



UNIVERSIDADE FEDERAL DO CEARÁ
CENTRO DE CIÊNCIAS
DEPARTAMENTO DE MATEMÁTICA
PROGRAMA DE PÓS-GRADUAÇÃO EM MATEMÁTICA EM REDE NACIONAL

LUIZ AUGUSTAVO ALMEIDA FEITOZA

SOBRE A EXISTÊNCIA E CONSTRUÇÃO DE UM TRIÂNGULO
DADAS SUAS BISSETRIZES INTERNAS

FORTALEZA

2018

LUIZ AUGUSTAVO ALMEIDA FEITOZA

SOBRE A EXISTÊNCIA E CONSTRUÇÃO DE UM TRIÂNGULO DADAS SUAS
BISSETRIZES INTERNAS

Dissertação apresentada ao Programa de Pós-graduação em Matemática em Rede Nacional do Departamento de Matemática da Universidade Federal do Ceará, como parte dos requisitos necessários para a obtenção do título de mestre em Matemática. Área de concentração: Ensino de Matemática.

Orientador: Prof. Dr. José Alberto Duarte Maia.

FORTALEZA

2018

Dados Internacionais de Catalogação na Publicação
Universidade Federal do Ceará
Biblioteca Universitária
Gerada automaticamente pelo módulo Catalog, mediante os dados fornecidos pelo(a) autor(a)

F335s Feitoza, Luiz Augustavo Almeida.
Sobre a Existência e Construção de um Triângulo dadas suas Bissetrizes Internas / Luiz Augustavo Almeida Feitoza. – 2018.
81 f. : il. color.

Dissertação (mestrado) – Universidade Federal do Ceará, Centro de Ciências, Departamento de Matemática, Programa de Pós-Graduação em Matemática em Rede Nacional, Fortaleza, 2018.
Orientação: Prof. Dr. José Alberto Duarte Maia.

1. Geometria. 2. Construções geométricas. 3. Álgebra abstrata. 4. Análise. I. Título.

CDD 510

LUIZ AUGUSTAVO ALMEIDA FEITOZA

SOBRE A EXISTÊNCIA E CONSTRUÇÃO DE UM TRIÂNGULO
DADAS SUAS BISSETRIZES INTERNAS

Dissertação de Mestrado apresentada ao Programa de Pós-graduação em Matemática em Rede Nacional do Departamento de Matemática da Universidade Federal do Ceará, como parte dos requisitos necessários para a obtenção do título de Mestre em Matemática.

Área de concentração: Ensino de Matemática.

Aprovada em 16/06/2018.

BANCA EXAMINADORA

Prof. Dr. José Alberto Duarte Maia (Orientador)
Universidade Federal do Ceará (UFC)

Prof. Dr. Ângelo Papa Neto
Instituto Federal de Educação, Ciência e Tecnologia do Ceará (IFCE)

Prof. Dr. Antonio Caminha Muniz Neto
Universidade Federal do Ceará (UFC)

À minha família

AGRADECIMENTOS

Agradeço primeiramente a natureza divina, por todas as vezes que se manifesta em coisas boas que acontecem na minha vida, sendo exemplo maior, a minha própria existência.

À minha família, em especial às pessoas, Maria Almeida da Silva (minha amada mãe que sempre buscou proporcionar a mim e às minhas irmãs as melhores condições para estudar, apoiando e incentivando esta prática, sendo a nossa primeira Professora), Jordearia Almeida Feitoza e Suinara Almeida Feitoza (minhas irmãs queridas, que também sempre me apoiam e proferem boas palavras no sentido de incentivo), e Augustinho Feitoza da Costa (meu amado pai, que com sua forma particular sempre demonstrou acreditar em mim).

À minha querida prima, Silvia Maria da Silva Feitoza, e também a toda sua família, que com seus esforços me ajudaram de diversas formas, possibilitando minha participação das aulas do Mestrado Profissional em Matemática em Rede Nacional - PROFMAT, da Universidade Federal do Ceará - UFC.

Aos professores do PROFMAT da UFC.

Ao meu orientador Professor Dr. José Alberto Duarte Maia pelo empenho dedicado, pela confiança que depositou em mim, e pelas sugestões, contribuições preciosas para a produção deste trabalho.

Ao Professor Dr. Antonio Caminha Muniz Neto (UFC), pelo apoio e incentivo à minha progressão nos estudos, e pela contribuição em relação ao tema desta dissertação.

Ao Professor Dr. José Valter Lopes Nunes (UFC) pelo apoio e incentivo aos estudos.

A todos os meus colegas da turma do PROFMAT - UFC (ENA 2016), pelo apoio. Entre estes destaco Edney Freitas Gregório, Francisco Daniel Carneiro de Castro, Jose Everardo Gomes dos Santos, Francisco José dos Santos Martins, Antônio José da Silva, Anderson Douglas Freitas Pedrosa e Anderson Leite Meira Gomes, pelo apoio e parceria durante o curso.

Aos meus professores do curso de Licenciatura em Matemática do Instituto Federal de Educação, Ciência e Tecnologia do Ceará - IFCE, Campus Canindé. Em especial à Professora Me. Luciana de Oliveira Souza Mendonça, Professora Dr. Ana Cláudia Gouveia de Sousa e Professor Me. Diego Ponciano de Oliveira Lima.

Ao Professor Genilson Gomes da Silva por me iniciar no Latex, e por todas as suas mensagens de estímulo relativo ao estudo da Matemática.

Ao meu colega e amigo Francisco Erilson Freire de Oliveira, por todas as contribuições relativas ao trabalho, e pela parceria que perdura desde que nos conhecemos durante o curso de Licenciatura em Matemática, do IFCE Campus Canindé.

Aos meus Professores da Educação Básica, Afrânio Soares da Silva e Francisco

Edilberto de Oliveira Costa, que proferiram palavras de grande importância para a minha decisão em iniciar o curso da Licenciatura em Matemática.

À Universidade Federal do Ceará - UFC.

À Coordenação de Aperfeiçoamento de Pessoal de Nível Superior - CAPES, pelo fomento por meio da bolsa de estudos.

“Se vi mais longe foi por estar de pé sobre ombros de gigantes”
(ISAAC NEWTON).

“A mais bela coragem é a confiança que devemos ter na capacidade do nosso esforço”
(COELHO NETO).

RESUMO

O presente trabalho consiste em apresentar resultados relativos às seguintes questões: dados três números positivos arbitrários m, n, p , existe um triângulo com bissetrizes internas de comprimento m, n, p ? É possível construir um tal triângulo com régua e compasso? Esta dissertação é resultado de uma pesquisa bibliográfica onde levantamos a história dos problemas em foco, e apresentamos a teoria necessária para as demonstrações. No primeiro capítulo introduzimos os problemas, comentando um pouco da história dos mesmos. Seguimos no segundo capítulo, apresentando as preliminares necessárias para o desenvolvimento das demonstrações dos problemas. Na sequência apresentamos as demonstrações pretendidas, e por fim concluímos o texto com nossas considerações, onde destacamos o reconhecimento da importância das inter-relações existentes entre elementos de diferentes áreas da Matemática.

Palavras-chave: Geometria. Construções geométricas. Álgebra abstrata. Análise.

ABSTRACT

The present paper consists of presenting results regarding the following questions: given three positive numbers arbitrary m, n, p , is there a triangle with internal bisectors of length m, n, p ? Is it possible to construct such a triangle with ruler and compass? This dissertation is the result of a bibliographical research where we raise the history of the problems in focus, and present the necessary theory for the demonstrations. In the first chapter we introduce the problems, commenting a little on their history. We continue in the second chapter, presenting the necessary preliminaries for the development of the demonstrations of the problems. In the sequence we present the intended demonstrations, and finally we conclude the text with our considerations, where we highlight the recognize the importance of the existing interrelations between elements of different areas of Mathematics

Keywords: Geometry. Geometric constructions. Abstract algebra. Analysis.

LISTA DE ILUSTRAÇÕES

Figura 1 – Construção do triângulo equilátero com compasso euclidiano.	16
Figura 2 – Equivalência entre o compasso euclidiano e o compasso moderno.	17
Figura 3 – Soma de segmentos.	17
Figura 4 – Subtração de segmentos.	18
Figura 5 – Transporte de ângulo.	18
Figura 6 – Soma e subtração de ângulos.	19
Figura 7 – Reta perpendicular.	19
Figura 8 – Reta mediatriz.	20
Figura 9 – Aplicação da construção da mediatriz.	20
Figura 10 – Reta paralela passando por um ponto dado.	21
Figura 11 – Retas paralelas distando \overline{AB} , sendo dado o segmento AB	21
Figura 12 – Divisão de segmentos em partes congruentes.	22
Figura 13 – Bissetriz de um ângulo.	22
Figura 14 – Arco capaz.	23
Figura 15 – Multiplicação e divisão de segmentos	23
Figura 16 – Quadrado inscrito em um círculo.	24
Figura 17 – Octógono.	25
Figura 18 – Segmento de comprimento \sqrt{r}	25
Figura 19 – Trissecção de um ângulo.	27
Figura 20 – Triângulo ABC sendo dados o lado BC e os ângulos \hat{A} e \hat{B}	27
Figura 21 – Triângulo ABC sendo dados o perímetro $2p$ e os ângulos \hat{B} e \hat{C}	28
Figura 22 – Triângulo ABC sendo dados o lado BC , a soma $\overline{AB} + \overline{AC}$ e o ângulo \hat{B}	28
Figura 23 – Triângulo ABC sendo dados o lado BC e as medianas M_b e M_c relativas respectivamente aos lados AC e AB	29
Figura 24 – Triângulo ABC sendo dadas as medianas M_a , M_b e M_c relativas respectivamente aos lados BC , AC e AB	29
Figura 25 – Seno, cosseno e tangente de um triângulo retângulo.	30
Figura 26 – Quadrado $ABCD$ de lado 1, nas circunstâncias do problema.	31
Figura 27 – Teorema da bissetriz.	32
Figura 28 – Prova do teorema da bissetriz, primeira parte.	32
Figura 29 – Prova do teorema da bissetriz, segunda parte.	32
Figura 30 – Lei dos Cossenos.	33
Figura 31 – Lei dos Cossenos, caso em que α é agudo.	33
Figura 32 – Lei dos Cossenos, caso em que α é obtuso.	33
Figura 33 – Bissetriz em função dos lados.	34
Figura 34 – Prova da proposição 2.4.	35

Figura 35 – Reta perpendicular construtível passando por $A \notin r$	57
Figura 36 – Reta perpendicular construtível passando por $A \in r$	57
Figura 37 – Plano XOY e ponto A	58
Figura 38 – Triângulo ABC e suas bissetrizes.	67
Figura 39 – Triângulo ABC , suas bissetrizes e o ponto J	68
Figura 40 – Triângulos com o mesmo círculo inscrito	68
Figura 41 – Triângulos com círculo inscrito s diferentes.	69
Figura 42 – Triângulos com bissetriz comum.	70
Figura 43 – Triângulos e suas bissetrizes.	70
Figura 44 – Triângulo com construções auxiliares.	71
Figura 45 – Triângulo isósceles e duas de suas bissetrizes internas.	73

SUMÁRIO

1	INTRODUÇÃO	13
2	PRELIMINARES	15
2.1	Elementos da geometria plana	15
2.1.1	Construções com régua e compasso	15
2.1.1.1	<i>Soma e subtração de segmentos</i>	17
2.1.1.2	<i>Transporte de ângulo</i>	18
2.1.1.3	<i>Soma e subtração de ângulos</i>	18
2.1.1.4	<i>Reta perpendicular</i>	19
2.1.1.5	<i>Mediatriz de um segmento</i>	19
2.1.1.6	<i>Retas paralelas</i>	21
2.1.1.7	<i>Divisão de segmentos</i>	22
2.1.1.8	<i>Bissetriz de um ângulo</i>	22
2.1.1.9	<i>Arco Capaz</i>	23
2.1.1.10	<i>Multiplificação e divisão de segmentos</i>	23
2.1.1.11	<i>Quadrado inscrito em um círculo</i>	24
2.1.1.12	<i>Polígonos regulares de 2^n lados</i>	24
2.1.1.13	<i>Segmento com comprimento \sqrt{r}</i>	25
2.1.2	Outros resultados importantes	30
2.1.2.1	<i>Relações trigonométricas do triângulo retângulo.</i>	30
2.1.2.2	<i>Teorema da bissetriz</i>	31
2.1.2.3	<i>Lei dos cossenos</i>	33
2.1.2.4	<i>Bissetrizes internas</i>	34
2.2	Elementos da álgebra	36
2.2.1	Anéis, corpos e homomorfismos	36
2.2.2	Anéis de polinômios	42
2.2.3	Extensões de corpos	49
2.3	Algebrização das construções com régua e compasso	56
2.4	Teorema do ponto fixo para contrações	59
3	EXISTÊNCIA E UNICIDADE	62
3.1	Um argumento geométrico para unicidade	67
4	CONSTRUTIBILIDADE.	73
5	CONCLUSÃO	77
	REFERÊNCIAS.	78
	APÊNDICE A - ALGUNS ELEMENTOS DE ANÁLISE	80

1 INTRODUÇÃO

O presente trabalho consiste em apresentar resultados relativos às seguintes questões: dados três números positivos arbitrários m, n, p , existe um triângulo com bissetrizes internas de comprimento m, n, p ? É possível construir um tal triângulo com régua e compasso? A resposta para a primeira interrogação é positiva enquanto para segunda, negativa.

Nossas referências indicam que as soluções para estes problemas só foram possíveis graças ao grande desenvolvimento matemático nos últimos séculos, no que diz respeito à Álgebra Abstrata e à Análise, e à aplicação destes conhecimentos na Geometria Elementar.

Em 1842, o matemático francês Orly Terquem (1782 - 1862) calculou o comprimento das bissetrizes internas de um triângulo em termos dos comprimentos dos lados do mesmo, encontrando um sistema de equações. Este sistema possibilitou concluir a existência de uma possibilidade analítica para determinarmos os comprimentos dos lados de um triângulo, dados os comprimentos das três bissetrizes internas. No entanto, na tentativa de desenvolver esta solução analítica, Terquem acabou encontrando uma equação de grau muito alto, o que tornou inviável a possível solução.

De 1842 a 1994, muitos esforços foram feitos em relação à busca pela solução do problema da existência, sendo objeto de estudo de matemáticos como Imme van Den Berg, Pierre Henri Brocard, W. Heymann, A. Korselt, Paul Barbarin e F. Neiss. Nossas pesquisas revelaram que a primeira solução, devida a Mironescu e Panaitopol, surgiu em 1994 (DINCA e JEAN, 2010), a qual encontra-se disponível em (MIRONESCU e PANAITOPOL, 1994).

No ano de 1843, respondendo a uma questão levantada em 1830 no volume 6 do Jornal *Fur Reine und Angewandte Mathematik* (Questão 12, p. 213 - 2014), von Renthe-Fink, calculou a área de um triângulo em termos de suas bissetrizes internas, concluindo que a equação para o raio do círculo inscrito deve ser do 16º grau, mas absteve-se de derivar essa equação explicitamente (DINCA e JEAN, 2010).

O problema da construção com régua e compasso do triângulo, foi proposto por Henry Brocard em 1875, não surgindo nenhuma solução na época. Assim como o problema da existência, foi objeto de pesquisa de muitos estudiosos, vindo a ser solucionado em 1937, quando F. Neiss mostrou que em geral a construção com régua e compasso é impossível (DINCA e JEAN, 2010).

A demonstração que faremos neste texto para impossibilidade da construção, foi desenvolvida em uma parceria entre os professores Dr. Antonio Caminha Muniz Neto e Dr. José Alberto Duarte Maia, ambos da Universidade Federal do Ceará, e publicada em junho de 2017, no serviço de e-print Arxiv, gerenciado pela Cornell University Library (NETO e MAIA, 2017).

A seguir, descrevemos brevemente o conteúdo dos capítulos seguintes dessa dis-

sertação.

No **Capítulo 2**, apresentamos as preliminares para desenvolvermos as demonstrações, objetos principais do texto. A importância deste capítulo reside na exposição dos principais elementos envolvidos com o objetivo do trabalho como todo. Iniciamos discorrendo um pouco sobre elementos da Geometria Plana, seguidos de alguns tópicos da Álgebra Abstrata, onde discutimos a algebrização das construções com régua e compasso, e concluímos com a apresentação de um resultado da Análise, conhecido como Teorema do Ponto Fixo para Contrações.

Munidos da teoria necessária, construímos no **Capítulo 3** a prova da existência e da unicidade de um triângulo, dados os comprimentos de suas bissetrizes internas. Concluímos este capítulo apresentando uma prova puramente geométrica para o fato da unicidade do triângulo, não recorrendo a quaisquer outros conhecimentos relativos a Trigonometria, Análise ou Álgebra Abstrata.

Realizamos no **Capítulo 4** a prova da impossibilidade da construção com régua e compasso de um triângulo, dados os comprimentos de suas bissetrizes internas.

E por fim, no **Capítulo 5**, expomos nossas considerações acerca do trabalho desenvolvido, ressaltando a importância das pesquisas na área da Álgebra Abstrata e da Análise, para a construção e desenvolvimento dos conhecimentos da ciência matemática.

2 PRELIMINARES

Apresentamos neste capítulo a teoria que fundamenta as demonstrações, objetivos centrais deste trabalho, presentes nos capítulos posteriores. Embora não seja nosso intuito construir um texto auto-suficiente, boa parte dos elementos utilizados no restante da dissertação serão aqui discutidos. Apresentamos definições e resultados importantes para uma boa compreensão do trabalho como um todo.

Iniciamos expondo os elementos relativos a Geometria Plana. Em seguida, os elementos da Álgebra, culminando na discursão acerca da algebrização das construções com régua e compasso.

Para finalizar o capítulo, discorreremos sobre condições que uma aplicação necessita satisfazer para possuir um único ponto fixo, enunciando e demonstrando o teorema do ponto fixo para contrações.

2.1 Elementos da geometria plana

Nesta seção abordaremos os elementos da geometria plana que serão de fundamental importância para o desenvolvimento do restante desse texto.

Discutindo um pouco sobre as construções com régua e compasso, expondo as construções mais elementares. Em seguida comentaremos a história relativa aos três problemas clássicos que foram objetos de investigação de inúmeros matemáticos por mais de 2000 anos, e realizaremos algumas das principais construções relativas aos triângulos, bem como observações pertinentes.

2.1.1 *Construções com régua e compasso*

Antes de mais nada, para se discutir sobre construções com régua e compasso, é importante compreendermos claramente o que é permitido fazer com uma régua sem escala (não graduada) e um compasso.

Com a utilização destes instrumentos e apoiados nos postulados de Euclides os gregos sabiam construir inúmeras figuras, realizando somente,

- 1) com a régua, o traço de uma reta de comprimento indefinido passando por dois pontos distintos dados;
- 2) com o compasso, um círculo com centro em um ponto dado e passando por um outro ponto também dado.

Para eles, solucionar um problema, provar uma proposição ou um teorema era equivalente a construir geometricamente uma solução.

É interessante saber que:

[...] o compasso de Euclides difere dos compassos modernos, uma vez que com estes é permitido traçar um círculo com centro num ponto qualquer e tendo como raio um segmento AB qualquer. Em outras palavras, permite-se transportar a distância AB ao centro C , usando para isso o compasso como [...] transportador [...]. O compasso euclidiano, por outro lado, desmonta-se quando se levanta um de seus braços do papel. Poderia parecer assim que o compasso moderno fosse mais poderoso que do que o euclidiano, ou compasso desmontável. Mas é bastante curioso que os dois instrumentos sejam equivalentes (EVES, 2004, p. 134).

Para verificar a equivalência entre o compasso moderno e o euclidiano, vejamos inicialmente como construir um triângulo ABC equilátero, dados os pontos A e B , com os instrumentos euclidianos.

No que segue, sempre que escrevermos \overline{XY} estaremos nos referindo ao comprimento do segmento XY .

Com a régua, ligue os pontos A e B obtendo o segmento AB . Em seguida, com o compasso trace o círculo de centro A e raio de medida \overline{AB} , e o círculo de centro B e raio de medida \overline{AB} . Chame de C e C' os pontos de interseção entre os dois círculos. Agora ligando A a C e B a C obtemos um triângulo equilátero com lado de comprimento \overline{AB} .

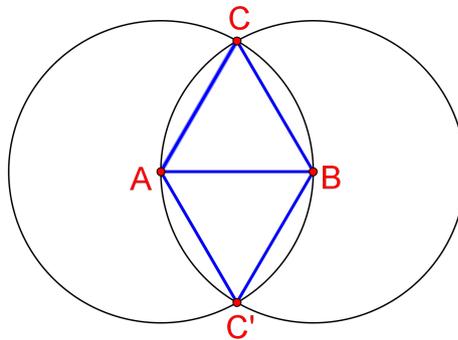


Figura 1 – Construção do triângulo equilátero com compasso euclidiano.

Podemos agora mostrar que os compassos moderno e o euclidiano são equivalentes. Ou seja, dados os pontos A , B e C , mostraremos que é possível construir o círculo de centro A e raio BC , utilizando o compasso euclidiano.

Construa como acima, o triângulo equilátero ABD e em seguida realize os seguintes procedimentos: trace o círculo de centro em B e raio \overline{BC} , e seja E sua interseção com a semi-reta \overrightarrow{BD} ; trace o círculo de centro D e raio \overline{DE} e seja F uma de suas interseções com a semi-reta \overrightarrow{AD} . Construa agora o círculo de centro em A e raio \overline{AF} . A imagem abaixo nos mostra os dois casos possíveis.

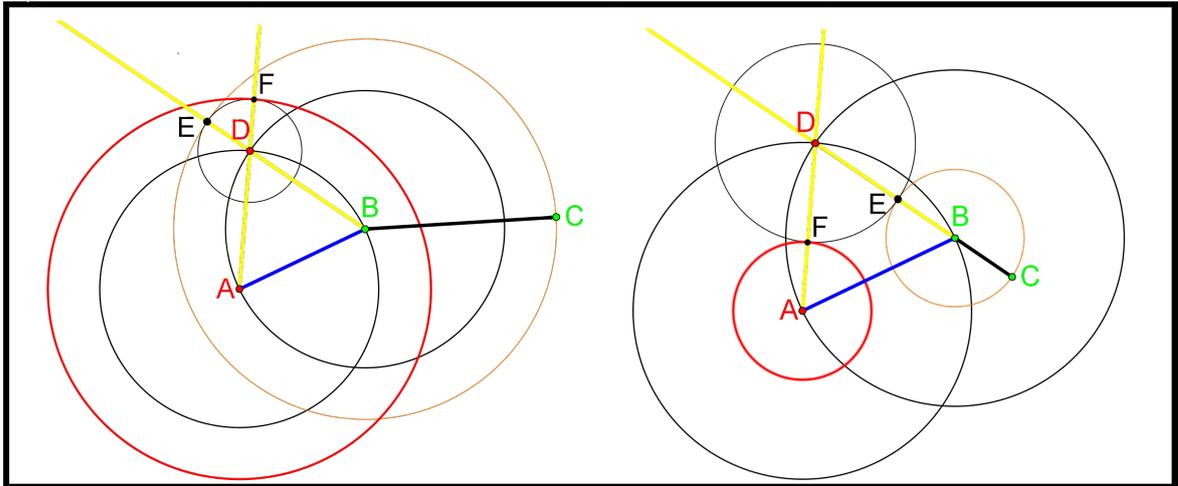


Figura 2 – Equivalência entre o compasso euclidiano e o compasso moderno.

Veja que se $\overline{BC} > \overline{AB}$ então $\overline{AF} > \overline{AD}$, se $\overline{BC} < \overline{AB}$ então $\overline{AF} < \overline{AD}$, e quando $\overline{BC} = \overline{AB}$ o segmento $\overline{AD} = \overline{AF}$.

Em qualquer dos casos, o círculo de centro em A e raio AF é aquele que queríamos construir pois $\overline{AF} = \overline{BC}$.

A seguir apresentaremos algumas das principais construções elementares que os gregos sabiam realizar, no plano, com os instrumentos euclidianos, segundo (WAGNER, 2007) e (REZENDE e QUEIROZ, 2008).

2.1.1.1 Soma e subtração de segmentos

Dados os segmentos AB e CD com $\overline{AB} > \overline{CD}$ construa os segmentos EF e GH tais que $\overline{EF} = \overline{AB} + \overline{CD}$ e $\overline{GH} = \overline{AB} - \overline{CD}$.

Construção:

Soma: Trace uma reta r e marque sobre ela um ponto O . Em seguida, transporte o segmento AB para r , obtendo um segmento OE tal que $\overline{OE} = \overline{AB}$. Agora, transporte o segmento CD para r , a partir do ponto O , obtendo um ponto F , tal que $\overline{OF} = \overline{CD}$ e $O \in EF$. Note que $\overline{EF} = \overline{AB} + \overline{CD}$.

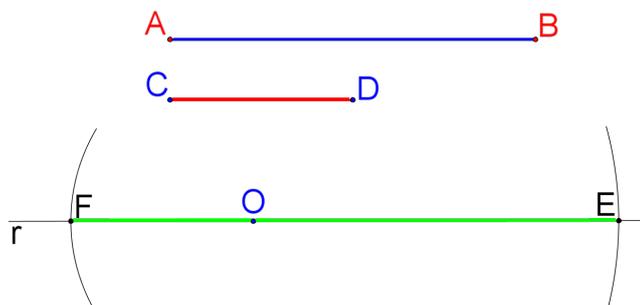


Figura 3 – Soma de segmentos.

Segunda parte: Trace uma reta r e marque sobre ela um ponto O . Em seguida, transporte o segmento AB para r , obtendo um segmento OH tal que $\overline{OH} = \overline{AB}$. Agora,

transporte o segmento CD para r , a partir do ponto O , obtendo um ponto G , tal que $\overline{OG} = \overline{CD}$ e $G \in OH$. Perceba que $\overline{GH} = \overline{AB} - \overline{CD}$.

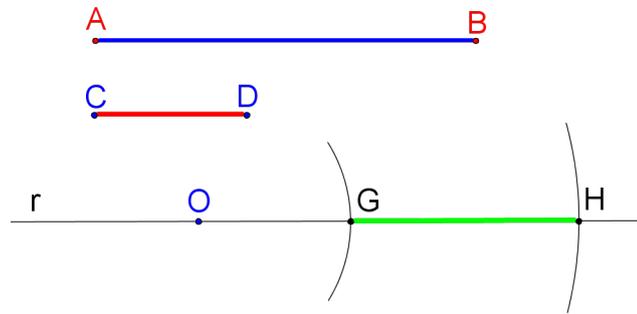


Figura 4 – Subtração de segmentos.

2.1.1.2 Transporte de ângulo

Dado um ângulo \widehat{AOB} , construa um ângulo $\widehat{CO'D}$ congruente a \widehat{AOB} .

Construção:

Trace o círculo de centro O e raio r arbitrário, obtendo os pontos $E \in \overrightarrow{OA}$ e $F \in \overrightarrow{OB}$. Em seguida, considere dois pontos do plano O' e D , e trace o círculo de centro O' e raio r , obtendo o ponto $G \in \overrightarrow{O'D}$. Para finalizar, construa o círculo de centro G e raio \overline{EF} , denotando por C , uma de suas interseções com o círculo de centro O' e raio r . Temos que $\widehat{CO'D} \cong \widehat{AOB}$. A Figura 5 ilustra a construção.

