ponta

no ponto B, obtendo assim uma abertura igual ao comprimento do segmento $\overline{AB}$, depois movemos o compasso sem alterar a abertura (o que é possível ao nosso compasso moderno) e colocamos a ponta seca em um novo ponto A', em seguida traçamos uma circunferência com raio $\overline{A'B'}$, (veja a figura acima) onde $\overline{A'B'} = \overline{AB}$.

Com tudo, o compasso dos tempos de hoje não muda as regras do "jogo"em nada. É possível mostrar que qualquer construção realizada com o compasso moderno, também pode ser realizada com o compasso "Grego", a única diferença é que eventualmente o compasso Grego possa envolver mais passos. Notemos por exemplo, que com qualquer um dos dois modelos (compasso Grego ou compasso moderno), podemos traçar a mediatriz de um segmento. Pois dado um segmento AB, colocamos a ponta seca do compasso em A e estenda a outra extremidade do compasso até B, tracemos uma circunferência de raio $\overline{AB}$, agora é só fazer o mesmo processo com a ponta seca em B, obtendo assim uma nova circunferência, e os pontos C e D de interseção entre as duas circunferências, depois com uma régua tracemos a mediatriz CD.

É claro que é preciso provar que $\overleftrightarrow{CD}$ é de fato a mediatriz do segmento AB, isso não será feito aqui, no entanto essa demonstração pode ser feita sem grande dificuldade.

7.2 Passando da geometria para álgebra

Nosso objetivo aqui, é juntar os conteúdos que estudamos do capítulo 1 até o capítulo 5 com os conteúdos estudados no capítulo 6, para isso começamos falando sobre os pontos construtíveis.

Como já foi dito, com a régua só é permitido traçar uma reta conhecendo seus dois pontos e ao compasso é permitido apenas traçar uma circunferência conhecendo seu centro e um ponto arbitrário da circunferência. O que é possível de se obter como resultado no final de cada passo é a intersecção entre duas retas, interseção entre retas e circunferências ou a interseção entre duas circunferências.

Resaltamos aqui, que a partir de agora nosso estudo será feito em cima do plano $\mathbb{R}^2$, com o objetivo de construirmos uma teoria que nos permita definir com precisão o que são pontos construtíveis, e assim, constatar que o conjunto de todos os números construtíveis forma um corpo.

Definição 7.1. *Seja $\mathcal{P}$ um subconjunto de $\mathbb{R}^2$ contendo pelo menos dois pontos distintos.*

Dizemos que uma reta r de $\mathbb{R}^2$ é uma reta em $\mathcal{P}$ se r contém dois distintos pontos de $\mathcal{P}$. Dizemos também que uma circunferência λ de $\mathbb{R}^2$ é uma circunferência em $\mathcal{P}$ se o centro de λ pertence a $\mathcal{P}$ e um ponto de $\mathcal{P}$ pertence a λ.

Seja r e s duas retas quaisquer em $\mathcal{P}$, consideremos também λ e Γ circunferências quaisquer em $\mathcal{P}$. as operações abaixo (i), (ii) e (iii) são chamadas de operações elementares em $\mathcal{P}$, e o conjunto $\langle\mathcal{P}\rangle$ é um subconjunto de $\mathbb{R}^2$, onde todos os seus pontos são construtíveis a partir de $\mathcal{P}$ usando as operações (i), (ii) e (iii).

(i) Interseção entre duas retas em $\mathcal{P}$: $(r \cap s) \in \langle\mathcal{P}\rangle$;

(ii) Interseção de uma reta em $\mathcal{P}$ e um circunferência em $\mathcal{P}$: $(r \cap \lambda) \subset \langle\mathcal{P}\rangle$;

(iii) Interseção de duas circunferências em $\mathcal{P}$: $(\lambda \cap \Gamma) \subset \langle\mathcal{P}\rangle$.

Notemos que, de certa forma a operação (iii) se reduz na operação (ii), pois se A e B são os pontos de interseção das circunferências λ e Γ, então os pontos A e B pertecem a $\mathcal{P}$, como por definição existe uma única reta r que passa por A e B, logo temos que r é uma reta em $\mathcal{P}$. Portanto a interseção das circunferências λ e Γ pode ser vista como interseção de λ com r e Γ com r.

Definição 7.2. *Um ponto $A \in \mathbb{R}^2$ é dito construtível a partir de $\mathcal{P}$ se for possível determinar A através das operações (i), (ii) e (iii). Vamos definir tambem o segmento unitário OU, ou seja $\overline{OU} = 1$.*

Exemplo 31. *Seja $O = (0,0)$, $U = (1,0)$ e $\mathcal{P}_0 = \{O, U\}$. Pela figura abaixo é possível perceber que fazendo uso das operações (i), (ii) e (iii), temos que $\langle\mathcal{P}_0\rangle = \{O, U, A_1, A_2, A_3, A_4\}$.*

