UNIVERSIDADE FEDERAL RURAL DE PERNAMBUCO
DEPARTAMENTO DE MATEMÁTICA
Mestrado Profissional em Matemática em Rede Nacional

MARCOS JOSÉ MIGUEL

CONSTRUÇÕES COM RÉGUA E COMPASSO

RECIFE
2018

UNIVERSIDADE FEDERAL RURAL DE PERNAMBUCO
DEPARTAMENTO DE MATEMÁTICA
Mestrado Profissional em Matemática em Rede Nacional

MARCOS JOSÉ MIGUEL

CONSTRUÇÕES COM RÉGUA E COMPASSO

Dissertação de mestrado apresentada ao Departamento de Matemática da Universidade Federal Rural de Pernambuco como requisito parcial para obtenção do título de Mestre em Matemática.

Orientador: Prof. Dr. RODRIGO JOSÉ GONDIM NEVES

RECIFE
2018

Dados Internacionais de Catalogação na Publicação (CIP)
Sistema Integrado de Bibliotecas da UFRPE
Biblioteca Central, Recife-PE, Brasil

M636c Miguel, Marcos José
Construções com régua e compasso / Marcos José Miguel. – 2018.
101 f. : il.

Orientador: Rodrigo José Gondim Neves.
Dissertação (Mestrado) – Universidade Federal Rural de Pernambuco, Mestrado Profissional em Matemática, Recife, BR-PE, 2018.
Inclui referências e apêndice(s).

1. Construções geométricas 2. Quadratura do círculo 3. Polígonos 4. Cubo 5. Ângulo 6. Régua de cálculo I. Neves, Rodrigo José Gondim, orient. II. Título

CDD 510

CONSTRUÇÕES COM RÉGUA E COMPASSO

MARCOS JOSÉ MIGUEL

Dissertação APROVADA, em 19/10/2018, como requisito parcial para obtenção do título de Mestre no Curso de Pós-Graduação Mestrado Profissional em Matemática em rede Nacional - PROFMAT, polo UFRPE - pela seguinte comissão examinadora:

Orientador:

Prof. Dr. RODRIGO JOSÉ GONDIM NEVES

Banca examinadora:

Profa. Dra. BÁRBARA COSTA DA SILVA
PROFMAT/UFRPE

Prof. Dr. ROBERTO CALLEJAS BEDREGAL
PROFMAT/UFPB

RECIFE
2018

Dedico às minhas filhas, Marília Silva Miguel e Letícia Silva Miguel, por serem a razão da minha vida.

Agradecimentos

A Deus pelo dom da existência e o enigma da graça.

Aos meus pais José Augusto Miguel e Lindalva Clotildes Miguel (*in memorian*).

Ao Professor Reginaldo Gomes da Silva que me fez apaixonar pelo estudo e ensino da matemática. Tornei-me professor de matemática graças a ele, primeiro a me mostrar em sala de aula, com suas aulas descontraídas e excelente didática, a beleza da matemática.

Ao Professor PhD Antônio Carlos Rodrigues Monteiro pelo estímulo permanente antes e durante a elaboração desta dissertação, bem como a constante inspiração, orientações e o paciente apoio proporcionados, sem os quais esta dissertação não teria sequer sido escrita.

A todos os professores do mestrado PROFMAT da UFRPE, em especial ao professor e orientador Rodrigo José Gondin Neves e à coordenadora, professora Bárbara Costa da Silva, pela dedicação e disponibilidade.

Ao Professor Dogival Maurício por sua ajuda Latexnicas durante a digitação desse trabalho.

Ao Professor de Língua Portuguesa Luiz Antônio de Oliveira Lima pelas leituras e correções.

A todos os colegas de turma do PROFMAT pelo incentivo, em especial aos amigos José Ribamar de Souza Neves e Murilo Ramos da Cunha Ribeiro, parceiros de estudos, pelas suas contribuições. Sou grato ao amigo Ribamar Neves por sua incansável ajuda durante a produção das figuras contidas nessa dissertação.

A Maria Rosa Vieira Barbosa pelo incentivo e paciência nos momentos de ausência os quais dediquei a escrever este trabalho.

Aos meus amigos Carlos Antônio Nery da Silva, Cláudio Francisco Lima, Clebson Ponciano da Silva, Éveny Emidio da Silva, Filipe Régis Acioli de Melo, Laís Santiago França, Luiz Carlos Gomes Rodrigues, Márcio Henrique Augusto Gomes, Mauro Bessa de Menezes, Paulo Tadeu Fonseca Pinto, Rafael Marinho de Albuquerque, Rivaldo Ferreira Barboza Filho, Rodrigo Lucas Tenório Calazans de Lira, Rogério dos Santos Mendes, os quais sempre me ajudaram proporcionando tempo e incentivo.

Arquimedes será lembrado enquanto Ésquilo foi esquecido, porque os idiomas morrem mas as ideias matemáticas permanecem. Imortalidade pode ser uma ideia tola, mas provavelmente um matemático tem a melhor chance que pode existir de obtê-la.
G. H. HARDY

Declaração

Eu, **MARCOS JOSÉ MIGUEL**, declaro para devidos fins e efeitos, que a dissertação sob título **CONSTRUÇÕES COM RÉGUA E COMPASSO**, entregue como Trabalho de Conclusão de Curso para obtenção do título de mestre, com exceção das citações diretas e indiretas claramente indicadas e referenciadas, é um trabalho original. Eu estou consciente que a utilização de material de terceiros incluindo uso de paráfrase sem a devida indicação das fontes será considerado plágio, e estará sujeito à processo administrativos da Universidade Federal Rural de Pernambuco e sanções legais. Declaro ainda que respeitei todos os requisitos dos direitos de autor e isento a Pós-graduação PROFMAT/UFRPE, bem como o orientador **Prof. Dr. RODRIGO JOSÉ GONDIM NEVES**, de qualquer ônus ou responsabilidade sobre a sua autoria.

Recife, 19 de Outubro de 2018.

MARCOS JOSÉ MIGUEL

Resumo

Os problemas de construções sempre ocuparam posição de destaque na Geometria. Apenas com o uso de régua e compasso podemos executar uma diversidade enorme de construções e em todas essas construções, a régua é utilizada apenas para traçar retas. Apesar de os gregos utilizarem outros instrumentos, a restrição clássica à utilização apenas da régua e do compasso era para eles um assunto de grande importância. Entre os problemas de construção com régua e compasso, o de construir um polígono regular de n lados é provavelmente o de maior interesse. As construções do triângulo equilátero, do quadrado, do pentágono regular e do hexágono regular são conhecidas desde a Antiguidade e ocupam (ou já ocuparam) posição de destaque no estudo da geometria nas escolas. No entanto, para alguns polígonos regulares essas construções (apenas com o uso de régua e compasso) não são possíveis. Como exemplo inicial podemos citar o heptágono regular. Existem outros problemas de construções que merecem posição de destaque e para os quais uma construção com régua e compasso não é possível. Como exemplos podemos citar os três problemas clássicos dos gregos: a duplicação do cubo (ou a construção da aresta de um cubo cujo volume é o dobro do de um cubo de aresta dada), a trissecção de um ângulo qualquer (ou a construção de dividir um ângulo arbitrário dado, em três partes iguais) e a quadratura do círculo (ou a construção de um quadrado com área igual à área de um círculo dado). A importância do estudo desses problemas reside no fato de que eles não podem ser resolvidos com régua e compasso apenas, apesar desses instrumentos serem utilizados para resolver muitos outros problemas de construção. A tentativa de encontrar solução para esses problemas influenciou a geometria grega, levando a descobertas importantes. Como exemplos dessas descobertas podemos citar as secções cônicas, algumas curvas cúbicas e quárticas e várias curvas transcendentes. Posteriormente um resultado de grande importância foi o desenvolvimento da teoria das equações ligadas a domínios de racionalidade, números algébricos e teoria dos grupos. Notamos com isso que a tentativa de resolver problemas como esses sem solução resultou em um dos mais significativos desenvolvimentos da Matemática. A proposta dessa dissertação é mostrar algumas construções clássicas, como a do heptadecágono regular e tratar da impossibilidade da construção por meio de régua e compasso, tais como duplicação de um cubo, trissecção de um ângulo, quadratura de um círculo (nesse caso faremos apenas a indicação da prova) e construções de polígonos regulares.

Palavras-chave: Construções geométricas, construções com régua e compasso, trissecção de um ângulo, duplicação do cubo, quadratura do círculo, construção de polígonos regulares, ciclotomia.

Abstract

The problems of constructions have always occupied a prominent position in geometry. Only with the use of ruler and compass we can carry out a huge diversity of constructions and in all these constructions, the ruler is used only to draw straight lines. Although the greeks use other instruments, the classical restriction to the use of only the ruler and the compass was a matter of great importance to them. Among the problems of constructions with ruler and compass, that of constructing a regular polygon of n sides is probably of greater interest. The constructions of the equilateral triangle, the square, the regular pentagon and the regular hexagon have been known since Antiquity and occupy (or have occupied) position in the study of geometry in schools. However, for some regular polygons this construction (only with the use of ruler and compass) is not possible. As example we can mention the regular heptagon. There are other construction problems that deserve prominent position and for which a construction with ruler and compass is not possible. As examples we can mention the three classic problems of the Greeks: the duplication of the cube (or the construction of the edge of a cube whose volume is the double of that of a cube of a given angle), the trisection of any angle (or the construction of dividing an arbitrary angle in three equal parts) and the quadrature of the circle (or the construction of a square with area equal to the area of a given circle). The importance of studying these problems lies in the fact that they cannot be solved with ruler and compass only, although these instruments are used to solve many other construction problems. The attempt to find a solution to these problems influenced greek geometry, leading to important discoveries. As examples of these discoveries we can mention: the conic sections, some cubic and quartic curves and several transcendent curves. Subsequently a result of great importance was the development of the theory of equations related to domains of rationality, algebraic numbers and group theory. We note that attempting to solve problems like these without solution has resulted in one of the most significant developments in mathematics. The purpose of this dissertation is to show some classic constructions, as the case of the regular polygon of seventeen sides, and to deal with the impossibility of construction by means of ruler and compass, such as: duplication of a cube, trisection of an angle, quadrature of a circle (in this case we will only indicate the proof) and constructions of regular polygons.

Key-word: Geometric constructions, constructions with ruler and compass, trisection of an angle, duplication of the cube, quadrature of the circle, construction of regular polygons, cyclotomy.

Lista de ilustrações

Sumário

INTRODUÇÃO

A fim de alcançar um público tão amplo quanto possível (presumindo-se apenas conhecimentos gerais obtidos em um curso de álgebra básica, disciplina dos cursos de graduação em matemática), nenhuma tentativa foi feita para atingir o nível de generalidade, precisão e integridade que são as marcas das dissertações de mestrado acadêmico em matemática. O foco será, antes, nas ideias, conceitos e técnicas, que serão apresentados apenas quando forem relevantes para o desenvolvimento da teoria necessária para prova do teorema sobre a construtibilidade dos polígonos regulares. Nessa dissertação, provas complicadas, como a da impossibilidade da quadratura do círculo e da recíproca do teorema que dá uma condição necessária para que um polígono regular de n lados seja construtível não puderam ser contempladas. Porém, as provas são, sem dúvida, a estrutura de qualquer envolvimento sério com a matemática. Na intenção do comprometimento, referências de onde encontrar as provas que foram omitidas são mencionadas.

O primeiro capítulo inicia-se com as regras básicas da construção geométrica com régua e compasso, as quais denominamos de regras do jogo, e sua interpretação algébrica. Aqui, a régua considerada não possui marcações, é apenas um instrumento que permite ligar dois pontos do plano. Procuramos esclarecer o que devemos entender por construção geométrica com régua e compasso apenas. Apresentamos também as construções geométricas clássicas, que já eram conhecidas pelos matemáticos gregos desde a antiguidade, seguidas pela álgebra das construções geométricas com régua e compasso. Finalizamos esse capítulo tratando de algo que está intimamente ligado às construções com régua e compasso, as extensões quadráticas. O segundo capítulo inicia-se com uma abordagem sobre corpos e suas extensões, sendo seu ponto alto o grau dessas extensões. Para o desenvolvimento dessa abordagem, fazemos uma revisão das definições e dos resultados de álgebra linear necessários para essa teoria. No terceiro capítulo, falamos sucintamente sobre polinômios irredutíveis, os quais desempenham o mesmo papel dos números primos no conjuntos dos números inteiros. Será apresentado, sem demonstração, o análogo ao Teorema da Fatoração Única no conjunto dos inteiros. Finalizando com o lema de Gauss e o teste de Eisenstein para a verificação da irredutibilidade de um polinômio sobre o conjuntos dos números racionais. O quarto capítulo inicia-se com o resultado que diz quando as raízes de uma equação cúbica são construtíveis por régua e compasso, seguido das provas da impossibilidade de resolver dois dos três problemas clássicos de construção (o problema da duplicação do cubo e o problema da trissecção de um ângulo arbitrário) deixados sem solução pelos gregos. No caso do terceiro problema clássico

de construção, a quadratura do círculo, fazemos apenas a indicação da prova. Em seguida, apresentamos as provas da não construtibilidade do heptágono e do eneágono regulares e as provas da construtibilidade do pentágono e do heptadecágono regulares. Damos um exemplo de um número algébrico de grau quatro que não é construtível com régua e compasso, seguido de uma caracterização dos números algébricos com grau uma potência de dois que são construtíveis. Apresentamos os primos de Fermat, os quais estão intimamente relacionados com os polígonos regulares construtíveis por régua e compasso, encerrando com dois casos um pouco gerais de polígonos construtíveis. O capítulo final, ponto alto dessa dissertação, apresenta as ferramentas necessárias para a demonstração da condição necessária do teorema de Gauss sobre polígonos regulares construtíveis por régua e compasso. Iniciamos com a função phi de Euler e caracterizamos em seguida os inteiros cuja imagem pela função phi de Euler é uma potência de dois. Tratamos das raízes n-ésimas de um número complexo, especialmente das raízes n-ésimas primitivas da unidade. Abordamos o polinômio ciclotômico, cujas raízes são as raízes n-ésimas primitivas da unidade. Este polinômio é uma peça de fundamental importância na construção da prova do teorema de Gauss. Finalizamos o capítulo com a prova da condição necessária do teorema de Gauss sobre quais polígonos regulares são construtíveis por régua e compasso. A condição suficiente não será provada, pois a prova depende de resultados básicos sobre grupos e de Teoria de Galois.

1 CONSTRUÇÕES COM RÉGUA E COMPASSO

O que se entende por construção geométrica com régua e compasso é algo que devemos esclarecer completamente antes de abordarmos problemas de construção. Se quisermos saber o que podemos construir com a régua (sem marcas) e o compasso apenas, temos que tornar preciso o que entendemos por construir. Temos que expressar em linguagem matemática o que podemos fazer com nossos instrumentos de construção.

1.1 AS REGRAS DO JOGO

Com a régua (sem marcas), podemos desenhar uma reta desde que sejam fornecidos dois pontos da reta. Algo que devemos enfatizar é que uma régua pode ser usada apenas para desenhar a reta passando por dois pontos dados e não pode ser usada para medir o comprimento. Esta é uma regra do jogo. Nossas construções serão feitas no chamado plano cartesiano.

Nada será feito de modo aleatório. No intuito de não deixar nada solto, para melhor acompanhar o que está acontecendo, não será permitido selecionar um ponto aleatoriamente e a qualquer momento; qualquer ponto selecionado já deve ter sido construído. Por outro lado, em primeiro lugar, devemos ter dois pontos dados a fim de usar a régua ou o compasso. Segue-se que devemos necessariamente partir de um conjunto formado por pelo menos dois pontos, a partir dos quais podemos construir novos pontos com nossos instrumentos. Daremos a seguir uma descrição de todos esses pontos adicionais que poderíamos teoricamente construir. Os pontos adicionais são obtidos por meio das interseções de retas e circunferências que podem ser construídas a partir do conjunto de pontos que temos a qualquer momento. O ponto adicional deve ser um ponto de:

i) a intersecção de duas retas construídas;

ii) a intersecção de uma reta construída e uma circunferência construída; ou

iii) a intersecção de duas circunferências construídas.

A seguir faremos cuidadosamente a definição de um ponto construtível com régua e compasso. A definição deve modelar o que é que podemos fazer com a régua e o compasso para formar novos pontos a partir do conjunto inicial $S_0 = \{(0,0),(1,0)\}$.

Definição 1. No plano cartesiano, um ponto é construtível se o ponto for o último de uma sequência finita de pontos P_1, P_2, $\cdots$, P_n de forma que cada ponto pertença ao conjunto $S_0 = \{(0,0),(1,0)\}$ ou seja obtido de uma das seguintes formas:

i) como a intersecção de duas retas, cada uma das quais passa por dois pontos que já apareceram anteriormente na sequência;

ii) como um ponto de intersecção de uma reta que passa por dois pontos que já apareceram anteriormente na sequência e de uma circunferência que passa por um ponto que já apareceu na sequência e tendo como centro um ponto que já apareceu na sequência; e

iii) como ponto de intersecção de duas circunferências, cada uma das quais passa por um ponto que já apareceu anteriormente na sequência e cada uma delas tem como centro um ponto que já apareceu anteriormente na sequência.

Definição 2. Uma reta construtível é uma reta que passa por dois pontos construtíveis.