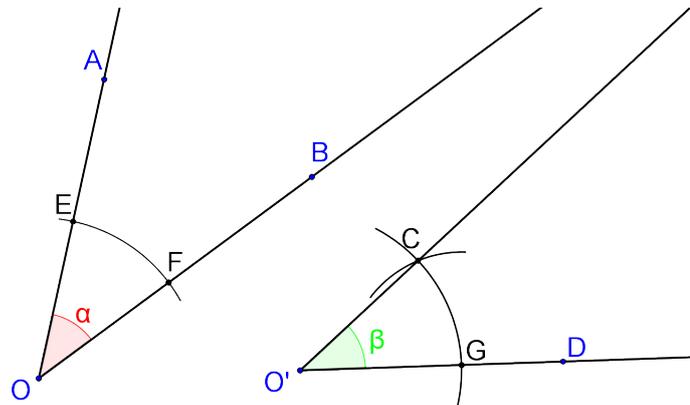


Figura 5 – Transporte de ângulo.

2.1.1.3 Soma e subtração de ângulos

Dados os ângulos \widehat{AOB} e $\widehat{CO'D}$ com $\widehat{AOB} > \widehat{CO'D}$, construa um ângulo \widehat{BOL} tal que $\widehat{BOL} = \widehat{AOB} + \widehat{CO'D}$, e um ângulo \widehat{BOK} tal que $\widehat{BOK} = \widehat{AOB} - \widehat{CO'D}$.

Construção:

Trace o círculo de centro O e raio r arbitrário, obtendo os pontos $E \in \overrightarrow{OA}$ e $F \in \overrightarrow{OB}$. Em seguida, trace o círculo de centro O' e raio r , obtendo o ponto $G \in \overrightarrow{O'D}$ e $H \in \overrightarrow{O'C}$. Para

finalizar, construa o círculo de centro E e raio \overline{GH} , denotando por L e K os pontos de suas interseções com o círculo de centro O e raio r . A figura abaixo ilustra os procedimentos.

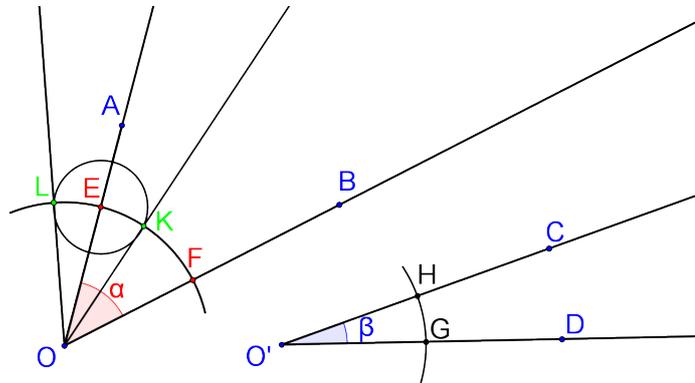


Figura 6 – Soma e subtração de ângulos.

Observe que $\widehat{BOL} = \widehat{AOB} + \widehat{CO'D}$, e $\widehat{BOK} = \widehat{AOB} - \widehat{CO'D}$. E note que nesta construção fizemos o transporte (2.1.1.2) do ângulo $\widehat{CO'D}$.

2.1.1.4 *Reta perpendicular*

Dados um ponto A e uma reta r , construa uma reta perpendicular a r passando por A . Temos dois casos: $A \in r$ ou $A \notin r$. Faremos uma única descrição da construção para os dois casos.

Construção:

Trace o círculo de raio r e centro em A , de modo que interseccione a reta em dois pontos, digamos B e C . Em seguida, trace os círculos centrados em B e C com raios $r' > r$. Denotemos a interseção entre os dois últimos círculos construídos por D e E . A reta determinada pelos pontos D e E passa por A e é perpendicular a r .

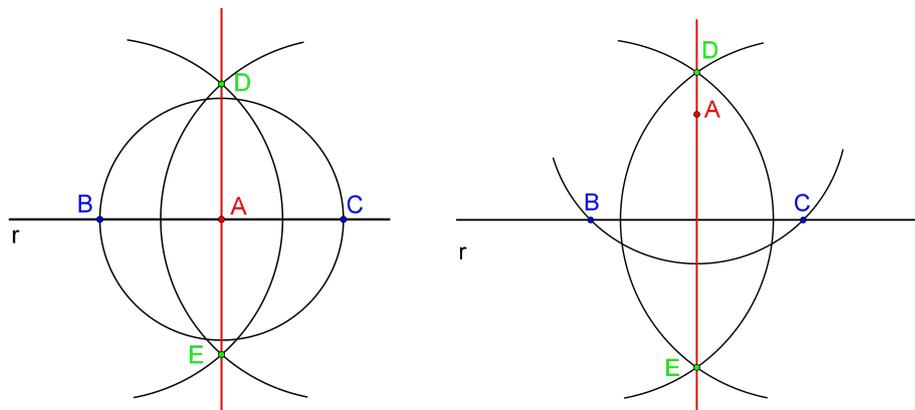


Figura 7 – Reta perpendicular.

2.1.1.5 *Mediatriz de um segmento*

Dado um segmento AB , construa a reta mediatriz.

Construção:

Trace os círculos centrados em A e B , de raio $r > \frac{1}{2}AB$. As interseções entre estes dois círculos são os pontos C e D . A reta que passa por estes dois pontos é a mediatriz do segmento AB , que intersecta AB no seu ponto médio.

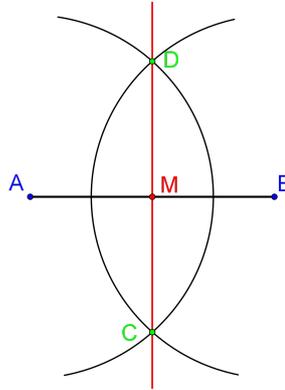


Figura 8 – Reta mediatriz.

Vejam agora um exemplo de aplicação da construção da mediatriz.

Exemplo 2.1. *Dados dois pontos, A e B , e uma reta r , tais que a mediatriz de AB intersecte r , construa o círculo que passa pelos dois pontos dados e que tem o centro sobre a reta r .*

Construção:

Trace a mediatriz do segmento AB , que intersecta r no ponto O . Como O pertence a mediatriz, segue que $\overline{OA} = \overline{OB}$. Agora, trace o círculo de centro O e raio \overline{OA} .

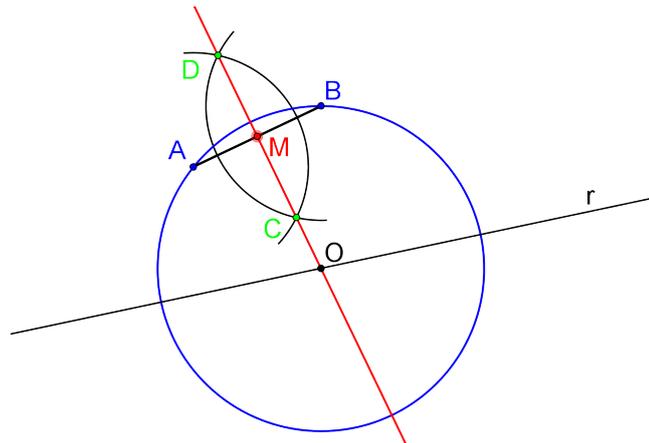


Figura 9 – Aplicação da construção da mediatriz.

Vale observar que se a reta r for a mediatriz do segmento AB , então existem infinitos círculos que tem centro sobre r e que passam por A e B . Caso contrário, o círculo construído é único, pois duas retas não paralelas concorrem em um único ponto.

2.1.1.6 Retas paralelas

Caso 1: Dados um ponto A e uma reta r , construa a reta s paralela a r , e passando por A .

Construção:

Tome um ponto O pertencente a r e trace o círculo de centro em O e raio \overline{OA} . Sejam B e C os pontos de interseção entre este círculo e a reta r . Agora, trace o círculo de centro em B e raio \overline{AC} , obtendo o ponto D , interseção deste círculo com o outro já construído, situado no mesmo semiplano de A em relação a reta r . Observe que os triângulos OAC e ODB são congruentes. Logo as distâncias dos pontos A e D para reta r são iguais, pois as alturas correspondentes dos dois triângulos possuem mesmo comprimento. Portanto, a reta s definida pelos pontos A e D é paralela a r e passa pelo ponto A .

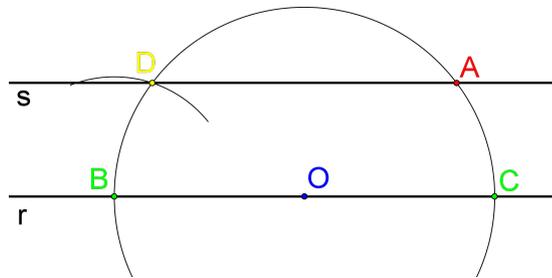


Figura 10 – Reta paralela passando por um ponto dado.

Caso 2: Dados um segmento AB e uma reta r , construa as retas paralelas a r , distando \overline{AB} de r .

Construção:

Tome um ponto O pertencente a reta r e construa a reta t perpendicular a r passando por O . Trace o círculo de centro em O e raio \overline{AB} , obtendo os pontos C e D , interseções de deste círculo com a reta t . Para finalizar, construa as retas paralelas a r e que passam pelos pontos C e D usando a descrição da Construção, anterior.

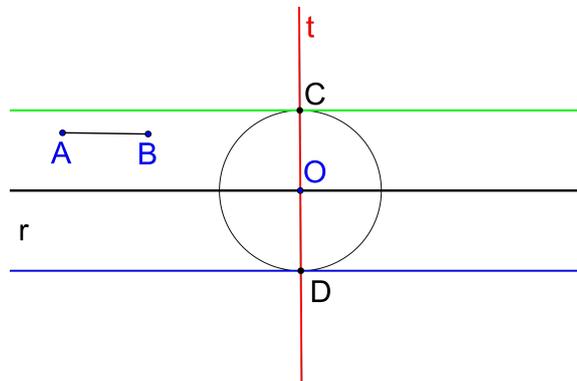


Figura 11 – Retas paralelas distando \overline{AB} , sendo dado o segmento AB .

2.1.1.7 Divisão de segmentos

Dado o segmento AB , divida-o em n segmentos congruentes.

Construção:

Pelo ponto A , trace uma semirreta \overrightarrow{AX} , com $X \notin \overrightarrow{AB}$. Sobre esta semirreta tome n pontos sucessivos, A_1, A_2, \dots, A_n , a partir de A , tais que $\overline{AA_1} = \overline{A_1A_2} = \overline{A_2A_3} = \dots = \overline{A_{n-1}A_n}$. Trace a reta r definida pelos pontos A_n e B , e construa as retas r_1, r_2, \dots, r_{n-1} , paralelas a r , passando respectivamente pelos A_1, A_2, \dots, A_{n-1} . As retas r_1, r_2, \dots, r_{n-1} intersectam o segmento AB respectivamente nos pontos B_1, B_2, \dots, B_{n-1} , e estes pontos, pelo Teorema de Tales, são tais que $\overline{AB_1} = \overline{B_1B_2} = \overline{B_2B_3} = \dots = \overline{B_{n-1}B}$.

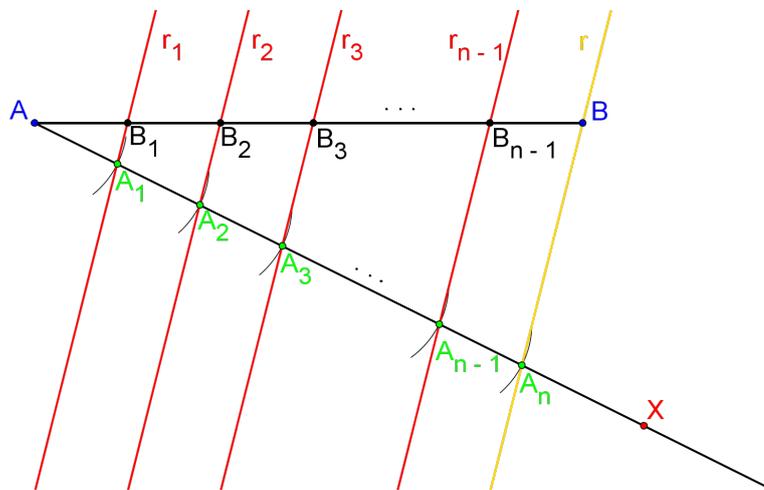


Figura 12 – Divisão de segmentos em partes congruentes.

Esta construção nos permite obter segmentos de comprimento fracionário em relação ao comprimento de outro segmento dado.

2.1.1.8 Bissetriz de um ângulo

Dado um ângulo \widehat{AOB} , construa a semirreta \overrightarrow{OM} tal que $\widehat{BOM} = \widehat{AOM}$.

Construção:

Trace o círculo de centro em O e raio arbitrário r , obtendo os pontos $C \in \overrightarrow{OA}$ e $D \in \overrightarrow{OB}$. Encontre o ponto médio M , de DC (2.1.1.5). A semirreta \overrightarrow{OM} é tal que $\widehat{BOM} = \widehat{AOM}$ como queríamos.

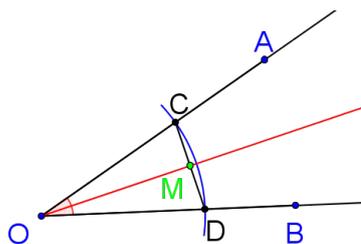


Figura 13 – Bissetriz de um ângulo.

2.1.1.9 Arco Capaz

Dado um segmento AB e um ângulo \widehat{CDE} , construir os arcos tais que qualquer de seus pontos, seja P um deles, determine ângulos $\widehat{APB} = \widehat{COD}$.

Construção:

A partir do ponto A e considerando o segmento AB , construa um ângulo congruente a \widehat{CDE} (2.1.1.2), obtendo a semirreta \overrightarrow{AX} , e trace reta s , mediatriz do segmento AB (2.1.1.5). Em seguida, construa a reta t perpendicular a semirreta \overrightarrow{AX} e passando por A (2.1.1.4). Seja O a interseção de s e t . Construa o arco de centro em O , situado no mesmo semiplano de O em relação a reta \overleftrightarrow{AB} , raio $\overline{OA} = \overline{OB}$ e extremidades A e B . Este é um dos arcos da construção. Obtemos o outro traçando o círculo de centro M , médio de AB , que determinará o ponto O' interseção desse círculo com s . Para finalizar, com centro em O' , construa o arco situado no mesmo semiplano de O' em relação a reta \overleftrightarrow{AB} , de raio $\overline{O'A} = \overline{O'B}$ e extremidades A e B .

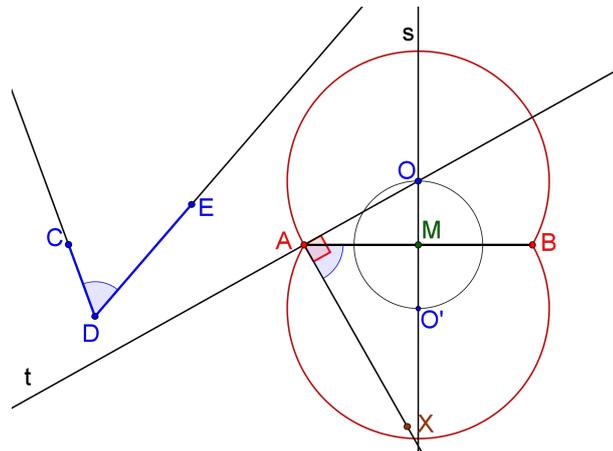


Figura 14 – Arco capaz.

2.1.1.10 Multiplicação e divisão de segmentos

Dada uma unidade de medida e dois segmentos de comprimentos a e b , construir segmentos de comprimentos $a \cdot b$ e a/b .

Construção:

Construa, utilizando a Construção 2.1.1.4, triângulos retângulos como na figura abaixo ¹,

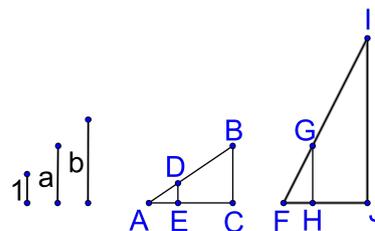


Figura 15 – Multiplicação e divisão de segmentos

¹ Fazemos apenas o caso em que $1 < a < b$, mas em todo caso podemos contruir triângulos retângulos que solucionam o problema.

onde $\overline{BC} = \overline{GH} = a$, $\overline{AC} = \overline{FJ} = b$ e $\overline{AE} = \overline{FH} = 1$.

Como $\triangle ABC \sim \triangle ADE$ e $\triangle FIJ \sim \triangle FGH$ segue

$$\frac{\overline{BC}}{\overline{AC}} = \frac{\overline{DE}}{\overline{AE}} \Rightarrow \frac{a}{b} = \frac{\overline{DE}}{1} \quad \therefore \overline{DE} = \frac{a}{b},$$

e

$$\frac{\overline{IJ}}{\overline{FJ}} = \frac{\overline{GH}}{\overline{FH}} \Rightarrow \frac{\overline{IJ}}{b} = \frac{a}{1} \quad \therefore \overline{IJ} = a \cdot b.$$

2.1.1.11 Quadrado inscrito em um círculo

Dado um círculo de centro O , construa um quadrado inscrito.

Construção:

Trace duas retas perpendiculares passando por O . As interseções, A, B, C e D , dessas retas com o círculo são os vértices de um quadrado.

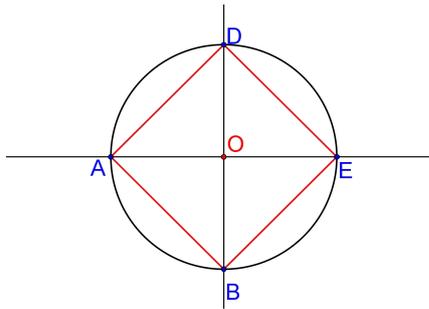


Figura 16 – Quadrado inscrito em um círculo.

Observe que esta construção é equivalente a dividir o círculo em quatro arcos congruentes.

2.1.1.12 Polígonos regulares de 2^n lados

Dado um círculo de centro O , construa um polígono de 2^n lados inscritos no círculo, com $n \geq 3$.

Construção:

Estas construções serão feitas por recorrência. Construa um quadrado inscrito no círculo e por bissetão de seus ângulos centrais obtenha o octógono regular inscrito (Figura 17). Realizando novamente a bissetão dos ângulos centrais, agora do octógono, obtenha o polígono de 2^4 lados inscrito no círculo. Seguindo desta forma, a partir do polígono de $2^{(n-1)}$ lados, por bissetão de seus ângulos centrais, obtenha o polígono regular inscrito com 2^n lados.

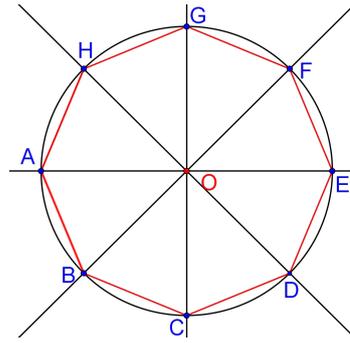


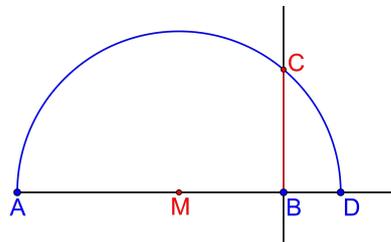
Figura 17 – Octógono.

2.1.1.13 Segmento com comprimento \sqrt{r}

Dada uma unidade de medida e um segmento AB tal que $\overline{AB} = r$, construa um segmento BC de modo que $\overline{BC} = \sqrt{r}$.

Construção:

Trace a semirreta \overrightarrow{AB} e sobre ela tome o ponto D tal que $\overline{AD} > \overline{AB} = r$ e $\overline{BD} = 1$ (unidade de medida). Encontre o ponto médio M do segmento AD e construa o semicírculo de centro M e raio $\overline{AM} = \overline{DM}$. Para finalizar construa a reta s , perpendicular a semirreta \overrightarrow{AB} passando pelo ponto B , obtendo o ponto C , interseção da reta s com o semicírculo. O segmento BC é tal que $\overline{BC} = \sqrt{r}$.

Figura 18 – Segmento de comprimento \sqrt{r} .

As construções que descrevemos acima, nos mostram que utilizando as construções mais básicas, os gregos conseguiam fazer uma quantidade enorme de novas construções, e cada vez mais complexas. Como vimos por meio da construção 2.1.1.13, era possível construir segmentos de comprimento \sqrt{r} , dado um segmento de comprimento r . Isto é, podemos construir segmentos com comprimentos irracionais da forma \sqrt{r} .

Também podemos observar que é possível construir polígonos regulares de 2^n lados, inscritos em um círculo, e embora não tenhamos realizado aqui, os gregos sabiam ainda construir os polígonos regulares de 3, 5, 6, 10, 12 e 20 lados, inscritos em um círculo, assim como os de $2^m n$ lados desde que soubessem construir o polígono de n lados, utilizando a bissetão dos ângulos centrais.

Segundo (HEFEZ e VILLELA, 2012, p. 201),

[...] por mais que os geômetras tentassem construir com régua e compasso o heptágono (polígono de 7 lados) e o eneágono (polígono de 9 lados), eles nunca conseguiram. Começou então a pairar a suspeita de que tais construções não seriam possíveis. Mas como provar tal impossibilidade? Uma coisa é provar que uma determinada figura é construtível, exibindo sua construção; outra coisa é mostrar que nenhuma construção poderá levar à obtenção de uma dada figura.

Os três famosos problemas deixados pelos gregos acerca da construtibilidade com régua e compasso são:

- I) **Duplicação do cubo:** Construir o lado de um cubo cujo volume é o dobro do de um cubo dado;
- II) **Trissecção do ângulo:** Dividir um ângulo arbitrário dado, em três partes iguais;
- III) **Quadratura do círculo:** Construir um quadrado com área igual à de um círculo dado.

Estes três problemas são exemplos de elementos de grande importância histórica para o desenvolvimento da Matemática. A busca ingente por soluções para os mesmos influenciou profundamente a geometria grega e levou a muitas descobertas, como as seções cônicas, muitas curvas cúbicas e quárticas e várias curvas transcendentes.

Somente no século XIX, mais de 2000 anos depois de os problemas terem sido concebidos, se estabeleceu a impossibilidade de tais construções utilizando apenas uma régua não graduada e um compasso. Tal fato se deu graças aos avanços nos estudos relativos a teoria dos corpos. (EVES, 2004).

Na proposição a seguir expomos uma argumentação que possibilita teoricamente trissectar um ângulo arbitrário com régua e compasso, desde que a régua utilizada seja graduada, isto é, possua marcas relacionadas a uma unidade definida. Este resultado está presente em (GONÇALVES, 2013), e é um dos problemas diretamente relacionados aos esforços pela solução da trissecção do ângulo, com os instrumentos euclidianos.

Proposição 2.1. *É possível realizar a trissecção de um ângulo arbitrário com régua graduada (com marcas) e compasso.*

Prova: Seja dado o ângulo $\alpha = \widehat{AOB}$. Considere que a régua utilizada possua marcas indicando segmentos de comprimento igual a a .

Com a régua, marque sobre as semirretas \overrightarrow{OA} e \overrightarrow{BO} os pontos X e Y respectivamente, de modo que $\overline{OX} = \overline{OY} = a$ e $O \in BY$, e em seguida construa o arco XOY de raio a (Figura 19).

Para cada ponto C no arco, com $C \neq X$, trace a semirreta \overrightarrow{XC} que intersecta a semirreta \overrightarrow{OY} no ponto D . Note que para $C = Y$ temos $D = Y$ e neste caso a distância

entre C e D é nula. Por outro lado, quando o ponto C se aproxima de X , a medida \overline{CD} cresce arbitrariamente. Logo, existe um ponto C pertencente ao arco de modo que $\overline{CD} = a$.

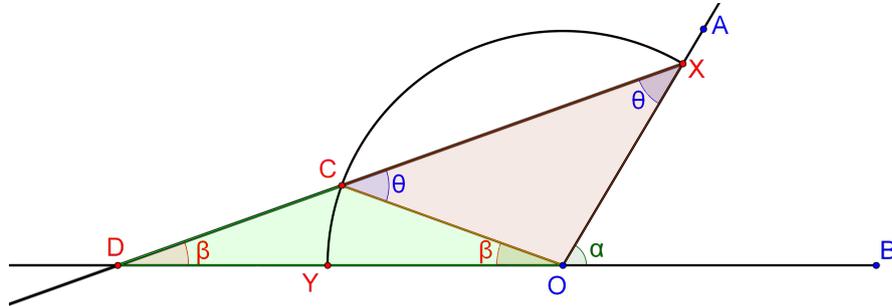


Figura 19 – Trissecção de um ângulo.

Afirmamos que $\widehat{XDO} = \frac{\alpha}{3}$. De fato, sejam $\widehat{XDO} = \beta$ e $\widehat{OXC} = \theta$. Como $\triangle COD$ e $\triangle XOC$ são isósceles por construção, temos que $\widehat{COD} = \beta$ e $\widehat{OCX} = \theta$, daí, $\theta = 2 \cdot \beta$ e $\alpha = \beta + \theta$ (ângulos externos aos triângulos COD e XOD respectivamente) implicam em $\beta = \frac{\alpha}{3}$, como queríamos. \square

Vale observar que a efetiva construção da trissecção de um ângulo, passa pela dificuldade de, mesmo com a régua graduada, encontrarmos o ponto C pertencente ao arco de modo que $\overline{DC} = a$.

Apresentamos agora, como exemplos, algumas das principais construções com os instrumentos euclidianos, relativas à triângulos. Nestes exemplos, sempre que usarmos α estaremos nos referindo ao ângulo \hat{A} do triângulo, assim como β ao ângulo \hat{B} e θ ao ângulo \hat{C} do triângulo.

Exemplo 2.2. *Construa o triângulo ABC sendo dados o lado BC e os ângulos \hat{A} e \hat{B} .*

Construção:

Transporte o ângulo \hat{B} para o segmento BC obtendo a semirreta \overrightarrow{BX} , e em seguida construa um arco capaz do ângulo \hat{A} relativo ao lado BC (2.1.1.10).

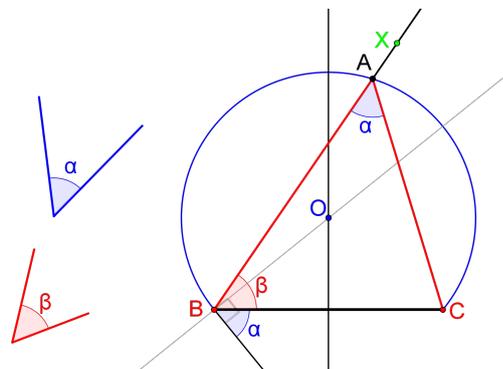


Figura 20 – Triângulo ABC sendo dados o lado BC e os ângulos \hat{A} e \hat{B} .

Marque o ponto A do triângulo, que é a interseção de \overrightarrow{BX} com o arco construído.

Exemplo 2.3. Construa o triângulo ABC sendo dados o perímetro $2p$ e os ângulos \hat{B} e \hat{C} .

Construção:

Construa o segmento RS tal que $\overline{RS} = 2p$. Transporte os ângulos \hat{B} e \hat{C} a partir dos pontos R e S respectivamente. Trace as bissetrizes dos ângulos resultados do transporte; as interseções destas bissetrizes determinam o ponto A .

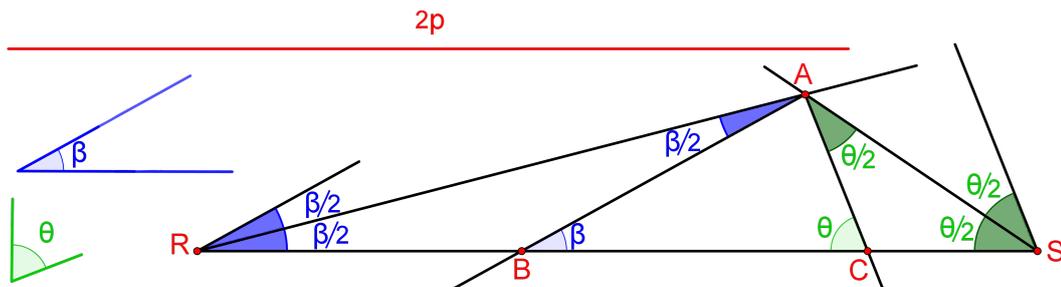


Figura 21 – Triângulo ABC sendo dados o perímetro $2p$ e os ângulos \hat{B} e \hat{C} .