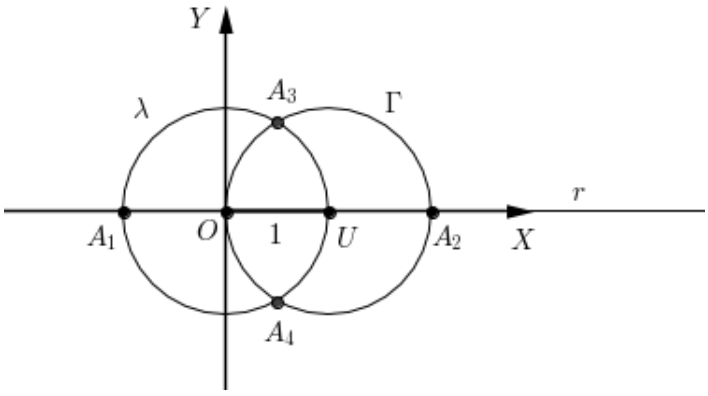

Figura 7.2: Pontos construtíveis

Na figura acima, a construçaão do conjunto $\langle\mathcal{P}_0\rangle$, podemos considerar a reta r, as circunferências λ e Γ como os passos dados para a construção dos pontos de $\langle\mathcal{P}_0\rangle$, é visível

que $A_1 \in \lambda \cap r$, $A_2 \in \Gamma \cap r$ e $\{A_3, A_4\} \subset \lambda \cap \Gamma$. Alem disso também é possível mostrar que $A_1 = (-1, 0)$, $A_2 = (2, 0)$, $A_3 = \left(\frac{1}{2}, \frac{\sqrt{3}}{2}\right)$ e $A_4 = \left(\frac{1}{2}, -\frac{\sqrt{3}}{2}\right)$.

De tudo que já foi visto, se $\mathcal{P}_0 = \{O, U\}$, definimos $\mathcal{P}_1 = \langle \mathcal{P}_0 \rangle$, $\mathcal{P}_2 = \langle \mathcal{P}_1 \rangle$, ..., $\mathcal{P}_{n+1} = \langle \mathcal{P}_n \rangle$, para todo n pertencente $\mathbb{N}$, e claramente temos que $\mathcal{P}_0 \subset \mathcal{P}_1 \subset \mathcal{P}_2 \subset \ldots \subset \mathcal{P}_n \subset \mathcal{P}_{n+1} \subset \mathbb{R}^2$. Tomando $\mathcal{P}_\infty = \mathcal{P}_0 \cup \mathcal{P}_1 \cup \mathcal{P}_2 \cup \ldots \cup \mathcal{P}_n \cup \ldots$, é visivel que $\mathcal{P}_\infty$ é um subconjunto infinito de $\mathbb{R}^2$, embora cada $\mathcal{P}_n$ seja subconjunto finito de $\mathbb{R}^2$. É imediato concluir que $\langle \mathcal{P}_\infty \rangle = \mathcal{P}_\infty$ e $(x, 0) \in \mathcal{P}_\infty, \forall x \in \mathbb{Z}$.

Agora podemos dizer que geralmente um ponto $A \in \mathbb{R}^2$, diz-se construtível a partir do conjunto $\mathcal{P}_0$, se existir o conjunto finito $\mathcal{P}_i \subset P_\infty$ $(i \in \mathbb{N})$, tal que todos os passos para a construção de A estão em $\mathcal{P}_i$. Em outras palavras, existe um número finito de passos a partir de $\mathcal{P}_0$ para a obtenção de A.

Exemplo 32. *Mostre que o ponto* $(0, 1)$ *é construido a partir de* $\mathcal{P}_2$.

Solução: Já sabemos que que $U = (1, 0)$ e $A_3 = (\frac{1}{2}, \frac{\sqrt{3}}{2})$ pertencem a $\mathcal{P}_1 = \langle \mathcal{P}_0 \rangle$, assim a reta $t = \overleftrightarrow{UA_3}$ é uma reta em $\mathcal{P}_2 = \langle \mathcal{P}_1 \rangle$. A circunferência λ_1 de centro A_3 e raio $\overline{UA_3}$ (veja afigura abaixo) é uma circunferência em $\mathcal{P}_2 = \langle \mathcal{P}_1 \rangle$. As equações $\sqrt{3}x + y = \sqrt{3}$ e $(x - \frac{1}{2})^2 + (y - \frac{\sqrt{3}}{2})^2 = \overline{UA_3}^2 = 1$ são equações da reta t e da circunferência λ_1 respectivamente. Seja o eixo OY representado por s, claramente se verifica que $(0, \sqrt{3}) = T \in t \cap \lambda_1 \cap s$, o que prova que T é construído a partir de $\mathcal{P}_2$. Ou seja s é uma reta em $\mathcal{P}_3 = \langle \mathcal{P}_2 \rangle$. Como O e U pertencem a $\mathcal{P}_3$, temos que $(0, 1)$ pertence a $\lambda \cap s$, como queriamos mostrar.