Definição 3. Uma circunferência construtível é uma circunferência que passa por um ponto construtível e tem como centro um ponto construtível.

Definição 4. Um número α é um número construtível se $(\alpha, 0)$ for um ponto construtível.

A seguir apresentamos oito sequências que são exemplos que satisfazem a condição sobre P_1, P_2, $\cdots$, P_n na definição de ponto construtível acima.

$(0,0)$

$(1,0)$

$(0,0),(1,0)$

$(1,0),(0,0),(2,0)$

$(0,0),(1,0),(-1,0),(0,\sqrt{3})$

$(0,0),(1,0),(2,0),(-2,0),(0,\sqrt{5})$

$(0,0),(1,0),(1/2,\sqrt{3}/2),(1/2,-\sqrt{3}/2),(1/2,0)$

$(0,0),(1,0),(2,0),(1/4,\sqrt{15}/4),(1/2,0)$

Além disso, podemos juntar duas ou mais dessas sequências para formar uma nova sequência que também satisfaz a condição sobre P_1, P_2, $\cdots$, P_n na definição de ponto construtível acima. Por exemplo, vamos formar uma nova sequência juntando a última sequência acima ao final da sexta sequência como a seguir:

$$(0,0),(1,0),(2,0),(-2,0),(0,\sqrt{5}),(0,0),(1,0),(2,0),(1/4,\sqrt{15}/4),(1/2,0)$$

Não há problema se alguns pontos aparecem mais de uma vez na sequência obtida anteriormente, o que importa é que a sequência de pontos satisfaz a condição necessária de que cada ponto pertença a $S_0 = \{(0,0),(1,0)\}$ ou seja obtido de uma das três maneiras mencionadas em i), ii) e iii) na definição 1.

A seguir, veremos que a definição 1 fornece as propriedades fundamentais de interseção de retas construtíveis e circunferências construtíveis.

Proposição 1.1.1. *O ponto de intersecção de duas retas construtíveis é um ponto construtível; um ponto de intersecção de uma reta construtível e uma circunferência construtível é um ponto construtível; e um ponto de intersecção de duas circunferências construtíveis é um ponto construtível.*

Demonstração. Suponha que a sequência finita de pontos Q_1, Q_2, $\cdots$, Q_m satisfaz as condições da definição 1. Isso significa que para cada um dos Q_i temos $Q_i = (0,0)$, $Q_i = (1,0)$, ou Q_i é obtido em uma das três maneiras denotadas por i), ii) e iii) na definição 1. Suponha que T é um ponto de intersecção de duas retas construtíveis, um ponto de intersecção de uma reta construtível e uma circunferência construtível, ou um ponto de intersecção de duas circunferências construtíveis. Agora, i) se o ponto T é um ponto de intersecção de duas retas construtíveis, então existem pontos construtíveis P, Q, R, S tais que T é um ponto na interseção da reta por P e Q e da reta por R e S; ii) se o ponto T é um ponto de interseção de uma reta construtível e uma circunferência construtível, então existem pontos P, Q, R, S tais que T é um ponto na interseção da reta por P e Q e a circunferência determinada por R e S; e iii) se o ponto T é um ponto de intersecção de duas circunferências construtíveis, então existem pontos construtíveis P, Q, R, S tais que T é um ponto na intersecção da circunferência determinada por P e Q e a circunferência determinada por R e S . Segue que, em qualquer um desses três casos, há uma sequência P_1, P_2, $\cdots$, P; uma sequência Q_1, Q_2, $\cdots$, Q; uma sequência R_1, R_2, $\cdots$, R;e a sequência S_1, S_2, $\cdots$, S tais que cada uma das quatro sequências satisfaz as condições da definição 1. Então a sequência P_1, P_2, $\cdots$, P, Q_1, Q_2, $\cdots$, Q, R_1, R_2, $\cdots$, R, S_1, S_2, $\cdots$, S deve satisfazer as condições da definição 1. Portanto, em qualquer um dos três casos, a sequência P_1, P_2, $\cdots$, P, Q_1, Q_2, $\cdots$, Q, R_1, R_2, $\cdots$, R,

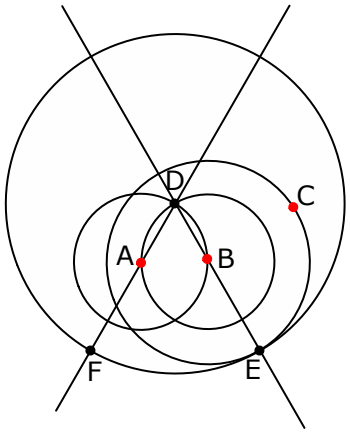
S_1, S_2, $\cdots$, S, T também satisfaz as condições da definição 1, e T é um ponto construtível de acordo com a definição 1.

■

Proposição 1.1.2. *A circunferência com centro construtível e raio a distância entre dois pontos construtíveis é construtível.*

Demonstração. Sejam A, B e C três pontos construtíveis (veja figura 1). Considere D um ponto de interseção da circunferência de centro em A e que passa por B e da circunferência com centro em B e que passa por A. Pela definição 3 essas circunferências são construtíveis. Segue da proposição anterior que D é um ponto construtível. Seja E o ponto de interseção da circunferência com centro em B e que passa por C e a reta que passa por D e B tal que B está entre D e E. Então, E é um ponto construtível, pois E é um ponto de interseção da circunferência construtível, com centro em B e que passa por C, e a reta construtível que passa por D e B. Seja F o ponto de interseção da circunferência com centro em D e que passa por E e a reta que passa por D e A. Como F é um ponto de interseção da circunferência construtível com centro em D e que passa por E e a reta construtível que passa por D e A, então F é um ponto construtível. Como os segmentos de reta BC e AF são iguais, então a circunferência com centro em A e raio a distância entre os pontos B e C e a circunferência com centro em A e que passa por F são iguais. Como a circunferência com centro em A e que passa por F é construtível, então a circunferência com centro em A e raio a distância entre os pontos B e C é construtível.

Figura 1 – Circunferência com centro construtível e raio a distância entre dois pontos construtíveis

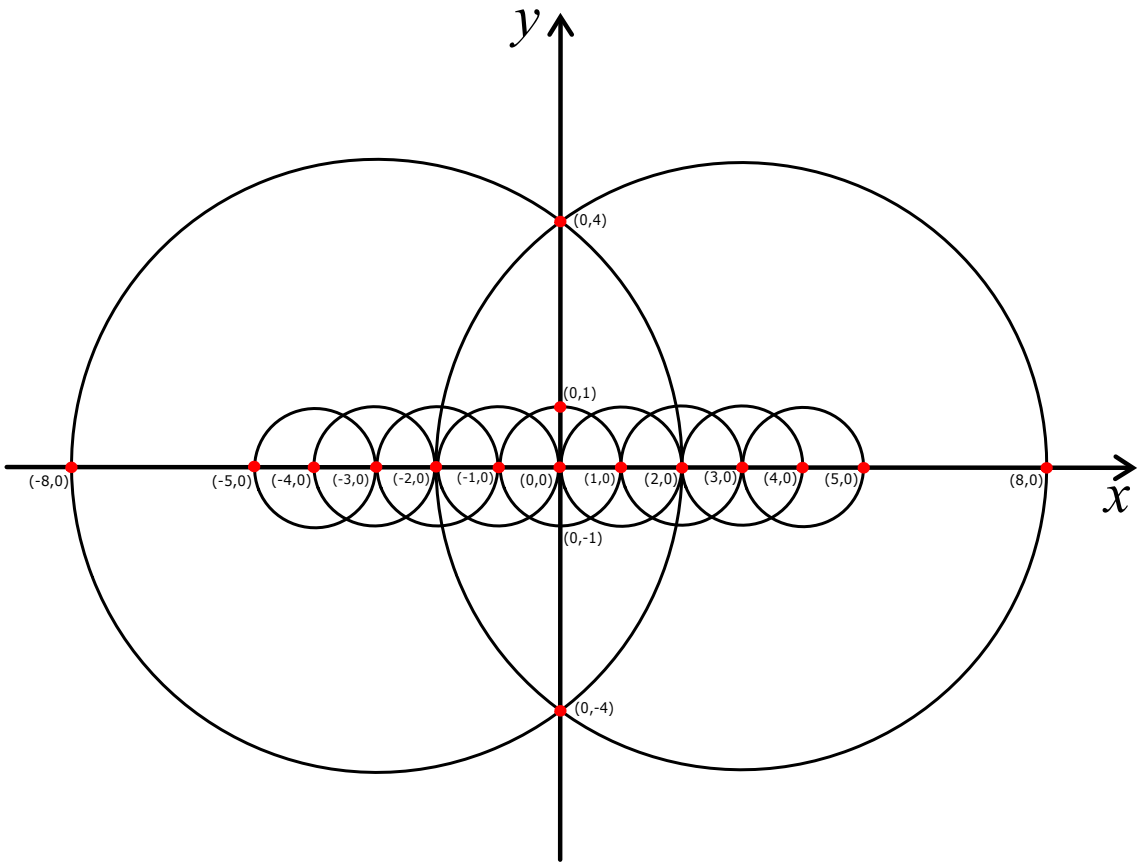


Fonte: Produzida pelo autor

■

Agora, precisamos distinguir entre todos os pontos (x, y) do plano cartesiano, aqueles que são os pontos construtíveis. Faremos isso no desenrolar da teoria. Começamos com os dois pontos $(0, 0)$ e $(1, 0)$. Isso significa que o eixo X é uma reta construtível. Segue que o ponto $(-1, 0)$ é construtível, pois este ponto está na interseção do eixo X e a circunferência construtível com centro $(0, 0)$ e que passa por $(1, 0)$. Segue de imediato que os pontos $(n, 0)$, em que n é um inteiro positivo ou negativo, são construtíveis. Para construí-los, desenhamos sucessivas circunferências com centros nos pontos $(0, 0)$, $(1, 0)$, $(-1, 0)$, $(2, 0)$, $(-2, 0)$, $(3, 0)$, $(-3, 0)$, $\cdots$, $(n, 0)$, $\cdots$.

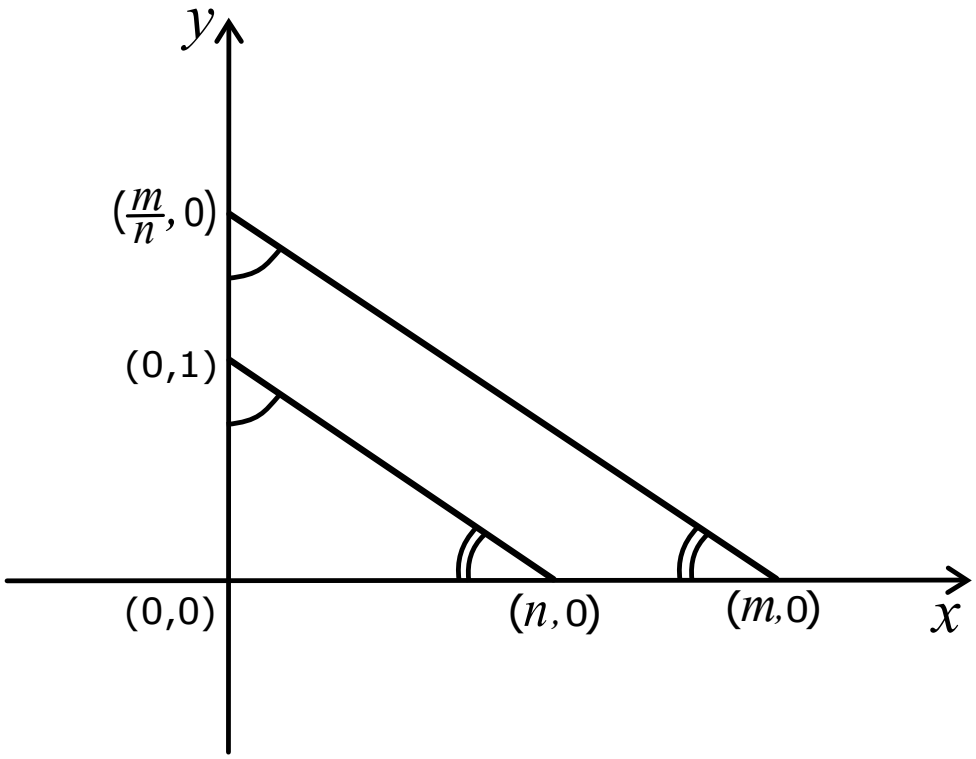
Figura 2 – Construção de pontos



Fonte: Produzida pelo autor

Note que desenhando circunferências com centros em $(3, 0)$ e $(-3, 0)$, passando por $(-2, 0)$ e $(2, 0)$, respectivamente, obtemos os pontos $(8, 0)$, $(-8, 0)$, $(0, 4)$ e $(0, -4)$. Dessa forma podemos obter os pontos $(0, m)$, em que m é número inteiro positivo ou negativo. De modo geral, dado um par de inteiros n e m, utilizando o método anterior, podemos construir o ponto (n, m) utilizando um número finito de passos. Também é possível, de acordo com a figura a seguir, construir o ponto $(m/n, 0)$.

Figura 3 – Construção do ponto $(m/n, 0)$



Fonte: Produzida pelo autor

A proposição a seguir generaliza as construções imediatamente acima.

Proposição 1.1.3. *i) Os eixos coordenados X e Y são retas construtíveis.*

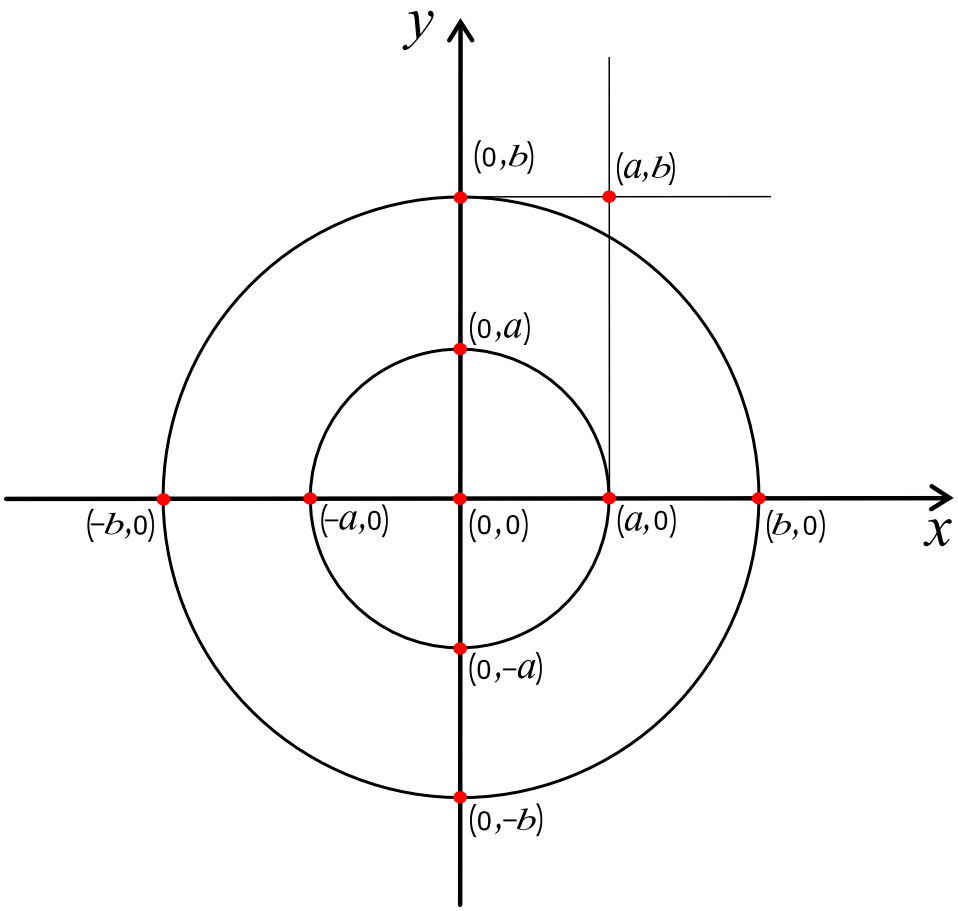
ii) Todos os pontos $(a, 0)$, $(-a, 0)$, $(0, a)$ e $(0, -a)$ são pontos construtíveis se qualquer um deles for um ponto construtível.

iii) O número α é um número construtível se, e somente se, $-\alpha$ é um número construtível.

iv) Os números inteiros são números construtíveis. O ponto (a, b) é um ponto construtível se, e somente se, os números a e b são números construtíveis.

Demonstração. Como podemos construir perpendiculares e paralelas por métodos euclidianos (isso veremos adiante), a proposição é evidente, considerando a figura a seguir.

Figura 4 – Alguns pontos construtíveis



Fonte: Produzida pelo autor

■

Vale ressaltar que o fato de que o eixo X é uma reta construtível não implica que todos os pontos no eixo X sejam pontos construtíveis. Analogamente, nem todo ponto em uma circunferência construtível é um ponto construtível.