Agora, construa os ângulos a partir do ponto A , de medida $\frac{\hat{B}}{2}$ e $\frac{\hat{C}}{2}$, obtendo respectivamente os pontos B e C do triângulo.

Exemplo 2.4. Construa o triângulo ABC sendo dados o lado BC , a soma $\overline{AB} + \overline{AC}$ e o ângulo \hat{B} .

Construção:

Transporte o ângulo β a partir de B obtendo a semirreta \overrightarrow{BX} . Sobre a semirreta \overrightarrow{BX} marque o ponto M tal que $\overline{BM} = \overline{AB} + \overline{AC}$. Trace a mediatriz do segmento \overline{MC} . A interseção da mediatriz com o segmento BM é o ponto A do triângulo.

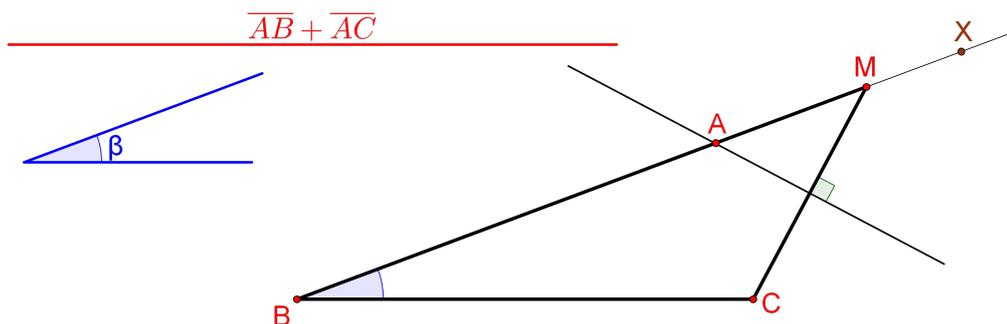


Figura 22 – Triângulo ABC sendo dados o lado BC , a soma $\overline{AB} + \overline{AC}$ e o ângulo \hat{B} .

Exemplo 2.5. Construa o triângulo ABC sendo dados o lado BC e as medianas M_b e M_c relativas respectivamente aos lados AC e AB .

Construção:

Construa os segmentos $\frac{2}{3}M_b$ e $\frac{2}{3}M_c$ (2.1.1.8). Trace os círculos de centros em B e C e raios respectivamente $\frac{2}{3}M_b$ e $\frac{2}{3}M_c$, obtendo o ponto O (baricentro do triângulo), interseção

entre eles. Sobre as semirretas \overrightarrow{BO} e \overrightarrow{CO} marque os pontos M_{AC} e M_{AB} respectivamente, tais que $\overline{BM_{AC}} = \overline{M_b}$ e $\overline{CM_{AB}} = \overline{M_c}$. Estes pontos são os pontos médios dos segmentos AC e AB . Para finalizar, marque o ponto A sobre a semirreta $\overrightarrow{BM_{AB}}$ de modo que $\overline{BM_{AB}} = \overline{M_{AB}A}$. O triângulo está construído.

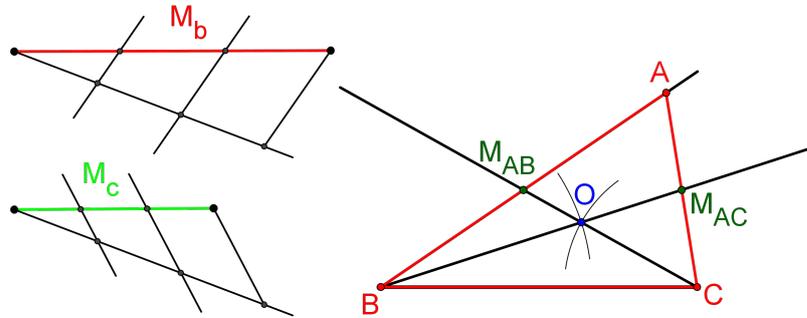


Figura 23 – Triângulo ABC sendo dados o lado BC e as medianas M_b e M_c relativas respectivamente aos lados AC e AB .

Exemplo 2.6. Construa o triângulo ABC sendo dadas as medianas M_a , M_b e M_c relativas respectivamente aos lados BC , AC e AB .

Construção:

Construa os segmentos $\frac{2}{3}M_a$, $\frac{2}{3}M_b$ e $\frac{2}{3}M_c$ (2.1.1.8) e em seguida o triângulo ARS tal que $\overline{AS} = \frac{2}{3}M_a$, $\overline{AR} = \frac{2}{3}M_b$ e $\overline{RS} = \frac{2}{3}M_c$. Para isso, considere os pontos R e X , e trace a semirreta \overrightarrow{RX} . Tome o ponto S sobre a semirreta \overrightarrow{RX} de modo que $\overline{RS} = \frac{2}{3}M_c$. Construa os círculos de centros em R e S , e raios respectivamente $\frac{2}{3}M_b$ e $\frac{2}{3}M_a$, obtendo o ponto A interseção entre eles (Figura 24). Agora, construa as retas r e s paralelas respectivamente as retas \overleftrightarrow{AS} , e \overleftrightarrow{AR} , marcando o ponto B , interseção entre elas. Sobre a semirreta \overrightarrow{RX} , tome o ponto C tal que $\overline{SC} = \frac{2}{3}M_c$.

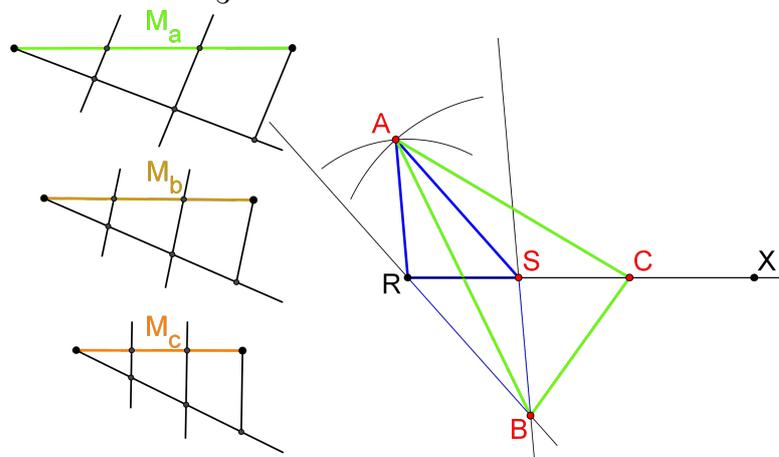


Figura 24 – Triângulo ABC sendo dadas as medianas M_a , M_b e M_c relativas respectivamente aos lados BC , AC e AB .

As construções acima nos mostram a construtibilidade de triângulos, conhecidos alguns de seus elementos. Os problemas da existência e construtibilidade de um triângulo dados os comprimentos de suas bissetrizes internas, assim como também os *três famosos problemas* supracitados, diferente destas construções que realizamos como exemplos e tantas outras possíveis em relação aos triângulos, permaneceram sem solução por bom tempo na história, haja vista que os conhecimentos geométricos não possibilitavam construir tais soluções.

A seguir, continuamos desenvolvendo as preliminares de Geometria, onde apresentamos outros resultados relevantes para este trabalho.

2.1.2 Outros resultados importantes

Nos próximos tópicos, expomos quatro resultados importantes relativos aos objetivos do trabalho. Seguimos essencialmente (NETO, 2013).

2.1.2.1 Relações trigonométricas do triângulo retângulo

Consideremos o triângulo ABC , retângulo em A , com $\widehat{ABC} = \beta$, e o sistema de coordenadas cartesianas XBY de modo que o semieixo positivo das abscissas coincida com a semirreta \overrightarrow{AB} e o lado BC do triângulo esteja situado no primeiro quadrante.

Trace o círculo de centro em B e raio 1 obtendo o ponto P , interseção deste círculo com a semirreta \overrightarrow{BC} , e seja Q o pé da perpendicular baixada de P ao eixo das abscissas.

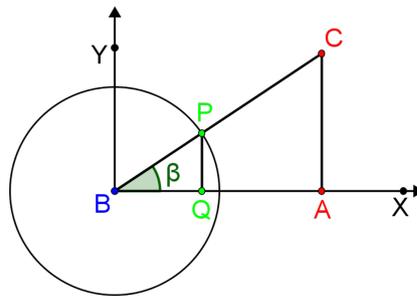


Figura 25 – Seno, cosseno e tangente de um triângulo retângulo.

Temos que $\triangle BPQ \sim \triangle BCA$. Daí,

$$\frac{\overline{AC}}{\overline{BC}} = \frac{\overline{QP}}{\overline{BP}}, \quad \frac{\overline{AB}}{\overline{BC}} = \frac{\overline{QB}}{\overline{BP}}, \quad e \quad \frac{\overline{AC}}{\overline{AB}} = \frac{\overline{QP}}{\overline{QB}}.$$

Como

$$\overline{QP} = \text{sen}\beta \quad e \quad \overline{QB} = \text{cos}\beta,$$

seguem das igualdades acima que

$$\frac{\overline{AC}}{\overline{BC}} = \text{sen}\beta, \quad \frac{\overline{AB}}{\overline{BC}} = \text{cos}\beta, \quad e \quad \frac{\overline{AC}}{\overline{AB}} = \text{tan}\beta.$$

Temos assim definidas as razões trigonométricas do triângulo ABC retângulo em A e com $\widehat{ABC} = \beta$, podendo portanto enunciar:

$$\begin{aligned} \operatorname{sen} \beta &= \frac{\text{cateto oposto a } \beta}{\text{hipotenusa}}, & \cos \beta &= \frac{\text{cateto adjacente a } \beta}{\text{hipotenusa}}, \\ \tan \beta &= \frac{\text{cateto oposto a } \beta}{\text{cateto adjacente a } \beta}. \end{aligned}$$

Exemplo 2.7. Seja $ABCD$ um quadrado de lado 1 e E um ponto sobre o lado CD , de modo que $\overline{AE} = \overline{AB} + \overline{CE}$. Se F é o ponto médio de CD , mostre que $\widehat{EAB} = 2 \cdot \widehat{FAD}$.

Demonstração: Como F é o ponto médio de CD , temos que $\overline{FD} = \frac{1}{2}$. Uma vez que o triângulo ADF é retângulo, segue $\tan \widehat{DAF} = \tan \beta = \frac{1}{2}$. Consideremos agora o ponto G pertencente ao segmento AB , de modo que o triângulo AGE seja retângulo. A figura abaixo ilustra o processo.

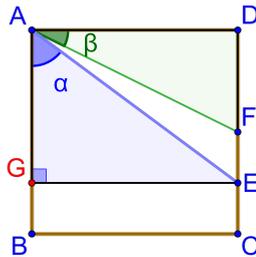


Figura 26 – Quadrado $ABCD$ de lado 1, nas circunstâncias do problema.

Do enunciado temos que $\overline{AE} = 1 + \overline{CE}$, e pela forma como tomamos o ponto G , ficamos com $\overline{GA} = 1 - \overline{CE}$. Daí, pelo Teorema de Pitágoras aplicado ao triângulo AGE segue,

$$(1 + \overline{CE})^2 = (1 - \overline{CE})^2 + 1^2 \Rightarrow \overline{CE} = \frac{1}{4}.$$

Logo, $\tan \alpha = \frac{1}{1 - \frac{1}{4}} = \frac{2 \cdot \frac{1}{2}}{1 - (\frac{1}{2})^2} = \frac{2 \cdot \tan \beta}{1 - (\tan \beta)^2} = \tan(2\beta) \quad \therefore \tan \alpha = \tan(2\beta)$. Portanto, como $0^\circ < \alpha < 90^\circ$ e $0^\circ < \beta < 90^\circ$ segue $\alpha = 2\beta$, isto é, $\widehat{EAB} = 2 \cdot \widehat{FAD}$. \square

2.1.2.2 Teorema da bissetriz

O resultado que apresentamos neste tópico é uma das mais importantes aplicações do Teorema de Thales.

Proposição 2.2. Seja ABC um triângulo, P é o pé da bissetriz interna e Q o pé da bissetriz externa relativas ao lado BC .

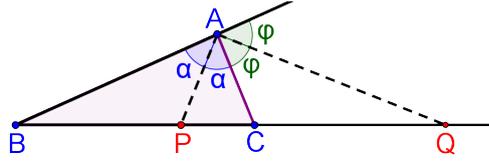


Figura 27 – Teorema da bissetriz.

As seguintes igualdades são satisfeitas,

$$\frac{\overline{QC}}{\overline{QB}} = \frac{\overline{AC}}{\overline{AB}} = \frac{\overline{CP}}{\overline{PB}}.$$

Prova: Suponhamos que $\overline{AC} < \overline{AB}$ (o caso $\overline{AB} < \overline{AC}$ é análogo). Pelo ponto C , construa a reta paralela a reta \overleftrightarrow{AQ} , obtendo o ponto $C' \in AB$.

Desta forma temos que o triângulo ACC' é isósceles, de base CC' , pois $\widehat{CC'A} = \widehat{QAX}$ (ângulos colaterais) e $\widehat{CAQ} = \widehat{ACC'}$ (alternos internos).

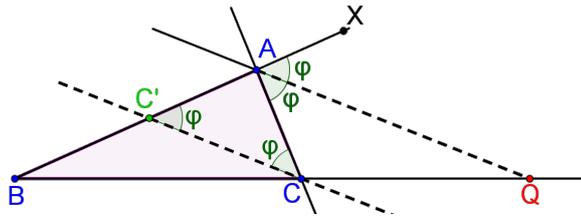


Figura 28 – Prova do teorema da bissetriz, primeira parte.

Daí, $\overline{AC'} = \overline{AC}$, e pelo teorema de Thales segue

$$\frac{\overline{QC}}{\overline{QB}} = \frac{\overline{AC'}}{\overline{AB}} = \frac{\overline{AC}}{\overline{AB}} \quad \therefore \quad \frac{\overline{QC}}{\overline{QB}} = \frac{\overline{AC}}{\overline{AB}}.$$

Para o que falta, construa a reta paralela a reta \overleftrightarrow{AP} e que passa por C , obtendo o ponto $C'' \in \overleftrightarrow{AB}$.

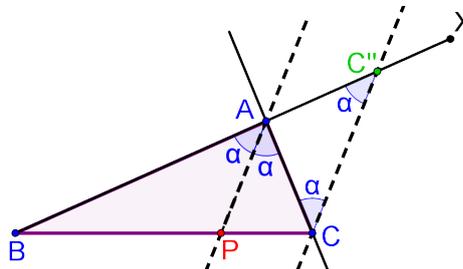


Figura 29 – Prova do teorema da bissetriz, segunda parte.

Assim temos que o triângulo ACC'' é isósceles, de base CC'' , pois $\widehat{BAP} = \widehat{AC''C}$ (ângulos colaterais) e $\widehat{PAC} = \widehat{ACC''}$ (alternos internos). Daí, $\overline{AC''} = \overline{AC}$, e pelo teorema de Thales segue

$$\frac{\overline{AC''}}{\overline{AB}} = \frac{\overline{AC}}{\overline{AB}} = \frac{\overline{CP}}{\overline{PB}} \quad \therefore \quad \frac{\overline{AC}}{\overline{AB}} = \frac{\overline{CP}}{\overline{PB}}.$$

□

2.1.2.3 Lei dos cossenos

A lei dos cossenos é uma generalização do Teorema de Pitágoras. Vejamos a seguinte

Proposição 2.3. Se ABC é um triângulo com $\overline{BC} = a$, $\overline{AC} = b$, $\overline{AB} = c$ e $\widehat{BAC} = \alpha$, então

$$a^2 = b^2 + c^2 - 2bc \cos \alpha.$$

Prova: A figura abaixo representa os três casos possíveis (α é agudo, reto, ou obtuso). No caso em que α é reto, temos que $\cos \alpha = 0$, e assim o Teorema de Pitágoras nos assegura que $a^2 = b^2 + c^2 - 2bc \cos \alpha$.

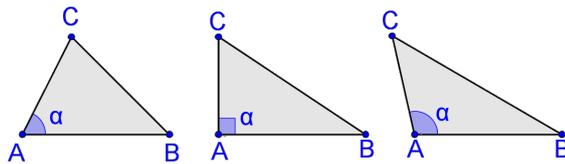


Figura 30 – Lei dos Cossenos.

Para os demais casos, seja H o pé da altura relativa ao lado AB , de modo que $\overline{CH} = h$.

Se o ângulo α é agudo, pelo Teorema de Pitágoras segue

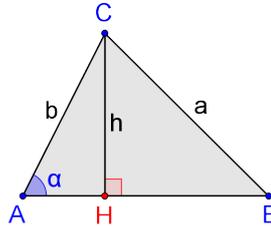


Figura 31 – Lei dos Cossenos, caso em que α é agudo.

$$\begin{aligned} a^2 &= h^2 + (c - \overline{AH})^2 \Rightarrow a^2 = h^2 + c^2 - 2c\overline{AH} + \overline{AH}^2 \Rightarrow \\ &\Rightarrow a^2 = (h^2 + \overline{AH}^2) + c^2 - 2c\overline{AH} \end{aligned} \quad (2.1)$$

e também $h^2 + \overline{AH}^2 = b^2$. Das relações trigonométricas temos $\frac{\overline{AH}}{b} = \cos \alpha \Rightarrow \overline{AH} = b \cos \alpha$. Daí, substituindo em (2.1) temos $a^2 = b^2 + c^2 - 2bc \cos \alpha$.

Se o ângulo α é obtuso, de modo análogo ao caso α agudo, temos,

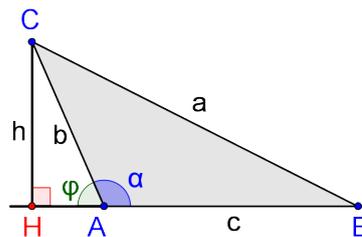


Figura 32 – Lei dos Cossenos, caso em que α é obtuso.

$$\begin{aligned}
 a^2 &= h^2 + (c + \overline{AH})^2 \Rightarrow a^2 = h^2 + c^2 + 2c\overline{AH} + \overline{AH}^2 \Rightarrow \\
 &\Rightarrow a^2 = (h^2 + \overline{AH}^2) + c^2 + 2c\overline{AH}
 \end{aligned} \tag{2.2}$$

e também $h^2 + \overline{AH}^2 = b^2$.

Das relações trigonométricas temos $\frac{\overline{AH}}{b} = \cos\varphi = -\cos\alpha \Rightarrow \overline{AH} = -b\cos\alpha$. Daí, substituindo em (2.2) obtemos $a^2 = b^2 + c^2 - 2bc\cos\alpha$. \square

2.1.2.4 Bissetrizes internas

O resultado apresentado neste tópico possibilita obtermos os comprimentos das bissetrizes internas de um triângulo, em função dos lados. Vejamos.

Proposição 2.4. *Seja ABC um triângulo com $\overline{BC} = a$, $\overline{AC} = b$, $\overline{AB} = c$.*

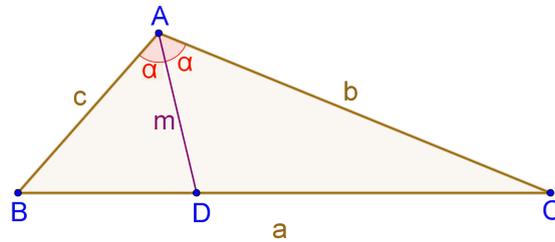


Figura 33 – Bissetriz em função dos lados.

Se m, n, p são os comprimentos das suas bissetrizes internas e s o seu semiperímetro, então temos,

$$m = \frac{2}{b+c} \sqrt{bcs(s-a)}, \tag{2.3}$$

com fórmulas semelhantes para n e p .

Antes de demonstrarmos a proposição Proposição 2.4, faremos o pequeno lema a seguir.

Lema 2.1. *Nas condições da figura Figura 33, vale a identidade*

$$\cos(\alpha) = \sqrt{\frac{s(s-a)}{bc}},$$

onde s é o semiperímetro do triângulo ABC .

Prova: A lei dos cossenos assegura que $a^2 = b^2 + c^2 - 2bc\cos(2\alpha)$, daí

$$\cos(2\alpha) = \frac{b^2 + c^2 - a^2}{2bc}.$$

Da trigonometria temos $\cos(\alpha) = \sqrt{\frac{1 + \cos(2\alpha)}{2}}$. Logo,

$$\begin{aligned}\cos(\alpha) &= \sqrt{\frac{1 + \frac{b^2 + c^2 - a^2}{2bc}}{2}} = \sqrt{\frac{2bc + b^2 + c^2 - a^2}{4bc}} = \sqrt{\frac{(b+c)^2 - a^2}{4bc}} \Rightarrow \\ \Rightarrow \cos(\alpha) &= \sqrt{\frac{(b+c+a)(b+c-a)}{4bc}} = \sqrt{\frac{\left(\frac{b+c+a}{2}\right)\left(\frac{b+c-a}{2}\right)}{bc}}.\end{aligned}$$

Isto é,

$$\cos(\alpha) = \sqrt{\frac{s(s-a)}{bc}}. \quad (2.4)$$

□

Prova da Proposição 2.4: Se $S(MNP)$ denota a área do triângulo MNP , então

$$S(ABC) = S(ABD) + S(ACD) \Rightarrow 2S(ABC) = 2S(ABD) + 2S(ACD),$$

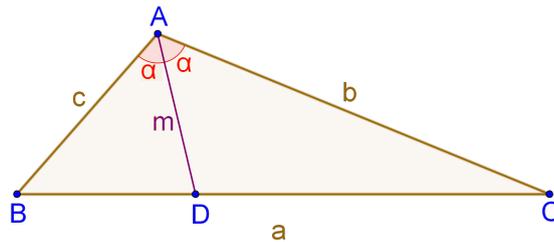


Figura 34 – Prova da proposição 2.4.

de modo que, usando a fórmula para calcular área de triângulos em função dos senos dos ângulos, $S(ABC) = \frac{1}{2}bc\text{sen}(2\alpha)$, $S(ABD) = \frac{1}{2}cm\text{sen}(\alpha)$ e $S(ACD) = \frac{1}{2}bm\text{sen}(\alpha)$, temos

$$bc\text{sen}(2\alpha) = bm\text{sen}(\alpha) + cm\text{sen}(\alpha)$$

e portanto,

$$m = \left(\frac{bc}{b+c}\right) \frac{\text{sen}(2\alpha)}{\text{sen}(\alpha)} = \left(\frac{2bc}{b+c}\right) \cos(\alpha) \quad \therefore \quad m = \left(\frac{2bc}{b+c}\right) \cos(\alpha).$$

Pelo lema anterior, a equação (2.4) nos dá

$$m = \left(\frac{2bc}{b+c}\right) \sqrt{\frac{s(s-a)}{bc}}$$

que implica em

$$m = \frac{2}{b+c} \sqrt{bcs(s-a)}.$$

□

2.2 Elementos da álgebra

Nesta seção apresentamos alguns resultados da álgebra que são importantes nos desenvolvimentos posteriores. Para mais detalhes o leitor pode consultar as obras (FILHO, 1990), (GARCIA e LEQUAIN, 2001), (GONÇALVES, 2013), e (HEFEZ e VILLELA, 2012).

2.2.1 Anéis, corpos e homomorfismos

Definição 2.1 (Anel). *Seja \mathbb{A} um conjunto não vazio onde estejam definidas duas operações, as quais chamamos de soma e produto em \mathbb{A} e denotamos por $+$ e \cdot ,*

$$\begin{array}{ccc} + : \mathbb{A} \times \mathbb{A} & \longrightarrow & \mathbb{A} \\ (a, b) & \longmapsto & a + b \end{array} \quad e \quad \begin{array}{ccc} \cdot : \mathbb{A} \times \mathbb{A} & \longrightarrow & \mathbb{A} \\ (a, b) & \longmapsto & a \cdot b \end{array} .$$

Dizemos que $(\mathbb{A}, +, \cdot)$ é um anel se as seguintes propriedades são satisfeitas para quaisquer que sejam a, b e $c \in \mathbb{A}$.

- i) $(a + b) + c = a + (b + c)$ (associatividade da soma);
- ii) $\exists 0 \in \mathbb{A}$ tal que $a + 0 = 0 + a = a$ (existência de elemento neutro para a soma);
- iii) $\forall x \in \mathbb{A}$ existe um único $y \in \mathbb{A}$ denotado por $y = -x$ tal que $x + y = y + x = 0$ (existência de inverso aditivo);
- iv) $a + b = b + a$ (comutatividade da soma);
- v) $(a \cdot b) \cdot c = a \cdot (b \cdot c)$ (associatividade do produto);
- vi) $a \cdot (b + c) = a \cdot b + a \cdot c$; $(a + b) \cdot c = a \cdot c + b \cdot c$ (distributividade à esquerda e à direita).

Complementos da definição 2.1

Se um anel $(\mathbb{A}, +, \cdot)$ satisfaz a propriedade:

- vii) $\exists 1 \in \mathbb{A}, 0 \neq 1$ tal que $x \cdot 1 = 1 \cdot x = x, \forall x \in \mathbb{A}$, dizemos que $(\mathbb{A}, +, \cdot)$ é um anel com unidade.

Se um anel $(\mathbb{A}, +, \cdot)$ satisfaz a propriedade:

- viii) $\forall x, y \in \mathbb{A}, x \cdot y = y \cdot x$, dizemos que $(\mathbb{A}, +, \cdot)$ é um anel comutativo, caso contrário dizemos que é “não comutativo”.

Se um anel $(\mathbb{A}, +, \cdot)$ satisfaz a propriedade:

xix) $x, y \in \mathbb{A}$, $x \cdot y = 0 \Rightarrow x = 0$ ou $y = 0$, dizemos que $(\mathbb{A}, +, \cdot)$ é um anel sem divisores de zero.

Se um anel $(\mathbb{A}, +, \cdot)$ é comutativo, com unidade e sem divisores de zero, dizemos que $(\mathbb{A}, +, \cdot)$ é um **domínio de integridade** ou simplesmente um **domínio**.

Por questão de comodidade e para não carregar o texto, a partir deste ponto, quando nos referirmos a um anel $(\mathbb{A}, +, \cdot)$, o denotaremos apenas pelo símbolo \mathbb{A} e entenderemos que este anel possui as duas operações como acima.

Definição 2.2 (Subanel). Um subconjunto não vazio \mathbb{B} de um anel \mathbb{A} é dito um subanel de \mathbb{A} se seguintes propriedades são satisfeitas:

- i) Se $a, b \in \mathbb{B}$, então $a + b \in \mathbb{B}$ (\mathbb{B} fechado para soma de \mathbb{A});
- ii) Se $a, b \in \mathbb{B}$, então $a \cdot b \in \mathbb{B}$ (\mathbb{B} é fechado para o produto de \mathbb{A});
- iii) \mathbb{B} é um anel considerando as operações herdadas de \mathbb{A} .

A proposição a seguir estabelece uma condição para que um subconjunto de um anel seja um subanel.

Proposição 2.5. Sejam \mathbb{A} um anel e \mathbb{B} um subconjunto de \mathbb{A} . Temos que \mathbb{B} é um subanel de \mathbb{A} se, e somente se, são válidas as seguintes afirmações,

- i) $0 \in \mathbb{B}$ (o elemento neutro de \mathbb{A} é o elemento de \mathbb{B});
- ii) $a, b \in \mathbb{B} \Rightarrow a - b \in \mathbb{B}$ (o conjunto \mathbb{B} é fechado para a diferença);
- iii) $a, b \in \mathbb{B} \Rightarrow a \cdot b \in \mathbb{B}$ (o conjunto \mathbb{B} é fechado para o produto).