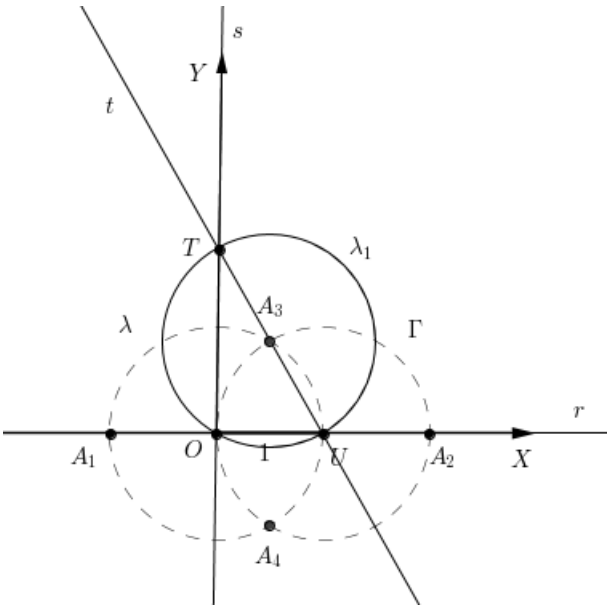

Figura 7.3: Construção do ponto (0 , 1)

Proposição 7.1. *Se A e B são pontos distintos em $\mathcal{P}_\infty$ então o ponto médio M do segmento AB pertence a $\mathcal{P}_\infty$ e as retas peperndiculasres a AB passando pelos pontos A, B e M são retas em $\mathcal{P}_\infty$.*

Demonstração. Para essa demonstração basta realizarmos os passos vistos nas subseções 6.1.2 e 6.1.4 do capítulo 6. □

Proposição 7.2. *Sejam A e r, respectivamente, um ponto construtível e uma reta construtível(retas construtíveis são retas contendo dois distintos pontos em $\mathcal{P}_\infty$) tais que $A \in r$. Sendo $B, C \in r$ pontos construtíveis então existe um ponto construtível $X \in r$ tal que $\overline{AX} = \overline{BC}$.*

A demonstração dessa proposição não tem grandes complicações e o leitor interessado, pode ter acesso a mesma consultando a referência [6] página 110.

Se $A = (x, o)$ e $B = (0, y)$ são pontos pertencentes a $\mathcal{P}_\infty$ então pela proposição 7.1 o ponto $C = (x, y)$ pertence a $\mathcal{P}_\infty$. A recíproca também é verdadeira, pois se $C = (x, y)$ pertence a $\mathcal{P}_\infty$, fazendo uso do compasso, tracemos uma circunferência λ conforme a figura abaixo, obtendo os pontos D e E, depois é só notar que os triângulos ODC e OCE são isósceles e o resto decorre do teoremas 6.2.

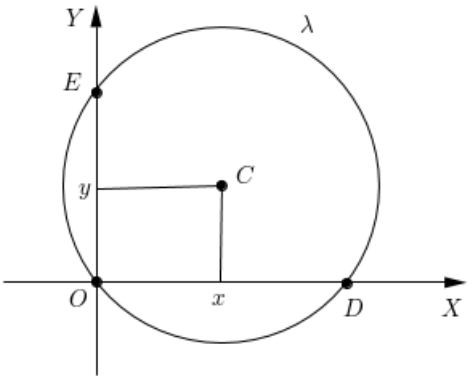

Figura 7.4: Pontos com coordenadas construtíveis

Todo elemento a pertencente ao conjunto $\mathbb{R}$ é naturalmente elemento de $\mathbb{R}^2$, para vermos isso basta escrever $a = (a, 0)$ ou $a = (0, a)$. Como já foi mostrado acima, os pontos que têm coordenadas construtíveis também é construtível e vice versa. Desta forma, definimos o subconjuto $\mathcal{C}_\mathbb{R} \subset \mathbb{R}$ onde $\mathcal{C}_\mathbb{R} = \{\alpha \in \mathbb{R} : \alpha \text{ é construtível }\}$.

Teorema 7.1. *O conjunto $\mathcal{C}_{\mathbb{R}}$ é fechado para as operações de adição e multiplicação. Em particular vale a subtração e a divisão.*

Demonstração. Seja $A, B \in \mathcal{C}_{\mathbb{R}}$, pontos de coordenadas a e b(vamos assumir sem perdas de generalidade que $a > b > 0$), respectivamente. Pela proposição 7.2 podemos construir uma circunferência λ de centro em A e raio $\overline{OB} = b$ (veja a figura abaixo), obtendo assim as coordenadas D e E de coordenadas $a - b$ e $a + b$.