1.2 CONSTRUÇÕES CLÁSSICAS

Esta seção tratará da resolução de alguns problemas geométricos clássicos. Geralmente esses problemas pedem para determinar se certas construções geométricas são possíveis utilizando apenas régua e compasso. Isso significa que nem sempre se trata de resolver problemas de desenho geométrico, mas apenas de responder se é possível ou não resolver o problema geométrico apenas usando uma régua (sem marca) e um compasso. Dentre as construções

geométricas que os gregos eram capazes de realizar apenas com o uso de régua (sem marca) e compasso, utilizando os postulados de Euclides, destacam-se as seguintes:

1. Dados um ponto P e uma reta s, traçar, passando pelo ponto P, uma reta perpendicular à reta s.

   Solução:

   Temos dois casos:

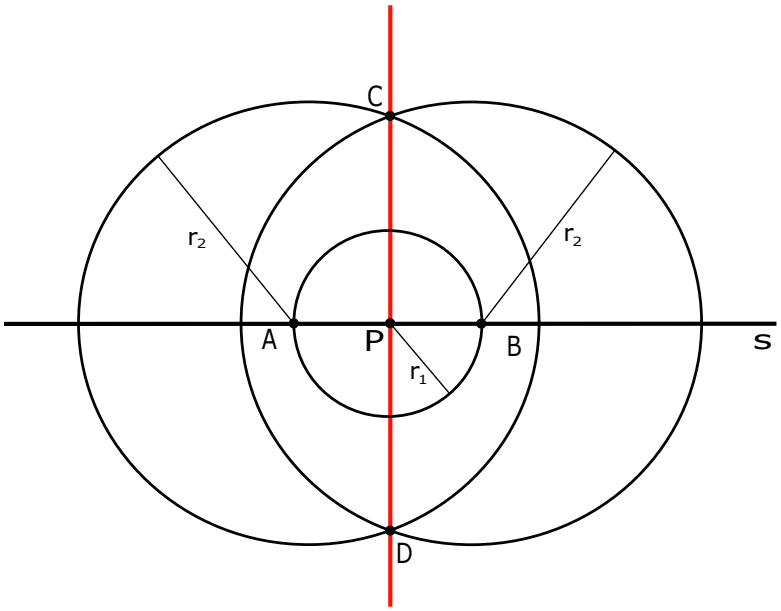
   a) O ponto P pertence à reta s,

   b) O ponto P não pertence à reta s.

   A construção a seguir abrange os dois casos.

   Trace uma circunferência com centro em P e raio r_1, que intersecte a reta em dois pontos A e B. Com centro em cada um desses pontos de intersecção trace uma circunferência de raio $r_2 > r_1$. Essas duas circunferências se intersectam em dois pontos C e D. A reta passando por C e D é a reta perpendicular à reta s passando por P.

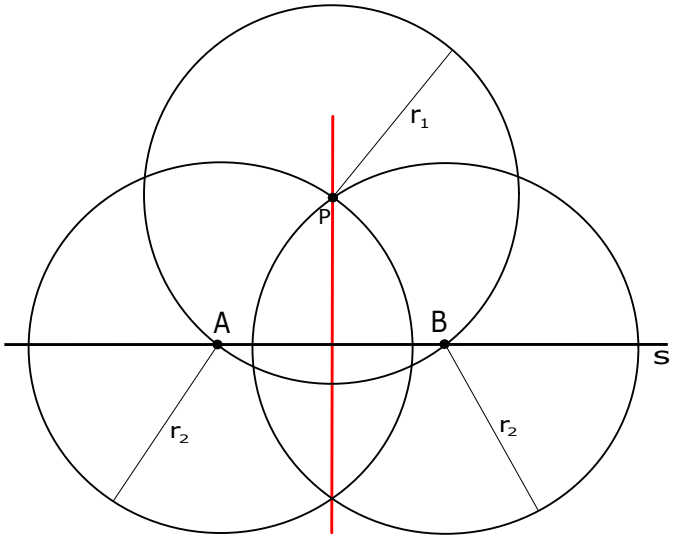
Figura 5 – Uma reta passando por um ponto P e perpendicular a uma reta s quando P pertence a s



Fonte: Produzida pelo autor

Note que se P não pertence à reta s, é suficiente considerar $r_1 = r_2$, quando um dos pontos de intersecção das duas circunferências traçadas por último é P.

Figura 6 – Uma reta passando por um ponto P e perpendicular a uma reta s quando P não pertence a s



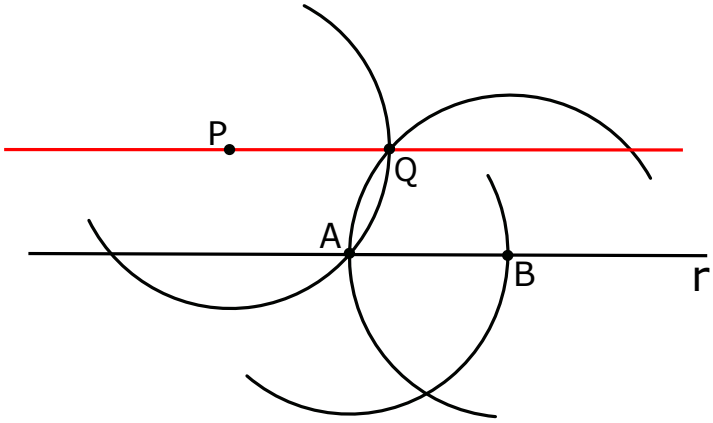
Fonte: Produzida pelo autor

2. Dados uma reta r e um ponto P que não pertence a r, traçar, passando por P, uma reta paralela à reta r.

   Solução:

   Trace três circunferências de mesmo raio. A primeira com centro em P, determinando um ponto A na reta r; a segunda com centro em A, determinando um ponto B na mesma reta e a terceira com centro em B, determinando um ponto Q na primeira circunferência. A reta s por P e Q é paralela à reta r, pois, da maneira como a construção foi executada, $PABQ$ é um losango e, portanto, seus lados PQ e AB são paralelos.

Figura 7 – Reta passando por um ponto P e paralela a uma reta r



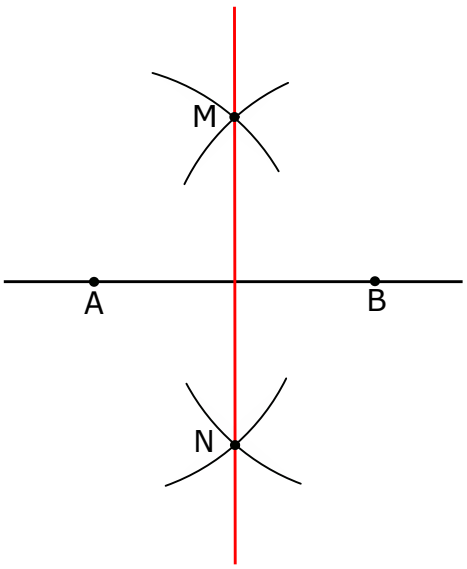
Fonte: Produzida pelo autor

3. Dado um segmento de reta AB , construa a sua mediatriz.

Solução:

A *mediatriz* do segmento AB é a reta perpendicular a AB que contém o seu ponto médio. *Para sua construção, trace duas circunferências de mesmo raio, com centros em A e B. Sejam M e N os pontos de interseção dessas circunferências. A reta que contém M e N é a mediatriz do segmento AB pois sendo $AMBN$ um losango, suas diagonais são perpendiculares em seus pontos médios.*

Figura 8 – Mediatriz de um segmento de reta



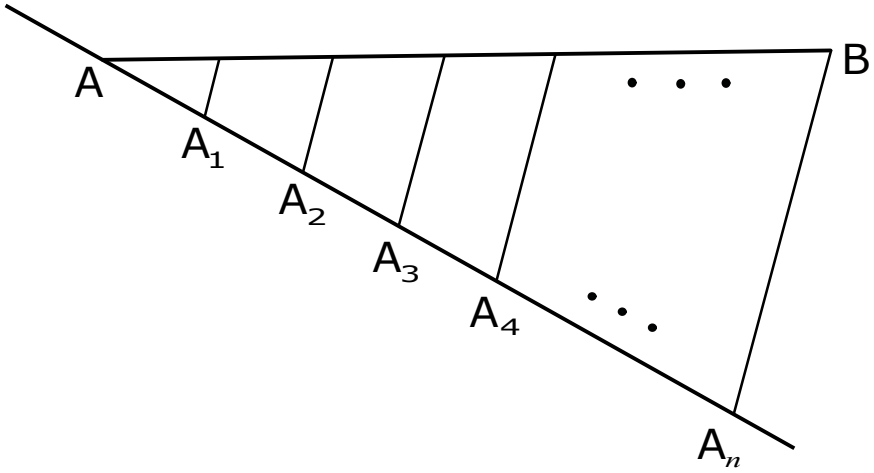
Fonte: Produzida pelo autor

4. Dado um segmento de reta AB (A e B construtíveis), divida-o em n partes iguais.

Solução:

Por uma das extremidades do segmento, A por exemplo, trace uma reta construtível (os pontos de coordenadas racionais são construtíveis) que não contenha o segmento AB. Sobre esta reta, a partir de A, marque com o compasso n segmentos iguais de comprimento a distância entre dois pontos construtíveis. Trace, passando pela extremidade mais afastada de A, do último desses segmentos, e pelo ponto B, uma reta r. Trace retas paralelas à reta r passando pelas extremidades de cada um dos segmentos citados. Os pontos de interseção dessas retas com o segmento AB o dividem em n partes iguais.

Figura 9 – Divisão de segmento de reta em n partes iguais



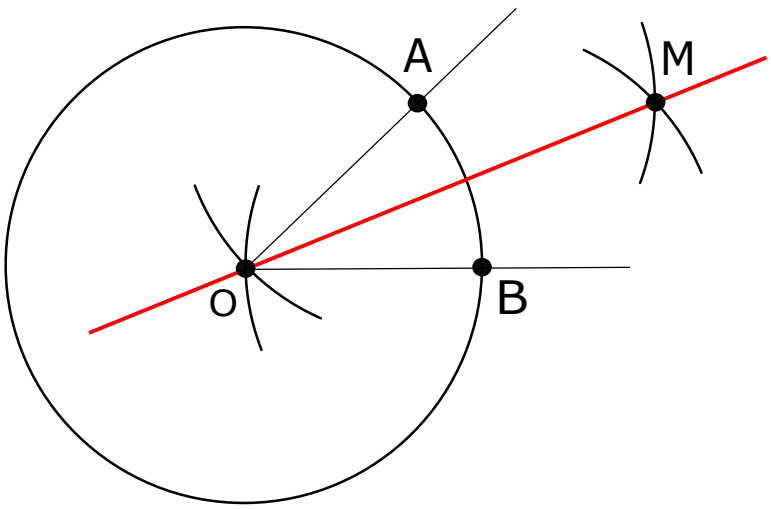
Fonte: Produzida pelo autor

5. Bissecção de um ângulo.

Solução:

Com centro no vértice O do ângulo, trace uma circunferência construtível. Com o mesmo raio trace duas circunferências com centros nos pontos A e B de interseção da circunferência construída anteriormente com os lados do ângulo. Trace a reta passando pelos pontos de interseção dessas duas últimas circunferências (um deles é o ponto O). Essa reta bissecta (divide em duas partes iguais) o ângulo dado e é denominada bissetriz do ângulo $\widehat{AOB}$.

Figura 10 – Bissecção de um ângulo



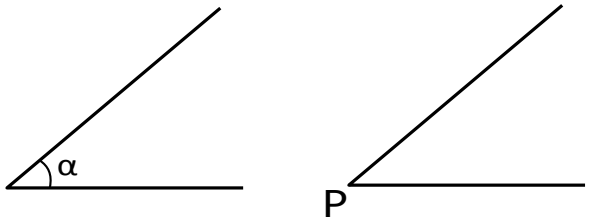
Fonte: Produzida pelo autor

6. Transporte, adição e subtração de ângulos

Solução:

Dado o ângulo de medida α graus, para transportá-lo até o ponto P, trace por P retas paralelas às retas que contém os lados do ângulo α .

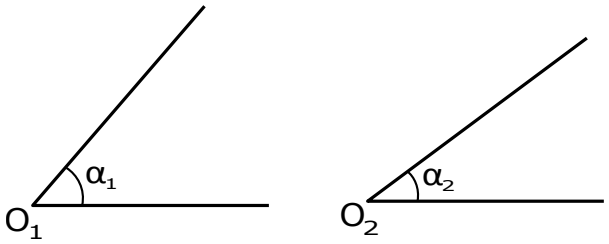
Figura 11 – Transportar ângulo



Fonte: Produzida pelo autor

Dados os ângulos de medidas α_1 e α_2, em graus, com vértices construtíveis O_1 e O_2.

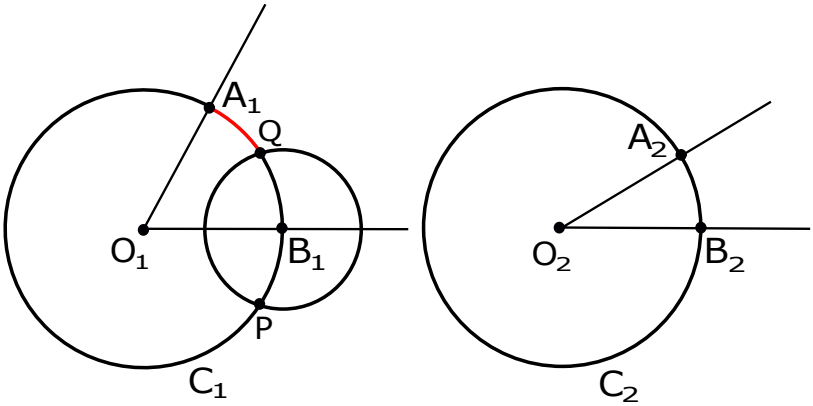
Figura 12 – Ângulos α_1 e α_2



Fonte: Produzida pelo autor

Com centro nos vértices O_1 e O_2, trace as circunferências construtíveis, C_1 e C_2, de mesmo raio. Sejam A_i e B_i os pontos de interseção do círculo C_i com os lados do ângulo α_i, para $i = 1, 2$. Com o compasso meça a distância d entre A_2 e B_2 (note que A_2 e B_2 são construtíveis). A circunferência de centro B_1 e raio d intersecta a circunferência C_1 nos pontos P e Q. Na figura a seguir, o ângulo $\widehat{A_1O_1P} = \alpha_1 + \alpha_2$ e o ângulo $\widehat{A_1O_1Q} = \alpha_1 - \alpha_2$, em que $\alpha_2 \leqslant \alpha_1$.

Figura 13 – Adição e subtração de ângulos



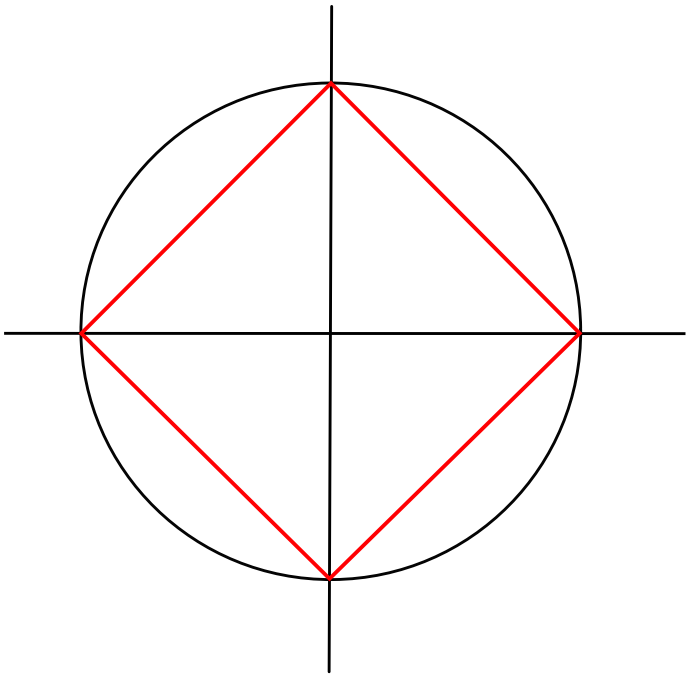
Fonte: Produzida pelo autor

7. Construção de um quadrado inscrito em uma circunferência

Solução:

Trace uma circunferência de centro construtível e, em seguida, trace duas retas perpendiculares quaisquer passando pelo centro da circunferência. Os quatro pontos de interseção dessas retas com a circunferência são os vértices do quadrado.

Figura 14 – Quadrado inscrito numa circunferência



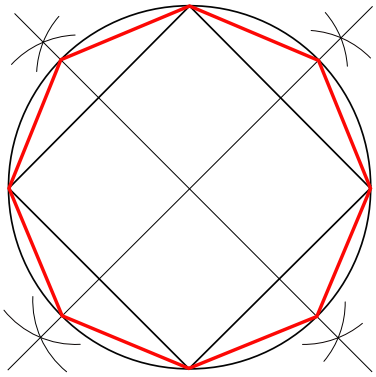
Fonte: Produzida pelo autor

8. Construção dos polígonos regulares com 2^n, $n \geqslant 3$, lados inscritos em uma circunferência

Solução:

Por recorrência, construa inicialmente um quadrado inscrito na circunferência. Por bissecção de seus ângulos centrais, obtemos o octógono regular inscrito na circunferência, e assim por diante. Partindo do polígono regular de 2^{n-1} lados, por bissecção de seus ângulos centrais, obtemos o polígono regular com 2^n lados inscrito na circunferência.