Prova:

[\Rightarrow] Se $\bar{0}$ for o elemento neutro de \mathbb{B} então $\bar{0} + \bar{0} = \bar{0} = \bar{0} + 0$, logo $\bar{0} = 0$, isto é, o elemento neutro de \mathbb{B} é o mesmo elemento neutro de \mathbb{A} . Dado $b \in \mathbb{B}$, seja $\bar{b} \in \mathbb{B}$ tal que $b + \bar{b} = \bar{0} = 0 = b + (-b)$, daí $\bar{b} = -b$. Consequentemente, dados $a, b \in \mathbb{B}$ temos $a - b = a + (-b) \in \mathbb{B}$. Por definição segue que o item iii) é válido.

[\Leftarrow] Pelo item i) temos que \mathbb{B} é não vazio, $\mathbb{B} \neq \emptyset$, e pelos itens i) e ii) segue $b \in \mathbb{B} \Rightarrow -b = 0 - b \in \mathbb{B}$. Daí, se $a, b \in \mathbb{B}$, então $a + b = a - (-b) \in \mathbb{B}$, ou seja, \mathbb{B} é fechado para a soma, e zero é o elemento neutro de \mathbb{B} . Como já sabemos por iii) que \mathbb{B} é fechado para o produto, e as propriedades associativa, comutativa, distributivas são herdadas de \mathbb{A} , temos que $(\mathbb{B}, +, \cdot)$ é um anel, e portanto subanel de \mathbb{A} . \square

Dado a pertencente a um anel comutativo com unidade \mathbb{A} , dizemos que a é invertível se existir um elemento $b \in \mathbb{A}$ tal que $a \cdot b = 1$. Pode-se verificar que quando existe, esse elemento b é único, o qual é dito inverso do elemento a , e o denotamos por a^{-1} , ou seja, $b = a^{-1}$.

Definição 2.3 (Corpo). Chamamos de corpo, um anel comutativo com unidade \mathbb{K} que satisfaz a seguinte propriedade:

$$\forall x \in \mathbb{K}, x \neq 0, \exists y \in \mathbb{K} \text{ tal que } x \cdot y = 1.$$

É importante notar aqui que todo corpo é um domínio de integridade, pois se $a \cdot b = 0$ com $b \neq 0$ então $(a \cdot b) \cdot b^{-1} = 0$, logo $a = 0$. Por outro lado o anel dos inteiros é um exemplo de domínio que não é corpo.

Exemplo 2.8. Os conjuntos \mathbb{Z} , \mathbb{Q} , \mathbb{R} , \mathbb{C} , munidos com as suas operações de soma e produto usuais, e $\mathbb{Z}[\sqrt{p}] = \{a + b\sqrt{p}; a, b \in \mathbb{Z}, p \text{ primo}\}$, $\mathbb{Q}[\sqrt{p}] = \{a + b\sqrt{p}; a, b \in \mathbb{Z}, p \text{ primo}\}$ com as operações dos reais, são anéis. Dentre eles, apenas os conjuntos \mathbb{Q} , \mathbb{R} , \mathbb{C} , e $\mathbb{Q}[\sqrt{p}]$ são corpos.

Definição 2.4 (Subcorpo). Um subconjunto não vazio \mathbb{F} de um corpo \mathbb{K} é um subcorpo de \mathbb{K} se, é fechado com respeito as operações induzidas de \mathbb{K} , e munido dessas operações ele é um corpo.

Definição 2.5 (Ideais). Seja \mathbb{A} um anel e \mathbb{I} um subanel de \mathbb{A} . Dizemos que \mathbb{I} é um ideal à esquerda de \mathbb{A} se $a \cdot b \in \mathbb{I}, \forall a \in \mathbb{A}, \forall b \in \mathbb{I}$ ($\mathbb{A} \cdot \mathbb{I} \subset \mathbb{I}$), e \mathbb{I} é um ideal à direita de \mathbb{A} se $b \cdot a \in \mathbb{I}, \forall a \in \mathbb{A}, \forall b \in \mathbb{I}$ ($\mathbb{I} \cdot \mathbb{A} \subset \mathbb{I}$). Se \mathbb{I} é simultaneamente um ideal à esquerda e à direita de \mathbb{A} , dizemos que \mathbb{I} é um ideal bilateral, ou simplesmente um ideal de \mathbb{A} ($\mathbb{A} \cdot \mathbb{I} \subset \mathbb{I}$ e $\mathbb{I} \cdot \mathbb{A} \subset \mathbb{I}$).

Definiremos agora uma importante relação em um anel. Seja \mathbb{A} um anel e \mathbb{I} um ideal de \mathbb{A} . Dados $a, b \in \mathbb{A}$, temos

$$a \equiv b \pmod{\mathbb{I}} \Leftrightarrow a - b \in \mathbb{I}.$$

Afirmamos que $\equiv \pmod{\mathbb{I}}$ é uma relação de equivalência. De fato,

- 1) $a \equiv a \pmod{\mathbb{I}}$ pois $0 = a - a \in \mathbb{I}$ (reflexividade);
- 2) $a \equiv b \pmod{\mathbb{I}} \Rightarrow b \equiv a \pmod{\mathbb{I}}$ pois se $a - b \in \mathbb{I}$ então $b - a = -(a - b) \in \mathbb{I}$ (simetria);
- 3) $a \equiv b \pmod{\mathbb{I}}$ e $b \equiv c \pmod{\mathbb{I}} \Rightarrow a \equiv c \pmod{\mathbb{I}}$ pois $a - b \in \mathbb{I}$ e $b - c \in \mathbb{I}$ implica $a - c = (a - b) + (b - c) \in \mathbb{I}$ (transitividade).

Denota-se por \bar{a} a classe de equivalência de $a \in \mathbb{A}$ segundo a relação $\equiv \pmod{\mathbb{I}}$. Desta forma,

$$\bar{a} = \{b \in \mathbb{A}; b \equiv a \pmod{\mathbb{I}}\}.$$

Considerando a relação definida, temos $b \in \bar{a}$ se, e somente se, $b - a \in \mathbb{I}$. Ou seja, para cada $b \in \bar{a}$ existe $x_b \in \mathbb{I}$ tal que $b = a + x_b$. Daí, denota-se ainda a classe \bar{a} por

$$\bar{a} = a + \mathbb{I} = \{a + x; x \in \mathbb{I}\}.$$

Chamamos de conjunto quociente de \mathbb{A} pelo ideal \mathbb{I} o conjunto $\mathbb{A}/\mathbb{I} = \{\bar{a} = a + \mathbb{I}; a \in \mathbb{A}\}$.

Definiremos ainda operações em \mathbb{A}/\mathbb{I} como abaixo,

$$+ : \mathbb{A}/\mathbb{I} \times \mathbb{A}/\mathbb{I} \longrightarrow \mathbb{A}/\mathbb{I} \quad \cdot : \mathbb{A}/\mathbb{I} \times \mathbb{A}/\mathbb{I} \longrightarrow \mathbb{A}/\mathbb{I}$$

$$(\bar{a}, \bar{b}) \longmapsto \overline{a+b} \quad e \quad (\bar{a}, \bar{b}) \longmapsto \overline{a \cdot b}.$$

O conjunto \mathbb{A}/\mathbb{I} munido das operações acima é um anel, o qual chamamos de anel quociente de \mathbb{A} por \mathbb{I} .

Definição 2.6 (Homomorfismo de anéis). *Sejam \mathbb{A} e \mathbb{A}' dois anéis. Uma função $f : \mathbb{A} \rightarrow \mathbb{A}'$ é chamada de homomorfismo de \mathbb{A} em \mathbb{A}' se satisfaz as seguintes condições:*

- i) $f(a + b) = f(a) + f(b) \quad \forall a, b \in \mathbb{A};$
- ii) $f(a \cdot b) = f(a) \cdot f(b) \quad \forall a, b \in \mathbb{A}.$

Neste contexto de homomorfismos, consideraremos a partir de agora os símbolos 0 e 1 como respectivamente os elementos neutro (da soma) e unidade relativos ao anel \mathbb{A} , e $0'$ e $1'$ como respectivamente os elementos neutro (da soma) e unidade relativos ao anel \mathbb{A}' .

Se \mathbb{A} e \mathbb{A}' são domínios de integridade e f é não nulo, então $f(1) = 1'$. Quando \mathbb{A} e \mathbb{A}' são anéis comutativos com unidade arbitrários, a condição $f(1) = 1'$ é exigida na definição de homomorfismo não nulo.

Exemplo 2.9. *Sejam \mathbb{A}, \mathbb{A}' anéis com unidade, e $f : \mathbb{A} \rightarrow \mathbb{A}'$ uma função definida por $f(a) = 0', \forall a \in \mathbb{A}$. Vejamos que f é um homomorfismo. Para isso, sejam $a, b \in \mathbb{A}$. Temos $f(a + b) = 0' = 0' + 0' = f(a) + f(b)$ e $f(a \cdot b) = 0' \cdot 0' = f(a) \cdot f(b)$.*

Quando um homomorfismo f de \mathbb{A} em \mathbb{A}' é bijetivo dizemos que f é um isomorfismo, e ainda que \mathbb{A} e \mathbb{A}' são isomorfos, denotando por $\mathbb{A} \simeq \mathbb{A}'$. Os homomorfismo f de \mathbb{A} em \mathbb{A} são chamados de endomorfismo e os isomorfismos de \mathbb{A} em \mathbb{A} são chamados de automorfismo. O conjunto dos endomorfismo e o dos isomorfismos são denotados respectivamente por $End(\mathbb{A})$ e $Aut(\mathbb{A})$. A definição de homomorfismo também se estende para corpos, e neste caso assumimos as mesmas formas de escrever e denotar estes homomorfismos, que as de anéis.

Vejamos agora dois resultados relativos aos homomorfismos de anéis.

Proposição 2.6. *Sejam \mathbb{A} e \mathbb{A}' anéis e $f : \mathbb{A} \rightarrow \mathbb{A}'$ um homomorfismo. Valem as seguintes afirmações,*

- i) $f(0) = 0';$
- ii) $f(-a) = -f(a) \quad \forall a \in \mathbb{A};$

iii) Se \mathbb{A} e \mathbb{A}' são domínios de integridade então ou f é a função constante zero ou $f(1) = 1'$;

iv) Se \mathbb{A} e \mathbb{A}' são corpos, então ou f é a função constante zero ou f é injetiva.

Prova:

i) Temos $0 = 0 + 0 \Rightarrow f(0) = f(0 + 0) = f(0) + f(0) \Rightarrow f(0) = 0'$;

ii) Seja $a \in \mathbb{A}$. Segue, $f(0) = f(a + (-a)) = f(a) + f(-a)$, ou seja $f(0) = f(a) + f(-a)$. Logo pelo item i), $f(a) + f(-a) = 0' \Rightarrow f(-a) = -f(a)$;

iii) Temos $f(1) = f(1 \cdot 1) = f(1) \cdot f(1) \Rightarrow 0' = f(1) \cdot f(1) + (-f(1)) = f(1)(f(1) + (-1))$. Como \mathbb{A}' é um domínio de integridade, temos que $f(1) = 0'$ ou $f(1) = 1'$. Se $f(1) = 0'$, então $f(a) = f(a \cdot 1) = f(a) \cdot f(1) = f(a) \cdot 0' = 0' \forall a \in \mathbb{A}$;

iv) Sejam \mathbb{A} e \mathbb{A}' corpos e suponhamos que f não é a função constante zero. Pelo item iii) temos que $f(1) = 1'$. Se $a, b \in \mathbb{A}$, e $f(a) = f(b)$ então $f(a - b) = 0'$. Suponhamos que $a \neq b \Rightarrow a - b \neq 0$. Uma vez que \mathbb{A} é um corpo, existe $c \in \mathbb{A}$ tal que $c \cdot (a - b) = 1$. Segue $f(c) \cdot f(a - b) = f(c) \cdot 0' = 1'$, o que é uma contradição. Logo se $a, b \in \mathbb{A}$, e $f(a) = f(b)$, então $a = b$, e portanto, f é injetiva. \square

A próxima proposição que apresentamos é conhecido na literatura como o primeiro teorema de homomorfismo, sendo um dos mais importantes resultados relativos aos homomorfismos de anéis.

Proposição 2.7. *Sejam \mathbb{A} e \mathbb{A}' anéis e $f : \mathbb{A} \rightarrow \mathbb{A}'$ um homomorfismo. Temos,*

i) $Imf = \{f(a); a \in \mathbb{A}\}$ é um subanel de \mathbb{A}' ;

ii) $N(f) = \{a \in \mathbb{A}; f(a) = 0'\}$ é um ideal de \mathbb{A} , e f é injetiva $\Leftrightarrow N(f) = \{0\}$;

iii) Os anéis $\mathbb{A}/N(f)$ e Imf são isomorfos.

Prova:

i) Utilizaremos a Proposição 2.5.

1) $0' = f(0) \in Imf$ pelo item i) da Proposição 2.6;

2) $f(a), f(b) \in Imf \Rightarrow f(a) + (-f(b)) = f(a - b) \in Imf$;

3) $f(a), f(b) \in Imf \Rightarrow f(a) \cdot f(b) = f(a \cdot b) \in Imf$.

ii) Mostraremos inicialmente que $N(f) = \{a \in \mathbb{A}; f(a) = 0'\}$ é um ideal de \mathbb{A} .

1) Novamente pelo item i) da Proposição 2.6 temos que $0 \in N(f)$, uma vez que $f(0) = 0'$;

2) $a, b \in N(f) \Rightarrow f(a-b) = f(a) + (-f(b)) = 0' + (-0') = 0'$, isto é, $a-b \in N(f)$;

3) $\forall a \in \mathbb{A}$ e $\forall b \in N(f)$, tem-se

$$f(a \cdot b) = f(a) \cdot f(b) = f(a) \cdot 0' = 0'$$

e

$$f(b \cdot a) = f(b) \cdot f(a) = 0' \cdot f(a) = 0',$$

isto nos diz que $a \cdot b \in N(f)$ e $b \cdot a \in N(f)$. Logo, por definição temos que $N(f)$ é um ideal de \mathbb{A} . Mais uma vez fizemos uso da Proposição 2.5. Para o que falta, notemos que se f for injetiva temos que $N(f) = \{0\}$, pois $f(0) = 0'$. Agora, se $a, b \in \mathbb{A}$, $f(a) = f(b)$ e $N(f) = \{0\}$, temos $f(a) + (-f(b)) = 0'$ ou seja, $f(a-b) = 0' \Rightarrow a-b \in N(f) = \{0\} \Rightarrow a=b$, e isso nos mostra que f é injetiva.

iii) Para provar este item, definiremos uma função F como abaixo,

$$\begin{aligned} F : \mathbb{A}/N(f) &\longrightarrow \text{Im}f \\ \bar{a} &\longmapsto f(a) \end{aligned}$$

mostraremos a mesma é bijetiva, e também um homomorfismo de anéis.

Notemos que dados $\bar{a}, \bar{b} \in \mathbb{A}/N(f)$ com $\bar{a} = \bar{b}$, segue $a-b \in N(f)$. Logo $f(a) = f(b)$. Isso nos assegura que F está bem definida, pois não depende da escolha de representantes.

A injetividade de F fica clara pelo item ii) desta própria proposição, ao observarmos que

$$N(F) = \{\bar{a} \in \mathbb{A}/N(f); F(\bar{a}) = f(a) = 0'\} = \{\bar{a} \in \mathbb{A}/N(f); a \in N(f)\} = \{\bar{0}\}.$$

Vejam agora que F é sobrejetiva:

$$\text{Im}F = \{F(\bar{a}); \bar{a} \in \mathbb{A}/N(f)\} = \{f(a); a \in \mathbb{A}\} = \text{Im}f,$$

isto é, o conjunto $\text{Im}F$ é igual ao contradomínio de F , ou seja, F é de fato sobrejetiva.

Por fim temos que F é um homomorfismo pois,

$$F(\bar{a} + \bar{b}) = F(\overline{a+b}) = f(a+b) \stackrel{1}{=} f(a) + f(b) = F(\bar{a}) + F(\bar{b}),$$

e

$$F(\bar{a} \cdot \bar{b}) = F(\overline{a \cdot b}) = f(a \cdot b) \stackrel{2}{=} f(a) \cdot f(b) = F(\bar{a}) \cdot F(\bar{b}).$$

As igualdades 1 e 2 nas equações acima decorrem do fato de f ser um homomorfismo. Portanto, F é um homomorfismo bijetivo, isto é, $\mathbb{A}/N(f) \simeq \text{Im}f$, como queríamos. \square

Faremos agora a construção de um corpo associado a um domínio de integridade. Esta construção nos possibilita, por exemplo, obtermos o conjunto dos números racionais a partir do conjunto dos números inteiros. Em geral, a partir de um domínio de integridade

qualquer, conseguimos estabelecer um corpo, o qual será denominado corpo de frações do domínio em questão.

Seja \mathbb{D} um domínio de integridade. Consideremos o conjunto $\mathbb{D}^\# = \mathbb{D} - \{0\}$. Definimos uma relação de equivalência no conjunto $A = \mathbb{D} \times \mathbb{D}^\# = \{(a, b); a \in \mathbb{D}, b \in \mathbb{D}^\#\}$ da seguinte forma: dados $(a, b), (c, d) \in A$, estes elementos estarão relacionados, o que indicaremos por $(a, b) \sim (c, d)$, se, e somente se, $a \cdot d = b \cdot c$ (escreveremos esta igualdade como $ad = bc$, entendendo que ocorre a operação produto).

Denotaremos por $\frac{a}{b}$ a classe de equivalência $\frac{a}{b} = \{(x, y) \in A; xb = ya\}$ e desta forma, $\frac{a}{b} = \frac{x}{y}$ se, e somente se, $xb = ya$ em \mathbb{D} . O símbolo A/\sim denotará o conjunto quociente, isto é,

$$A/\sim = \left\{ \frac{a}{b}, a \in \mathbb{D}, b \in \mathbb{D}^\# \right\}.$$

Definimos operações $+$ e \cdot em A/\sim como segue,

$$\frac{a}{b} + \frac{c}{d} = \frac{ad + bc}{bd} \quad e \quad \frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd},$$

as quais pode-se verificar que estão bem definidas pois não dependem da escolha dos representantes, e com estas operações, o conjunto quociente é um corpo, o qual chamamos de corpo de frações do domínio \mathbb{D} .

Consideremos o conjunto $\tilde{\mathbb{D}} = \left\{ \tilde{a} = \frac{a}{1}; a \in \mathbb{D} \right\} \subset A/\sim = \left\{ \frac{a}{b}, a \in \mathbb{D}, b \in \mathbb{D}^\# \right\}$. Sem muito trabalho podemos mostrar que $\tilde{\mathbb{D}}$ é um domínio de integridade sendo $\tilde{1}$ e $\tilde{0}$ seus elementos unidade e neutro, respectivamente. Além disso, é de fácil verificação que a função

$$\begin{aligned} \varphi : \mathbb{D} &\longrightarrow \tilde{\mathbb{D}} \\ a &\longmapsto \tilde{a} \end{aligned}$$

é um isomorfismo, ou seja, $\mathbb{D} \simeq \tilde{\mathbb{D}} \subset A/\sim$. Por esta razão dizemos que \mathbb{D} está imerso em $A/\sim = K_R(\mathbb{D})$, o corpo de frações de \mathbb{D} .

2.2.2 Anéis de polinômios

Neste tópicos discorreremos sobre um dos mais importantes exemplos de anel, os chamados anéis de polinômios.

Definição 2.7 (Polinômio). *Seja \mathbb{A} um anel e (a_0, a_1, a_2, \dots) uma sequência de elementos de \mathbb{A} ($a_i \in \mathbb{A}, \forall i \in \mathbb{N} \cup \{0\}$). Dizemos que a sequência (a_0, a_1, a_2, \dots) é um Polinômio sobre \mathbb{A} se existir um índice $k \in \mathbb{N} \cup \{0\}$ tal que $a_n = 0$ para todo $n > k$, e chamamos os elementos a_i de coeficientes do polinômio (a_0, a_1, a_2, \dots) . Em outras palavras, uma sequência de elementos de \mathbb{A} é um Polinômio quando apresenta um número finito de termos não nulos.*

O conjunto de todos os polinômios com coeficientes no anel \mathbb{A} é denotado pelo símbolo \mathcal{A} . Neste conjunto definimos as duas operações seguintes, respectivamente, adição e multiplicação,

$$\begin{aligned} + : \quad \mathcal{A} \times \mathcal{A} &\longrightarrow \mathcal{A} \\ ((a_0, a_1, a_2, \dots), (b_0, b_1, b_2, \dots)) &\longmapsto (c_0, c_1, c_2, \dots) \end{aligned}$$

sendo $c_i = a_i + b_i, \forall i \in \mathbb{N} \cup \{0\}$.

$$\begin{aligned} \cdot : \quad \mathcal{A} \times \mathcal{A} &\longrightarrow \mathcal{A} \\ ((a_0, a_1, a_2, \dots), (b_0, b_1, b_2, \dots)) &\longmapsto (d_0, d_1, d_2, \dots) \end{aligned}$$

onde $d_i = \sum_{\lambda+\mu=i} a_\lambda \cdot b_\mu, \forall i \in \mathbb{N} \cup \{0\}$.

Podemos mostrar que o conjunto \mathcal{A} munido das operações acima é um anel, com as mesmas características de \mathbb{A} , isto é: se \mathbb{A} é um anel com unidade ou comutativo ou um domínio de integridade então \mathcal{A} também o é. Algumas destas afirmações estão provadas em (BIAZZI, 2014).

Até agora, os anéis \mathbb{A} e \mathcal{A} são conjuntos cujos elementos possuem natureza distinta. Consideremos o conjunto $\mathbb{L} = \{(a, 0, 0, \dots, 0, 0, \dots); a \in \mathbb{A}\}$. É possível mostrar que \mathbb{L} é um subanel de \mathcal{A} , e mais ainda, que $\mathbb{L} \simeq \mathbb{A}$. A partir deste isomorfismo, identificamos cada elemento $a \in \mathbb{A}$ ao polinômio $(a, 0, 0, \dots, 0, 0, \dots) \in \mathbb{L}$, escrevendo $a = (a, 0, 0, \dots, 0, 0, \dots)$. Uma vez considerado esta identificação temos que $\mathbb{A} \subset \mathcal{A}$, e os elementos de \mathbb{A} passam a ser polinômios, chamados de polinômios constantes. Da multiplicação definida no anel \mathcal{A} e sendo este um anel com unidade temos que, se $a = (a, 0, 0, \dots) \in \mathbb{A}$ e $g = (b_0, b_1, b_2, \dots, b_n, 0, 0, \dots) \in \mathcal{A}$ então

$$a \cdot g = (a, 0, 0, \dots) \cdot (b_0, b_1, b_2, \dots, b_n, 0, 0, \dots) = (a \cdot b_0, a \cdot b_1, a \cdot b_2, a \cdot \dots, a \cdot b_n, 0, 0, \dots).$$

Seja $X = (0, 1, 0, 0, \dots, 0, \dots) \in \mathbb{L}$. Temos,

$$\begin{aligned} X^1 &= X = (0, 1, 0, 0, \dots, 0, \dots); \\ X^2 &= X \cdot X = (0, 0, 1, 0, \dots, 0, \dots); \\ X^3 &= X \cdot X \cdot X = (0, 0, 0, 1, \dots, 0, \dots); \\ &\vdots \end{aligned}$$

segundo assim, um argumento indutivo mostra que o polinômio X^n possui somente o coeficiente $a_n = 1$ não nulo. Ou seja, $X^n = (a_0, a_1, a_2, \dots, a_n, 0, \dots)$, onde $a_n = 1$ e $a_i = 0, \forall i \neq n$. Considerando o exposto até aqui, dado $f = (a_0, a_1, a_2, \dots, a_n, 0, 0, \dots) \in \mathcal{A}$, temos

$$\begin{aligned} f &= (a_0, 0, 0, \dots, 0, 0, 0, \dots) + (0, a_1, 0, \dots, 0, 0, 0, \dots) + (0, 0, a_2, \dots, 0, 0, 0, \dots) + \dots + \\ &+ (0, 0, 0, \dots, a_n, 0, 0, \dots) = a_0 + a_1 \cdot (0, 1, 0, \dots, 0, 0, 0, \dots) + a_2 \cdot (0, 0, 1, \dots, 0, 0, 0, \dots) = \\ &= a_0 + a_1 \cdot X + a_2 \cdot X^2 + \dots + a_n \cdot X^n \quad \therefore f = a_0 + a_1 \cdot X + a_2 \cdot X^2 + \dots + a_n \cdot X^n. \end{aligned}$$

Obtemos assim a notação usual dos polinômios, denotando o polinômio f por $f(X)$. Com esta notação, passamos a escrever os polinômios de \mathcal{A} como expressão do tipo $a_0 + a_1 \cdot X + a_2 \cdot X^2 + \dots + a_n \cdot X^n$, e então utilizamos o símbolo $\mathbb{A}[X]$ para denotar o conjunto destas expressões, ou seja, o conjunto dos polinômios $f(X)$ com coeficientes em \mathbb{A} . Por comodidade, escrevemos $f(X) = a_0 + a_1X + a_2X^2 + \dots + a_nX^n$, subentendendo a operação realizada em cada parcela de $f(X) = f$.

Com esta notação usual, as operações em $\mathcal{A}[X]$ se traduzem da seguinte forma. Dados $f(X) = \sum_{j=0}^n a_j X^j$ e $g(X) = \sum_{j=0}^m b_j X^j$ em $\mathbb{A}[X]$, a operação de adição correspondente a,

$$f(X) + g(X) = \sum_{j=0}^M d_j X^j,$$

onde $d_j = a_j + b_j$ para $0 \leq j \leq M = \max\{n, m\}$, enquanto a operação de multiplicação associada é dada como abaixo,

$$f(X) \cdot g(X) = \sum_{j=0}^{n+m} e_j X^j,$$

onde $e_j = \sum_{\lambda+\mu=j} a_\lambda \cdot c_\mu$, para $0 \leq j \leq n + m$.

Podemos definir polinômios sobre um anel \mathbb{A} em duas indeterminadas X e Y , construindo o anel $\mathbb{B}[Y]$ na indeterminada Y onde $\mathbb{B} = \mathbb{A}[X]$, denotando o conjunto destes polinômios por $\mathbb{A}[X, Y]$. Podemos ainda repetir iteradamente esta construção para obtermos os anéis $\mathbb{A}[X_1, X_2, \dots, X_m]$ dos polinômios em m indeterminadas X_1, X_2, \dots, X_m com coeficientes no anel \mathbb{A} .

Definição 2.8 (Grau de um polinômio na indeterminada X). *Seja $f(X) \in \mathbb{A}[X]$ um polinômio não nulo com coeficientes $a_0, a_1, a_2, \dots, a_n X^n$. O grau de $f(X)$, denotado por $\partial f(X) = \partial f$ ou $gr(f(X)) = gr(f)$, é número $n \in \mathbb{N} \cup \{0\}$ tal que $a_n \neq 0$ e $a_i = 0, \forall i > n$. O grau não é definido para o polinômio nulo.*

Nessas condições, dizemos que a_n é chamado coeficiente dominante, ou coeficiente líder de f , e quando este é igual a 1, dizemos que f é um polinômio mônico. Notemos que os polinômios de $\mathbb{A}[X]$ que possuem grau igual a zero são os polinômios constantes.

A proposição abaixo estabelece a relação existente entre o grau da soma e do produto de dois polinômios, e o grau dos polinômios envolvidos na operação considerada.