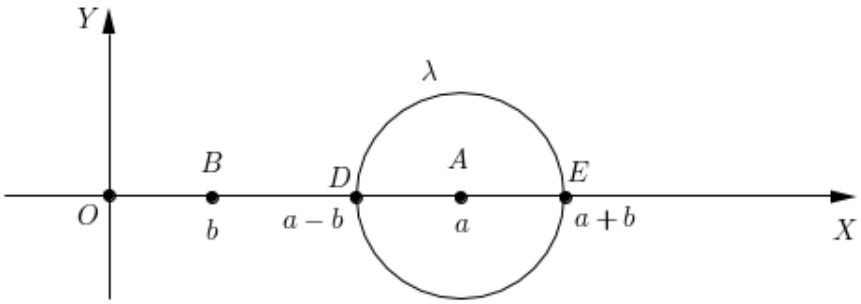

Figura 7.5: Adição e subtração

Para mostar que ab é construtível, vamos considerá que $U = (1, 0) = 1$ e r uma reta concorrente com o eixo OX (veja figura abaixo). Depois com o compasso centrado em O e raio $\overline{OU} = 1$ traçamos a circunferência λ e encontramos o ponto $D \in r$, da mesma forma com o compasso centrado em O e raio $\overline{OA} = a$, traçamos a circunferência Γ e encontramos o ponto $E \in r$, e finalizamos traçando por E a reta $\overleftrightarrow{EF}$ paralela a reta $\overleftrightarrow{DB}$ onde F é um ponto de coordenda x, pertencente ao eixo OX. Pelo teorema 6.1, temos:

$$\frac{\overline{OD}}{\overline{OB}} = \frac{\overline{OE}}{\overline{OF}} \Rightarrow \frac{1}{b} = \frac{a}{x} \Rightarrow x = ab$$

.

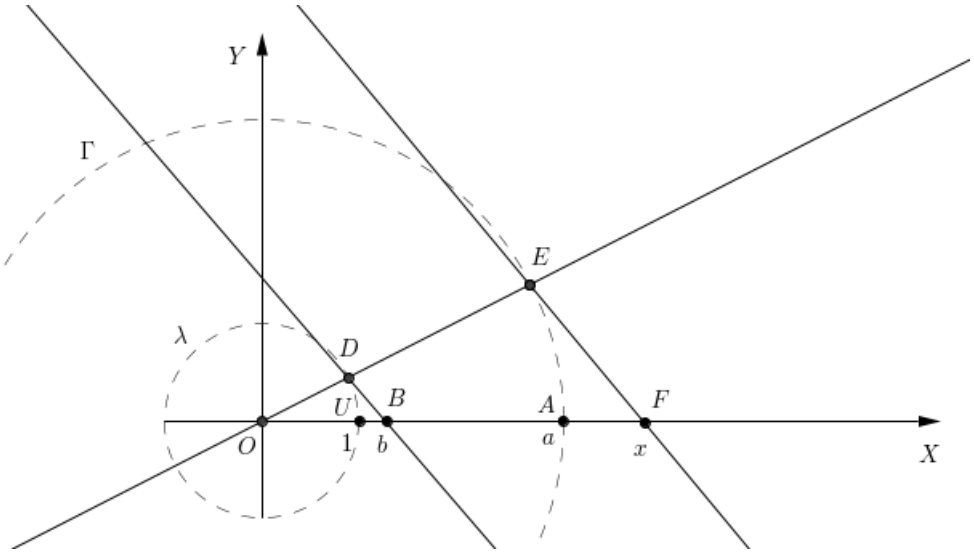

Figura 7.6: Multiplicação de pontos construtíveis

Portanto pelos passos acima o ponto F de coordenada ab é construtível.

Vamos mostra agora que o ponto de coordenada $\frac{b}{a}$ é construtível. Para mostrarmos este fato basta na figura acima traçar a reta $\overleftrightarrow{DK}$ paralela a reta $\overleftrightarrow{EB}$ onde K pertence ao segmento OB e tem cordenada k(veja a figura abaixo). Novamente pelo teorema 6.1, temos:

$$\frac{\overline{OE}}{\overline{OB}} = \frac{\overline{OD}}{\overline{OK}} \Rightarrow \frac{a}{b} = \frac{1}{k} \Rightarrow k = \frac{b}{a}.$$

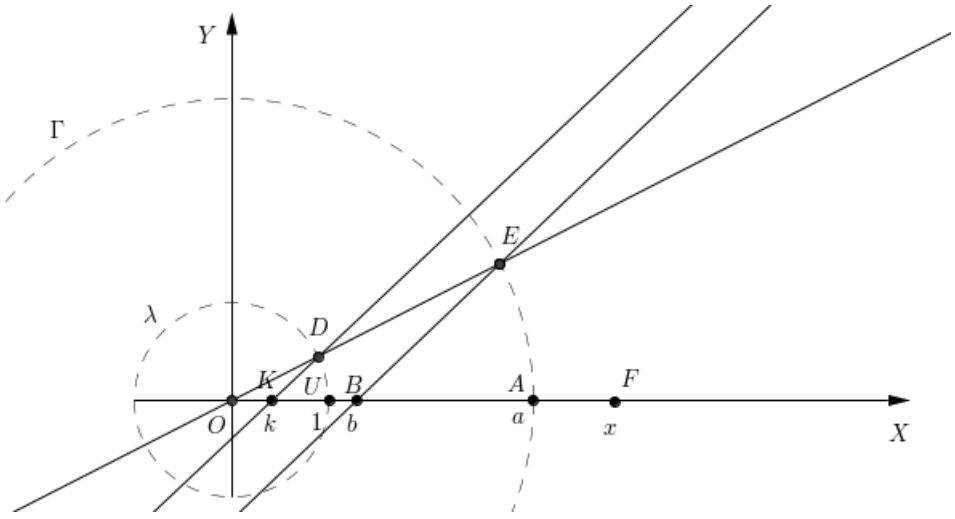

Figura 7.7: Divisão de pontos construtíveis

E portanto $\frac{b}{a}$ é construtível. □

7.3 Corpo dos Números Construtíveis

De posse do conhecimento adquirido até aqui, podemos citar e provar os próximos teoremas.