Figura 15 – Octógono inscrito numa circunferência



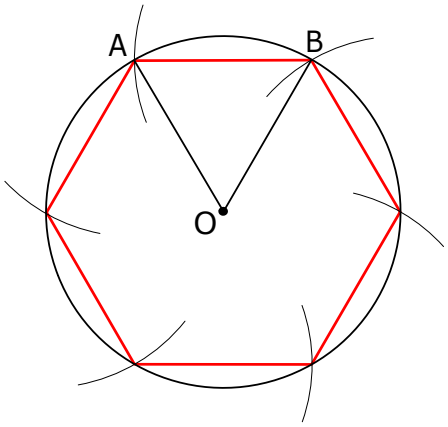
Fonte: Produzida pelo autor

9. Construção do hexágono regular

Solução:

Como o ângulo central do hexágono regular é 60^o e o triângulo AOB é isósceles, temos $\widehat{OAB} = \widehat{OBA} = 60^o$. Segue que o triângulo AOB é equilátero, e o lado do hexágono é igual ao raio da circunferência circunscrita.

Figura 16 – Hexágono regular



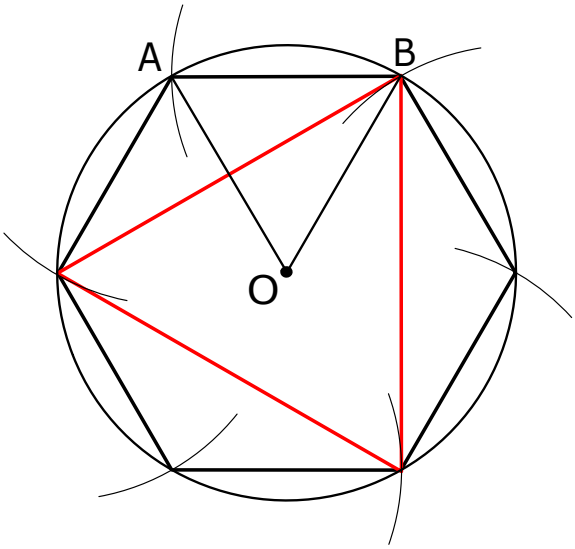
Fonte: Produzida pelo autor

10. Construção do triângulo equilátero

Solução:

Como o ângulo central do hexágono regular é 60^o *e o triângulo* AOB *é isósceles, temos* $\widehat{OAB} = \widehat{OBA} = 60^o$. *Segue que o triângulo* AOB *é equilátero e o lado do hexágono é igual ao raio da circunferência circunscrita. A partir do hexágono obtemos o triângulo equilátero unindo alternadamente os vértices do hexágono.*

Figura 17 – Triângulo equilátero

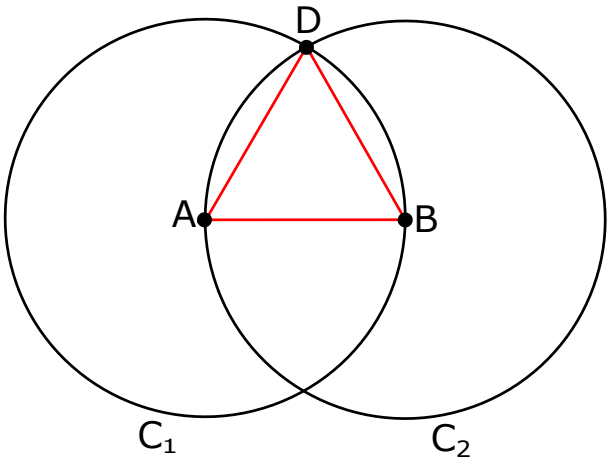


Fonte: Produzida pelo autor

Podemos construir o triângulo equilátero independente da construção do héxagono regular. A seguir apresentamos essa construção.

Sejam A *e* B *pontos construtíveis. Com centro em* A *e passando por* B *construa a circunferência* C_1. *Com centro em* B *e passando por* A *construa a circunferência* C_2. *As circunferências* C_1 *e* C_2 *são construtíveis, pela definição* 3. *Seja* D *um ponto de interseção entre* C_1 *e* C_2. *Como* D *é um ponto de interseção entre duas circunferências construtíveis,* D *é um ponto construtível. Note que, como* $AB = BD = AD$, *o triângulo* ABD *é equilátero.*

Figura 18 – Triângulo equilátero



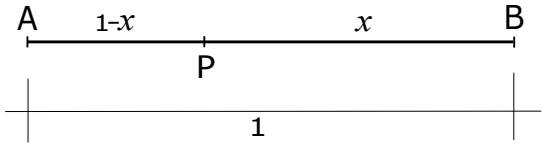
Fonte: Produzida pelo autor

11. Construção do pentágono regular

Solução:

Os matemáticos gregos faziam a construção de um pentágono regular dividindo um segmento de comprimento unitário em uma razão média e extrema. Dizemos que um ponto P divide um segmento de reta unitário AB em uma razão média e extrema se o segmento maior, de comprimento x, for a média proporcional entre o comprimento total, segmento de comprimento unitário, e o segmento menor, de comprimento $1-x$, isto é, $\dfrac{1}{x} = \dfrac{x}{1-x}$ ou $x^2 + x - 1 = 0$.

Figura 19 – Segmento dividido em uma razão média e extrema

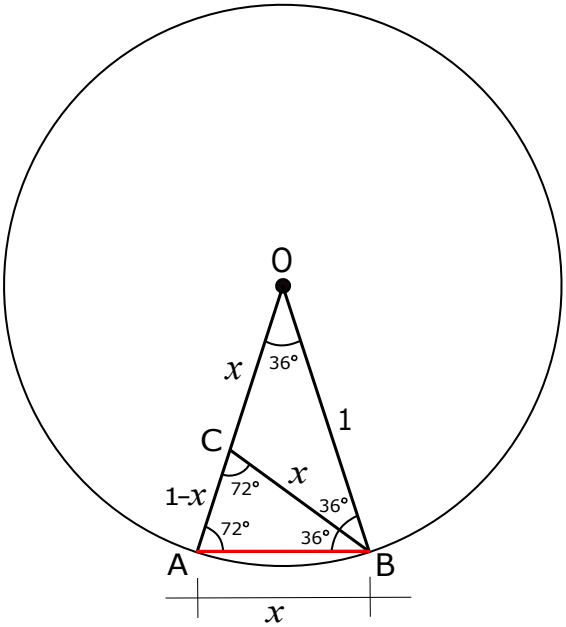


Fonte: Produzida pelo autor

Para mostrar como essa proporção está relacionada ao pentágono regular, procederemos de acordo com o seguinte.

Considere a circunferência de centro O e raio unitário. Seja $\widehat{AOB} = 36^o$ um ângulo central com A e B sobre a circunferência (ângulo central subentendido por um lado de um decágono regular). Segue que o $\widehat{OAB} = \widehat{ABO} = 72^o$. Trace BC como bissetriz do $\widehat{ABO}$. Assim, temos $AB = BC = CO = x$ e $AC = 1 - x$.

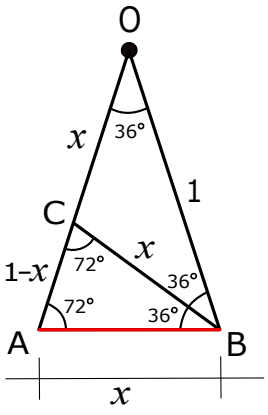
Figura 20 – Lado de um decágono regular



Fonte: Produzida pelo autor

Como a bissetriz do ângulo de um triângulo divide o lado oposto em dois segmentos que são proporcionais aos lados adjacentes ao ângulo, $\frac{1}{x} = \frac{x}{1-x}$*, dividindo o segmento OA em uma razão média e extrema. Assim, temos* $x^2 + x - 1 = 0$ *e* $x = \frac{\sqrt{5}-1}{2}$.

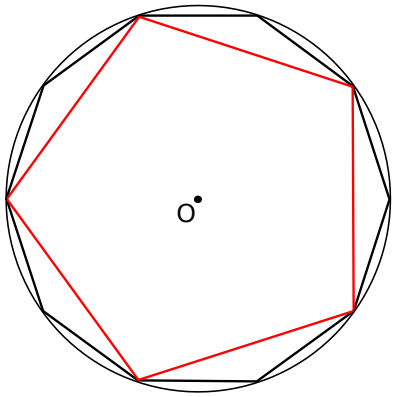
Figura 21 – Lado de um decágono regular



Fonte: Produzida pelo autor

Portanto, é possível construir o lado de um decágono regular, já que se trata de raiz de equação quadrática com coeficientes inteiros, e consequentemente o pentágono regular pode ser formado unindo alternadamente os vértices do decágono.

Figura 22 – Decágono e pentágono regulares

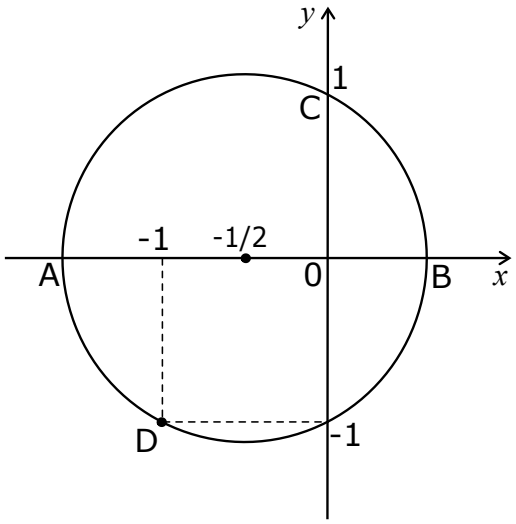


Fonte: Produzida pelo autor

Note que o esboço feito anteriormente seria válido como uma construção no sentido clássico apenas se o ângulo de 36^o (ou, de modo equivalente, o ângulo de 72^o) é construtível, o que equivale a afirmar que $cos36^o$ (ou consequentemente o $cos72^o$) é construtível. Aplicando a lei dos cossenos no triângulo AOB, com relação ao ângulo $\widehat{AOB} = 36^o$, obtemos $cos36^o = \dfrac{\sqrt{5}+1}{4}$. Usando o fato de que $cos(2x) = 2cos^2x - 1$, obtemos $cos72^o = \dfrac{\sqrt{5}-1}{4}$ (ou observando o triângulo AOB, pois $cos72^o = x/2$). A construção a seguir mostra como construir o número $2cos72^o$.

Construa a circunferência com diâmetro CD, em que $C = (0,1)$ e $D = (-1,-1)$, e intercepte o eixo das abscissas nos pontos A e B.

Figura 23 – Construção do número $2cos72^o = \dfrac{\sqrt{5}-1}{2}$



Fonte: Produzida pelo autor

O centro dessa circunferência é o ponto médio do segmento CD, isto é, o ponto $(-1/2, 0)$. O raio r da circunferência pode ser obtido calculando a distância entre os pontos $(-1/2, 0)$ e $(0, 1)$. Assim,

$$r^2 = \left(-\frac{1}{2} - 0\right)^2 + (0-1)^2 = \frac{1}{4} + 1 = \frac{5}{4}.$$

Portanto, a equação da circunferência é

$$\left(x + \frac{1}{2}\right)^2 + (y-0)^2 = \frac{5}{4}$$

que após algumas simplificações, obtemos

$$x^2 + x + y^2 - 1 = 0.$$

Para obtermos as abscissas dos pontos A e B, devemos ter $y = 0$. Assim, substituindo $y = 0$ na equação da circunferência, obtemos a equação quadrática

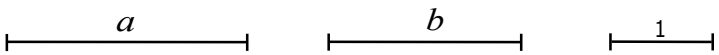
$$x^2 + x - 1 = 0$$

cujas raízes são $\dfrac{\sqrt{5}-1}{2}$ e $\dfrac{-\sqrt{5}-1}{2}$ que são as abscissas dos pontos A e B. Assim, o ângulo de 36^o (e consequentemente o de 72^o) é construtível.

1.3 ÁLGEBRA DAS CONSTRUÇÕES COM RÉGUA E COMPASSO

Os matemáticos gregos, por meio de teoremas geométricos, foram capazes de construir qualquer elemento geométrico que pudesse ser obtido através de um número finito de operações racionais e extração de raízes quadradas a partir de elementos dados. Suponha que sejam dados os elementos a, b e a *unidade*. Os gregos construiriam $a + b$, $a - b$, ab, a/b, a^2 e $\sqrt{a}$. A seguir mostraremos como construir essas operações. Para isso, considere dados os segmentos de comprimentos a, b e uma unidade de medida.

Figura 24 – Segmentos de comprimentos a, b e uma unidade de medida



Fonte: Produzida pelo autor

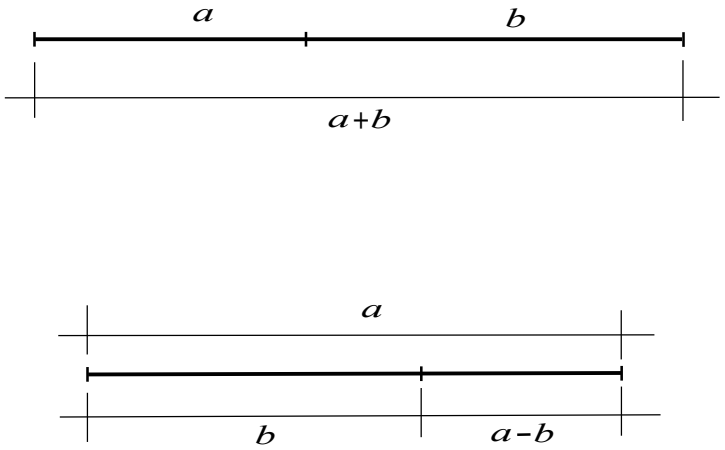
1.3.1 Construção de $a + b$ e $a - b$

Construir segmentos de comprimentos $a + b$ e $a - b$.

Solução:

Os segmentos de comprimentos $a+b$ e $a-b$ podem ser construídos de acordo com as figuras a seguir.

Figura 25 – Segmentos de comprimentos $a+b$ e $a-b$



Fonte: Produzida pelo autor

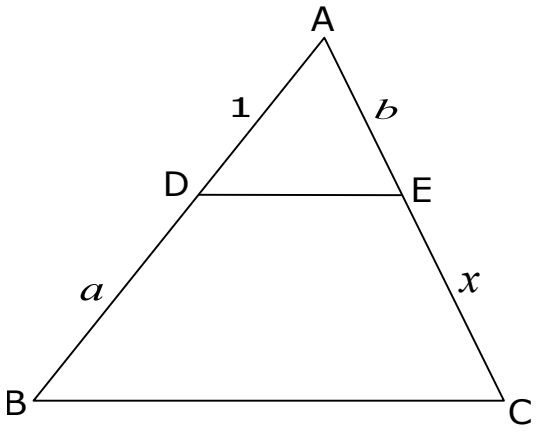
1.3.2 Construção de ab e a/b

Construir dois segmentos de comprimentos ab e a/b.

Solução:

A figura a seguir mostra como construir ab.

Figura 26 – Segmento de comprimento ab



Fonte: Produzida pelo autor

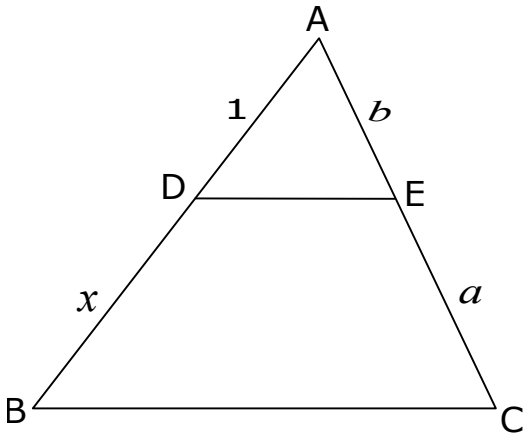
Se $\overline{DE}$ é construído paralelo a $\overline{BC}$, temos:

$$\frac{1}{a} = \frac{b}{x}$$

$$x = ab$$

A figura a seguir mostra como construir a/b.

Figura 27 – Segmento de comprimento a/b



Fonte: Produzida pelo autor

Sendo $\overline{DE}$ paralelo a $\overline{BC}$, temos:

$$\frac{1}{x} = \frac{b}{a}$$

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

Note que, em ambas as construções, utilizamos o teorema linear de Tales.

1.3.3 Construção de $\sqrt{a}$

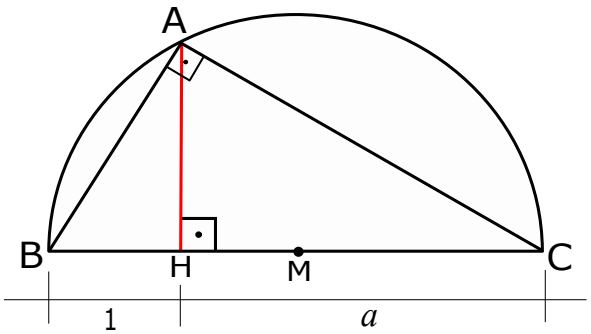
Construir um segmento de comprimento $\sqrt{a}$.

Solução:

Construa um segmento de comprimento $a + 1$ conectando um segmento de reta de comprimento 1 com um segmento de comprimento a (a um número construtível) de modo que estejam contidos numa mesma reta. Encontre o ponto médio M desse segmento e trace

uma semicircunferência com centro em M com raio igual a $(a+1)/2$. Pelo ponto H, onde são conectados os dois segmentos, construa a perpendicular à reta que passa por H e M. O comprimento do segmento dessa perpendicular compreendido entre a reta e a semicircunferência é igual a $\sqrt{a}$.