Proposição 2.8. *Sejam $f(X)$ e $g(X)$ polinômios não nulos pertencentes a $\mathbb{A}[X]$, sendo \mathbb{A} um domínio de integridade. Temos,*

- i) $f(X) + g(X) \neq 0 \Rightarrow \partial(f(X) + g(X)) \leq \max\{\partial f(X), \partial g(X)\};$
- ii) $\partial(f(X) \cdot g(X)) = \partial f(X) + \partial g(X).$

Prova:

i) Sejam n e m os graus de $f(X)$ e $g(X)$, respectivamente. Suponhamos sem perda de generalidade que $n > m$. Neste caso, o coeficiente dominante de $f(X) + g(X)$ é a_n , e então $\partial(f(X) + g(X)) = n = \max\{\partial f(X), \partial g(X)\}$. No caso em que $n = m$ temos que o coeficiente dominante de $f(X) + g(X)$ é $a_n + b_n$, e assim $\partial(f(X) + g(X)) = n$ se $a_n + b_n \neq 0$ e $\partial(f(X) + g(X)) < n$ se $a_n + b_n = 0$;

ii) Efetuado a multiplicação $f(X) \cdot g(X)$ temos que o coeficiente dominante é $c_{n+m} = \sum_{\lambda+\mu=n+m} a_\lambda \cdot b_\mu$. Como por definição para todo $i > n$ temos $a_i = 0$ e para todo $i > m$, temos $b_i = 0$, segue que $c_{n+m} = a_n \cdot b_m$. Logo $\partial(f(X) \cdot g(X)) = n+m = \partial f(X) + \partial g(X)$. \square

Observação 2.1. *Seja $f(X)$ um polinômio invertível pertencente a $\mathbb{A}[X]$. Logo, existe $g(X) \in \mathbb{A}[X], g(X) \neq 0$ tal que $f(X) \cdot g(X) = 1$. Pelo item ii) da proposição acima segue que $f(X) = a \neq 0$ é um polinômio constante ($a \in \mathbb{A}$ é invertível). Com isso fica claro que os elementos invertíveis em $\mathbb{A}[X]$ são exatamente os elementos invertíveis em \mathbb{A} . Vale notar que se \mathbb{A} não for um domínio de integridade esta última afirmação pode não ser verdadeira, por exemplo o polinômio $2X + 1 \in \mathbb{Z}_4[X]$ é invertível e coincide com seu inverso multiplicativo.*

A proposição a seguir é conhecida na literatura por *algoritmo da divisão*.

Proposição 2.9 (Algoritmo de Euclides). *Seja \mathbb{A} um anel. Se $f(X), g(X) \in \mathbb{A}[X]$, com $g(X) \neq 0$ e coeficiente líder invertível em \mathbb{A} , então, existem únicos $q(X), r(X) \in \mathbb{A}[X]$, tais que*

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

onde $r(X) = 0$ ou $\partial r(X) < \partial g(X)$.

Prova: Sejam $f(X) = a_0 + a_1X + a_2X^2 + \dots + a_nX^n$ e $g(X) = b_0 + b_1X + b_2X^2 + \dots + b_mX^m$, onde $\partial f = n$ e $\partial g = m$.

Provaremos primeiro a existência. Se $f(X) = 0$, tomamos $q(X) = r(X) = 0$. Analisemos o caso em que $f(X) \neq 0$. Podemos assumir que $n \geq m$, pois se $n < m$ tomamos $q(X) = 0$ e $r(X) = f(X)$.

Consideremos o polinômio $f_1(X) = f(X) - a_n b_m^{-1} X^{n-m} g(X)$. Vejamos que o polinômio $a_n b_m^{-1} X^{n-m} g(X)$ tem coeficiente líder a_n e grau n , logo $\partial f_1(X) = 0$ ou $\partial f_1(X) < \partial f(X)$. Faremos indução sobre o grau de $f(X)$. Se $n = 0$ e $n \geq m$ então $m = 0$ e $f_1(X) = 0$, logo $f(X) = a_0 b_0^{-1} g(X)$, com $q(X) = a_0 b_0^{-1}$ e $r(X) = 0$. Por outro lado, se $n > 0$ e $f_1(X) \neq 0$, pela hipótese de indução existem $q_1(X), r_1(X)$ tais que

$$f_1(X) = q_1(X)g(X) + r_1(X)$$

onde $r_1(X) = 0$ ou $\partial r_1(X) < \partial g(X)$. Com isso temos

$$f(X) = (q_1(X) + a_n b_m^{-1} X^{n-m})g(X) + r_1(X).$$

Tomemos $q(X) = q_1(X) + a_n b_m^{-1} X^{n-m}$ e $r(X) = r_1(X)$. Portanto existem $q(X), r(X) \in \mathbb{A}[X]$, tais que $f(X) = q(X)g(X) + r(X)$, onde $r(X) = 0$ ou $\partial r(X) < \partial g(X)$.

Para prova da unicidade sejam $q_1(X), q_2(X), r_1(X)$ e $r_2(X)$ pertencentes a $\mathbb{A}[X]$ tais que

$$f(X) = q_1(X)g(X) + r_1(X) = q_2(X)g(X) + r_2(X),$$

onde $r_i(X) = 0$ ou $\partial r_i(X) < \partial g(X), i \in \{1, 2\}$. Da igualdade acima temos

$$(q_1(X) - q_2(X))g(X) = r_2(X) - r_1(X).$$

Observemos que se $q_1(X) \neq q_2(X)$ temos que o grau do polinômio $(q_1(X) - q_2(X))g(X)$ é maior que ou igual ao grau de $g(X)$, enquanto o grau de $r_2(X) - r_1(X)$ é menor que o grau de $g(X)$, sendo a última igualdade uma clara contradição. Logo $q_1(X) = q_2(X)$, o que implica em $r_1(X) = r_2(X)$. Portanto, os polinômios $g(X)$ e $r(X)$ são únicos. \square

Quando $r(X) = 0$ na proposição acima, dizemos que o polinômio $g(X)$ divide o polinômio $f(X)$, e denotamos isso por $g(X) \mid f(X)$. O conjunto dos múltiplos de $g(X)$ é denotado por $g\mathbb{A}[X]$, em outras palavras $g\mathbb{A}[X] = \{h(X)g(X); h(X) \in \mathbb{A}[X]\}$.

Sejam \mathbb{B} um subanel de um anel \mathbb{A} , $f(X) = a_0 + a_1X + a_2X^2 + \dots + a_nX^n \in \mathbb{B}[X]$ e $\alpha \in \mathbb{A}$. A expressão $a_0 + a_1\alpha + a_2\alpha^2 + \dots + a_n\alpha^n \in \mathbb{A}$ é denotada por $f(\alpha)$, e chamada de avaliação do polinômio $f(X)$ em α . Quando $f(\alpha) = a_0 + a_1\alpha + a_2\alpha^2 + \dots + a_n\alpha^n = 0$ dizemos que α é raiz de $f(X)$. A proposição a seguir é conhecida como teste da raiz.

Proposição 2.10. *Seja $f(X) \in \mathbb{A}[X] - \{0\}$. Vale a seguinte afirmação: α é raiz de $f(X)$ se, e somente se, $g(X) = X - \alpha$ divide $f(X)$. Isto é, $f(\alpha) = 0 \Leftrightarrow g(X) \mid f(X)$.*

Prova:

[\Rightarrow] Pela Proposição 2.9 temos que existem $q(X), r(X) \in \mathbb{A}[X]$, tais que

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

onde $r(X) = 0$ ou $\partial r(X) < \partial g(X) = 1$. Logo $r(X) = 0$ ou $\partial r(X) = 0$. Em qualquer caso $r(X) = r \in \mathbb{A}$. Logo $f(X) = q(X)g(X) + r$ com, $r \in \mathbb{A}$. Com isso temos

$$0 = f(\alpha) = q(\alpha)g(\alpha) + r = r$$

pois $g(\alpha) = 0$. Daí $f(X) = q(X)g(X)$, ou seja, $g(X) \mid f(X)$.

[\Leftarrow] Se $g(X) \mid f(X)$ então existe $q(X) \in \mathbb{A}[X]$ tal que $f(X) = q(X)g(X)$. Logo, $f(\alpha) = q(\alpha)g(\alpha) = 0$ uma vez que $g(\alpha) = 0$. Portanto α é raiz de $f(X)$. \square

Definição 2.9. *Sejam $f(X), g(X) \in \mathbb{K}[X] - \{0\}$, sendo \mathbb{K} corpo. O máximo divisor comum de $f(X)$ e $g(X)$ é o polinômio mônico $d(X) \in \mathbb{K}[X] - \{0\}$, denotado por $d(X) = \text{MDC}(f(X), g(X))$, que satisfaz as duas propriedades abaixo:*

i) $d(X)$ divide $f(X)$ e $g(X)$, isto é, $d(X) \mid f(X), g(X)$;

ii) Se $d'(X) \in \mathbb{K}[X] - \{0\}$ divide $f(X)$ e $g(X)$, então $d'(X) \mid d(X)$.

Dizemos que os polinômios $f(X), g(X) \in \mathbb{K}[X] - \{0\}$ são relativamente primos, ou primos entre si, quando $MDC(f(X), g(X)) = 1$. A proposição a seguir garante a existência do MDC.

Proposição 2.11. *Dados $f(X), g(X) \in \mathbb{K}[X] - \{0\}$ onde \mathbb{K} é corpo, se*

$$S = \{a(X)f(X) + b(X)g(X); a(X), b(X) \in \mathbb{K}[X]\},$$

então existe um único polinômio mônico $d(X) \in \mathbb{K}[X] - \{0\}$ tal que,

i) $S = d\mathbb{K}[X]$, sendo que $d(X) \mid f(X), g(X)$;

ii) Se $d'(X) \in \mathbb{K}[X] - \{0\}$ divide $f(X)$ e $g(X)$, então $d'(X) \mid d(X)$.

Prova:

i) Se $d(X) \in S - \{0\}$ mônico de modo que

$$\partial d(X) = \min\{\partial h(X); h(X) \in S - \{0\}\},$$

temos que $S = d\mathbb{K}[X]$, pois, sendo $d(X) = a_0(X)f(X) + b_0(X)g(X)$ onde $a_0(X), b_0(X) \in \mathbb{K}[X]$, e $c(X) \in \mathbb{K}[X]$, então,

$$c(X)d(X) = (c(X)a_0(X))f(X) + (c(X)b_0(X))g(X) \in S,$$

ou seja, $d\mathbb{K}[X] \subset S$. Por outro lado, seja $h(X) = a(X)f(X) + b(X)g(X) \in S$ onde $a(X), b(X) \in \mathbb{K}[X]$, pelo Algoritmo de Euclides (Proposição 2.9) existem $q(X), r(X) \in \mathbb{K}[X]$, tais que

$$h(X) = q(X)d(X) + r(X),$$

onde $r(X) = 0$ ou $\partial r(X) < \partial d(X)$. Mas se $r(X) \neq 0$, então $\partial r(X) < \partial d(X)$ e além disso

$$\begin{aligned} r(X) &= h(X) - q(X)d(X) = \\ &= (a(X)f(X) + b(X)g(X)) - (a_0(X)f(X) + b_0(X)g(X))q(X) = \\ &= (a(X) - a_0(X)q(X))f(X) + (b(X) - b_0(X)q(X))g(X) \in S, \end{aligned}$$

o que contradiz o fato de $\partial d(X) = \min\{\partial h(X); h(X) \in S - \{0\}\}$. Logo $r(X) = 0$ e então $h(X) = q(X)d(X) \in d\mathbb{K}[X]$, ou seja $S \subset d\mathbb{K}[X]$ e assim $S = d\mathbb{K}[X]$. Para o que falta acerca do item i), percebamos que tomando $a(X) = 1$ e $b(X) = 0$ temos claramente que $f(X) \in S = d\mathbb{K}[X]$, e tomando $a(X) = 0$ e $b(X) = 1$ temos $g(X) \in S = d\mathbb{K}[X]$, e assim $d(X) \mid f(X), g(X)$.

ii) Se $d'(X) \in \mathbb{K}[X] - \{0\}$ divide $f(X)$ e $g(X)$, então $f(X) = d'(X)f'(X)$ e $g(X) = d'(X)g'(X)$, onde $f'(X), g'(X) \in \mathbb{K}[X]$.

Seja $h(X) = a(X)f(X) + b(X)g(X) \in S$, $a(X), b(X) \in \mathbb{K}[X]$, temos

$$h(X) = a(X)f(X) + b(X)g(X) = (a(X)f'(X) + b(X)g'(X))d'(X) \in d'\mathbb{K}[X].$$

o que mostra $d(X) \in S = d\mathbb{K}[X] \subset d'\mathbb{K}[X]$. Logo $d(X) = c(X)d'(X)$, com $c(X) \in \mathbb{K}[X]$, ou seja, $d'(X) \mid d(X)$, como queríamos.

Para provar a unicidade de $d(X)$, suponhamos que exista um polinômio mônico $d_1(X)$ satisfazendo as condições i) e ii) assim como $d(X)$. Pelo item ii) segue que $d(X) \mid d_1(X)$ e $d_1(X) \mid d(X)$, daí $d(X) = h_1(X)d_1(X)$ e $d_1(X) = g_1(X)d(X)$, com $h_1(X), g_1(X) \in \mathbb{K}[X]$. Destas duas últimas igualdades temos $\partial d_1(X) \leq \partial d(X)$ e $\partial d(X) \leq \partial d_1(X)$, logo $\partial d_1(X) = \partial d(X)$. Daí $h_1(X), g_1(X)$ são constantes, isto é, $h_1(X), g_1(X) \in \mathbb{K}$. \square

Observação 2.2. Se $f(X), g(X) \in \mathbb{K}[X] - \{0\}$ são tais que $MDC(f(X), g(X)) = 1$ (relativamente primos), então, pela proposição anterior segue que existem $a(X), b(X) \in \mathbb{K}[X]$ tais que $a(X)f(X) + b(X)g(X) = 1$. Ainda, se $d(X) = MDC(f(X), g(X))$ e existem $a(X), b(X) \in \mathbb{K}[X]$ tais que $a(X)f(X) + b(X)g(X) = 1$, novamente pela proposição anterior temos que $1 \in d\mathbb{K}[X]$, ou seja, $d(X) \mid 1$. Uma vez que $d(X) = MDC(f(X), g(X))$ é unitário, temos que $d(X) = 1$.

Seja \mathbb{D} um domínio de integridade. Dados $a, b \in \mathbb{D}$ com $a \neq 0$, dizemos que a divide b e denotamos por $a \mid b$ se existir um elemento $c \in \mathbb{D}$ tal que $b = ac$.

Vejamos agora a definição de Máximo Divisor Comum de um subconjunto de elementos de um domínio. Sejam $a_1, a_2, \dots, a_m \in \mathbb{D}$. Dizemos que $d \in \mathbb{D}$ é o máximo divisor comum dos elementos $a_1, a_2, \dots, a_m \in \mathbb{D}$, e o denotamos por $d = MDC(a_1, a_2, \dots, a_m)$, se d divide cada um destes elementos e ainda, se $d' \in \mathbb{D}$ também dividir cada um destes elementos, então d' divide d .

Para a proposição que segue, utilizaremos a definição de domínio fatorial. Indicamos a obra (GARCIA E LEQUAIN, 2001) para consulta acerca desta definição e de mais informações sobre a teoria dos anéis.

A proposição abaixo estabelece um critério de pesquisa de raízes de $f(X)$ (com coeficientes em $\mathbb{D}[X] - \mathbb{D}$, onde \mathbb{D} é um domínio fatorial), pertencentes ao corpo de frações \mathbb{K} de \mathbb{D} . Vejamos.

Proposição 2.12. Sejam \mathbb{D} um domínio de integridade, \mathbb{K} o seu corpo de frações e $f(X) = a_0 + a_1X + a_2X^2 + \dots + a_nX^n \in \mathbb{D}[X] - \mathbb{D}$. Se $\alpha = \frac{r}{s} \in \mathbb{K}$ é uma raiz de $f(X)$ em $\mathbb{K}[X]$ e $MDC(r, s) = 1$, então $r \mid a_0$ e $s \mid a_n$.

Prova: Como $\alpha = \frac{r}{s} \in \mathbb{K}$ é raiz de $f(X)$ temos que,

$$0 = f\left(\frac{r}{s}\right) = a_0 + a_1\left(\frac{r}{s}\right) + a_2\left(\frac{r}{s}\right)^2 + \dots + a_{n-1}\left(\frac{r}{s}\right)^{n-1} + a_n\left(\frac{r}{s}\right)^n.$$

Desta igualdade obtemos, multiplicando-a por s^n ,

$$0 = a_0s^n + a_1rs^{n-1} + a_2r^2s^{n-2} + \dots + a_{n-1}r^{n-1}s + a_nr^n, \quad (2.5)$$

que implica em

$$-(a_0s^n + a_1rs^{n-1} + a_2r^2s^{n-2} + \dots + a_{n-1}r^{n-1}s) = a_nr^n.$$

Observemos que s divide o lado esquerdo da igualdade acima, logo $s \mid a_nr^n$. Como $MDC(r, s) = 1$ temos $MDC(r^n, s) = 1$, e isso nos mostra que $s \mid a_n$. De modo análogo, de (2.5) temos

$$-(a_1rs^{n-1} + a_2r^2s^{n-2} + \dots + a_{n-1}r^{n-1}s + a_nr^n) = a_0s^n,$$

onde r divide o lado esquerdo, e conseqüentemente divide a_0s^n , e então, uma vez que $MDC(r, s) = 1$ temos $MDC(r, s^n) = 1$ e daí $r \mid a_0$. \square

Definição 2.10. *Seja $f(X) \in \mathbb{K}[X] - \mathbb{K}$. Dizemos que $f(X)$ é irredutível em $\mathbb{K}[X]$ se ao escrevermos $f(X)$ como $f(X) = g(X)h(X)$, com $g(X), h(X) \in \mathbb{K}[X]$, necessariamente tenhamos $g(X)$ ou $h(X)$ constante. Ou seja,*

$$f(X) = g(X)h(X), \quad g(X), h(X) \in \mathbb{K}[X] \quad \Rightarrow \quad g(X) \in \mathbb{K} \quad \text{ou} \quad h(X) \in \mathbb{K}.$$

Caso contrário, dizemos que $f(X)$ é redutível em $\mathbb{K}[X]$.

Com esta definição finalizamos este tópico, que já possui grande parte de toda a teoria que necessitaremos mais adiante.

2.2.3 Extensões de corpos

Discutiremos a seguir um pouco mais sobre algumas definições e resultados da álgebra, que serão fundamentais para nossos objetivos.

Sejam \mathbb{K} corpo e \mathbb{F} um subcorpo de \mathbb{K} . Neste contexto dizemos que \mathbb{K} é uma extensão de \mathbb{F} , e escrevemos $\mathbb{K} \mid \mathbb{F}$ ou,

$$\begin{array}{c} \mathbb{K} \\ | \\ \mathbb{F} \end{array}$$

Temos que

$$\mathbb{R} \mid \mathbb{Q}, \quad \mathbb{C} \mid \mathbb{R}, \quad \mathbb{C} \mid \mathbb{Q},$$

são exemplos de extensões de corpos.

Dada uma extensão $\mathbb{K} \mid \mathbb{F}$, dizemos que um elemento $\alpha \in \mathbb{K}$ é algébrico sobre \mathbb{F} se existir um polinômio $f(X) \in \mathbb{F}[X] - \{0\}$ tal que $f(\alpha) = 0$, isto é, α é uma raiz de

$f(X) \in \mathbb{F}[X] - \{0\}$. Um elemento $\alpha \in \mathbb{K}$ que não é algébrico sobre \mathbb{F} é dito transcendente sobre \mathbb{F} . Se todo $\alpha \in \mathbb{K}$ for algébrico sobre \mathbb{F} dizemos que a extensão $\mathbb{K} | \mathbb{F}$ é algébrica. Se $\alpha \in \mathbb{K}$ for algébrico sobre \mathbb{F} , o polinômio mônico e de menor grau com coeficientes em \mathbb{F} que se anula em α é dito polinômio mínimo, ou polinômio minimal de α sobre \mathbb{F} .

Quando estamos no contexto dos números reais como extensão dos racionais, convencionou-se chamar os elementos reais transcendentos sobre \mathbb{Q} apenas como números transcendentos. Do mesmo modo os elementos algébricos sobre \mathbb{Q} são chamados de números algébricos.

Proposição 2.13. *Sejam $\mathbb{K} | \mathbb{F}$ uma extensão de corpos e $\alpha \in \mathbb{K}$. Se $p(X) \in \mathbb{F}[X]$ mônico é tal que $p(\alpha) = 0$, então as afirmações abaixo são equivalentes:*

- i) $p(X)$ é o polinômio minimal de α sobre \mathbb{F} ;
- ii) se $q(X) \in \mathbb{F}[X]$ é tal que $q(\alpha) = 0$, então $p(X) | q(X)$;
- iii) $p(X)$ é irredutível.

Prova:

i) \Rightarrow ii) Seja $p(X)$ o polinômio minimal de α sobre \mathbb{F} , e $q(X) \in \mathbb{F}[X]$ tal que $q(\alpha) = 0$. Pela Algoritmo de Euclides (Proposição 2.9) existem $g(X), r(X) \in \mathbb{F}[X]$ tais que

$$q(X) = g(X)p(X) + r(X),$$

com $r(X) = 0$ ou $\partial r(X) < \partial p(X)$. Daí segue,

$$0 = q(\alpha) = g(\alpha)p(\alpha) + r(\alpha) \Rightarrow r(\alpha) = 0.$$

O que implica em $r(X) = 0$ pois $p(X)$ é um polinômio de menor grau tal que α é raiz. Logo $p(X) | q(X)$.

ii) \Rightarrow iii) Sejam $f(X), g(X) \in \mathbb{F}[X]$ tais que $p(X) | f(X)g(X)$. Logo, existe $h(X) \in \mathbb{F}[X]$ tal que $f(X)g(X) = p(X)h(X)$. Daí

$$f(\alpha)g(\alpha) = p(\alpha)h(\alpha) = 0 \therefore f(\alpha)g(\alpha) = 0,$$

e uma vez que \mathbb{K} é um corpo segue $f(\alpha) = 0$ ou $g(\alpha) = 0$, implicando no fato de $p(X)$ dividir $f(X)$ ou $g(X)$. Provamos até aqui que se $p(X)$ divide o produto $f(X)g(X)$ de dois polinômios, então divide um dos fatores, $f(X)$ ou $g(X)$. Escrevamos $p(X) = f_1(X)g_1(X) \in \mathbb{F}[X]$ não nulos. Com esta escrita de $p(X)$ temos que o mesmo divide o produto $f_1(X)g_1(X)$ pois $f_1(X)g_1(X) = p(X)h_1(X)$ onde $h_1(X) = 1 \in \mathbb{F}[X]$, e pelo que mostramos a pouco, temos $p(X) | f_1(X)$ ou $p(X) | g_1(X)$. Suponhamos sem perda de generalidade que $p(X) | f_1(X)$. Logo, $f_1(X) = p(X)s(X)$ para algum $s(X) \in \mathbb{F}[X]$ e

$$p(X) = f_1(X)g_1(X) = p(X)s(X)g_1(X) \Rightarrow p(X)(1 - s(X)g_1(X)) = 0,$$

o que nos fornece $1 = s(X)g_1(X)$, uma vez que \mathbb{F} é corpo e $p(X) \neq 0$. Logo, da Observação 2.1 temos $0 \neq g_1(X) \in \mathbb{F}$, ou seja, $g_1(X)$ é constante, e portanto $p(X)$ é irredutível.

iii) \Rightarrow i) Seja $f(X)$ um polinômio minimal de α sobre \mathbb{F} , e $p(X) \in \mathbb{F}[X]$ mônico, irredutível e tal que $p(\alpha) = 0$. Temos que $f(X) \mid p(X)$ pela implicação i) \Rightarrow ii) que já provamos, logo existe $q(X) \in \mathbb{F}$ tal que $p(X) = q(X)f(X)$. Como $p(X)$ é irredutível e $f(X)$ não é constante uma vez que é polinômio minimal, temos que $q(X) \in \mathbb{F}$. Para finalizar, sendo $p(X)$ e $f(X)$ ambos mônicos, nos resta uma única possibilidade para $q(X)$, temos $q(X) = 1$, e assim concluímos que $p(X) = f(X)$. \square

Pela implicação **iii) \Rightarrow i)** da proposição acima temos claramente que o polinômio minimal de um elemento $\alpha \in \mathbb{K}$ sobre o corpo \mathbb{F} é único.

Consideremos a extensão de corpos $\mathbb{K} \mid \mathbb{F}$. Dado $\alpha \in \mathbb{K}$, denotamos por $\mathbb{F}[\alpha]$ o menor subanel ² de \mathbb{K} que contém $\mathbb{F} \cup \{\alpha\}$.

Proposição 2.14. *Se $\Psi : \mathbb{F}[X] \rightarrow \mathbb{K}$ é definida por $\Psi(f(X)) = f(\alpha)$, então Ψ é um homomorfismo tal que:*

- i) $Im\Psi = \mathbb{F}[\alpha]$, $\mathbb{F} \subset \mathbb{F}[\alpha] \subset \mathbb{K}$;
- ii) α é transcendente sobre \mathbb{F} se, e somente se, $N(\Psi) = \{0\}$;
- iii) $\mathbb{F}[X]/N(\Psi) \simeq \mathbb{F}[\alpha]$.

Prova: Mostraremos inicialmente que Ψ é de fato um homomorfismo. Para tanto, sejam $f(X) = \sum_{j=0}^n a_j X^j$ e $g(X) = \sum_{j=0}^n b_j X^j$ em $\mathbb{F}[X]$, onde $n = \max\{\partial f(X), \partial g(X)\}$.

Temos $f(X) + g(X) = \sum_{j=0}^n (a_j + b_j) X^j$. Daí segue

$$\Psi(f(X) + g(X)) = \sum_{j=0}^n (a_j + b_j) \alpha^j = \sum_{j=0}^n a_j \alpha^j + \sum_{j=0}^n b_j \alpha^j = \Psi(f(X)) + \Psi(g(X)).$$

Por indução podemos facilmente mostrar que para todo $m \in \mathbb{N}$ temos

$$\Psi\left(\sum_{k=0}^m f_k(X)\right) = \sum_{k=0}^m \Psi(f_k(X)). \quad (2.6)$$

Veremos agora que $\Psi(f(X) \cdot g(X)) = \Psi(f(X)) \cdot \Psi(g(X))$. A igualdade (2.6) nos assegura que

$$\Psi(f(X) \cdot g(X)) = \Psi\left(\sum_{j=0}^n a_j X^j g(X)\right) = \sum_{j=0}^n \Psi(a_j X^j g(X)). \quad (2.7)$$

² Isso significa que se \mathbb{L} é um subanel de \mathbb{K} que também contém \mathbb{F} e α , então $\mathbb{F}[\alpha] \subset \mathbb{L}$.

Notemos que para cada $j \in \{0, 1, \dots, n\}$ vale

$$\Psi(a_j X^j g(X)) = \Psi\left(a_j X^j \sum_{l=0}^n b_l X^l\right) \quad (2.8)$$

$$= \Psi\left(\sum_{l=0}^n a_j b_l X^{l+j}\right) \quad (2.9)$$

$$= \sum_{l=0}^n a_j b_l \alpha^{l+j} \quad (2.10)$$

$$= a_j \alpha^j \sum_{l=0}^n b_l \alpha^l = a_j \alpha^j \Psi(g(X)). \quad (2.11)$$

Agora, as equações (2.7) e (2.11) nos dão

$$\Psi(f(X) \cdot g(X)) = \sum_{j=0}^n a_j \alpha^j \Psi(g(X)) = \Psi(f(X)) \cdot \Psi(g(X)).$$

i) Como $\mathbb{F}[\alpha]$ é o menor subanel de \mathbb{K} que contém \mathbb{F} e α , temos que também contém as potências de α e assim todas as expressões do tipo $f(\alpha) = \Psi(f(X))$ onde $f(X) \in \mathbb{F}[X]$. Isso mostra que $Im\Psi \subset \mathbb{F}[\alpha]$.