Teorema 7.2. *O conjunto $\mathcal{C}_\mathbb{R}$ munido das operações soma e multiplicação é subcorpo de $\mathbb{R}$ contendo $\mathbb{Q}$.*

Demonstração. Sabemos que $\mathbb{Z} \subset \mathcal{C}_\mathbb{R}$. Para provarmos que $\mathcal{C}_\mathbb{R}$ é subcorpo de $\mathbb{R}$, temos que provar,

(1) $a, b \in \mathcal{C}_\mathbb{R} \Rightarrow a - b \in \mathcal{C}_\mathbb{R}$

(2) $a, b \in \mathcal{C}_\mathbb{R} \Rightarrow a \cdot b \in \mathcal{C}_\mathbb{R}$

(3) $0 \neq a \in \mathcal{C}_\mathbb{R} \Rightarrow \frac{1}{a} \in \mathcal{C}_\mathbb{R}$.

No entanto as condições (1), (2) e (3) são perfeitamente justificadas pelo teorema 7.1.

Sabemos que $\mathbb{Z} \subset \mathcal{C}_\mathbb{R}$. Se $x \in \mathbb{Q}$ então existe $a, b \in \mathbb{Z}$ tal que $x = \frac{b}{a}$. Como a e b são inteiros construtíveis, pelo teorema 7.1, $x = \frac{b}{a}$ é construtível. O que prova que $\mathbb{Q} \subset \mathcal{C}_\mathbb{R}$. □

Definição 7.3. *Seja $(a, b) \in \mathcal{P}_n$, os elementos a e b são naturalmente coordenadas em $\mathcal{P}_n$. Definimos o conjunto A_n como sendo o conjunto de todas as coordenadas em $\mathcal{P}_n$.*

É fato que, todo elemento $(a, b) \in \mathbb{R}^2$ pode ser escrito como a soma $(a, 0) + (0, b)$. Relembrando o que já mencionamos antes, podemos fazer $= (a, 0)$ e $b = (0, b)$. Portanto se $(a, b) \in \mathcal{P}_n$, então pela definição anterior $a, b \in A_n$, e consequentemente $A_n \subset \mathcal{C}_\mathbb{R}$ para todo $n \in \mathbb{N}$.

Seja $K_0 = \mathbb{Q}$, consideremos as extensões $K_1 = \mathbb{Q}[A_1], K_2 = \mathbb{Q}[A_2], \ldots, K_n = \mathbb{Q}[A_n], \ldots$. Como $A_0 \subset A_1 \subset A_2 \subset \ldots \subset A_n \subset \ldots \subset \mathcal{C}_\mathbb{R}$ e pelo teorem 7.2, $\mathbb{Q} \subset \mathcal{C}_\mathbb{R}$, temos: $\mathbb{Q} = K_0 \subset K_1 \subset K_2 \subset \ldots \subset K_n \subset K_{n+1} \subset \ldots \subset \mathcal{C}_\mathbb{R}$.

Claramente se ver agora que se $\alpha \in \mathcal{C}_\mathbb{R}$, então existe n pertencente a $\mathbb{N}$ tal que $(\alpha, 0) \in \mathcal{P}_n$, e pela definição 7.3 $\alpha \in A_n$. Dai segue imediatamente que:

$$K_\infty = K_0 \cup K_1 \cup K_2 \cup K_n \cup \ldots = \mathcal{C}_\mathbb{R}.$$

Teorema 7.3. *$\mathcal{C}_\mathbb{R}$ é uma extensão algébrica dos racionais tal que para todo a pertencente a $\mathcal{C}_\mathbb{R}$ temos que o grau $[\mathbb{Q}[a] : \mathbb{Q}]$ é uma potência de 2.*

Demonstração. Para provarmos esse teorema, basta que para todo α pertencente a $\mathcal{C}_{\mathbb{R}}$, temos que $[\mathbb{Q}[\alpha] : \mathbb{R}] = 2^r$ para algum $r \in \mathbb{N}$.