Figura 28 – Segmento de comprimento $\sqrt{a}$



Fonte: Produzida pelo autor

Note que o triângulo ABC na figura é retângulo em A e o segmento AH é a altura relativa à hipotenusa. Sabemos que das relações métricas no triângulo retângulo a medida da altura relativa à hipotenusa é média geométrica entre as medidas das projeções determinadas pelos catetos sobre a hipotenusa. Assim, temos $AH^2 = BH \cdot HC = 1 \cdot a$ resultando em $AH = \sqrt{a}$.

1.3.4 Construção da raiz da equação $ax + b = c$

Dasdos os segmentos de medidas a, b e c, construa a raiz da equação $ax + b = c$.

Solução:

A raiz da equação é $x = (c-b)/a$. Assim, inicialmente construímos $c-b$ e em seguida $(c-b)/a$.

1.3.5 Construção das raízes da equação $x^2 - ax + b = 0$

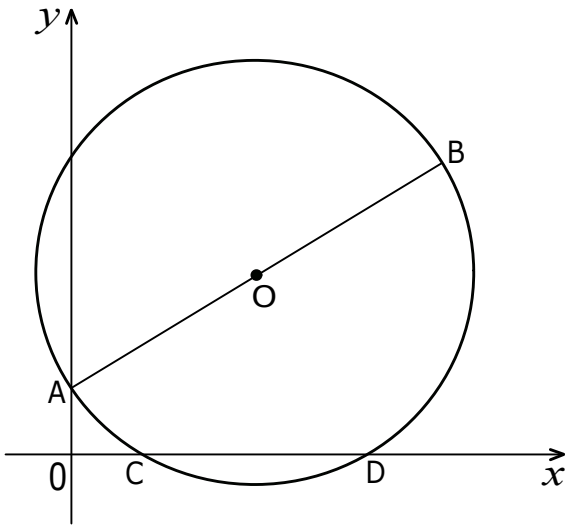
Dasdos os segmentos de medidas a e b, construa as raízes da equação $x^2 - ax + b = 0$.

Solução:

Para construir as raízes da equação quadrática $x^2 - ax + b = 0$ $(a^2 > 4b)$, construímos uma circunferência de diâmetro AB, em que $A = (0, 1)$ e $B = (a, b)$. Então as abscissas

dos pontos C e D (os pontos onde a circunferência intercepta o eixo das abscissas) serão as raízes da equação quadrática.

Figura 29 – Raízes da equação quadrática $x^2 - ax + b = 0$ $(a^2 > 4b)$



Fonte: Produzida pelo autor

O centro da circunferência acima é o ponto médio do segmento AB. Assim, temos

$$O = \left(\frac{0+a}{2}, \frac{1+b}{2}\right) = \left(\frac{a}{2}, \frac{b+1}{2}\right).$$

O raio r da circunferência pode ser obtido calculando a distância entre os pontos O e A. Logo,

$$r^2 = \left(\frac{a}{2} - 0\right)^2 + \left(\frac{b+1}{2} - 1\right)^2 = \frac{a^2}{4} + \frac{(b-1)^2}{4}.$$

Portanto, a equação da circunferência é

$$\left(x - \frac{a}{2}\right)^2 + \left(y - \frac{b+1}{2}\right)^2 = \frac{a^2}{4} + \frac{(b-1)^2}{4}$$

que após algumas simplificações, obtemos

$$x^2 + y^2 - ax - (b+1)y + b = 0.$$

Note que, para obtermos as abscissas dos pontos C e D, devemos ter $y = 0$. Assim, substituindo $y = 0$ na equação da circunferência, obtemos a equação quadrática

$$x^2 - ax + b = 0$$

cujas raízes são as abscissas dos pontos C e D.

1.3.6 Extensões quadráticas

Lembrando que um número racional é um quociente p/q, em que p e q são inteiros com $q \neq 0$. Um número real que não é racional é denominado de número irracional. A seguir daremos uma definição de corpo adequada à nossa investigação.

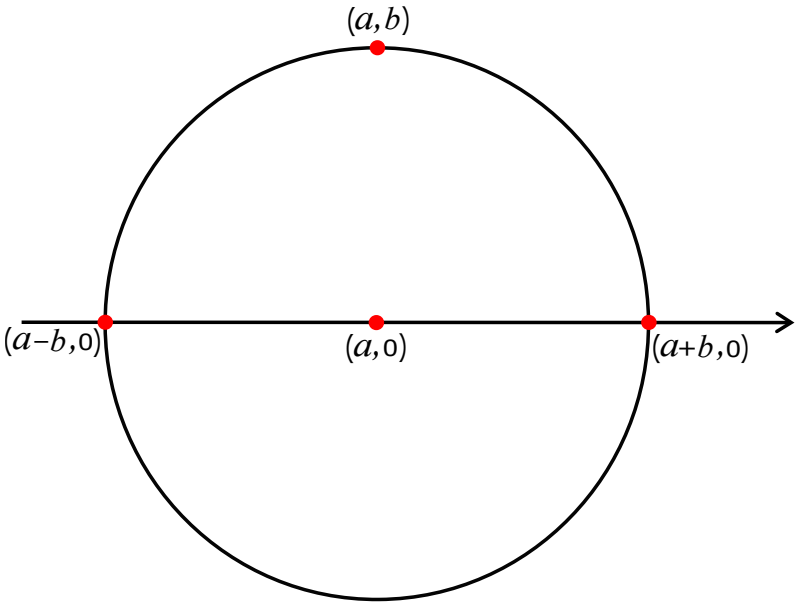
Definição 5. Um corpo $\mathbb{K}$ é um subconjunto dos números reais que contém os números 0 e 1 e tal que $a+b$, $a-b$, ab e a/c, com $c \neq 0$ pertencem a $\mathbb{K}$ sempre que a, b, e c pertencem a $\mathbb{K}$. Um corpo $\mathbb{K}_{\mathbb{E}}$ é um corpo euclidiano sempre que $a > 0$ pertencente a $\mathbb{K}_{\mathbb{E}}$ implica $\sqrt{a}$ pertencente a $\mathbb{K}_{\mathbb{E}}$.

Na definição anterior assumiremos que o leitor saiba que os racionais e os reais formam um corpo, mas os irracionais não formam um corpo. Outros corpos diferentes de $\mathbb{Q}$ e $\mathbb{R}$ serão mencionados nessa teoria. O primeiro destes aparece na proposição a seguir.

Proposição 1.3.1. *Os números construtíveis formam um corpo.*

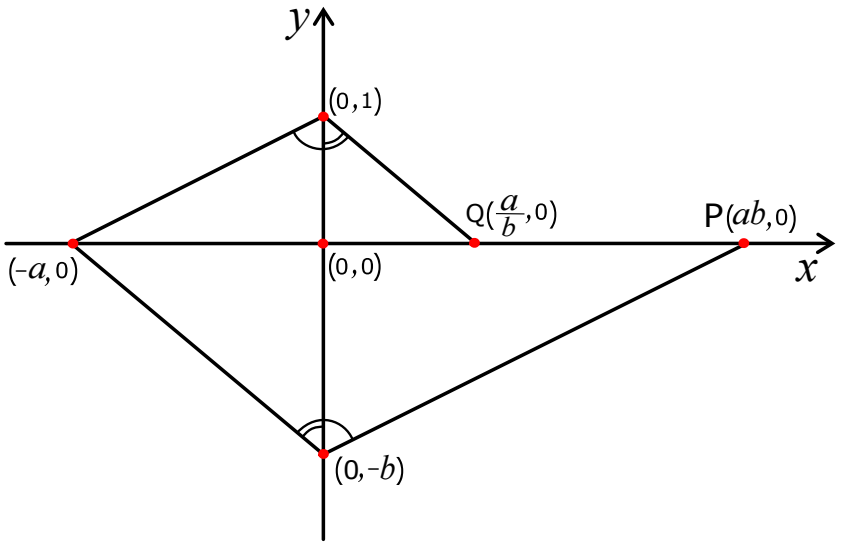
Demonstração. A proposição segue das figuras a seguir.

Figura 30 – Os números construtíveis formam um corpo



Fonte: Produzida pelo autor

Figura 31 – Os números construtíveis formam um corpo



Fonte: Produzida pelo autor

Da semelhança entre os triângulos da figura 31, obtemos as coordenadas dos pontos P e Q.

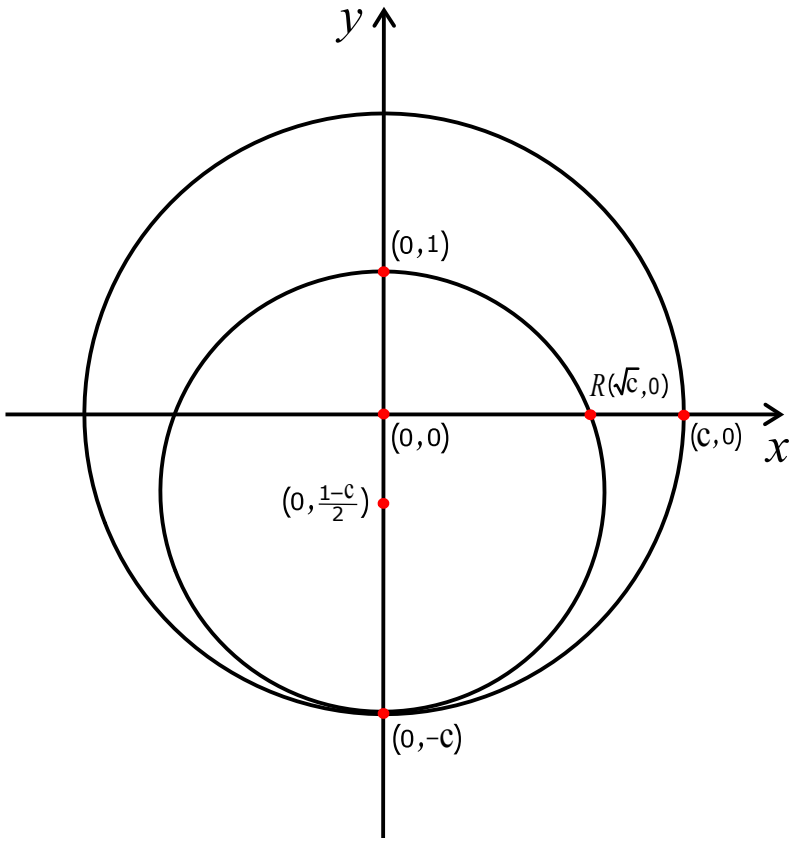
■

Os números racionais são construtíveis, mas nem todo número construtível é um número racional. Além de podermos realizar as quatro operações aritméticas de adição, subtração, multiplicação e divisão nos números construtíveis, também podemos realizar a extração de raízes quadradas de número maiores ou iguais a zero. Assim, segue da definição de corpo euclidiano a proposição a seguir.

Proposição 1.3.2. *Os números construtíveis formam um corpo euclidiano.*

Demonstração. Seja $c > 0$ um número construtível. Considere a circunferência construtível de centro $(0, 0)$ e que passa pelo ponto $(c, 0)$. Construa a circunferência que tem como centro o ponto médio do segmento cujas extremidades são os pontos $(0, 1)$ e $(0, -c)$, isto é, o ponto $(0, (1 - c)/2)$. Note que o raio dessa circunferência é igual a $(1 + c)/2$. Assim, sua equação é $x^2 + y^2 + (c - 1)y - c = 0$ da qual, fazendo $y = 0$, obtemos as abscissas dos pontos de sua interseção com o eixo das abscissas. Note que um desses pontos é o ponto R da figura a seguir.

Figura 32 – Os números construtíveis formam um corpo euclidiano



Fonte: Produzida pelo autor

■

Dizer que a é um quadrado em um corpo $\mathbb{K}$ significa que há um número b em $\mathbb{K}$ tal que $a = b^2$. De outro modo, o número a pertencente a $\mathbb{K}$ é um quadrado em $\mathbb{K}$ se, e somente se, $\sqrt{a}$ também pertence a $\mathbb{K}$. Assim, um corpo $\mathbb{K}$ é um corpo euclidiano se todo número positivo em $\mathbb{K}$ for um quadrado em $\mathbb{K}$. O corpo $\mathbb{Q}$ dos racionais não é um corpo euclidiano, pois 2, por exemplo, um número racional positivo, mas $\sqrt{2}$ não é um número racional. Por outro lado, 2 é um quadrado em $\mathbb{R}$, pois $\sqrt{2}$ está em $\mathbb{R}$. O corpo $\mathbb{R}$ dos números reais é um exemplo de corpo euclidiano.

A seguir faremos a construção algébrica, que é de fundamental importância para o estudo das construções com régua e compasso. A ideia é estender um dado corpo $\mathbb{K}$ para formar um novo corpo, de modo que este novo corpo contenha um novo número específico, além de todos os números do corpo $\mathbb{K}$ dado anteriormente. Isso é algo fácil de ser feito no caso especial em que o quadrado do número específico a ser adicionado pertence ao corpo $\mathbb{K}$ dado anteriormente. Por exemplo, $\sqrt{2}$ não pertence a $\mathbb{Q}$, mas $\left(\sqrt{2}\right)^2$ pertence a $\mathbb{Q}$. Faremos agora

a construção do menor corpo que contém $\sqrt{2}$ e todos os números racionais. A proposição a seguir nos diz, não só como fazer isso, mas como generalizar essa construção. Isto é, a proposição nos mostrar como estender um corpo dado $\mathbb{K}$ pela raiz quadrada de um número positivo que pertence ao corpo $\mathbb{K}$.

Proposição 1.3.3. *Se $\mathbb{K}$ é um corpo e c é um número positivo pertencente a $\mathbb{K}$, mas $\sqrt{c}$ não pertence a $\mathbb{K}$, então $\{a+b\sqrt{c} \mid a,b \in \mathbb{K}\}$ é um corpo.*

Demonstração. Para mostrar que todos os números $a+b\sqrt{c}$, com a, b e c pertencentes a $\mathbb{K}$ e $\sqrt{c}$ não pertencente a $\mathbb{K}$, formam um corpo, procedemos da seguinte forma:

i) $(a_1+b_1\sqrt{c})+(a_2+b_2\sqrt{c}) = (a_1+a_2)+(b_1+b_2)\sqrt{c}$

ii) $(a_1+b_1\sqrt{c})-(a_2+b_2\sqrt{c}) = (a_1-a_2)+(b_1-b_2)\sqrt{c}$

iii) $(a_1+b_1\sqrt{c})(a_2+b_2\sqrt{c}) = (a_1a_2+b_1b_2c)+(a_1b_2+b_1a_2)\sqrt{c}$

iv) $\dfrac{a_1+b_1\sqrt{c}}{a_2+b_2\sqrt{c}} = \dfrac{a_1+b_1\sqrt{c}}{a_2+b_2\sqrt{c}} \cdot \dfrac{a_2-b_2\sqrt{c}}{a_2-b_2\sqrt{c}} = \dfrac{a_1a_2-b_1b_2}{a_2^2-b_2^2c} + \dfrac{a_2b_1-a_1b_2}{a_2^2-b_2^2c}\sqrt{c}$

v) $\dfrac{1}{a+b\sqrt{c}} = \dfrac{1}{a+b\sqrt{c}} \cdot \dfrac{a-b\sqrt{c}}{a-b\sqrt{c}} = \dfrac{a}{a^2-b^2c} + \dfrac{-b}{a^2-b^2c}\sqrt{c}$

Como a_1, b_1, a_2, b_2, c são números pertencentes a $\mathbb{K}$, a soma, produto, diferença e quociente de quaisquer dois destes números pertencem a $\mathbb{K}$. Portanto, todos os números da forma $a+b\sqrt{c}$ formam um corpo o qual contém o corpo $\mathbb{K}$ como subcorpo. ■

Se c é um número positivo pertencente ao corpo $\mathbb{K}$, mas $\sqrt{c}$ não pertence a $\mathbb{K}$, usaremos a notação $\mathbb{K}(\sqrt{c})$ para representar o corpo $\{a+b\sqrt{c} \mid a,b \in \mathbb{K}\}$.

Definição 6. Denominamos o corpo $\mathbb{K}(\sqrt{c})$ de extensão quadrática do corpo $\mathbb{K}$ no caso de c não ser quadrado em $\mathbb{K}$. Se $\mathbb{K}_1 = \mathbb{K}\left(\sqrt{c_1}\right)$, $\mathbb{K}_2 = \mathbb{K}_1\left(\sqrt{c_2}\right)$, $\cdots$, $\mathbb{K}_n = \mathbb{K}_{n-1}\left(\sqrt{c_n}\right)$, então faremos $\mathbb{K}_n = \mathbb{K}\left(\sqrt{c_1}, \sqrt{c_2}, \cdots, \sqrt{c_n}\right)$ e chamaremos cada uma das extensões $\mathbb{K}$, $\mathbb{K}_1$, $\mathbb{K}_2$, $\cdots$, $\mathbb{K}_n$ de extensão quadrática iterada de $\mathbb{K}$. Denotaremos por $\mathbb{L}$ a união de todas as torres de extensões quadráticas do corpo $\mathbb{Q}$.

Partindo da ideia de uma extensão quadrática da proposição anterior, concluímos que uma extensão quadrática é apenas uma extensão quadrática de uma extensão quadrática de uma extensão quadrática $\cdots$ de uma extensão quadrática. Desse modo, é permitido apenas uma cadeia finita de extensões. Assim, $\mathbb{L}$ é a união de todas as extensões quadráticas dos racionais. O corpo $\mathbb{R}$ não possui extensões quadráticas obtidas pela adjunção de raiz quadrada

de um número real positivo, já que todo número real positivo é um quadrado em $\mathbb{R}$. Segue que um corpo euclidiano não possui extensões quadráticas.