Por outro lado, dado $\beta \in \mathbb{F}[\alpha]$ temos que $\beta \in Im\Psi$. De fato, se $\beta \in \mathbb{F}[\alpha]$ então é uma expressão do tipo $a_0 + a_1(\alpha) + a_2(\alpha)^2 + \dots + a_n(\alpha)^n = f(\alpha)$, onde $a_0, a_1, a_2, \dots, a_n \in \mathbb{F}$. Notemos que se $\beta \in \mathbb{F}$, então na expressão $a_0 + a_1(\alpha) + a_2(\alpha)^2 + \dots + a_n(\alpha)^n = f(\alpha)$ teremos $a_0 = \beta$ e $a_i = 0 \forall i \geq 1$. Logo $Im\Psi \supset \mathbb{F}[\alpha]$. Portanto, $Im\Psi = \mathbb{F}[\alpha]$, e claramente $\mathbb{F} \subset \mathbb{F}[\alpha] \subset \mathbb{K}$, como queríamos.

ii) Se α é transcendente sobre \mathbb{F} , então o único polinômio $g(X) \in \mathbb{F}[X]$ tal que $g(\alpha) = 0$ é o polinômio nulo. Logo o único elemento de $\mathbb{F}[X]$ tal que sua imagem por Ψ seja zero é o polinômio nulo, isto é, $N(\Psi) = \{0\}$. Reciprocamente, se $N(\Psi) = \{0\}$, então $\forall f(X) \in \mathbb{F}[X] - \{0\}$ temos

$$0 \neq \Psi(f(X)) = f(\alpha).$$

Logo, $\forall f(X) \in \mathbb{F}[X] - \{0\}$ temos $f(\alpha) \neq 0$, e portanto α é transcendente sobre \mathbb{F} .

iii) Como pelo item i) desta proposição temos que $Im\Psi = \mathbb{F}[\alpha]$, segue do item iii) da Proposição 2.7 que $\mathbb{F}[X]/N(\Psi) \simeq \mathbb{F}[\alpha]$. \square

Observação 2.3. Vale atentar para o fato de que se α é transcendente sobre \mathbb{F} , então os itens **ii)** e **iii)** da proposição acima nos fornecem o isomorfismo $\mathbb{F}[X] \simeq \mathbb{F}[\alpha]$.

Definição 2.11. Sejam $\mathbb{K} | \mathbb{F}$ uma extensão de corpos e $\alpha \in \mathbb{K}$. Chamamos de adjunção de α a \mathbb{F} , e o denotamos por $\mathbb{F}(\alpha)$, o menor subcorpo³ de \mathbb{K} que contém $\mathbb{F} \cup \{\alpha\}$.

Esta definição nos possibilita obtermos corpos intermediários entre \mathbb{K} e \mathbb{F} , uma vez que $\mathbb{F} \subset \mathbb{F}(\alpha) \subset \mathbb{K}$, com $\alpha \in \mathbb{F}(\alpha)$. A adjunção de α a \mathbb{F} é única. Para mostrar isso basta notar que se $\mathbb{F}_1(\alpha)$ é uma outra adjunção de α a \mathbb{F} , então

³ $\mathbb{F}(\alpha)$ é um subcorpo de \mathbb{K} tal que se \mathbb{L} também é um subcorpo de \mathbb{K} contendo \mathbb{F} e α , então $\mathbb{F}(\alpha) \subset \mathbb{L}$.

$$\mathbb{F}(\alpha) \subset \mathbb{F}_1(\alpha) \quad \text{e} \quad \mathbb{F}_1(\alpha) \subset \mathbb{F}(\alpha),$$

logo $\mathbb{F}(\alpha) = \mathbb{F}_1(\alpha)$.

Sem muito trabalho podemos mostrar que o conjunto,

$$\left\{ \frac{f(\alpha)}{g(\alpha)}; f(X), g(X) \in \mathbb{F}[X], \text{ com } g(\alpha) \neq 0 \right\}$$

é um corpo. E como todo subcorpo de \mathbb{K} que contém $\mathbb{F} \cup \{\alpha\}$ deve conter necessariamente este conjunto, temos que

$$F(\alpha) = \left\{ \frac{f(\alpha)}{g(\alpha)}; f(X), g(X) \in \mathbb{F}[X], \text{ com } g(\alpha) \neq 0 \right\}.$$

Para os próximos resultados sobre os quais discutimos, necessitamos considerar definições e resultados próprios da Álgebra Linear. Optamos por não apresentá-los aqui para não sobrecarregar o texto, mas indicamos as obras (BOLDRINI, 1980), (HEFEZ e FERNANDEZ, 2016) e (LIMA, 2005) para possíveis consultas.

Considerando a extensão de corpos $\mathbb{K} | \mathbb{F}$ e recordando a definição de espaço vetorial, notamos que o corpo \mathbb{K} é um espaço vetorial sobre o corpo de escalares \mathbb{F} . Chamamos de grau da extensão $\mathbb{K} | \mathbb{F}$, e denotamos por $[\mathbb{K} : \mathbb{F}]$, a dimensão do espaço do espaço vetorial \mathbb{K} sobre \mathbb{F} . Se o espaço vetorial \mathbb{K} sobre \mathbb{F} for finito, dizemos que a extensão $\mathbb{K} | \mathbb{F}$ é finita e denotamos isso por $[\mathbb{K} : \mathbb{F}] < \infty$.

A proposição que apresentamos a seguir é de fundamental importância para este texto.

Proposição 2.15. *Sejam $\mathbb{K} | \mathbb{F}$ uma extensão de corpos e $\alpha \in \mathbb{K}$ algébrico sobre \mathbb{F} . Se n é o grau do polinômio minimal de α sobre \mathbb{F} , então $[\mathbb{F}(\alpha) : \mathbb{F}] = n$ e $\{1, \alpha, \alpha^2, \dots, \alpha^{n-1}\}$ é uma base de $\mathbb{F}(\alpha)$ sobre \mathbb{F} .*

Prova: Vamos mostrar inicialmente que todo elemento de $\mathbb{F}(\alpha)$ pode ser escrito como combinação linear dos elementos $1, \alpha, \alpha^2, \dots, \alpha^{n-1}$, isto é, mostraremos que o conjunto $\{1, \alpha, \alpha^2, \dots, \alpha^{n-1}\}$ gera o espaço vetorial $\mathbb{F}(\alpha)$ sobre \mathbb{F} . Para tanto, dado $\beta \in \mathbb{F}(\alpha)$ temos que existem $f(X), g(X) \in \mathbb{F}[X]$ tais que $\beta = \frac{f(\alpha)}{g(\alpha)}$ com $g(\alpha) \neq 0$. Consideremos que $p(X)$ seja o polinômio minimal de α sobre \mathbb{F} . Notemos que se $p(X) | g(X)$, então $g(X) = p(X)h(X)$ para algum $h(X) \in \mathbb{F}$, e daí segue $g(\alpha) = p(\alpha)h(\alpha) = 0$ pois $p(\alpha) = 0$, todavia sabemos que $g(\alpha) \neq 0$. Logo $p(X)$ não divide $g(X)$. Como pela Proposição 2.13 sabemos que $p(X)$ é irredutível, e uma vez que $p(X)$ não divide $g(X)$, temos $MDC(g(X), p(X)) = 1$. Segue da Observação 2.2, que existem $a(X), b(X) \in \mathbb{F}[X]$ tais que

$$a(X)g(X) + b(X)p(X) = 1,$$

que nos fornece

$$a(\alpha)g(\alpha) + b(\alpha)p(\alpha) = 1,$$

e então $a(\alpha)g(\alpha) = 1 \quad \therefore \quad a(\alpha) = \frac{1}{g(\alpha)}$, e assim ficamos com $\beta = \frac{f(\alpha)}{g(\alpha)} = a(\alpha)f(\alpha)$. Agora, pelo Algoritmo de Euclides (Proposição 2.9) existem $q(X), r(X) \in \mathbb{F}[X]$ tais que

$$a(X)f(X) = q(X)p(X) + r(X),$$

com $r(X) = 0$ ou $\partial r(X) < \partial p(X) = n$. Daí segue,

$$\beta = a(\alpha)f(\alpha) = q(\alpha)p(\alpha) + r(\alpha) = r(\alpha) \quad \therefore \quad \beta = r(\alpha).$$

Como $r(X) \in \mathbb{F}[X]$ temos que existem $b_0, b_1, \dots, b_{n-1} \in \mathbb{F}$ tais que $r(X) = b_0 + b_1X + \dots + b_{n-1}X^{n-1}$, uma vez que $\partial r(X) < n$. Logo, $\beta = b_0 + b_1\alpha + \dots + b_{n-1}\alpha^{n-1}$, mostrando que $\{1, \alpha, \alpha^2, \dots, \alpha^{n-1}\}$ gera $\mathbb{F}(\alpha)$ sobre \mathbb{F} .

Nos resta provar que o conjunto $\{1, \alpha, \alpha^2, \dots, \alpha^{n-1}\}$ é linearmente independente, o que faremos supondo por absurdo que existam $c_0, c_1, \dots, c_{n-1} \in \mathbb{F}$, com $c_j \neq 0$ para algum $j \in \{0, 1, 2, \dots, n-1\}$, tais que

$$c_0 + c_1\alpha + \dots + c_{n-1}\alpha^{n-1} = 0.$$

Neste caso teríamos que o polinômio $h(X) = c_0 + c_1X + \dots + c_{n-1}X^{n-1}$ é não nulo de grau menor do que n e tal que $h(\alpha) = 0$, um claro absurdo tendo em vista que $\partial p(X) = n$. Logo $c_j = 0$ para todo $j \in \{0, 1, 2, \dots, n-1\}$, e assim, $\{1, \alpha, \alpha^2, \dots, \alpha^{n-1}\}$ é linearmente independente sobre \mathbb{F} .

Portanto, $\{1, \alpha, \alpha^2, \dots, \alpha^{n-1}\}$ é uma base de $\mathbb{F}(\alpha)$ sobre \mathbb{F} e $[\mathbb{K} : \mathbb{F}] = n$, como queríamos. \square

A importância desta proposição reside no fato de que, no contexto do enunciado da mesma, para encontrar o grau da extensão $\mathbb{F}(\alpha) \mid \mathbb{F}$ basta encontrar o polinômio minimal de α sobre \mathbb{F} , o que pode ser feito buscando os polinômios com coeficientes em \mathbb{F} que possuem α como uma de suas raízes, e verificando qual deles é irredutível.

Proposição 2.16. *Sejam $\mathbb{F} \subset \mathbb{L} \subset \mathbb{K}$ corpos. Se $[\mathbb{K} : \mathbb{L}] < \infty$ e $[\mathbb{L} : \mathbb{F}] < \infty$, então $[\mathbb{K} : \mathbb{F}] < \infty$ e $[\mathbb{K} : \mathbb{F}] = [\mathbb{K} : \mathbb{L}][\mathbb{L} : \mathbb{F}]$.*

Prova: Sejam $\{v_1, v_2, \dots, v_r\}$ uma base de \mathbb{K} sobre \mathbb{L} e $\{u_1, u_2, \dots, u_s\}$ uma base de \mathbb{L} sobre \mathbb{F} . Provaremos que o conjunto

$$\beta = \left\{ v_i u_j; \begin{array}{l} i = 1, 2, \dots, r \\ j = 1, 2, \dots, s \end{array} \right\}$$

é uma base de \mathbb{K} sobre \mathbb{F} .

Iniciamos mostrando que β gera \mathbb{K} sobre \mathbb{F} . Seja $a \in \mathbb{K}$. Temos que existem $\lambda_1, \lambda_2, \dots, \lambda_r \in \mathbb{L}$ tais que,

$$a = \lambda_1 v_1 + \lambda_2 v_2 + \dots + \lambda_r v_r.$$

Como $\lambda_1, \lambda_2, \dots, \lambda_r \in \mathbb{L}$ e $\{u_1, u_2, \dots, u_s\}$ é uma base de \mathbb{L} sobre \mathbb{F} temos que existem $\alpha_{ij} \in \mathbb{F}$ com $1 \leq i \leq r$ e $1 \leq j \leq s$ tais que

$$\lambda_i = \alpha_{i1}u_1 + \alpha_{i2}u_2 + \dots + \alpha_{is}u_s.$$

Daí segue que

$$a = \sum_{i,j} \alpha_{ij}v_iu_j, \quad \alpha_{ij} \in \mathbb{F}, \quad 1 \leq i \leq r, \quad 1 \leq j \leq s.$$

Logo, β gera \mathbb{K} sobre \mathbb{F} .

Mostraremos agora que β é linearmente independente em \mathbb{K} sobre \mathbb{F} . Sejam $\alpha_{ij} \in \mathbb{F}$, $1 \leq i \leq r$, $1 \leq j \leq s$, de modo que

$$\sum_{i,j} \alpha_{ij}v_iu_j = (\alpha_{11}u_1 + \alpha_{12}u_2 + \dots + \alpha_{1s}u_s)v_1 + \dots + (\alpha_{r1}u_1 + \alpha_{r2}u_2 + \dots + \alpha_{rs}u_s)v_r = 0.$$

Como os u_j 's $\in \mathbb{L}$ e os vetores v_i 's são linearmente independentes em \mathbb{K} sobre \mathbb{L} , temos que

$$\begin{cases} \alpha_{11}u_1 + \alpha_{12}u_2 + \dots + \alpha_{1s}u_s = 0 \\ \alpha_{21}u_1 + \alpha_{22}u_2 + \dots + \alpha_{2s}u_s = 0 \\ \vdots \quad \vdots \\ \alpha_{r1}u_1 + \alpha_{r2}u_2 + \dots + \alpha_{rs}u_s = 0 \end{cases}.$$

Uma vez que os elementos α_{ij} 's estão em \mathbb{F} , segue pela independência linear dos u_j 's em \mathbb{L} sobre \mathbb{F} , que cada $\alpha_{ij} = 0$, $1 \leq i \leq r$, $1 \leq j \leq s$. Logo, β é um conjunto linearmente independente de \mathbb{K} sobre \mathbb{F} .

Portanto, sendo o conjunto β uma base de \mathbb{K} sobre \mathbb{F} , e notando que o mesmo possui rs elementos, segue $[\mathbb{K} : \mathbb{F}] < \infty$ e $[\mathbb{K} : \mathbb{F}] = [\mathbb{K} : \mathbb{L}][\mathbb{L} : \mathbb{F}]$, como queríamos. \square

Assim como é dada na Definição 2.11, a construção da adjunção pode ser ampliada, ao considerarmos $\mathbb{F}(\alpha_1) \subset \mathbb{K}$ e $\alpha_2 \in \mathbb{K}$; denotando $(\mathbb{F}(\alpha_1))(\alpha_2) = \mathbb{F}(\alpha_1, \alpha_2) \subset \mathbb{K}$, como o menor subcorpo de \mathbb{K} que contém $\mathbb{F}(\alpha_1) \cup \{\alpha_2\} \in \mathbb{K}$. E por ser o menor subcorpo de \mathbb{K} que contém $\mathbb{F}(\alpha_1) \cup \{\alpha_2\} \in \mathbb{K}$ segue,

$$\mathbb{F}(\alpha_1, \alpha_2) = \left\{ \frac{f(\alpha_1, \alpha_2)}{g(\alpha_1, \alpha_2)}; f(X_1, X_2), g(X_1, X_2) \in \mathbb{F}[X_1, X_2], \text{ com } g(\alpha_1, \alpha_2) \neq 0 \right\}.$$

Sejam $\alpha_1, \alpha_2, \dots, \alpha_{n-1}, \alpha_n \in \mathbb{K}$. Recursivamente, podemos obter o menor subcorpo de \mathbb{K} que contém $\mathbb{F}(\alpha_1, \alpha_2, \dots, \alpha_{n-1}) \cup \{\alpha_n\} \in \mathbb{K}$, denotando por

$$\mathbb{F}(\alpha_1, \alpha_2, \dots, \alpha_{n-1})(\alpha_n) = \mathbb{F}(\alpha_1, \alpha_2, \dots, \alpha_{n-1}, \alpha_n), \text{ sendo}$$

$$\begin{aligned} & \mathbb{F}(\alpha_1, \alpha_2, \dots, \alpha_{n-1}, \alpha_n) = \\ & = \left\{ \frac{f(\alpha_1, \alpha_2, \dots, \alpha_n)}{g(\alpha_1, \alpha_2, \dots, \alpha_n)}; f, g \in \mathbb{F}[X_1, X_2, \dots, X_n], \text{ com } g(\alpha_1, \alpha_2, \dots, \alpha_n) \neq 0 \right\}. \end{aligned}$$

2.3 Algebrização das construções com régua e compasso

Neste tópico abordaremos o problema de algebrizar as construções com régua e compasso, relacionando elementos e resultados da álgebra que apresentamos até agora com a construtibilidade de figuras planas. Especificamente, objetivamos estabelecer uma condição a qual um dado segmento que pode ser construído com régua e compasso, satisfaça. Isso nos possibilitará afirmar se um segmento é ou não construtível com régua e compasso. As referências consultadas para o estudo e escrita deste tópico foram (BHATTACHARYA; JAIN e NAGPAUL, 1994), (GONÇALVES, 2013) e (HEFEZ e VILLELA, 2012).

Recordemos do início do tópico Construções com Régua e Compasso (Página 15), o que é permitido fazer com uma régua não graduada e um compasso. E consideremos o plano cartesiano \mathbb{R}^2 como a região onde todas as construções sobre as quais comentaremos estão presentes. Além disso, sempre que for nossa intenção afirmar que um determinado elemento é construtível com régua e compasso, diremos apenas que tal elemento é “construtível”.

Seja S um subconjunto do \mathbb{R}^2 , que contenha pelo menos dois pontos. Um segmento do \mathbb{R}^2 é dito construtível a partir de S se seus extremos pertencem a S . Dizemos que uma reta em \mathbb{R}^2 é construtível a partir de S se a mesma contiver pelo menos dois pontos distintos de S , e dizemos que um círculo em \mathbb{R}^2 é construtível a partir de S se seu centro e um de seus pontos pertencem a S .

Por meio das seguintes construções, chamadas de construções fundamentais, ou construções elementares em S , construímos novos objetos geométricos a partir de S .

- i) ligar dois pontos por um segmento de reta;
- ii) traçar uma reta por dois pontos;
- iii) traçar um círculo que tenha o centro e um de seus pontos em S .

Um ponto $A \in \mathbb{R}^2$ é construtível a partir de S se é interseção entre duas retas, ou uma reta e um círculo, ou ainda dois círculos, construídos a partir S . Logo, se A é construtível a partir de S , então suas coordenadas satisfazem um sistema composto por equações de retas ou círculos, e assim, uma vez que a equação de uma reta tem grau 1 e a do círculo tem grau 2, temos que suas coordenadas são raízes de equações com, no máximo, grau igual a 2.

Proposição 2.17. *Se uma reta r e um ponto A pertencentes ao \mathbb{R}^2 são ambos construtíveis, então a reta perpendicular a r que passa por A é construtível.*

Prova:

Caso 1: $A \notin r$.

Uma vez que a reta r é construtível, temos que possui pelo menos dois pontos construtíveis. Seja A_0 um destes pontos. Construamos o círculo de centro A e que passa por A_0 . Se r for tangente a este círculo, então a reta $\overleftrightarrow{AA_0}$ resolve o problema. Se não

for este o caso, tomemos o ponto A_1 interseção do círculo com a reta r . Neste caso as retas $\overleftrightarrow{AA_0}$ e $\overleftrightarrow{AA_1}$ são construtíveis e suas interseções com o círculo determinam os pontos construtíveis A_2 e A_3 respectivamente. Para finalizar, construamos o círculo com centro em A_0 e raio $\overline{A_0A_2} > \overline{AA_0}$, e o círculo com centro A_1 e raio $\overline{A_1A_3} > \overline{AA_1}$.

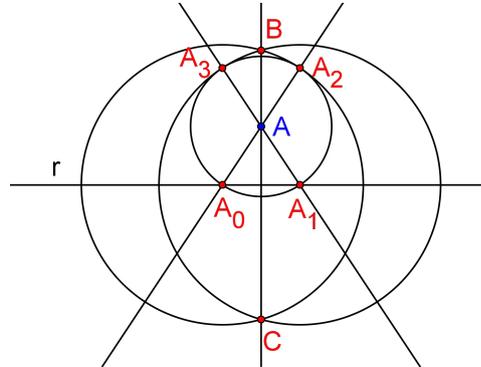


Figura 35 – Reta perpendicular construtível passando por $A \notin r$.

Estes dois círculos possuem raios de mesmo comprimento (pois os pontos A_0 e A_2 , e A_1 e A_3 são diametralmente opostos), são construtíveis, e sendo os pontos B e C suas interseções, então estes pontos são construtíveis. Logo a reta \overleftrightarrow{BC} é construtível. E além disso, pela Construção 2.1.1.4 é perpendicular a reta r e passa por A .

Caso 2: $A \in r$.

De modo análogo ao caso anterior, tomemos o ponto $A_0 \in r$ construtível e construamos o círculo de centro A e que passa por A_0 , determinando o ponto A_1 (construtível) interseção deste círculo com r . Agora, construamos os círculos de centros A_0 e A_1 raio $\overline{A_0A_1} > \overline{AA_0}$.

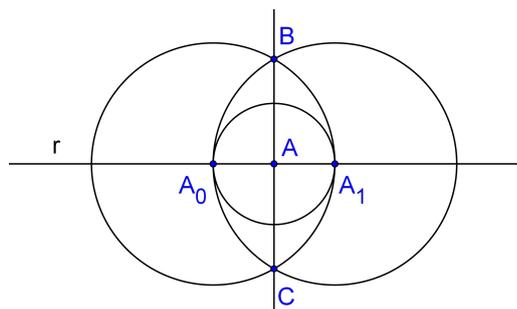


Figura 36 – Reta perpendicular construtível passando por $A \in r$.

A reta \overleftrightarrow{BC} , onde B e C são as interseções destes círculos, é construtível. E como já sabemos, é perpendicular a reta r e passa por A . \square

Denotaremos por C o subconjunto dos pontos de \mathbb{R}^2 que são construtíveis a partir de $S = \{(0, 0), (1, 0)\} \subset \mathbb{R}^2$, e por C^* o subconjunto dos números reais composto pelas coordenadas de todos os pontos de C .

Dizemos que um número $a \in \mathbb{R}$ é construtível se os pontos $(a, 0), (0, a) \in \mathbb{R}^2$ são construtíveis. Com esta definição, e considerando a Construção 2.1.1.4 podemos provar a seguinte proposição.

Proposição 2.18. *Um ponto $A = (a, b) \in \mathbb{R}^2$ é construtível se, e somente se, as suas coordenadas $a, b \in \mathbb{R}$ são números construtíveis.*

Prova:

[\Rightarrow] Consideremos o plano cartesiano OXY e $A = (a, b) \in \mathbb{R}^2$ um ponto construtível. Construamos as retas r e s , perpendiculares respectivamente aos eixos \overleftrightarrow{OX} e \overleftrightarrow{OY} , e que passam pelo A .

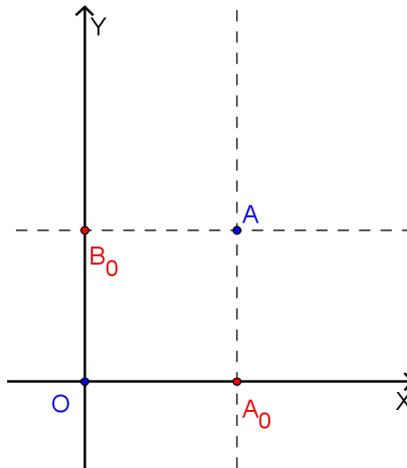


Figura 37 – Plano XOY e ponto A .

As interseções das retas r e s com os eixos \overleftrightarrow{OX} e \overleftrightarrow{OY} determinam respectivamente os pontos $A_0 = (a, 0)$ e $B_0 = (0, b)$, logo os mesmos são construtíveis, pois pela proposição anterior as retas r e s são construtíveis.

[\Leftarrow] Suponhamos que $a, b \in \mathbb{R}$ sejam números construtíveis, isto é, os pontos $A_0 = (a, 0)$ e $B_0 = (0, b)$ são construtíveis. Construamos as retas r e s , perpendiculares respectivamente aos eixos \overleftrightarrow{OX} e \overleftrightarrow{OY} , e passando respectivamente pelos pontos A_0 e B_0 .

A interseção da reta r com a reta s determina o ponto $A = (a, b)$. Logo, $A = (a, b) \in \mathbb{R}^2$ é construtível. \square

Das construções elementares do tópico Construções com Régua e Compasso (Página 15), temos que a soma, a diferença, o produto e o quociente de dois números construtíveis são construtíveis, e portanto temos que C^* é um subcorpo dos números reais que contém o conjunto dos números racionais, $\mathbb{Q} \subset C^*$.

Pelo que temos até então, um ponto $A \in \mathbb{R}^2$ é construtível se existirem pontos $A_1, A_2, A_3, \dots, A_r \in \mathbb{R}^2$, onde $A_1 = (a_1, b_1) = (0, 0), A_2 = (a_2, b_2) = (0, 1), A_3 = (a_3, b_3), \dots, A_r = (a_r, b_r)$ e cada um dos $A_i, i \in \{3, 4, \dots, r\}$ pode ser obtido por meio das construções elementares que envolvam os pontos anteriores a ele na sequência, sendo $A = A_r$.

Seja K um subcorpo de \mathbb{R} que contém \mathbb{Q} , e também as coordenadas de uma coleção de pontos construtíveis de \mathbb{R}^2 . Já sabemos que se o ponto $A = (\alpha, 0) \in \mathbb{R}^2$ é construtível a partir de pontos que tem suas coordenadas em K , então pode ser obtido por meio de uma sequência de construções elementares envolvendo pontos construtíveis que possuem suas coordenadas em K . Neste caso dizemos que o número $\alpha \in \mathbb{R}$ é construtível a partir K . Quando $\alpha \notin K$, consideramos o corpo $K(\alpha) \supset K$.

Proposição 2.19. *Seja K um subcorpo de \mathbb{R} como denotado no parágrafo anterior. Temos que $K(\alpha) | K$ tem grau no máximo igual a 2, isto é, $[K(\alpha) : K] \leq 2$.*

Prova: Pelo exposto até aqui, o ponto $A = (\alpha, 0)$ é interseção de duas retas, ou de uma reta e um círculo, ou ainda interseção de dois círculos, determinados a partir de pontos construtíveis que possuem suas coordenadas em K . Ou seja, o ponto A satisfaz um sistema envolvendo equações do tipo

$$ax + by + c = 0, \quad a, b, c \in K, \quad (2.12)$$

$$x^2 + y^2 + 2gx + 2fy + d = 0, \quad g, f, d \in K. \quad (2.13)$$

Uma vez que A satisfaz um sistema envolvendo (2.12) ou (2.13) temos que α é raiz de uma equação com coeficientes em K , de grau no máximo igual a dois. Portanto, o resultado segue da Proposição 2.15. \square

Com esta proposição fica estabelecido que, se um segmento de comprimento $\alpha \in \mathbb{R}$ é construtível a partir de pontos construtíveis de \mathbb{R}^2 , tais que suas coordenadas pertençam a um corpo $K \subset \mathbb{R}$, então o polinômio minimal de α sobre K tem grau no máximo igual a dois.

Concluimos a apresentação de toda a teoria necessária para demonstração que faremos, acerca da não construtibilidade de um triângulo, dados os comprimentos de suas bissetrizes internas. No próximo tópico, expomos o resultado fundamental para a demonstração elementar da existência e unicidade de um tal triângulo.