Seja $\alpha \in \mathcal{C}_{\mathbb{R}}$. Assim existe $n \in \mathbb{N}$ tal que $\alpha \in K_n = \mathbb{Q}[A_n]$. Como $K_n = \mathbb{Q}[A_n] \supset \mathbb{Q}[\alpha] \supset \mathbb{Q}$, pelo teorema 5.4 $[\mathbb{Q}[\alpha] : \mathbb{Q}]$ divide $[K_n : \mathbb{Q}]$. Portanto é suficiente provarmos que $[K_n : \mathbb{Q}]$ é uma potência de dois, ou seja $[K_n : \mathbb{Q}] = 2^s$ para algum $s \in \mathbb{N}$.

Vamos provar que $[K_n : \mathbb{Q}]$ é uma potência de dois por indunção sobre n. Assim se $n = 0$ então $[K_0 = \mathbb{Q} : \mathbb{Q}] = 1 = 2^0$, e o teorema é válido. Claramente se ver que se $n = 1$, então $K_1 = \mathbb{Q}[\sqrt{3}]$, e como $\{1, \sqrt{3}\}$ é uma base desse espaço vetorial sobre $\mathbb{Q}$, temos que $[\mathbb{Q}[\sqrt{3}] : \mathbb{Q}] = 2$, e o teorema também é válido.

Supondo por indução que $[K_i : \mathbb{Q}]$ é uma potência de dois para todo $0 \leq i < n$, vamos provar que $[K_n : \mathbb{Q}]$ é uma potência de dois.

Como $K_n \supset K_{n-1} \supset \mathbb{Q}$ e pelo teorema 5.4 $[K_n : \mathbb{Q}] = [K_n : K_{n-1}] \cdot [K_{n-1} : \mathbb{Q}]$ temos que que é suficiente provarmos que $[K_n : K_{n-1}]$ é uma potência de dois.

Seja $L = K_n$ e $L_0 = K_{n-1}$. Sabemos que $L = L_0[A_n]$. Se $A_n = \{\alpha_1, \alpha_2, \ldots, \alpha_k\}$ temos então que $L = L_0[\alpha_1, \alpha_2, \ldots, \alpha_k]$.

Se denotarmos, $L_0 \subset L_1 = L_0[\alpha_1] \subset L_2 = L_1[\alpha_2] \subset \ldots \subset L_i = L_{i-1}[\alpha_i] \subset \ldots \subset L_k = L$ então pelo colorário 5.1 é suficiente provarmos que $[L_i : L_{i-1}]$ é potência de dois para $1 \leq i \leq k$. Como $L_i = L_{i-1}[\alpha_i]$ e $\alpha_i \in A_n$, existe $\beta_i \in A_n$ tal que (α_i, β_i) ou (β_i, α_i) pertencem a $\mathcal{P}_n$. Sem perda de generalidade vamos supor que $(\alpha_i, \beta_i) \in \mathcal{P}_n$.

Como $\mathcal{P}_n = \langle \mathcal{P}_{n-1} \rangle$ temos que (α_i, β_i) é obtido por uma das três operações elementares em $\mathcal{P}_{n-1}$. Pode-se provar sem grandes dificuldades, usando ferramentas da geometria analítica que α_i terá que satisfazer uma equação de grau menor ou igual a 2 com coeficientes sobre o corpo $K_{n-1} = \mathbb{Q}[A_{n-1}]$.

Ora, como $K_{n-1} = L_0 \subset L_{i-1}$ para $1 \leq i \leq k$, segue que α_i é raiz de um polinômio de grau 1 ou 2 sobre L_{i-1}, e pelo teorema 5.3, $[L_i : L_{i-1}] = 1$ ou 2. Como queriamos demonstrar. □

7.4 Prova da Impossibilidade

Foi visto na seção anterior que para um número a pertencente a $\mathbb{R}^2$ ser um ponto construtível, basta que suas coordenadas sejam construtíveis. Isto nos levou ao fato de que um número a é construtível se a extensão $\mathcal{C}_{\mathbb{R}}$ é algébrica dos racionais e $[\mathbb{Q}[a] : \mathbb{Q}]$ é

uma potência de 2. Esse último resultado é crucial para provarmos as impossibilidades clássicas.

Teorema 7.4. *Não existe $a \in \mathcal{C}_{\mathbb{R}}$, tal que o volume do cubo de aresta a seja o dobro do volume do cubo de aresta* 1.

Demonstração. Claramente um cubo de aresta 1 tem volume igual a 1. Para duplicarmos seu volume, temos que encontrar a medida $a \in \mathcal{C}_{\mathbb{R}}$, tal que:

$$a^3 = 2 \Rightarrow a^3 - 2 = 0.$$

Portanto, podemos relacionar a equação acima com o polinômio $x^3 - 2$, assim pelo critério de Eisenstein $irr(a, \mathbb{Q}) = x^3 - 2$, e pelo teorema 5.3 temos que ter $[\mathbb{Q}[a] : \mathbb{Q}] = 3$, o que é um absurdo pelo teorema 7.3. Portanto a não é construtível, logo não podemos duplicar o volume do cubo usando apenas régua e compasso.

□

Teorema 7.5. *Não existe $a \in \mathcal{C}_{\mathbb{R}}$, tal que a área do quadrado de lado a seja igual a área do círculo de raio* 1.