O diagrama a seguir mostra uma torre de corpos sobre os racionais. O corpo $\mathbb{K}_{i+1}$ é uma extensão quadrática do corpo $\mathbb{K}_i$. Então o corpo $\mathbb{K}_i$ está contido no corpo $\mathbb{K}_{i+1}$, e o corpo $\mathbb{K}_n$ é uma extensão quadrática dos racionais. A união dos números em todas essas torres sobre os racionais é $\mathbb{L}$.

$$
\begin{array}{l}
\mathbb{K}_n = \mathbb{K}_{n-1} = \mathbb{Q}(\sqrt{c_1}, \sqrt{c_2}, \cdots, \sqrt{c_n}) \\
| \\
\vdots \\
| \\
\mathbb{K}_{i+1} = \mathbb{K}_i(\sqrt{c_{i+1}}) = \mathbb{Q}(\sqrt{c_1}, \sqrt{c_2}, \cdots, \sqrt{c_{i+1}}) \\
| \\
\mathbb{K}_i = \mathbb{K}_{i-1}(\sqrt{c_i}) = \mathbb{Q}(\sqrt{c_1}, \sqrt{c_2}, \cdots, \sqrt{c_i}) \\
| \\
\vdots \\
| \\
\mathbb{K}_3 = \mathbb{K}_2(\sqrt{c_3}) = \mathbb{Q}(\sqrt{c_1}, \sqrt{c_2}, \sqrt{c_3}) \\
| \\
\mathbb{K}_2 = \mathbb{K}_1(\sqrt{c_2}) = \mathbb{Q}(\sqrt{c_1}, \sqrt{c_2}) \\
| \\
\mathbb{K}_1 = \mathbb{Q}(\sqrt{c_1}) \\
| \\
\mathbb{Q}
\end{array}
$$

Segue da proposição 1.3.2 que, se todos os números em um corpo $\mathbb{K}$ são números construtíveis, então os números em uma extensão quadrática $\mathbb{K}(\sqrt{c})$ são também números construtíveis. Portanto, por iteração, se o número α estiver em uma extensão quadrática real dos racionais, então α é um número construtível.

Proposição 1.3.4. *Se α pertence a $\mathbb{L}$, então α é um número construtível.*

Considerando a forma dos números pertencentes a $\mathbb{L}$, essa proposição não traz nenhuma novidade. O que é surpreendente é a recíproca, a qual pretendemos provar. Para isso faremos uso de quatro lemas, cujas ideias não são difíceis. Partimos de um conjunto de pontos construtíveis, em seguida construimos novos pontos com a régua e o compasso. Esses novos pontos são obtidos como a interseção de retas e circunferências construtíveis, e as equações

algébricas que precisamos resolver para encontrar as coordenadas desses pontos não requerem mais do que as quatro operações aritméticas (adição, subtração, multiplicação e divisão) e extração de raízes quadradas. Portanto, é de se esperar que as coordenadas de qualquer ponto construtível pertençam a uma extensão quadrática dos racionais.

Apesar deste argumento parecer que comprova a afirmação da próxima proposição, que é a recíproca da proposição anterior, os detalhes são mencionados a seguir.

Lema 1.3.5. *i) Se uma reta passa por dois pontos que possuem as coordenadas pertencentes a um corpo $\mathbb{K}$, então essa reta possui uma equação com coeficientes pertencentes a $\mathbb{K}$.*

ii) Se o centro de uma circunferência e um ponto pelo qual ela passa possuem coordenadas pertencentes ao corpo $\mathbb{K}$, então essa circunferência possui um equação com coeficientes pertencentes a $\mathbb{K}$

Demonstração. i) A equação da reta que passa pelos pontos $P_1 = (a, b)$ e $P_2 = (c, d)$, com a, b, c, d pertencentes ao corpo $\mathbb{K}$, é $(d-b)x+(a-c)y+(bc-ad) = 0$ ou $Ax+By+C = 0$, em que $A = d - b$, $B = a - c$ e $C = bc - ad$. Segue da definição de corpo que A, B e C pertencem ao corpo $\mathbb{K}$.

ii) A equação da circunferência com centro no ponto (a, b) e que passa pelo ponto (c, d), com a, b, c e d pertencentes a $\mathbb{K}$, é $x^2+y^2+(-2a)x+(-2b)y+[c(2a-c)+d(2b-d)] = 0$ que é equivalente a $(x-a)^2+(y-b)^2 = (c-a)^2+(d-b)^2$. Segue da definição de corpo que os coeficientes da equação pertencem ao corpo $\mathbb{K}$.

■

Lema 1.3.6. *Se duas retas de equações com coeficientes pertencentes a um corpo $\mathbb{K}$ se interceptam, então o ponto de interseção possui coordenadas pertencentes ao corpo $\mathbb{K}$.*

Demonstração. Sejam $a_1x+b_1y+c_1 = 0$ e $a_2x+b_2y+c_2 = 0$ as equações das retas, em que a_1, b_1, c_1, a_2, b_2, c_2 pertencem a um corpo $\mathbb{K}$. O ponto de interseção da reta, obtido por meio da solução do sistema de equações, tem abscissa $x_0 = \dfrac{b_1c_2 - b_2c_1}{a_1b_2 - a_2b_1}$ e ordenada $y_0 = \dfrac{a_2c_1 - a_1c_2}{a_1b_2 - a_2b_1}$. Note que $a_1b_2 - a_2b_1 \neq 0$, caso contrário as retas seriam paralelas. Pela definição de corpo x_0 e y_0 pertencem a $\mathbb{K}$. ■

Lema 1.3.7. *Se uma reta e uma circunferência se interceptam e suas equações possuem coeficientes pertencentes a um corpo $\mathbb{K}$, então o ponto de interseção possui coordenadas pertencentes ao corpo $\mathbb{K}$ ou a uma extensão quadrática de $\mathbb{K}$.*

Demonstração. Suponha que a reta de equação $ax + by + c = 0$ intercepta a circunferência de equação $x^2 + y^2 + fx + gy + h = 0$ nos pontos (x_0, y_0), em que a, b, c, f, g, h pertencem a um corpo $\mathbb{K}$. Pela solução do sistema, obtemos $x_0 = \dfrac{abg - 2ac - b^2 f \pm b\sqrt{d}}{2(a^2 + b^2)}$ e $y_0 = \dfrac{abf - 2bc - a^2 g \mp a\sqrt{d}}{2(a^2 + b^2)}$, em que $d = (fb - ag)^2 + 4c(af + gb - c) - 4h(a^2 + b^2)$. Para que a reta e a circunferência se interceptem d deve ser não-negativo. Se d for um quadrado em $\mathbb{K}$, então as coordenadas dos pontos de interseção pertencem a $\mathbb{K}$, pela definição de corpo. No entanto, se d não é um quadrado em $\mathbb{K}$, então pelo menos um dos x_0 ou y_0 não pertence a $\mathbb{K}$, já que tanto a quanto b não pode ser 0. Nestes casos x_0 e y_0 pertencem a $\mathbb{K}(\sqrt{d})$, que é uma extensão quadrática de $\mathbb{K}$. ■

Lema 1.3.8. *Se duas circunferências de equações com coeficientes pertencentes a um corpo $\mathbb{K}$ se interceptam, então os pontos de interseção possuem coordenadas pertencentes ao corpo $\mathbb{K}$ ou a uma extensão quadrática de $\mathbb{K}$.*

Demonstração. Sejam $x^2+y^2+f_1x+g_1y+h_1 = 0$ e $x^2+y^2+f_2x+g_2y+h_2 = 0$ as equações das circunferências, em que f_1, g_1, h_1, f_2, g_2, h_2 pertencem a um corpo $\mathbb{K}$. O sistema formado por essas equações é equivalente ao sistema formado pelas equações $(f_1-f_2)x+(g_1-g_2)y+(h_1-h_2)$ e $x^2 + y^2 + f_2x + g_2y + h_2 = 0$ cuja primeira equação é obtida pela subtração ou adição das equações do primeiro sistema. Sendo assim, este lema segue do lema anterior. ■

A seguir afirmaremos e provaremos que as coordenadas de um ponto construtível pertencem a uma extensão quadrática dos racionais.

Proposição 1.3.9. *As coordenadas de um ponto construtível pertencem a uma torre de extensões quadráticas do corpo dos racionais.*

Demonstração. Seja P um ponto construtível. Da definição de ponto construtível, vemos que P deve ser o último de uma sequência de pontos P_1, P_2, $\cdots$, P_n cada um dos quais é $(0, 0)$, $(1, 0)$, ou é obtido de uma das três formas a seguir:

i) como a intersecção de duas retas, cada uma passando por dois pontos que já apareceram na sequência;

ii) como um ponto de intersecção de uma reta que passam por dois pontos que aparecem anteriormente na sequência e de uma circunferência que passa por um ponto anterior e tendo um ponto anterior como centro;

iii) como um ponto de intersecção de duas circunferências, cada uma das quais passa por um ponto anterior na sequência e cada uma delas tem um ponto anterior como centro.

Pela sequência dos quatro lemas anteriores, podemos associar P_1 com os racionais e observar que cada ponto P_i para $i > 1$ pode ser associado a um corpo $\mathbb{K}_i$ tal que as coordenadas de P_i pertencem a $\mathbb{K}_i$ e tal que $\mathbb{K}_i$ seja igual a $\mathbb{K}_{i-1}$ ou a uma extensão quadrática de $\mathbb{K}_{i-1}$. Assim, $\mathbb{K}_n$ é uma torre de extensões quadráticas dos racionais, e as coordenadas de P pertencem a $\mathbb{K}_n$.

■

A proposição anterior nos diz que se α é um número construtível, então α deve pertencer a $\mathbb{L}$. Essa é a recíproca da proposição 1.3.4. Segue que $\mathbb{L}$ deve ser um corpo, já que os números construtíveis formam um corpo. Como um corpo deve conter 1 e, portanto, todos os racionais e como um corpo euclidiano deve ser fechado quanto a tomar raiz quadrada, significando que se $x > 0$ pertence ao corpo então $\sqrt{x}$ pertence ao corpo, concluímos que $\mathbb{L}$ deve ser o menor corpo euclidiano. Como $\mathbb{Q}$ é o menor corpo, então $\mathbb{L}$ é o menor corpo euclidiano.

Corolário 1.3.10. *O ponto P é um ponto construtível se, e somente se, as coordenadas de P pertencerem a $\mathbb{L}$. O número α é um número construtível se, e somente se, α pertencer ao corpo $\mathbb{L}$.*

Veremos a seguir que cada número construtível é algébrico (sobre $\mathbb{Q}$), ou seja é raiz de um polinômio não nulo com coeficientes inteiros. Dado que o conjunto dos números algébricos é enumerável (está em bijeção com os números naturais), segue que o conjunto dos números construtíveis também é enumerável. Para a demonstração veja a referência FIGUEIREDO.

2 EXTENSÕES DE CORPOS

A ideia de polinômios irredutíveis sobre o corpo $\mathbb{Q}$ nos remete à seguinte questão: qual é o menor corpo $\mathbb{K} \supset \mathbb{Q}$ no qual podemos reduzir um dado polinômio? O Teorema Fundamental da Álgebra diz que todos os polinômios são redutíveis a polinômios de grau 1 sobre o corpo dos números complexos, indicado por $\mathbb{C}$, mas nosso polinômio pode ser completamente redutível em um corpo menor. Isso leva ao conceito de extensões de corpos.

Definição 7. Se $\mathbb{K}$ e $\mathbb{F}$ são corpos tais que $\mathbb{F} \supset \mathbb{K}$, dizemos que $\mathbb{F}$ é uma uma extensão do corpo $\mathbb{K}$. Uma extensão de corpo $\mathbb{F}$ é chamada simples se puder ser obtida associando um único elemento ao corpo $\mathbb{K}$. Se um corpo puder ser atingido associando uma série de elementos únicos, então teremos uma cadeia de extensões de corpos simples.

Mais especificamente, podemos associar as raízes de uma equação ao corpo dos números racionais, criando assim um corpo maior que permite que um polinômio seja reduzido ainda mais. No caso do polinômio $p(x) = x^2 - 3$, um corpo maior é $\mathbb{Q}(\sqrt{3})$ (lido $\mathbb{Q}$ associado com $\sqrt{3}$). Os elementos deste corpo são os números da forma $a+b\sqrt{3}$, em que a e b pertencem a $\mathbb{Q}$. Como veremos mais adiante, este também é um exemplo de um corpo de decomposição com polinômio mínimo $p(x) = x^2 - 3$.

2.1 ESPAÇOS VETORIAIS DE DIMENSÃO FINITA

Nesta seção revisaremos as definições e resultados de álgebra linear necessárias para o desenvolvimento posterior desta dissertação.

2.1.1 Definição e exemplos de espaços vetoriais

Inicialmente, veremos sucintamente algumas noções de espaço vetorial e base. Poderíamos desenvolver as propriedades que usaremos posteriormente sem nunca citar um espaço vetorial. Porém, isso levaria à repetição de alguns argumentos. Na definição de espaço vetorial a seguir, referimo-nos a vetores sem os definir. Entenda-se por vetor qualquer objeto matemático que satisfaça a condição de estar em um espaço vetorial. Nas aplicações que temos os vetores que aparecem são formadores de números reais. Porém, há vetores que não são números reais.

Definição 8. Sejam $\mathbb{K}$ um corpo qualquer e $\mathbb{V}$ um conjunto não vazio munido de uma operação a qual chamaremos de adição e uma operação a qual chamaremos de multiplicação por escalar (quando multiplicamos elementos de $\mathbb{K}$ por elementos de $\mathbb{V}$). Assim, estão definidas:

$$\begin{array}{rccc} + : \mathbb{V} \text{ x } \mathbb{V} & \to & \mathbb{V} \\ (u,\, v) & \mapsto & u+v \end{array} \quad \text{e} \quad \begin{array}{rccc} \mathbb{K} \text{ x } \mathbb{V} & \to & \mathbb{V} \\ (k,\, v) & \mapsto & kv \end{array}$$

Dizemos que $\mathbb{V}$ munido dessas operações é um espaço vetorial sobre o corpo $\mathbb{K}$ se são verificados o seguintes axiomas para quaisquer u, v, $w \in \mathbb{V}$ e k_1, $k_2 \in \mathbb{K}$:

A1. $(u+v)+w = u+(v+w)$ (associatividade da adição)

A2. $u+v = v+u$ (comutatividade da adição)

A3. Existe um único vetor $0 \in \mathbb{V}$ tal que $v+0 = 0+v = v$ para todo $v \in \mathbb{V}$ (existência de elemento neutro da adição)

A4. Para cada $v \in \mathbb{V}$ existe um único $-v \in \mathbb{V}$ tal que $v+(-v) = 0$ (existência de inverso aditivo)

A5. $k_1(u+v) = k_1u + k_1v$ (multiplicação é distributiva com respeito à adição de vetores)

A6. $(k_1+k_2)u = k_1u+k_2u$ (multiplicação por escalares é distributiva com respeito à adição de vetores)

A7. $k_1(k_2u) = k_2(k_1u) = (k_1k_2)u$

A8. $1 \cdot u = u$ para cada $u \in \mathbb{V}$

Seguem alguns exemplos de espaços vetoriais cuja verificação dos axiomas anteriores são imediatas.

Exemplo 1. Sejam $\mathbb{K}$ um corpo qualquer, $\mathbb{M} \supset \mathbb{K}$ uma extensão de $\mathbb{K}$ e $\alpha \in \mathbb{M}$. Podemos verificar que $\mathbb{K}[\alpha]$, munido das operações de espaço vetorial, é um espaço vetorial sobre $\mathbb{K}$. De modo geral, uma extensão de corpos $\mathbb{M} \supset \mathbb{K}$ pode ser vista como um espaço vetorial sobre o corpo $\mathbb{K}$

Exemplo 2. Considerando o corpo dos racionais $\mathbb{Q}$ e a extensão quadrática $\mathbb{Q}(\sqrt{2})$, é fácil verificar que $\mathbb{Q}(\sqrt{2})$ é um espaço vetorial sobre $\mathbb{Q}$. De fato, a adição de vetores em $\mathbb{Q}(\sqrt{2})$ é definida por $(a+b\sqrt{2})+(c+d\sqrt{2}) = (a+c)+(b+d)\sqrt{2}$, o produto de um escalar em $\mathbb{Q}$ e um vetor em $\mathbb{Q}(\sqrt{2})$ definido como produto usual de números reais, o negativo de um vetor $a+b\sqrt{2}$ definido como $(-a)+(-b)\sqrt{2}$ e $0+0\sqrt{2}$ sendo 0. De modo geral, é fácil perceber que qualquer extensão quadrática $\mathbb{Q}(\sqrt{\alpha})$ com $\alpha \in \mathbb{Q}$ pode ser considerada como um espaço vetorial sobre $\mathbb{Q}$.