2.4 Teorema do Ponto Fixo para Contrações

O objetivo desta seção é especificamente enunciar e demonstrar o teorema do ponto fixo para contrações. As nossas principais referências para o que segue são: (BRANDÃO, 2007), (DINCA e JEAN, 2010), (LIMA, 2016) e (LIMA, 2004).

Expomos abaixo três definições essenciais em relação ao que será discutido na próxima proposição.

Definição 2.12. *Seja $C \subset \mathbb{R}^n$ um conjunto não vazio e $T : C \rightarrow \mathbb{R}^n$ uma aplicação. Dizemos que T é uma contração se existir uma constante $k \in \mathbb{R}$, sendo $0 \leq k < 1$ tal que*

$$\|T(X) - T(Y)\| \leq k\|X - Y\|, \quad \forall X, Y \in C \subset \mathbb{R}^n$$

Neste caso, costuma-se ainda dizer que T é uma k -contração.

Definição 2.13. *Seja T uma aplicação. Um ponto X pertencente ao domínio de T é dito “Ponto Fixo de T ” se $T(X) = X$. Obviamente o ponto X pertence ao contradomínio da aplicação em questão.*

Definição 2.14. *Uma aplicação $f : A \rightarrow \mathbb{R}^n$, definida no conjunto $A \subset \mathbb{R}^m$, é chamada de função Lipschitziana se existir $c > 0$ tal que $\|f(X) - f(Y)\| \leq c\|X - Y\|$ para todos $X, Y \in A$. O número c é chamado uma constante de Lipschitz da função f .*

Sem dificuldade podemos provar que toda função Lipschitziana é contínua, o pode ser visto em (LIMA, 2004, p.22).

A seguir enunciamos e provamos o resultado central deste tópico. Em meio a prova citaremos alguns elementos que estão expostos no apêndice.

Proposição 2.20 (Teorema do Ponto Fixo para Contrações). *Seja C um subconjunto não vazio, fechado e limitado do \mathbb{R}^n . Se $T : C \rightarrow C$ é uma k -contração, então T possui um único ponto fixo em C .*

Prova: Utilizaremos a função auxiliar $f : C \rightarrow \mathbb{R}$ definida por

$$f(X) = \|X - T(X)\|.$$

Dado $X_0 \in C$ tal que $f(X_0) = 0$, temos $0 = f(X_0) = \|X_0 - T(X_0)\|$, logo $X_0 = T(X_0)$. Ou seja, todo zero de f é um ponto fixo de T . Assim, nosso problema se reduz a provar que f possui um único zero em C . Provaremos primeiro a existência. Para tanto, dados $X, Y \in C$, temos que

$$\|f(X) - f(Y)\| = \left| \|X - T(X)\| - \|Y - T(Y)\| \right| \leq \quad (2.14)$$

$$\leq \|X - Y + T(Y) - T(X)\| \leq \quad (2.15)$$

$$\leq \|X - Y\| + \|T(Y) - T(X)\| \leq \quad (2.16)$$

$$\leq \|X - Y\| + k\|Y - X\| = \quad (2.17)$$

$$= \|X - Y\| + k\|X - Y\| = \quad (2.18)$$

$$= (1 + k)\|X - Y\|. \quad (2.19)$$

Da equação (2.14) para inequação (2.15) usamos a desigualdade (A.6)⁴, de (2.15) para (2.16) a desigualdade triangular (A.5), e de (2.16) para (2.17) o fato de T ser uma k -contração. Obtemos então que

$$\|f(X) - f(Y)\| \leq (1 + k)\|X - Y\|,$$

⁴ Esta inequação, bem como algumas proposições que citaremos a seguir, estão presentes no Apêndice.

o que nos diz que f é Lipschitziana, logo contínua em C . Agora, uma vez que C é um subconjunto limitado e fechado de \mathbb{R}^n , o Teorema de Weierstrass - Princípio Max/min (Proposição A.1) nos assegura que f possui ponto de mínimo em C . Logo existe $X_0 \in C$ tal que

$$f(X_0) \leq f(X), \quad \forall X \in C.$$

Observemos que, como $T(X_0) \in C$, vale

$$f(X_0) \leq f(T(X_0)) \tag{2.20}$$

e além disso, para todo $X \in C$,

$$f(T(X)) = \|T(X) - T(T(X))\|,$$

o que nos dá

$$f(T(X)) \leq k\|X - T(X)\| = kf(X),$$

uma vez que $\|T(X) - T(T(X))\| \leq k\|X - T(X)\|$ pois T é uma k -contração. Temos então,

$$f(T(X)) \leq kf(X), \quad \forall X \in C. \tag{2.21}$$

Logo, segue das inequações (2.20) e (2.21),

$$\begin{aligned} f(X_0) \leq f(T(X_0)) &\leq kf(X_0) \Rightarrow \\ \Rightarrow f(X_0) - kf(X_0) &\leq 0. \end{aligned}$$

E então, como $k < 1$, temos $f(X_0) = 0$. Ou seja, $X_0 \in C$ é um zero da função f , e portanto é um ponto fixo de T .

Nos resta provar a unicidade, que é imediato uma vez que supondo X_1 e X_2 pontos fixos de T temos

$$\|X_1 - X_2\| = \|T(X_1) - T(X_2)\| \leq k\|X_1 - X_2\|$$

que nos dá $\|X_1 - X_2\| = 0$, pois $k < 1$, logo $X_1 = X_2$. □

Com esta proposição, concluímos em fim, todas as preliminares necessárias para as demonstrações, objetivos centrais deste texto, que realizaremos nos próximos capítulos.

3 EXISTÊNCIA E UNICIDADE

Neste capítulo, munidos da teoria necessária, apresentamos as demonstrações da existência e da unicidade de um triângulo, dadas suas bissetrizes internas. Nossas principais referências acerca destas demonstrações são (DINCA e JEAN, 2010) e (MIRONESCU e PANAITOPOL, 1994).

Iniciamos recordando da Proposição 2.4, que nos fornece o comprimento das bissetrizes de um triângulo em função dos seus lados. Este resultado foi apresentado a partir da Página 34. Lembremos que a, b e c são os comprimentos dos lados, e m, n e p os comprimentos das bissetrizes internas do triângulo.

Da equação (2.3) temos,

$$m = \frac{2}{b+c} \sqrt{bc \left(\frac{a+b+c}{2} \right) \left(\frac{b+c-a}{2} \right)},$$

que elevando ao quadrado ambos os membros temos

$$m^2 = \frac{4bc}{(b+c)^2} \left(\frac{(b+c+a)(b+c-a)}{4} \right),$$

implicando em

$$4m^2 = \frac{4bc}{(b+c)^2} [(b+c)^2 - a^2].$$

Desta última igualdade obtemos

$$\begin{aligned} 4m^2 &= \frac{4bc}{(b+c)^2} [(b+c)^2 - a^2] = \\ &= \frac{2bc - (-2bc)}{(b+c)^2} [(b+c)^2 - a^2] = \\ &= \frac{2bc - (-2bc) + (b^2 + c^2) - (b^2 + c^2)}{(b+c)^2} [(b+c)^2 - a^2] = \\ &= \frac{(b^2 + 2bc + c^2) - (b^2 - 2bc + c^2)}{(b+c)^2} [(b+c)^2 - a^2] = \\ &= \frac{(b+c)^2 - (b-c)^2}{(b+c)^2} [(b+c)^2 - a^2], \end{aligned}$$

ou seja,

$$4m^2 = \frac{(b+c)^2 - (b-c)^2}{(b+c)^2} [(b+c)^2 - a^2]. \quad (3.1)$$

Agora, da equação (3.1) segue

$$\begin{aligned} 4m^2 &= \frac{(b+c)^2(b+c)^2 - (b-c)^2(b+c)^2 - (b+c)^2a^2 + (b-c)^2a^2}{(b+c)^2} = \\ &= (b+c)^2 - (b-c)^2 - a^2 + \frac{(b-c)^2a^2}{(b+c)^2} = \\ &= (b+c)^2 + \frac{(b-c)^2a^2}{(b+c)^2} - [a^2 + (b-c)^2]. \end{aligned}$$

Obtemos então

$$4m^2 = (b+c)^2 + \frac{(b-c)^2 a^2}{(b+c)^2} - [a^2 + (b-c)^2].$$

Escrevendo a equação acima como

$$4m^2 = (b+c)^2 + \frac{(b-c)^2 a^2}{(b+c)^2} + [2(b-c)a - 2(b-c)a] - [a^2 + (b-c)^2],$$

temos por um lado

$$\begin{aligned} 4m^2 &= (b+c)^2 + \frac{2(b+c)(b-c)a}{(b+c)} + \frac{(b-c)^2 a^2}{(b+c)^2} - 2(b-c)a - [a^2 + (b-c)^2] = \\ &= \left[(b+c) + \frac{(b-c)a}{(b+c)} \right]^2 - [a^2 + 2a(b-c) + (b-c)^2] = \\ &= \left[(b+c) + \frac{(b-c)a}{(b+c)} \right]^2 - [a + (b-c)]^2, \end{aligned}$$

isto é,

$$4m^2 = \left[(b+c) + \frac{(b-c)a}{(b+c)} \right]^2 - [a + (b-c)]^2, \quad (3.2)$$

e por outro lado,

$$\begin{aligned} 4m^2 &= (b+c)^2 - \frac{2(b+c)(b-c)a}{(b+c)} + \frac{(b-c)^2 a^2}{(b+c)^2} + 2(b-c)a - [a^2 + (b-c)^2] = \\ &= \left[(b+c) - \frac{(b-c)a}{(b+c)} \right]^2 - [a^2 - 2a(b-c) + (b-c)^2] = \\ &= \left[(b+c) - \frac{(b-c)a}{(b+c)} \right]^2 - [a - (b-c)]^2, \end{aligned}$$

portanto,

$$4m^2 = \left[(b+c) - \frac{(b-c)a}{(b+c)} \right]^2 - [a - (b-c)]^2. \quad (3.3)$$

Segue das equações (3.2) e (3.3) que

$$4m^2 = \left[(b+c) \pm \frac{(b-c)a}{(b+c)} \right]^2 - [a \pm (b-c)]^2.$$

Da equação (3.2) temos

$$\begin{aligned} 4m^2 + (a+b-c)^2 &= \left[\frac{(b+c)^2 + (b-c)a}{(b+c)} \right]^2 \Rightarrow \\ &\Rightarrow \sqrt{4m^2 + (a+b-c)^2} = \frac{(b+c)^2 + ba - ca}{(b+c)}. \end{aligned} \quad (3.4)$$

E da equação (3.3)

$$4m^2 + (a+c-b)^2 = \left[\frac{(b+c)^2 - (b-c)a}{(b+c)} \right]^2 \Rightarrow$$

$$\Rightarrow \sqrt{4m^2 + (a + c - b)^2} = \frac{(b + c)^2 - ba + ca}{(b + c)}. \quad (3.5)$$

Somando (3.4) com (3.5) obtemos

$$\begin{aligned} \sqrt{4m^2 + (a + b - c)^2} + \sqrt{4m^2 + (a + c - b)^2} &= 2\frac{(b + c)^2}{(b + c)} \Rightarrow \\ \Rightarrow \sqrt{4m^2 + (a + b - c)^2} + \sqrt{4m^2 + (a + c - b)^2} &= 2(b + c). \end{aligned} \quad (3.6)$$

De modo totalmente análogo, obtemos igualdades como (3.6) envolvendo os comprimentos n e p , das outras duas bissetrizes do triângulo ABC .

Agora, sendo s o semiperímetro do triângulo ABC , tomemos

$$s - a = \frac{b + c - a}{2} = x, \quad s - b = \frac{a + c - b}{2} = y \quad e \quad s - c = \frac{a + b - c}{2} = z, \quad (3.7)$$

e assim temos,

$$a = y + z, \quad b = z + x, \quad e \quad c = x + y.$$

Da equação (3.6) segue

$$\begin{aligned} 2(b + c) = 4x + 2a &= \sqrt{4m^2 + (2z)^2} + \sqrt{4m^2 + (2y)^2} \Rightarrow \\ \Rightarrow 4x + 2a &= 2(\sqrt{m^2 + z^2} + \sqrt{m^2 + y^2}) \Rightarrow \\ \Rightarrow 2x + a &= \sqrt{m^2 + z^2} + \sqrt{m^2 + y^2} \Rightarrow \\ \Rightarrow x &= \frac{1}{2}\sqrt{m^2 + z^2} + \frac{1}{2}\sqrt{m^2 + y^2} - \frac{a}{2} \Rightarrow \\ \Rightarrow x &= \frac{1}{2} \left[(\sqrt{m^2 + z^2} - z) + (\sqrt{m^2 + y^2} - y) \right]. \end{aligned} \quad (3.8)$$

Ao obtermos as equações análogas a (3.6) envolvendo n e p podemos escrever

$$y = \frac{1}{2} \left[(\sqrt{n^2 + x^2} - x) + (\sqrt{n^2 + z^2} - z) \right], \quad (3.9)$$

e também

$$z = \frac{1}{2} \left[(\sqrt{p^2 + y^2} - y) + (\sqrt{p^2 + x^2} - x) \right]. \quad (3.10)$$

Para todo $\alpha > 0$ definimos a função contínua $f_\alpha : \mathbb{R}_+ \rightarrow (0, \alpha/2]$ dada por

$$f_\alpha(t) = \frac{1}{2} (\sqrt{\alpha^2 + t^2} - t).$$

Podemos verificar sem dificuldades que,

$$f'_\alpha(t) = \frac{1}{2} \left(\frac{t}{\sqrt{\alpha^2 + t^2}} - 1 \right) < 0, \quad \forall t \geq 0,$$

onde $f'_\alpha(t)$ denota a derivada de f_α aplicada no ponto t , logo f_α é decrescente e $|f'_\alpha(t)| < \frac{1}{2}$ para $t > 0$, o que nos dá pelo Teorema do Valor Médio (Proposição A.3),

$$|f_\alpha(t) - f_\alpha(t')| < \frac{1}{2}|t - t'| \quad \forall t \neq t' \in \mathbb{R}_+. \quad (3.11)$$

Assim, considerando o conjunto $C = [0, m] \times [0, n] \times [0, p] \in \mathbb{R}^3$, definimos a aplicação contínua $F : C \rightarrow C$ dada por

$$F(x, y, z) = (f_m(z) + f_m(y), f_n(x) + f_n(z), f_p(y) + f_p(x)). \quad (3.12)$$

Da forma como definimos a aplicação F , pelas equações (3.8), (3.9) e (3.10) temos que $F(x, y, z) = (x, y, z)$, onde x, y, z são como em (3.7) e m, n, p os comprimentos das bissetrizes internas do triângulo.

Por outro lado, os comprimentos dos lados do triângulo são $y + z, z + x, x + y$. Daí, o problema da existência e unicidade de um triângulo dados os comprimentos de suas bissetrizes internas é equivalente à existência e unicidade de um ponto fixo de F . Se tal ponto existir, então o sistema de equações formado por (3.8), (3.9) e (3.10) possui solução única, o que implica diretamente na existência e unicidade do triângulo com lados de comprimentos a, b e c .

Proposição 3.1. *Sejam $X = (x, y, z)$ e $X' = (x', y', z')$ pertencentes a C . Afirmamos que*

$$\|F(X) - F(X')\| < \|X - X'\|. \quad (3.13)$$

Prova: De fato,

$$\begin{aligned} S &= \|F(X) - F(X')\| = \|F(x, y, z) - F(x', y', z')\| = \\ &= \|(f_m(z) + f_m(y), f_n(x) + f_n(z), f_p(y) + f_p(x)) - (f_m(z') + f_m(y'), f_n(x') + f_n(z'), f_p(y') + f_p(x'))\| = \\ &= \|(f_m(z) + f_m(y) - f_m(z') - f_m(y'), f_n(x) + f_n(z) - f_n(x') - f_n(z'), f_p(y) + f_p(x) - f_p(y') - f_p(x'))\| = \\ &= \|(f_m(z) - f_m(z') + f_m(y) - f_m(y'), f_n(x) - f_n(x') + f_n(z) - f_n(z'), f_p(y) - f_p(y') + f_p(x) - f_p(x'))\| < \\ &< \|(\frac{1}{2}|z - z'| + \frac{1}{2}|y - y'|, \frac{1}{2}|x - x'| + \frac{1}{2}|z - z'|, \frac{1}{2}|y - y'| + \frac{1}{2}|x - x'|)\| = \\ &= \frac{1}{2}\|(|z - z'| + |y - y'|, |x - x'| + |z - z'|, |y - y'| + |x - x'|)\| = \\ &= \frac{1}{2}\sqrt{(|z - z'| + |y - y'|)^2 + (|x - x'| + |z - z'|)^2 + (|y - y'| + |x - x'|)^2}. \end{aligned}$$

Na passagem (1) usamos a desigualdade (3.11) em cada coordenada. Com isso obtemos,

$$S < \frac{1}{2}\sqrt{(|z - z'| + |y - y'|)^2 + (|x - x'| + |z - z'|)^2 + (|y - y'| + |x - x'|)^2}. \quad (3.14)$$

Consideremos as seguintes mudanças de variáveis,

$$A = |x - x'|, \quad B = |y - y'|, \quad C = |z - z'|.$$

Reescrevendo a desigualdade (3.14) temos,

$$\begin{aligned}
\|F(X) - F(X')\| &< \frac{1}{2}\sqrt{(C+B)^2 + (A+C)^2 + (B+A)^2} = \\
&= \frac{1}{2}\sqrt{2(A^2 + B^2 + C^2) + 2(AB + AC + BC)} = \\
&= \frac{1}{2}\sqrt{(A^2 + B^2 + C^2) + [(A^2 + B^2 + C^2) + 2(AB + AC + BC)]} = \\
&= \frac{1}{2}\sqrt{(A^2 + B^2 + C^2) + (A + B + C)^2} = \\
&= \sqrt{\frac{(A^2 + B^2 + C^2) + (A + B + C)^2}{4}},
\end{aligned}$$

obtendo,

$$\|F(X) - F(X')\| < \sqrt{\frac{(A^2 + B^2 + C^2) + (A + B + C)^2}{4}}. \quad (3.15)$$

Para concluir, mostraremos que

$$\sqrt{\frac{(A^2 + B^2 + C^2) + (A + B + C)^2}{4}} \leq \sqrt{(A^2 + B^2 + C^2)} = \|X - X'\|.$$

Pela desigualdade de Cauchy-Schwarz (Proposição A.4) temos

$$(A + B + C)^2 \leq (1^2 + 1^2 + 1^2)(A^2 + B^2 + C^2),$$

e então segue,

$$\begin{aligned}
&(A + B + C)^2 \leq 3(A^2 + B^2 + C^2) \Rightarrow \\
&\Rightarrow (A + B + C)^2 \leq 4(A^2 + B^2 + C^2) - (A^2 + B^2 + C^2) \Rightarrow \\
&\Rightarrow \frac{(A^2 + B^2 + C^2) + (A + B + C)^2}{4} \leq (A^2 + B^2 + C^2) \Rightarrow \\
&\Rightarrow \sqrt{\frac{(A^2 + B^2 + C^2) + (A + B + C)^2}{4}} \leq \sqrt{(A^2 + B^2 + C^2)}. \quad (3.16)
\end{aligned}$$

Portanto, pelas desigualdades (3.15) e (3.16) temos $\|F(X) - F(X')\| < \|X - X'\|$, como queríamos. \square

Na proposição seguinte provamos que a aplicação F possui um único ponto fixo, concluindo finalmente a demonstração da existência e unicidade de um triângulo dados os comprimentos das suas bissetrizes internas.

Proposição 3.2. *A aplicação F definida em (3.12) possui um único ponto fixo em C .*

Prova: Mostraremos inicialmente a unicidade. Para tanto, suponhamos que X_1 e X_2 sejam pontos fixos de F , isto é, $F(X_1) = X_1$ e $F(X_2) = X_2$. Pela desigualdade (3.13) temos

$$\|X_1 - X_2\| = \|F(X_1) - F(X_2)\| < \|X_1 - X_2\|,$$

que é absurdo. Isso nos diz que se existir um ponto fixo de F , ele é único.

Para prova da existência, seja λ_k uma sequência de números reais contida no intervalo $(0, 1)$, convergente e com limite igual 1. Para cada $k \in \mathbb{N}$, consideremos a aplicação $T_k : C \rightarrow C$ definida por $T_k = \lambda_k F$. Temos que, dados $X \neq X'$ pertencentes a C ,

$$\|T_k(X) - T_k(X')\| = \|\lambda_k F(X) - \lambda_k F(X')\| = \lambda_k \|F(X) - F(X')\| < \lambda_k \|X - X'\|,$$

isto é,

$$\|T_k(X) - T_k(X')\| < \lambda_k \|X - X'\|,$$

logo T_k é uma λ_k -contração com $\lambda_k \in (0, 1)$. Pelo Teorema do Ponto Fixo para Contrações (Proposição 2.20), obtemos para cada $k \in \mathbb{N}$, um único ponto fixo X_k de T_k . Agora, pelo Teorema de Bolzano-Weierstrass (Proposição A.2), a menos que, de passar a uma subsequência, podemos admitir que X_k converge para algum $X_0 \in C$. As relações $X_k = \lambda_k F(X_k)$, $n \in \mathbb{N}$ e a continuidade de F implicam que $X_0 = F(X_0)$, de modo que (X_k) converge para o único ponto fixo X_0 de F . \square

3.1 Um argumento Geométrico para unicidade

Como vimos, dados três números reais, existe um único triângulo tal que suas bissetrizes internas possuem estes números como seus comprimentos. Neste tópico apresentamos uma demonstração puramente geométrica para o fato da unicidade, não recorrendo a quaisquer outros conhecimentos relativos a trigonometria, análise e também à fórmula do comprimento das bissetrizes internas em função dos lados. A referência estudada acerca da argumentação que construímos aqui foi essencialmente (OXMAN, 2008).

Mostraremos que se existirem dois triângulos com bissetrizes internas de comprimentos iguais a três números dados, então estes triângulos são congruentes.

Iniciaremos mostrando que em um triângulo ABC , onde AD , BE e CF são suas bissetrizes internas, e o ponto I é seu incentro, temos $\overline{AI} > \overline{ID}$, $\overline{BI} > \overline{IE}$ e $\overline{CI} > \overline{IF}$. Para provarmos este fato, consideremos os pontos $G \in BC$, $H \in AC$, interseções do círculo inscrito do ΔABC com os lados BC e AC respectivamente, e $\varphi = \widehat{ADC}$ como na figura abaixo.

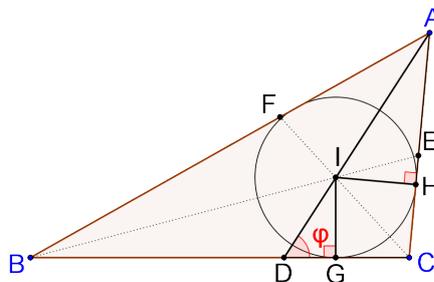


Figura 38 – Triângulo ABC e suas bissetrizes.

Uma vez que φ é ângulo externo ao triângulo ABD , denotando $\alpha = \widehat{BAC}$ e $\beta = \widehat{ABC}$ temos $\varphi = \beta + \frac{\alpha}{2} > \frac{\alpha}{2}$. Daí, existe um ponto $J \in AH$ tal que $\widehat{IJH} = \varphi$, pois $\widehat{HAI} = \frac{\alpha}{2}$.

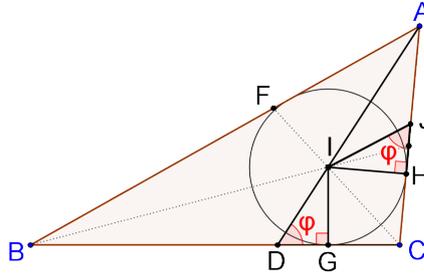


Figura 39 – Triângulo ABC , suas bissetrizes e o ponto J .

Agora, observemos que $\triangle DGI \equiv \triangle JHI$ pelo caso AAL de congruência de triângulos, e daí $\overline{ID} = \overline{IJ}$. Uma vez que os triângulos AIH e JIH são retângulos, e $\overline{AH} > \overline{JH}$ segue $\overline{IA} > \overline{IJ}$. Portanto $\overline{IA} > \overline{ID}$ como afirmamos, e de modo totalmente análogo mostramos que $\overline{BI} > \overline{IE}$ e $\overline{CI} > \overline{IF}$.

As duas proposições apresentadas abaixo serão essenciais para a demonstração do resultado central deste capítulo.

Proposição 3.3. *Sejam os triângulos ABC e $AB'C'$ que possuem o ângulo \hat{A} em comum. Suponhamos que o círculo inscrito do $\triangle AB'C'$ não seja maior que o círculo inscrito do $\triangle ABC$. Se $\hat{C}' > \hat{C}$, então a bissetriz de \hat{C}' é menor que a bissetriz de \hat{C} .*

Prova: Considerando CF e $C'F'$ as bissetrizes internas dos triângulos ABC e $AB'C'$ respectivamente, relativas aos ângulos \hat{C} e \hat{C}' . Provaremos que $\overline{C'F'} < \overline{CF}$.

Caso 1: Os triângulos têm mesmo círculo inscrito. Podemos assumir sem perda de generalidade que $\hat{B} > \hat{B}'$ e que o ponto C' está entre A e C . Seja I o centro do círculo inscrito comum dos triângulos.

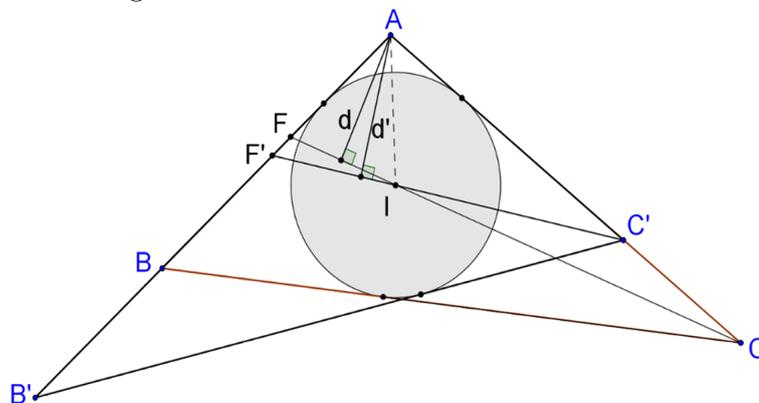


Figura 40 – Triângulos com o mesmo círculo inscrito.

Afirmamos que a área do $\triangle IFF'$ é menor que a área do $\triangle ICC'$. De fato, como $\overline{IF} < \overline{IC}$ e $\overline{IF'} < \overline{IC'}$, considerando IC como base do $\triangle ICC'$, IF como base do $\triangle IFF'$ e

notando que $\widehat{C'IC'} = \widehat{F'IF'}$ (opostos pelo vértice), temos que a altura do triângulo $\Delta IFF'$ relativa ao segmento IF é menor que a altura do triângulo $\Delta ICC'$ relativa ao segmento IC , daí

$$[IFF'] < [ICC'] \quad (3.17)$$

Sejam d, d' as distâncias de A para as bissetrizes CF e $C'F'$ respectivamente. Como $\widehat{AIF'} = \widehat{IAC'} + \widehat{AC'I} = \frac{\widehat{A} + \widehat{C'}}{2} < 90^\circ$, temos $\widehat{AIF} < \widehat{AIF'} < 90^\circ$, e assim $d < d'$. Agora, por (3.17) temos

$$[IFF'] + [IC'AF] < [ICC'] + [IC'AF],$$

que nos dá $[AF'C'] < [AFC]$, implicando em

$$\frac{1}{2}d'\overline{C'F'} < \frac{1}{2}d\overline{CF} \Rightarrow \frac{d'}{d}\overline{C'F'} < \overline{CF}.$$

Como $d < d'$ temos que $\frac{d'}{d} > 1$ e com isso segue $\overline{C'F'} < \overline{CF}$.