Demonstração. Sabemos da geometria plana que a área de um círculo de raio r é dada pela fórmula matemática πr^2. Considerando um círculo de raio 1, claramente sua área é π. Supondo que exista $a \in \mathcal{C}_{\mathbb{R}}$ tal que $a^2 = \pi \Rightarrow a = \sqrt{\pi} \in \mathcal{C}_{\mathbb{R}}$. Pelo teorema 7.1 $\mathcal{C}_{\mathbb{R}}$ é fechado para a operação multiplicação, assim $a^2 \in \mathcal{C}_{\mathbb{R}} \Rightarrow a^2 = a \cdot a = \sqrt{\pi} \cdot \sqrt{\pi} = \pi \in \mathcal{C}_{\mathbb{R}}$, logo pelo teorema 7.3, π é algébrico sobre $\mathbb{Q}$, o que é um absurdo. Portanto $\pi \notin \mathcal{C}_{\mathbb{R}}$ e $a \notin \mathcal{C}_{\mathbb{R}}$. □

Para a demonstração da trissecção do ângulo vamos relembrar nossos estudos no capítulo 1 sobre circunferência trigonométrica. Pela definição 2.1 um ponto P pertencente a circunferência trigonométrica λ, determina um arco de comprimento c no sentido anti-horário, tal que as coordenadas de P é $cos(c)$ e $sen(c)$. Como foi mostrado, um ponto $P \in \mathbb{R}^2$ é construtível se, e somente se suas coordenadas forem construtíveis. Portanto um ângulo de medida c radiano é construtível se $cos(c)$ também for.

Proposição 7.3. *O número $cos\left(\frac{\pi}{9}\right)$ não é construtível.*

Demonstração. Seja $\alpha = \frac{\pi}{9}$, assim $3\alpha = \frac{\pi}{3}$. Pela tabela 1.1 do capítulo 1, temos que $cos\left(\frac{\pi}{3}\right) = \frac{1}{2} = cos(3\alpha)$. Pelas proposições 2.1 e 2.2, temos:

$$cos(3\alpha) = cos(\alpha + 2\alpha)$$
$$= cos(\alpha)cos(2\alpha) - sen(\alpha)sen(2\alpha)$$
$$= cos(\alpha)(cos^2(\alpha) - sen^2(\alpha)) - sen(\alpha)(2sen(\alpha)cos(\alpha))$$
$$= cos^3(\alpha) - cos(\alpha)sen^2(\alpha) - 2sen^2(\alpha)cos(\alpha)$$
$$= cos^3(\alpha) - 3cos(\alpha)sen^2(\alpha)$$
$$= cos^3(\alpha) - cos(\alpha)(1 - cos^2(\alpha))$$
$$= 4cos^3(\alpha) - 3cos(\alpha) = \frac{1}{2}.$$

Assim:

$$4cos^3(\alpha) - 3cos(\alpha) = \frac{1}{2}$$
$$\Rightarrow 8cos^3(\alpha) - 6cos(\alpha) - 1 = 0$$
$$\Rightarrow 8cos^3\left(\frac{\pi}{9}\right) - 6cos^2\left(\frac{\pi}{9}\right) - 1 = 0.$$

Podemos relacionar essa última equação com o poilinômio $p(x) = 8x^3 - 6x - 1$. Pelo critério de Eisenstein $p(x)$ é irredutível sobre $\mathbb{Q}$ e portanto pelo teorema 5.3 $[\mathbb{Q}[cos\left(\frac{\pi}{9}\right)] : \mathbb{Q}] = 3$, e portanto pelo teorema 7.3, $cos\left(\frac{\pi}{9}\right)$ não é construtível. □

Teorema 7.6. *É impossível, com o uso apenas de régua não graduada e compasso, trissectar o ângulo de* 60^o.

Demonstração. Para demonstrarmos esse teorema, vamos considerar a circunferência trigonométriva λ da figura 2.3 do capítulo 1. É visivel que trissectar o ângulo de 60^o, é equivalente a construir com régua e compasso na circunferência λ os arcos $\overset{\frown}{AP}$, $\overset{\frown}{AP_1}$ e $\overset{\frown}{AP_2}$, de comprimentos $\frac{\pi}{9}$, $\frac{2\pi}{9}$ e $\frac{\pi}{3}$ respectivamente. Claramente o ângulo de 20^o corresponde ao arco $\overset{\frown}{AP_2}$ de medida $\frac{\pi}{9}$. E pela proposição 7.3, o ponto P_2 (lembre que a abscissa de P_2 é $cos\left(\frac{\pi}{9}\right)$) é não construtível, e portanto o ângulo de 60^o também é não construtível. □

Com este último resultado cumprimos com o objetivo desse trabalho.

Capítulo 8

Considerações Finais

É visível que a matemática do último século tem tido uma tendência para a abstração, o que faz do ensino da matemática atual um desafio para os professores. Acredita-se que uma maneira de facilitar o ensino em sala de aula é propiciando ao aluno a construção do conhecimento matemático. Ao analisarmos a construção histórica do conhecimento matemático, percebemos que a maior parte desse conhecimento, tem sido elaborado a partir das tentativas do homem, de compreender seu mundo e representá-lo através de equações matemática, para assim poder tirar o máximo de informações do objeto estudado.