Exemplo 3. Sejam $\mathbb{K}$ um corpo qualquer e $\mathbb{K}^n = \mathbb{K} \times \mathbb{K} \times \cdots \times \mathbb{K}$ o conjunto de todas as n-uplas $(a_1, a_2, \cdots, a_n)$ em que cada $a_i \in \mathbb{K}$, isto é, $\mathbb{K}^n = \{(a_1, a_2, \cdots, a_n) : a_i \in \mathbb{K}, i = 1, 2, \cdots, n\}$. Segue que $\mathbb{K}^n$ munido das operações definidas nos axiomas acima é um espaço vetorial sobre o corpo $\mathbb{K}$.

Exemplo 4. Sejam X um conjunto não vazio e $\mathbb{K}$ um corpo qualquer. Denotamos por $F(X, \mathbb{K})$ o conjunto de todas as funções $f : X \longrightarrow \mathbb{K}$. O conjunto $F(X, \mathbb{K})$ se torna um espaço vetorial sobre o corpo $\mathbb{K}$ quando se define a soma $(f + g)(x) = f(x) + g(x)$ para todo $x \in X$ e o produto $(kf)(x) = k \cdot f(x)$ para todo $x \in X$ e $k \in \mathbb{K}$. Note que, variando o conjunto X, obtemos diversos exemplos de espaços vetoriais da forma $F(X, \mathbb{K})$. Em particular, fazendo $X = \{1, 2, \cdots, n\}$ e $\mathbb{K} = \mathbb{R}$ obtemos $F(X, \mathbb{R}) = \mathbb{R}^n$ que é um espaço vetorial sobre $\mathbb{R}$.

Se considerarmos $\mathbb{K} = \mathbb{Q}$ e $\mathbb{V} = \mathbb{Q}(\alpha)$, em que $\mathbb{Q}(\alpha)$ é uma extensão quadrática de $\mathbb{Q}$ ou qualquer outro corpo de números reais, então, como no exemplo anterior, podemos considerar quaisquer tais corpos como um espaço vetorial sobre $\mathbb{Q}$. Nesse caso, a adição de vetores é a adição de números reais, a multiplicação de um escalar e um vetor é a multiplicação de números reais, o negativo de um vetor é seu negativo como um número real e o 0 é o elemento neutro identidade da adição. Os espaços vetoriais obtidos desta maneira são de fundamental importância para nossa teoria.

2.1.2 Dependência e independência linear

O objetivo desta seção é descrever certos tipos de subconjuntos de espaços vetoriais que serão úteis para nossa teoria. Para isso considere $\mathbb{V}$ um espaço vetorial sobre um corpo $\mathbb{K}$. Denotaremos os vetores em $\mathbb{V}$ por x_1, x_2, $\cdots$, e escalares em $\mathbb{K}$ por a_1, a_2, $\cdots$.

Definição 9. Um conjunto finito $\{x_1, x_2, \cdots, x_n\}$ de vetores do espaço vetorial $\mathbb{V}$ sobre $\mathbb{K}$ é dito linearmente dependente sobre $\mathbb{K}$ se existem escalares a_1, a_2, $\cdots$, a_n, não todos nulos, em $\mathbb{K}$ tais que $a_1x_1 + a_2x_2 + \cdots + a_nx_n = 0$, caso não existam tais escalares, isto é, $a_1x_1 + a_2x_2 + \cdots + a_nx_n = 0$ apenas se $a_1 = a_2 = \cdots = a_n = 0$, então dizemos que o conjunto de vetores $\{x_1, x_2, \cdots, x_n\}$ é linearmente independente sobre $\mathbb{K}$.

A menos que seja necessário mencionar o corpo $\mathbb{K}$, omitiremos o termo "sobre $\mathbb{K}$"quando escrevermos sobre conjuntos linearmente dependentes e linearmente independentes. Simbolicamente usaremos LD para linearmente dependente e LI para linearmente independente. É conveniente escrever que os vetores x_1, x_2, $\cdots, x_n$ são LD ou LI escrevendo que o conjunto $\{x_1, x_2, \cdots, x_n\}$ é LD ou LI.

A seguir discutiremos alguns exemplos.

Exemplo 5. Considerando $\mathbb{V} = \mathbb{Q}(\sqrt{c})$ e $\mathbb{K} = \mathbb{Q}$, em c não é um quadrado em $\mathbb{Q}$. Nesse espaço vetorial $\{1, \sqrt{c}\}$ é um conjunto LI. Para mostrar que $\{1, \sqrt{c}\}$ é LI sobre $\mathbb{Q}$ considere a, b pertencentes a $\mathbb{Q}$ tais que $a \cdot 1 + b \cdot \sqrt{c} = 0$ com $b \neq 0$. Segue que $\sqrt{c} = -\dfrac{a}{b}$. Como $\mathbb{Q}$ é um corpo e a, b pertencem a $\mathbb{Q}$, temos que $-\dfrac{a}{b}$ pertence a $\mathbb{Q}$. Assim, $\sqrt{c}$ pertence a $\mathbb{Q}$. Mas isso é uma contradição já que c não é um quadrado em $\mathbb{Q}$. Portanto, para que $a \cdot 1 + b \cdot \sqrt{c} = 0$ seja satisfeita devemos ter $b = 0$ o que implica $a = 0$. Consequentemente, os vetores 1 e $\sqrt{c}$ pertencentes a $\mathbb{Q}(\sqrt{c})$ são LI sobre $\mathbb{Q}$.

Exemplo 6. O que dizer sobre o conjunto $\{1 + \sqrt{c}, 1 - \sqrt{c}\}$, em que c não é um quadrado em $\mathbb{Q}$? Para verificar se esse conjunto é LD ou LI, considere que existem a e b pertencentes a $\mathbb{Q}$ tais que $a(1 + \sqrt{c}) + b(1 - \sqrt{c}) = 0$. Note que a igualdade pode ser reescrita como $(a + b) + (a - b)\sqrt{c} = 0$. Se $a - b \neq 0$ e $(a + b) + (a - b)\sqrt{c} = 0$, então $\sqrt{c} = -\dfrac{a+b}{a-b}$. Como $\mathbb{Q}$ é um corpo, $\sqrt{c}$ pertence a $\mathbb{Q}$ que é uma contradição, já que c não é um quadrado em $\mathbb{Q}$. Portanto, para que $(a+b)+(a-b)\sqrt{c} = 0$ seja satisfeita devemos ter $a - b = 0$ o que implica $a + b = 0$. Consequentemente, $a = b = 0$, e os vetores $1 + \sqrt{c}$ e $1 - \sqrt{c}$ são LI em $\mathbb{Q}(\sqrt{c})$.

Exemplo 7. Por fim, o conjunto $\{1 + \sqrt{c}, \ \dfrac{1}{2} + \dfrac{1}{2}\sqrt{c}\}$ é LD sobre $\mathbb{Q}$, pois tomando -1 e 2 em $\mathbb{Q}$ obtemos $(-1)(1 + \sqrt{c}) + 2\left(\dfrac{1}{2} + \dfrac{1}{2}\sqrt{c}\right) = 0$.

Definição 10. Sejam $x_1, x_2, \cdots, x_n$ vetores de $\mathbb{V}$. Dizemos que x é uma combinação linear de $x_1, x_2, \cdots, x_n$ sobre $\mathbb{K}$ se, existem escalares $a_1, a_2, \cdots, a_n$ pertencentes a $\mathbb{K}$ tais que $x = a_1x_1 + a_2x_2 + \cdots + a_nx_n$.

Note que, se x é uma combinação linear $\mathbb{K}$, temos $x = 1 \cdot x$, $1 \neq 0$ e $1 \cdot x - (a_1x_1 + a_2x_2 + \cdots + a_nx_n) = 0$. Segue que, se $\{x_1, x_2, \cdots, x_n\}$ é um conjunto LI, então x é uma combinação linear de $x_1, x_2, \cdots, x_n$ se, e somente se, $\{x, x_1, x_2, \cdots, x_n\}$ é um conjunto LD.

Proposição 2.1.1. *Se $\{x_1, x_2, \cdots, x_n\}$ é um conjunto finito de vetores não nulos de $\mathbb{V}$ com pelo menos dois elementos, então $\{x_1, x_2, \cdots, x_n\}$ é LD se, e somente se, existe um inteiro k , com $2 \leq k \leq n$ tal que x_k é uma combinação linear sobre $\mathbb{K}$ de $x_1, x_2, \cdots, x_{k-1}$.*

Demonstração. Inicialmente suponha que exista tal k, isto é,

$$x_k = \sum_{i=1}^{k-1}$$

com $a_i \in \mathbb{K}$. Se $k < n$, temos

$$\sum_{i=1}^{k-1} a_ix_i - x_k + \sum_{i=k+1}^{n} 0x_i = 0,$$

e se $k = n$,

$$\sum_{i=1}^{n-1} a_i x_i - x_n = 0.$$

Em qualquer caso, como -1, o coeficiente de x_k nas duas identidades, é diferente de zero, o conjunto $\{x_1, x_2, \cdots, x_n\}$ é LD por definição. Agora suponha que o conjunto $\{x_1, x_2, \cdots, x_n\}$ é LD. Escolha k entre os elementos do conjunto $\{2, 3, \cdots, n\}$ para ser o primeiro inteiro tal que $\{x_1, x_2, \cdots, x_k\}$ é LD. Pela hipótese de que o conjunto $\{x_1, x_2, \cdots, x_n\}$ é LD, tal k existe; pode ser 2, pode ser 3, pode ser n, mas não pode ser 1, já que nenhum dos x_i's é zero. Da definição de dependência linear, segue que existem escalares $a_1, a_2, \cdots, a_k$ pertencentes a $\mathbb{K}$, não todos nulos, tais que

$$\sum_{i=1}^{k} a_i x_i = 0.$$

Contudo, $a_k \neq 0$, pois se $a_k = 0$, teríamos

$$\sum_{i=1}^{k-1} a_i x_i = 0$$

com a_i não todos nulos, isto é, o conjunto $\{x_1, x_2, \cdots, x_k\}$ seria LD, contrariando a nossa escolha de k. Por outro lado, se $a_k \neq 0$ podemos dividir

$$\sum_{i=1}^{k-1} a_i x_i = 0$$

por a_k e obtemos

$$\sum_{i=1}^{k-1} \left(\frac{-a_i}{a_k} \right) x_i = 0.$$

Note que $\dfrac{-a_i}{a_k}$ pertence a $\mathbb{K}$, já que $a_k \neq 0$ e $\mathbb{K}$ é um corpo. Portanto, x_k é uma combinação linear de $x_1, x_2, \cdots, x_{k-1}$ sobre $\mathbb{K}$. ■

Embora não pareça, estamos lentamente construindo uma prova de para quais inteiros n podemos ou não construir um polígono regular de n lados com régua e compasso apenas. Um elo fundamental na prova é o da dimensão de um espaço vetorial e como, em certas circunstâncias, as dimensões de dois espaços vetoriais podem estar relacionadas. Definiremos dimensão através do conceito de uma base, que nós introduziremos a seguir.

2.1.3 Bases e dimensão

Definição 11. Uma base finita de $\mathbb{V}$ é qualquer conjunto LI finito $B = \{x_1, x_2, \cdots, x_n\}$ de vetores de $\mathbb{V}$ tais que cada vetor de $\mathbb{V}$ é uma combinação linear de elementos de B sobre $\mathbb{K}$.

Note que $B = \{x_1, x_2, \cdots, x_n\}$ conforme definido acima é um gerador de $\mathbb{V}$.

Proposição 2.1.2. *i) Todo espaço vetorial $\mathbb{V}$ sobre um corpo $\mathbb{K}$ possui uma base.*

ii) Se um espaço vetorial $\mathbb{V}$ sobre um corpo $\mathbb{K}$ possui uma base com n elementos, então toda base de $\mathbb{V}$ possui n elementos.

Demonstração. Veja HEFEZ nas referências bibliográficas.

■

Definição 12. Um espaço vetorial $\mathbb{V}$ tem dimensão finita se ele tem uma base finita. Se o número de elementos nessa base de $\mathbb{V}$ sobre um corpo $\mathbb{K}$ é n definiremos n como sendo a dimensão de $\mathbb{V}$ sobre $\mathbb{K}$ a qual denotaremos por $[\mathbb{V} : \mathbb{K}]$.

Os únicos espaços vetoriais que trataremos aqui serão os de dimensão finita, e daqui em diante vamos nos referir a uma base finita como simplesmente uma base. Note que a definição anterior só faz sentido se cada base para um dado espaço vetorial $\mathbb{V}$ tiver o mesmo número de elementos. A seguir daremos alguns exemplos de bases.

Exemplo 8. Se $\mathbb{K}$ é um corpo contido em $\mathbb{C}$ e c é um complexo que não é um quadrado em $\mathbb{K}$ então $\mathbb{K}(\sqrt{c}) = \{a + b\sqrt{c}/a, b \in \mathbb{K}\}$ sobre $\mathbb{K}$ tem a bas $1, \sqrt{c}$.

Exemplo 9. $\mathbb{Q}(\sqrt{2})(\sqrt{3})$ tem a base $1, \sqrt{2}, \sqrt{3}, \sqrt{6}$ sobre $\mathbb{Q}$.

Exemplo 10. $\mathbb{Q}(\sqrt{2})(\sqrt{3})(\sqrt{5})$ tem a base $1, \sqrt{2}, \sqrt{3}, \sqrt{5}, \sqrt{6}, \sqrt{10}, \sqrt{15}, \sqrt{30}$ sobre $\mathbb{Q}$.

2.2 EXTENSÕES ALGÉBRICAS

A partir deste ponto, se $\mathbb{K}$ é um corpo qualquer, então $\mathbb{F} \supset \mathbb{K}$ denotará uma extensão de $\mathbb{K}$.

Definição 13. Dizemos que α pertencente a $\mathbb{F}$ é algébrico sobre $\mathbb{K}$ se α é raiz de um polinômio não nulo $p(x)$ pertencente a $\mathbb{K}[x]$. Caso contrário dizemos que α é transcendente sobre $\mathbb{K}$.

É claro que, como α pertencente a $\mathbb{K}$ é raiz do polinômio $p(x) = x - \alpha$, temos que α é algébrico sobre $\mathbb{K}$. No caso em que os elementos são algébricos ou transcendentes sobre $\mathbb{Q}$, diremos simplesmente que são algébricos ou transcendentes. Por exemplo, $\sqrt{2}$ é raiz do polinômio $p(x) = x^2 - 2$, portanto $\sqrt{2}$ é algébrico. Enquanto que π é transcendente.

Definição 14. Se para todo α pertencente a $\mathbb{F} \supset \mathbb{K}$, α é algébrico sobre $\mathbb{K}$ dizemos que $\mathbb{F} \supset \mathbb{K}$ é uma extensão algébrica.

Definição 15. Se α pertencente a $\mathbb{F}$ é algébrico sobre $\mathbb{K}$ e $p(x)$ é um polinômio mônico, de menor grau, pertencente a $\mathbb{K}[x]$, tal que $p(\alpha) = 0$, dizemos que $p(x)$ é o polinômio mínimo de α sobre $\mathbb{K}$.

Pela minimalidade do grau de $p(x)$ segue que $p(x)$ é o único polinômio mônico irredutível sobre $\mathbb{K}$, que será indicado por $p(x) = min(\alpha, \mathbb{K})$, tal que $p(\alpha) = 0$.

Definição 16. Se α pertence a $\mathbb{F} \supset \mathbb{K}$ e $p(x)$ é um polinômio pertencente a $\mathbb{K}[x]$, definimos $\mathbb{K}(\alpha)$ como sendo o conjunto dos $p(\alpha)$, isto é, $\mathbb{K}(\alpha) = \{p(\alpha) : p(x) \in \mathbb{K}[x]\}$. Note que $\mathbb{F} \supset \mathbb{K}(\alpha) \supset \mathbb{K}$.

Exemplo 11. Se $\sqrt{2} \in \mathbb{R} \supset \mathbb{Q}$, vamos encontrar $\mathbb{Q}(\sqrt{2})$. Por definição temos $\mathbb{Q}(\sqrt{2}) = \{p(\sqrt{2}) : p(x) \in \mathbb{Q}[x]\}$. Como $p(x)$ pertence a $\mathbb{Q}[x]$, segue do algoritmo da divisão que existem $q(x)$ e $r(x)$ pertencentes a $\mathbb{Q}[x]$ tais que $p(x) = q(x) \cdot (x^2 - 2) + r(x)$, em que $r(x) = bx + a$, com a e b pertencentes a $\mathbb{Q}$. Segue que $p(\sqrt{2}) = q(\sqrt{2}) \cdot (\sqrt{2}^2 - 2) + r(\sqrt{2}) = r(\sqrt{2}) = a + b\sqrt{2}$. Note que $\mathbb{R} \supset \mathbb{Q}(\alpha) \supset \mathbb{Q}$.

2.3 GRAU DE UMA EXTENSÃO

Definição 17. Seja $\mathbb{K}$ um corpo qualquer. Dizemos que uma extensão $\mathbb{F} \supset \mathbb{K}$ é finita se $[\mathbb{F} : \mathbb{K}] = n$. Caso contrário, dizemos que a extensão $\mathbb{F} \supset \mathbb{K}$ é infinita. O grau da extensão $\mathbb{F} \supset \mathbb{K}$ é definido como sendo o valor $[\mathbb{F} : \mathbb{K}] = n$.