Caso 2: O círculo inscrito do triângulo $AB'C'$ é menor que o círculo inscrito do triângulo ABC (Figura 41). Como o círculo inscrito do $\Delta AB'C'$ está dentro do ΔABC , construímos a tangente ao círculo inscrito do triângulo $AB'C'$, $\overline{B''C''}$ paralela a BC .

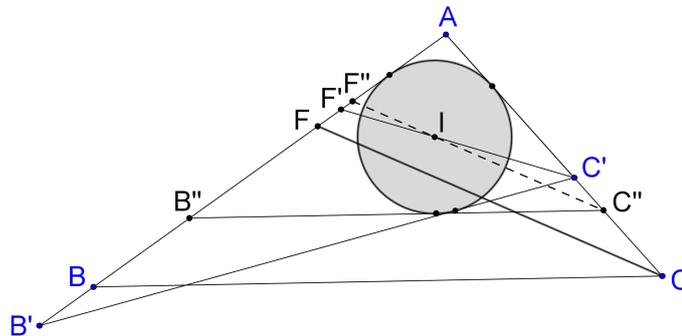


Figura 41 – Triângulos com círculo inscrito s diferentes.

Seja $C''F''$ bissetriz interna do triângulo $AB''C''$. Temos $C''F'' \parallel CF$ e

$$\overline{C''F''} < \overline{CF}. \quad (3.18)$$

Observemos que $\widehat{AC''B''} = \widehat{ACB} < \widehat{AC'B'}$, logo pelo **Caso 1** segue

$$\overline{C'F'} < \overline{C''F''}, \quad (3.19)$$

e por fim as desigualdades (3.18) e (3.19) nos dão $\overline{C'F'} < \overline{CF}$. \square

Proposição 3.4. *Sejam os triângulos ABC e $AB'C'$ que possuem o ângulo \widehat{A} em comum. Suponhamos que a bissetriz AD seja comum aos dois triângulos e que o ângulo comum \widehat{A} não seja maior que qualquer outro ângulo do $\Delta AB'C'$. Se $\widehat{C'} > \widehat{C}$, então a bissetriz de $\widehat{C'}$ é menor que a bissetriz de \widehat{C} .*

Prova: Se o círculo inscrito do triângulo $AB'C'$ não for maior que o do triângulo ABC , então o resultado segue pela Proposição 3.3.

Consideremos que o círculo inscrito do triângulo $AB'C'$ é maior que o do triângulo ABC (Figura 42). Nesse caso o segmento BC intersecta o círculo inscrito do $\Delta AB'C'$.

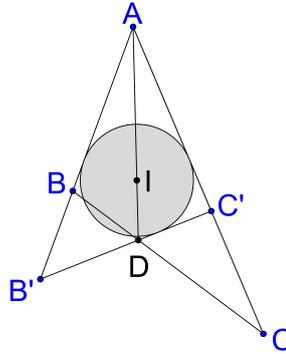


Figura 42 – Triângulos com bissetriz comum.

Construamos a tangente ao círculo inscrito do $\Delta AB'C'$ que passa por C , intersectando AB' no ponto B'' situado entre B e B' . Sejam CF e $C'F'$ bissetrizes internas dos triângulos ABC e $AB'C'$, relativas aos ângulos \widehat{C} e \widehat{C}' respectivamente. Mostraremos que $\overline{C'F'} < \overline{CF}$.

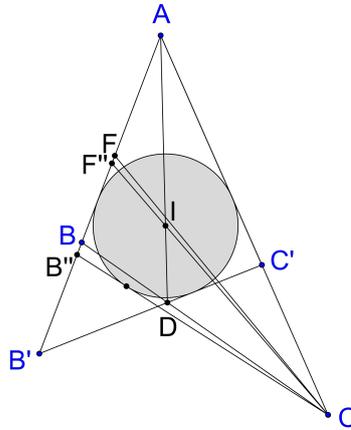


Figura 43 – Triângulos e suas bissetrizes.

Seja CF'' bissetriz do triângulo $AB''C$. Como B está entre A e B'' , e sendo CF e CF'' bissetrizes dos triângulos ABC e $AB''C$, temos que F está entre A e F'' . Segue então da Proposição 3.3 que

$$\overline{C'F'} < \overline{CF''}. \quad (3.20)$$

Observando os triângulos BCF'' e BCF temos $\widehat{BCF''} < \widehat{BCF}$, e com isso notamos que

$$\overline{CF''} < \overline{CF}. \quad (3.21)$$

Das equações (3.20) e (3.21) concluímos que $\overline{C'F'} < \overline{CF}$. \square

Utilizando as proposições acima, faremos agora a demonstração do resultado comentado no início dessa seção.

Proposição 3.5. *Se as bissetrizes internas do triângulo ABC são respectivamente de mesmo comprimento que as bissetrizes internas do triângulo $A'B'C'$, então estes triângulos são congruentes.*

Prova: Sejam AD, BE e CF as bissetrizes internas do triângulo ABC , e $\overline{A'D'} = \overline{AD}, \overline{B'E'} = \overline{BE}, \overline{C'F'} = \overline{CF}$, onde $A'D', B'E'$ e $C'F'$ são as bissetrizes do triângulo $A'B'C'$.

No caso em que $\widehat{A} = \widehat{A'}, \widehat{B} = \widehat{B'}$ e $\widehat{C} = \widehat{C'}$, pela semelhança do triângulo ABC com $A'B'C'$, e do triângulo ABD com $A'B'D'$ concluímos que os triângulos ABC e $A'B'C'$ são congruentes.

Suponhamos sem perda de generalidade que $\widehat{A'}$ não seja maior que qualquer outro ângulo dos triângulos ABC e $A'B'C'$. Construimos um triângulo AB_1C_1 congruente ao triângulo $A'B'C'$ que tem AD como bissetriz do ângulo B_1AC_1 .

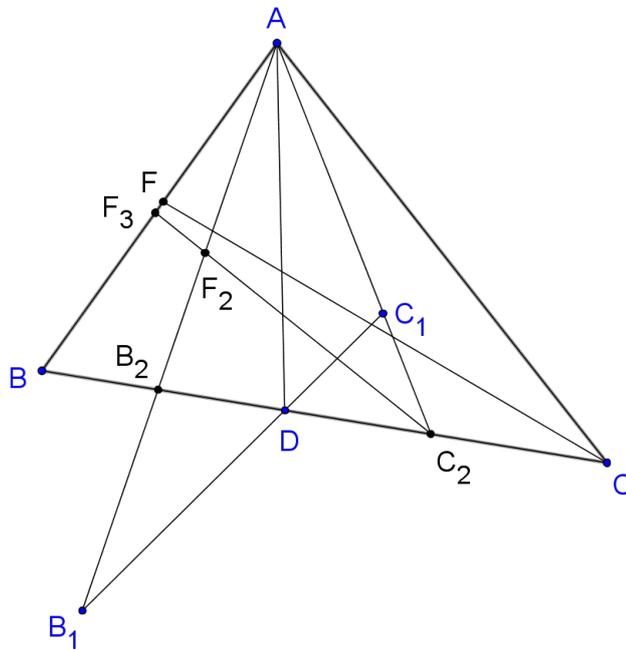


Figura 44 – Triângulo com construções auxiliares.

Se $\widehat{A'} = \widehat{A}$ e $\widehat{C'} > \widehat{C}$ temos que os triângulos ABC e AB_1C_1 satisfazem as condições da Proposição 3.4. Logo $\overline{C'F'} < \overline{CF}$, uma contradição.

Se $\widehat{A'} < \widehat{A}$ e os as retas $\overleftrightarrow{AB_1}$ e $\overleftrightarrow{AC_1}$ intersectam BC nos pontos B_2 e C_2 respectivamente, podemos assumir sem perda de generalidade que C_1 está entre A e C_2 , podendo coincidir com C_2 (Figura 44).

Consideremos agora que a bissetriz do ângulo $\widehat{AC_2B_2}$ intersecte AB_2 no ponto F_2 e AB no ponto F_3 . Observemos que os triângulos AB_1C_1 e AB_2C_2 também satisfazem as condições da Proposição 3.4, o que nos dá

$$\overline{C'F'} < \overline{C_2F_2} < \overline{C_2F_3}. \quad (3.22)$$

Agora, percebamos que o círculo inscrito do triângulo ABC_2 é menor que o do triângulo ABC . Com isso, e uma vez que $\widehat{AC_2B} > \widehat{ACB}$, a Proposição 3.3 nos assegura

que $\overline{C_2F_3} < \overline{CF}$, e por fim, da desigualdade (3.22) segue $\overline{C'F'} < \overline{CF}$, absurdo. Portanto os triângulos ABC e $A'B'C'$ são congruentes. \square

4 CONSTRUTIBILIDADE

Este capítulo é devotado à demonstração da impossibilidade de construção com régua e compasso de um triângulo, dados os comprimentos de suas bissetrizes internas. Seguimos a argumentação de (NETO e MAIA, 2017), nossa principal referência acerca deste resultado.

Mostraremos que se o triângulo for isósceles, a impossibilidade segue por um conjunto de resultados que apresentamos nas preliminares. E isto é suficiente para afirmarmos a impossibilidade de construção em geral, vejamos.

Consideremos um triângulo ABC , isósceles de base BC , com AM e BP suas bissetrizes internas, conforme mostra a Figura 45. Assumimos que sejam conhecidos os comprimentos $l = \overline{AB} = \overline{AC}$, $b = \overline{BC}$, $q = \overline{AM}$ e $p = \overline{BP}$.

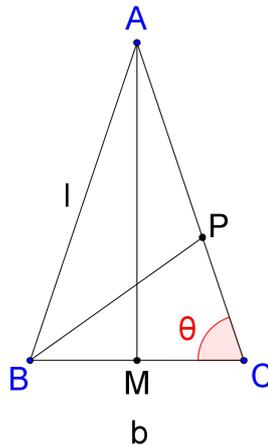


Figura 45 – Triângulo isósceles e duas de suas bissetrizes internas.

Observe que, sendo o triângulo ABC isósceles, temos que AM também é altura e mediana, logo segue pelo que discutimos no tópico “Relações Trigonômicas do Triângulo Retângulo” (Página 30), que

$$\cos(\theta) = \frac{b}{2l},$$

e aplicando o Teorema de Pitágoras no triângulo ACM obtemos $l^2 - \frac{b^2}{4} = q^2$ que implica em,

$$(2l + b)(2l - b) = 4q^2. \quad (4.1)$$

Aplicando o Teorema da Bissetriz (Proposição 2.2), com respeito a bissetriz interna BP , temos,

$$\frac{\overline{AP}}{\overline{CP}} = \frac{\overline{AB}}{\overline{BC}},$$

logo considerando $x = \overline{CP}$, obtemos

$$\frac{l - x}{x} = \frac{l}{b} \Rightarrow (l - x)b = xl \Rightarrow lb - xb = xl \Rightarrow x = \frac{bl}{b + l},$$

e pela Lei dos Cossenos (Proposição 2.3) segue do triângulo BPC que

$$p^2 = b^2 + x^2 - (2bx)\cos(\theta),$$

onde substituindo o valor de x e de $\cos(\theta)$, temos

$$\begin{aligned} p^2 &= b^2 + \left(\frac{bl}{b+l}\right)^2 - 2b\left(\frac{bl}{b+l}\right) \cdot \frac{b}{2l} = \\ &= \frac{b^2(b+l)^2 + b^2l^2 - b^3(b+l)}{(b+l)^2} = \\ &= \frac{b^2(b^2 + 2bl + l^2) + b^2l^2 - b^4 - b^3l}{(b+l)^2} = \\ &= \frac{b^4 + 2b^3l + b^2l^2 + b^2l^2 - b^4 - b^3l}{(b+l)^2} = \\ &= \frac{b^3l + 2b^2l^2}{(b+l)^2} = \\ &= \frac{b^2l(b+2l)}{(b+l)^2}, \end{aligned}$$

que dá

$$2l + b = \frac{p^2(b+l)^2}{b^2l}. \quad (4.2)$$

Substituindo o valor de $(2l + b)$ dado pela equação (4.2) acima na equação (4.1) temos,

$$\begin{aligned} \left(\frac{p^2(b+l)^2}{b^2l}\right)(2l-b) &= 4q^2 \Rightarrow \\ \Rightarrow p^2(b+l)^2(2l-b) &= 4q^2b^2l \Rightarrow \\ \Rightarrow (b^2 + 2bl + l^2)(2lp^2 - bp^2) - 4q^2b^2l &= 0 \Rightarrow \\ \Rightarrow (2b^2lp^2 + 4p^2bl^2 + 2p^2l^3) - (p^2b^3 + 2b^2lp^2 + p^2bl^2) - 4q^2b^2l &= 0 \Rightarrow \\ \Rightarrow 2p^2l^3 + 3p^2bl^2 - 4q^2b^2l - p^2b^3 &= 0. \end{aligned}$$

Dividindo esta última equação por b^3 obtemos

$$2p^2\left(\frac{l}{b}\right)^3 + 3p^2\left(\frac{l}{b}\right)^2 - 4q^2\left(\frac{l}{b}\right) - p^2 = 0.$$

Note que a menos de uma homotetia podemos supor $p = 1$, pois se um triângulo é construtível, então qualquer triângulo semelhante a ele também o é. Deste modo concluímos que $\frac{l}{b}$ é uma raiz do polinômio de terceiro grau,

$$f(X) = 2X^3 + 3X^2 - 4q^2X - 1.$$

Estabeleceremos agora a irredutibilidade de $f(X)$ em $\mathbb{Q}(q)[X]$, para algum $q > 0$. Para este fim, de agora em diante tomemos $q > 0$ transcendente.

Se $f(X)$ fosse redutível em $\mathbb{Q}(q)[X]$, poderia ser escrito da forma

$$f(X) = g_0(X)h_0(X),$$

onde $g_0(X), h_0(X) \in \mathbb{Q}(q)[X] - \mathbb{Q}(q)$, e como é um polinômio de grau 3, teríamos que $g_0(X)$ ou $h_0(X)$ seria de grau 1. Consideremos sem perda de generalidade que $\partial g_0(X) = 1$, ou seja, $g_0(X) = a_1X + a_0$ com $a_1, a_0 \in \mathbb{Q}(q)$ logo

$$f(X) = g_0(X)h_0(X) = (a_1X + a_0)h_0(X) = (X + \alpha)h_1(X),$$

onde $\alpha = a_0a_1^{-1} \in \mathbb{Q}(q)$ e $h_1(X) = a_1h_0(X) \in \mathbb{Q}(q)[X]$. Desta forma, temos que o polinômio $X + \alpha$ divide $f(X)$, e portanto, pela Proposição 2.10 segue que $\alpha \in \mathbb{Q}(q)$ é uma raiz de $f(X)$. Ou seja, existiriam $g(X), h(X) \in \mathbb{Q}[X] \setminus \{0\}$ tais que $\frac{g(q)}{h(q)} = \alpha$ com $f(\alpha) = 0$.

Aplicando o critério de pesquisa de raízes de $f(X)$ (discutido por meio da Proposição 2.12) pertencentes ao corpo $\mathbb{Q}(q)$, temos $g(q) \mid 1$ em $\mathbb{Q}(q)$. Assim sendo, podemos assumir que $g(q) = 1$, que implica em

$$\alpha = \frac{1}{h(q)},$$

e como $f(\alpha) = 0$ segue

$$2 \left[\frac{1}{h(q)} \right]^3 + 3 \left[\frac{1}{h(q)} \right]^2 - 4q^2 \left[\frac{1}{h(q)} \right] - 1 = 0,$$

que ao multiplicarmos por $[h(q)]^3$ obtemos

$$2 + 3h(q) - 4q^2[h(q)]^2 - [h(q)]^3 = 0,$$

que nos dá

$$2 + 3h(q) = [h(q)]^2[4q^2 + h(q)]. \quad (4.3)$$

Do item iii) da Proposição 2.14 seguido da Observação 2.3 temos que os anéis $\mathbb{Q}[q]$ e $\mathbb{Q}[X]$ são isomorfos, isto é, $\mathbb{Q}[q] \simeq \mathbb{Q}[X]$. Logo, como $h(q) \in \mathbb{Q}[q]$ segue que a equação (4.3) é equivalente a

$$2 + 3h(X) = [h(X)]^2[4X^2 + h(X)]. \quad (4.4)$$

Notemos que $4X^2 + h(X) \neq 0$ pois caso contrário teríamos pelo lado direito da equação acima que $h(X) = -4X^2$, ou seja $\partial h(X) = 2$. Mas pelo lado esquerdo $h(X) = \frac{-2}{3}$ que nos dá $\partial h(X) = 0$, absurdo. Uma vez que $4X^2 + h(X) \neq 0$ temos que o grau do lado esquerdo da equação é igual ao grau de $h(X)$ e o grau do lado direito é maior que duas vezes o grau de $h(X)$, um outro absurdo. Logo a equação (4.4) é impossível, e assim segue que o polinômio $f(X)$ não possui raiz em $\mathbb{Q}(q)$, desse modo é irredutível em $\mathbb{Q}(q)[X]$.

Agora, suponhamos por contradição que seja possível construir com régua e compasso o triângulo ABC , conhecendo os comprimentos $p = 1$ e q .

Pelo que apresentamos nas preliminares, temos que existe uma sequência finita de construções elementares que possibilita construir os lados do triângulo ABC , e pela Construção 2.1.1.10 segue que o segmento de comprimento $\frac{l}{b}$ é construtível.

Por outro lado, $\frac{l}{b}$ é construtível em $\mathbb{Q}(p, q) = \mathbb{Q}(q)$ implica, considerando a Proposição 2.19, no fato do grau da extensão $\mathbb{Q}(q)(l/b) | \mathbb{Q}(q)$ ser igual 1 ou 2, isto é, $[\mathbb{Q}(q, l/b) : \mathbb{Q}(q)] \leq 2$. No entanto, mostramos que $f(X)$ é irredutível em $\mathbb{Q}(q)[X]$, e pela Proposição 2.15 temos

$$[\mathbb{Q}(q, l/b) : \mathbb{Q}(q)] = 3.$$

Portanto o número $\frac{l}{b}$ não é construtível, contradizendo o fato de os segmentos de comprimentos l e b serem construtíveis.

5 CONCLUSÃO

Como vimos no decorrer do texto, para demonstrar os resultados objetivos centrais da dissertação, utilizamos elementos não só da Geometria, mas também da Álgebra Abstrata e da Análise. Juntos, estes elementos nos deram condições de realizarmos as demonstrações.

A Matemática de modo geral possui uma característica histórica que está se apresentando mais claramente em nossa contemporaneidade: por já termos um acúmulo muito grande de conhecimentos descobertos ou construídos, mais fortemente na atualidade percebemos o quanto estes conhecimentos, que se apresentam nas várias áreas da Matemática, se inter-relacionam, em alguns casos se complementando e em outros se constituindo como os mesmos elementos sob óticas diferentes.

Faz-se necessário compreendermos estas inter-relações para que o desenvolvimento científico desta arte (a Matemática) continue num movimento crescente.

Nesse aspecto, a quantidade de resultados expostos em função da construção das demonstrações objetivos do trabalho, e o fato de serem de diferentes áreas da Matemática, compõem um exemplo claro acerca da característica que citamos acima.

Acreditamos que a parte inicial deste texto possa ser utilizada como referência complementar, em um curso de construções geométricas voltado para a Educação Básica.

Consideramos ainda que o texto como um todo, constitui-se em uma referência a mais para o estudo dos elementos da Álgebra Abstrata em nível de graduação e pós-graduação, e como uma aplicação na Geometria Elementar de parte dos assuntos comumente tratados em disciplinas voltadas para o estudos de Estruturas Algébricas.

Esperamos que esta dissertação motive estudantes de Matemática em nível de graduação e pós-graduação a se atentarem para as relações existentes na construção e desenvolvimento da ciência matemática, até mesmo pela característica desta área do conhecimento de possibilitar tantos desenvolvimentos teóricos em diferentes direções.

REFERÊNCIAS

- ALENCAR FILHO, E. **Elementos de Teoria dos Anéis**. 1. Ed. São Paulo: NOBEL, 1990.
- BIAZZI, R. N. 2014. 74 fl. **Polinômios Irredutíveis: Critérios e Aplicações**. Dissertação (Mestrado em Matemática) - Instituto de Geociências e Ciências Exatas, Universidade Estadual Julio de Mesquita Filho, São Paulo/SP, 2014.
- BHATTACHARYA, P. B.; JAIN, S. K. e NAGPAUL, S. R. **Basic Abstract Algebra**. 2. ed. New York: Cambridge University, 1994.
- BRANDÃO, B. M. S. **Teorema do Ponto Fixo para Contrações**. [s.l.]: Universidade Federal de Maringá, 2007. Disponível em <<http://www.dma.uem.br/kit/20/ponto-fixo.pdf>>. Acesso em: 06/02/2018.
- BOLDRINI, José Luiz et al. **Álgebra Linear**. 3. ed. ampl e rev. São Paulo, SP: Harper & Row do Brasil, 1980.
- DINCA, G. e JEAN, M. **A constructive fixed point approach to the existence of a triangle with prescribed angle bisector lengths**. In: STEVIN, Simon. Belgian Mathematical Society - Simon Stevin. Bulletin, v. 17, n. 2, p. 333-341, 2010.
- EVES, H. **Introdução à História da Matemática**. Tradução de Hygino H. Domingues. 3. ed. São Paulo: UNICAMP, 2004.
- GARCIA, A. ; LEQUAIN, Y. **Elementos de Álgebra**. 5. ed. Rio de Janeiro: IMPA, 2001. (Projeto Euclides)
- GONÇALVES, A. **Introdução à Álgebra**. 5. ed. Rio de Janeiro: IMPA, 2013. (Projeto Euclides)
- HEFEZ, A. e VILLELA, M. L. T. **Polinômios e Equações Algébricas**. 1. ed. Rio de Janeiro: SBM, 2012. (Coleção PROFMAT)
- _____. **Introdução à Álgebra Linear**. 2. ed. Rio de Janeiro: SBM, 2016. (Coleção PROFMAT)
- LIMA, E. L **Curso de Análise**. v. 1. 14. ed. Rio de Janeiro: IMPA, 2016.
- _____. **Curso de Análise**. V. 2. 14. ed. Rio de Janeiro: IMPA, 2004.
- _____. **Álgebra Linear**. 7. ed. Rio de Janeiro: IMPA, 2005.
- MIRONESCU, P. e PANAITOPOL, L. **The existence of a triangle with prescribed angle bisector lengths**. American Mathematical Monthly, v. 101, p. 58-60, 1994.

MUNIZ NETO, A. C. **Tópicos de Matemática Elementar: polinômios**. Rio de Janeiro: SBM, 2016. (Coleção Professor de Matemática)

_____. **Geometria**. 1. ed. Rio de Janeiro: SBM, 2013. (Coleção PROFMAT)

MUNIZ NETO, A. C.; MAIA, A. D. **On the impossibility of constructing a triangle given its internal bisectors**. [s.l.]: Cornell University Library. Disponível em <<https://arxiv.org/pdf/1706.08508.pdf>>. Acesso em 15/02/2018.

OXIMAN, V. **A purely geometric proof of the uniqueness of a triangle with prescribed angle bisectors**. Forum Geometricorum, v. 8, p. 197-200, 2008.

REZENDE E. Q. F e QUEIROZ, M. L. B. de. **Geometria Euclidiana plana e construções geométricas**. 2. ed. São Paulo: UNICAMP, 2008.

WAGNER E.; CARNEIRO, Jose Paulo Q. **Construções Geométricas**. 6. ed. Rio de Janeiro: Sociedade Brasileira de Matemática, 2007. (Coleção Professor de Matemática)

APÊNDICE A - ALGUNS ELEMENTOS DE ANÁLISE

ALGUNS ELEMENTOS DE ANÁLISE QUE FORAM CITADOS NO TEXTO

Iniciamos enunciando o Princípio do Máximo e Mínimo (Max/min), conhecido como Teorema de Weierstrass, para funções reais.

Proposição A.1 (Teorema de Weierstrass). *Toda função real contínua $f : C \rightarrow \mathbb{R}$, onde C é um subconjunto não vazio, fechado e limitado de \mathbb{R}^n , possui pontos de máximo e mínimo. Ou seja, existem $X_0, X_1 \in C$ tais que $f(X_0) \leq f(X) \leq f(X_1), \forall X \in C$.*

O resultado que enunciamos a seguir é conhecido como Teorema de Bolzano-Weierstrass, sendo de muita importância na demonstração da existência de um triângulo dadas suas bissetrizes internas.

Proposição A.2 (Teorema de Bolzano-Weierstrass). *Toda sequência limitada do \mathbb{R}^n possui uma subsequência convergente.*

Outro resultado muito importante é o Teorema do Valor Médio, que enunciamos abaixo.

Proposição A.3 (Teorema do Valor Médio, de Lagrange). *Seja $f : [a, b] \rightarrow \mathbb{R}$ contínua. Se f é diferenciável em (a, b) , então existe $c \in (a, b)$, qual que*

$$f(b) - f(a) = (b - a)f'(c).$$

Finalizamos com a proposição abaixo, seguida de uma desigualdade que justificam implicações presentes na demonstração da existência.

Proposição A.4 (Desigualdade de Cauchy-Schwarz). *Se $X = (X_1, X_2, \dots, X_n)$ e $Y = (Y_1, Y_2, \dots, Y_n)$ pertencem a \mathbb{R}^n , então*

$$(X_1Y_1 + X_2Y_2 + \dots + X_nY_n)^2 \leq (X_1^2 + X_2^2 + \dots + X_n^2)(Y_1^2 + Y_2^2 + \dots + Y_n^2).$$

Prova: Temos,

$$(X_1Y_1 + X_2Y_2 + \dots + X_nY_n)^2 = \sum_i X_i^2 Y_i^2 + \sum_{i < j} 2X_i Y_i X_j Y_j \tag{A.1}$$

$$\leq \sum_i X_i^2 Y_i^2 + \sum_{i < j} X_i^2 Y_j^2 + X_j^2 Y_i^2 \tag{A.2}$$

$$= \sum_{i,j} X_i^2 Y_j^2 \tag{A.3}$$

$$= (X_1^2 + X_2^2 + \dots + X_n^2)(Y_1^2 + Y_2^2 + \dots + Y_n^2) \tag{A.4}$$

Da igualdade (A.1) para desigualdade (A.2) usamos o fato de que se $a, b \in \mathbb{R}$ então $a^2 + b^2 \geq 2ab$, pois $(a - b)^2 \geq 0$. □

Com a desigualdade de Cauchy-Shwarz mostramos facilmente que

$$\|X + Y\| \leq \|X\| + \|Y\|, \quad (\text{A.5})$$

para todos $X, Y \in \mathbb{R}^n$, chamada de desigualdade triangular.

Vejamos que vale a desigualdade abaixo.

$$\left| \|X\| - \|Y\| \right| \leq \|X - Y\|, \quad (\text{A.6})$$

para todos X e Y pertencentes a \mathbb{R}^n . De fato, escrevendo $X = (X - Y) + Y$ temos $\|X\| = \|(X - Y) + Y\|$ que pela desigualdade triangular nos dá $\|X\| \leq \|X - Y\| + \|Y\|$, ou seja, $\|X\| - \|Y\| \leq \|X - Y\|$. De modo análogo, $\|Y\| - \|X\| \leq \|Y - X\|$, o que implica em $\left| \|X\| - \|Y\| \right| \leq \|X - Y\|$, pois $\|(X - Y)\| = \|(Y - X)\|$, $\forall X, Y \in \mathbb{R}^n$.