É possível que os três problemas estudado aqui tenham surgido da necessidade cotidiana dos Gregos de fazer algumas construções geométricas, as quais de forma direta ou indireta, necessitava da solução para um dos três problemas, por exemplo, os Gregos preocupavam-se com a construção de polígonos regulares, e é bem provável que o problema da trissecção do ângulo tenha surgido neste contexto, pois a construção de um polígono regular com nove lados necessita da trissecção de um ângulo.

Os três problemas clássicos mostram de forma clara as limitações dos instrumentos Euclidianos (régua não graduada e compasso). A trajetória percorrida pelos três problemas, do surgimento até a prova das impossibilidades levou um período de tempo de mais de dois mil anos. O porque de ter decorrido tanto tempo para os três problemas serem resolvidos, deve estar basicamente em duas razões, pois as construções requeridas são impossíveis, e embora os problemas sejam geométricos, foi necessário o desenvolvimento da álgebra, para se ter ferramentas matemáticas que justificasse a impossibilidade, em particular, foi necessário o desenvolvimento das extensões de corpos sobre os números racionais no século XIX.

Provamos nesse trabalho, que o ângulo de 60^o não pode ser trissecçado usando régua não graduada e compasso. No entanto, vale dizer que existe sim ferramentas geométricas que permite a trissecção de qualquer ângulo, em particular o ângulo de 60^o, uma delas é a trissecção feita por Arquimedes usando apenas régua e compasso para um ângulo α qualquer. O leitor interessado em ver tal demonstração, pode consultá-la na referência [1], páginas 106 e 107. Vale resaltar que o autor deixa claro que em um dado passo da demonstração, é feita uma violação as regras usuais das construções com régua e compasso.

A presente pesquisa, foi constuída pensando em quais tópicos da geometria e álgebra são fundamentais para fazer a justificativa da impossibilidade clássica. A partir dai, foi traçado um caminho entre a geometria plana e álgebra, na busca por ferramentas entre essas duas áreas da matemática, que justifique tal impossibilidade. Foi explicado os conceitos de polinômios irredutíveis e extensões algébricas. Por fim, foi feito uma associação entre extensões algébricas e espaços vetoriais, levando ao grau de uma extensão, trabalhamos também construções geométricas para ser possível construir o corpo dos pontos construtíveis e termos condições e ferramentas para provar os três problemas clássico.

Esperamos que esse trabalho tenha cumprido com seu objetivo, e também possa agradar os futuros leitores.

Referências Bibliográficas

[1] Aaboe, A. *Episódios da história da matemática/Aaboe Asger; tradução de João Bosco Pitombeira* . Rio de Janeiro: SBM, 2013. 191 p. (Coleção do Professor de Matemática; 18).

[2] Dolce, O., Pompeo, J. N. *Fundamentos de matemática elementar 9.* 8 ed. São Paulo: Atual, 2005.

[3] do Carmo, M. P., Morgado, A. C., Wagner, E. *Trigonometria Números Complexos.* 3 ed. Rio de Janeiro: SBM, 2005. 122 p. (Coleção Professor de Matemática).

[4] Freitas, J. M. *Os três problemas clássicos da Matemática grega.* São José do Rio Preto: UNESP, 2014. 75f. (Dissertação de mestrado).

[5] Garcia, A., Lequain, Y. *Elementos de Álgebra.* 6 ed. Rio de Janeiro: IMPA, 2012. 326 p. (Projeto Euclides).

[6] Gonçalves, A. *Introdução à Álgebra.* 5 ed. Rio de Janeiro: IMPA, 2009. 194 p. (Projeto Euclides).

[7] Hefez, A. *Aritmética.* Rio de Janeiro: SBM, 2014. 338 p. (Coleção PROFMAT).

[8] Hefez, A. *Curso de Álgebra* . 5 ed. Rio de Janeiro: IMPA, 2014. 213 p. (Coleção Matemática Universitária).

[9] Lima, E. L. *Álgebra Linear.* 8 ed. Rio de Janeiro: IMPA, 2009. 357 p. (Coleção Matemática Universitária).

[10] Muniz Neto, A. C. *Tópicos de Matemática Elementar: geometria euclidiana plana.* 2 ed. Rio de Janeiro: SBM, 2013. 464 p. (Coleção Professor de Matemática).

[11] Roque, T. *História da Matemática: uma visão crítica, desfazendo mitos e lendas.* Rio de Janeiro: Zahar, 2012.

[12] Silvares, A. A. *Números algébricos e transcedentes: uma abordagem para o ensino básico.* Ilhéus - BA: UESC, 2016. 42f. : il. (Dissertação de mestrado).

[13] Steinbruch, A., Winterle, P. *Álgebra Linear.* 2 ed. São Paulo: Pearson Makron Books, 1987.