Proposição 2.3.1. *Se $\mathbb{K}$ é um corpo qualquer e $\mathbb{F} \supset \mathbb{K}$ é uma extensão de $\mathbb{K}$, então:*

i) se $\mathbb{F} \supset \mathbb{K}$ finita, logo $\mathbb{F} \supset \mathbb{K}$ é algébrica.

ii) se α pertencente a $\mathbb{F} \supset \mathbb{K}$ é um elemento algébrico sobre $\mathbb{K}$ e o grau de $min(\alpha, \mathbb{K})$ é igual a n, logo $B = \{1, \alpha, \alpha^2, \cdots, \alpha^{n-1}\}$ é uma base do espaço vetorial $\mathbb{K}(\alpha)$ sobre o corpo $\mathbb{K}$ e $[\mathbb{K}(\alpha) : \mathbb{K}] = n$.

iii) se α pertencente a $\mathbb{F} \supset \mathbb{K}$ é um elemento transcendente sobre $\mathbb{K}$, então a extensão $\mathbb{K}(\alpha) \supset \mathbb{K}$ é infinita.

Demonstração. i) Suponha que $[\mathbb{F} : \mathbb{K}] = m$ e α pertence a $\mathbb{F} \supset \mathbb{K}$. Como $\mathbb{K}(\alpha)$ é um subespaço de $\mathbb{F}$ temos que $[\mathbb{K}(\alpha) : \mathbb{K}] \leq m$. Se $[\mathbb{K}(\alpha) : \mathbb{K}] = n$, então o conjunto $\{1, \alpha, \alpha^2, \cdots, \alpha^{n-1}, \alpha^n\}$ é LD, já que n é o número máximo de elementos LI, e sendo assim, existem escalares a_0, a_1, a_2, $\cdots$, a_n não todos nulos tais que $a_n\alpha^n + a_{n-1}\alpha^{n-1} +$

$\cdots + a_2\alpha^2 + a_1\alpha + a_0$. Isso mostra que α é raiz de um polinômio com coeficientes em $\mathbb{K}$. Portanto, α é algébrico sobre $\mathbb{K}$.

Note que a recíproca de i) não é verdadeira, pois existem extensões algébricas infinitas. O subcorpo dos números complexos que consistem de todos os números algébricos sobre $\mathbb{Q}$ é um exemplo de uma extensão infinita de $\mathbb{Q}$.

ii) Seja α pertencente a $\mathbb{F} \supset \mathbb{K}$ um elemento algébrico sobre $\mathbb{K}$ tal que o grau de $min(\alpha, \mathbb{K})$ é igual a n. Sabemos que todo elemento de $\mathbb{K}(\alpha)$ pode ser unicamente escrito como combinação linear de $1, \alpha, \alpha^2, \cdots, \alpha^{n-1}$ sobre $\mathbb{K}$. Sendo assim, $B = \{1, \alpha, \alpha^2, \cdots, \alpha^{n-1}\}$ é uma base de $\mathbb{K}(\alpha)$ sobre $\mathbb{K}$. Isso mostra que $[\mathbb{K}(\alpha) : \mathbb{K}] = n$.

iii) Se $\mathbb{K}(\alpha) \supset \mathbb{K}$ fosse uma extensão finita, pelo item i) $\mathbb{K}(\alpha) \supset \mathbb{K}$ seria algébrica. Portanto, α seria algébrico sobre $\mathbb{K}$.

■

Segue imediatamente da proposição anterior que, se α pertencente a $\mathbb{F} \supset \mathbb{K}$, então as seguintes afirmações são equivalentes:

i) α é algébrico sobre $\mathbb{K}$.

ii) $[\mathbb{K}(\alpha) : \mathbb{K}]$ é finito.

iii) $\mathbb{K}(\alpha)$ é uma extensão algébrica de $\mathbb{K}$.

A seguir veremos que o grau de uma extensão simples é igual ao grau do polinômio mínimo do elemento associado. Como vimos anteriormente, o elemento $\sqrt{3}$ associado a $\mathbb{Q}$ tem $min(\alpha, \mathbb{Q}) = x^2 - 3$. Segue que $[\mathbb{Q}(\sqrt{3}) : \mathbb{Q}] = 2$.

Proposição 2.3.2. *Seja α um número algébrico sobre o corpo $\mathbb{K}$. Então $\mathbb{K}(\alpha) = \mathbb{K}[\alpha]$, e $\mathbb{K}(\alpha)$ é finito sobre $\mathbb{K}$. O grau $[\mathbb{K}(\alpha) : \mathbb{K}]$ é igual ao grau de $min(\alpha, \mathbb{K})$.*

Demonstração. Sejam $p(x) = min(\alpha, \mathbb{K})$ e $f(x)$ um polinômio pertencente a $\mathbb{K}[x]$ tal que $f(\alpha) \neq 0$. Assim, $p(x)$ não divide $f(x)$, e portanto existem polinômios $g(x)$ e $h(x)$ tais que $g(x)p(x) + h(x)f(x) = 1$. Segue que $h(\alpha)f(\alpha) = 1$, isto é, $f(\alpha)$ é invertível em $\mathbb{K}[\alpha]$. Consequentemente $\mathbb{K}[\alpha]$ é um corpo, e assim sendo deve ser igual a $\mathbb{K}(\alpha)$. Seja $d = \partial(p(x))$. O conjunto $\{\alpha^{d-1}, \alpha^{d-2}, \cdots, \alpha^2, \alpha, 1\}$ é LI sobre $\mathbb{K}$, caso contrário suponha que $a_{d-1}\alpha^{d-1} + a_{d-2}\alpha^{d-2} + \cdots + a_2\alpha^2 + a_1\alpha + 1 = 0$ com a_i pertencente a $\mathbb{K}$ não todos nulos. Seja $g(x) = a_{d-1}x^{d-1} + a_{d-2}x^{d-2} + \cdots + a_2x^2 + a_1x + a_0$. Então $g(x) \neq 0$, já que a_i não são todos nulos, e $g(\alpha) = 0$. Portanto, $p(x)$ divide $g(x)$ que é uma contradição. Finalmente, seja $f(\alpha)$

pertencente a $\mathbb{K}[\alpha]$ em que $f(x)$ pertence a $\mathbb{K}[x]$. Existem polinômios $q(x)$ e $r(x)$ pertencentes a $\mathbb{K}[x]$ tais que $\partial(r(x)) < d$ e $f(x) = q(x)p(x)+r(x)$. Então $f(\alpha) = r(\alpha)$ e vimos que 1, α, α^2, $\cdots$, α^{d-2}, α^{d-1} geram $\mathbb{K}[\alpha]$ como um espaço vetorial sobre $\mathbb{K}$. Isso prova nossa proposição. ■

O fato do grau de uma extensão simples ser igual ao grau do polinômio mínimo do elemento associado será de fundamental importância para nossos argumentos no momento de mostrar se certos números são construtíveis, encontrando seus polinômios mínimos e mostrando que seus corpos de decomposição têm extensões de grau uma potência de dois sobre $\mathbb{Q}$. Um resultado importante relativo às extensões de corpos é a multiplicatividade do grau, como veremos a seguir.

Proposição 2.3.3 (A multiplicatividade do grau de uma extensão)**.** *Sejam $\mathbb{K}$ um corpo e $\mathbb{E} \supset \mathbb{F}$ extensões de $\mathbb{K}$. Se $[\mathbb{E} : \mathbb{F}]$, $[\mathbb{F} : \mathbb{K}]$ são finitos, então $[\mathbb{E} : \mathbb{K}]$ é finito e $[\mathbb{E} : \mathbb{K}] = [\mathbb{E} : \mathbb{F}] \cdot [\mathbb{F} : \mathbb{K}]$.*

Demonstração. Sejam $\{x_i\}_{i\in I}$ uma base de $\mathbb{F}$ sobre $\mathbb{K}$ e $\{y_j\}_{i\in J}$ uma base de $\mathbb{E}$ sobre $\mathbb{F}$. Note que é suficiente provar que $\{x_i y_j\}_{(i,j)\in I\times J}$ é uma base de $\mathbb{E}$ sobre $\mathbb{K}$. Seja $z \in \mathbb{E}$. Por hipótese existem $a_j \in \mathbb{F}$, não todos nulos, tais que

$$z = \sum_{j\in J} a_j y_j.$$

Para cada $j \in J$ existem elementos $b_{ji} \in \mathbb{K}$, não todos nulos, tais que

$$a_j = \sum_{i\in I} b_{ji} x_i$$

e, portanto

$$z = \sum_j \sum_i b_{ji} x_i y_j.$$

Isso mostra que $\{x_i y_j\}$ é um conjunto de geradores de $\mathbb{E}$ sobre $\mathbb{K}$. Resta mostrar que $\{x_i y_j\}$ é LI. Seja $\{c_{ij}\}$ um conjuntos de elementos de $\mathbb{K}$, não todos nulos, tais que

$$\sum_j \sum_i c_{ij} x_i y_j = 0.$$

Então para cada j, temos

$$\sum_i c_{ij} x_i,$$

pois $\{y_i\}$ é LI sobre $\mathbb{F}$. Finalmente, $c_{ij} = 0$ para cada i, pois $\{x_i\}$ é LI sobre $\mathbb{K}$, provando assim a proposição. ■

Sabemos que, se um número α é construtível, então $\sqrt{\alpha}$ é construtível. Usando esse fato, note que cada vez que extraímos uma raiz quadrada em um corpo não euclidiano, estendemos esse corpo por uma extensão de grau 2. Portanto, todas as extensões atingidas deste modo têm como grau uma potência de 2, como veremos a seguir.

Proposição 2.3.4. *Se α é construtível, então $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 2^m$ para algum inteiro $m \geq 0$.*

Demonstração. Seja α um número construtível. Segue da definição de números construtíveis que existe uma torre de extensões de corpos de grau dois de $\mathbb{Q}$ para $\mathbb{Q}(\alpha)$. Da multiplicatividade do grau temos $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 2^m$. ■

A condição de que $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 2^m$, embora necessária, não é suficiente para a construtibilidade. Mais adiante, daremos um exemplo de um número algébrico de grau uma potência de 2 não construtível por régua e compasso.

3 POLINÔMIOS IRREDUTÍVEIS

Sendo $\mathbb{K}$ um corpo, denotaremos por $\mathbb{K}[x]$ o conjunto dos polinômios com coeficientes pertencentes ao corpo $\mathbb{K}$. Destacaremos aqui os polinômios pertencentes a $\mathbb{K}[x]$ que, comparando $\mathbb{K}[x]$ com o conjunto dos números inteiros $\mathbb{Z}$, desempenham o mesmo papel dos números primos pertencentes a $\mathbb{Z}$. Chamaremos esses polinômios de polinômios irredutíveis sobre o corpo $\mathbb{K}$.

Definição 18. Seja $p(x)$ um polinômio pertecente a $\mathbb{K}[x]$ tal que o grau de $p(x)$ seja pelo menos 1. Dizemos que $p(x)$ é um polinômio irredutível sobre $\mathbb{K}$ se sempre que $p(x) = p_1(x) \cdot p_2(x)$, em que $p_1(x)$, $p_2(x)$ são polinômios pertencentes a $\mathbb{K}[x]$, temos $p_1(x) = k_1$ ou $p_2(x) = k_2$, em que k_1 e k_2 são constantes pertencentes a $\mathbb{K}$. Se $p(x)$ não é irredutível sobre $\mathbb{K}$, dizemos que $p(x)$ é redutível sobre $\mathbb{K}$.

Note que todo polinômio de grau 1 sobre um corpo $\mathbb{K}$ é irredutível sobre $\mathbb{K}$.

O polinômio $p(x) = x^2 + 2$ é irredutível sobre o corpo $\mathbb{Q}$, mas é redutível sobre o corpo $\mathbb{Q}[\sqrt{2}]$. Segue que um polinômio pertencente a $\mathbb{K}[x]$ pode ser irredutível sobre $\mathbb{K}$ e redutível sobre uma extensão quadrática de $\mathbb{K}$.

A seguir mostraremos o análogo ao Teorema da Fatoração Única em $\mathbb{Z}$. Para isso usaremos $a \cdot p_1(x) \cdot p_2(x) \cdot \cdots \cdot p_r(x)$ considerando a possibilidade $p(x) = a$ quando $r = 0$, em que $a \neq 0$ é um elemento de $\mathbb{K}$ e $p_1(x)$, $p_2(x)$, $\cdots$, $p_r(x)$ são polinômios irredutíveis sobre $\mathbb{K}$.

Proposição 3.0.1. *Seja $\mathbb{K}$ um corpo. Todo polinômio $p(x)$ não nulo pertencente a $\mathbb{K}[x]$ pode ser escrito de modo único como $p(x) = a \cdot p_1(x) \cdot p_2(x) \cdot \cdots \cdot p_r(x)$ (a menos da constante a e da ordem dos polinômios $p_1(x)$, $p_2(x)$, $\cdots$, $p_r(x)$) , em que a é um elemento não nulo de $\mathbb{K}$ e $p_1(x)$, $p_2(x)$, $\cdots$, $p_r(x)$ são polinômios mônicos (distintos ou não) irredutíveis sobre $\mathbb{K}$.*

Demonstração. Veja a referência GONÇALVES. ■

3.1 O LEMA DE GAUSS E O TESTE DE EISENSTEIN PARA VERIFICAÇÃO DA IRREDUTIBILIDADE DE POLINÔMIOS

Nem sempre é fácil verificar a irredutibilidade de um polinômio. Veremos nesta seção uma proposição que nos fornece condições suficientes para que um polinômio de coeficientes racionais seja irredutível sobre $\mathbb{Q}$. É evidente que, se multiplicarmos o polinômio pelo

$m.m.c.$ dos denominadores dos coeficientes do polinômio, podemos admitir que o polinômio tem coeficientes inteiros. Primeiramente provaremos o Lema de Gauss o qual afirma que a irredutibilidade de um polinômio sobre $\mathbb{Z}$ é equivalente à irredutibilidade desse polinômio sobre $\mathbb{Q}$.

Proposição 3.1.1 (Lema de Gauss). *Se $p(x)$ é um polinômio pertencente a $\mathbb{Z}[x]$ tal que $p(x)$ é irredutível sobre $\mathbb{Z}$, então $p(x)$ é irredutível sobre $\mathbb{Q}$.*

Demonstração. Suponha que $p(x)$ seja irredutível sobre $\mathbb{Z}$ mas $p(x) = p_1(x) \cdot p_2(x)$, em que $p_1(x)$ e $p_2(x)$ pertencem a $\mathbb{Q}[x]$ e $1 \leq \partial p_1(x) \leq \partial p_2(x) \leq \partial p(x)$. Note que existe um inteiro a tal que $a \cdot p(x) = p_3(x) \cdot p_4(x)$, em que $p_3(x)$ e $p_4(x)$ pertencem a $\mathbb{Z}[x]$. Assim temos:

$p_3(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots a_2 x^2 + a_1 x + a_0$ em que $a_i \in \mathbb{Z}$.

$p_4(x) = b_m x^m + b_{m-1}x^{m-1} + \cdots b_2 x^2 + b_1 x + b_0$ em que $b_i \in \mathbb{Z}$.

Considere que existe um primo p tal que p divide a. Mostraremos que p divide a_i para todo $i \in \{1, 2, \cdots, n\}$ ou p divide b_j para todo $j \in \{1, 2, \cdots, m\}$.

Suponha que existe $i \in \{1, 2, \cdots, n\}$ e existe $j \in \{1, 2, \cdots, m\}$ tais que p não divide a_i e p não divide b_j e sejam i e j menores possíveis com esta propriedade.

Como p divide a temos que p divide o coeficiente de x^{i+j} do polinômio $ap(x) = p_3(x) \cdot p_4(x)$, ou seja, p divide $(a_{i+j} \cdot b_0 + a_{i+j-1} \cdot b_1 + \cdots + a_i \cdot b_j + \cdots + a_1 \cdot b_{i+j-1} + a_0 \cdot b_{i+j})$

Pela escolha de i e j temos que p divide cada parcela de $(a_{i+j} \cdot b_0 + a_{i+j-1} \cdot b_1 + \cdots + a_i \cdot b_j + \cdots + a_1 \cdot b_{i+j-1} + a_0 \cdot b_{i+j})$, exceto $a_i \cdot b_j$ que é o coeficiente de x^{i+j} do polinômio $ap(x) = p_3(x) \cdot p_4(x)$.

Como p divide toda a expressão, p também divide $a_i \cdot b_j$ e como p é primo temos que p divide a_i ou p divide b_j, contradizendo a escolha de i e j. Segue que, se p é primo e p divide a, então p divide a_i para todo $i \in \{1, 2, \cdots, n\}$ ou p divide b_j para todo $j \in \{1, 2, \cdots, m\}$.

Sem perda de generalidade, considere que p divide a_i para todo $i \in \{1, 2, \cdots, n\}$. Segue que, $p_3(x) = p \cdot p_5(x)$, em que $p_5(x)$ pertence a $\mathbb{Z}[x]$, e considerando $a = p \cdot b$ temos $p \cdot b \cdot p(x) = p \cdot p_4(x) \cdot p_5(x)$ daí $b \cdot p(x) = p_4(x) \cdot p_5(x)$.

Como o número de fatores primos de a é finito, se continuarmos com o argumento acima, teremos $p(x) = p_r(x) \cdot p_s(x)$, em que $p_r(x)$ e $p_s(x)$ pertencem a $\mathbb{Z}[x]$. Isso contradiz a irredutibilidade de $p(x)$ sobre $\mathbb{Z}[x]$. ■

Proposição 3.1.2 (Teste de Eisenstein). *Seja $p(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_2 x^2 + a_1 x + a_0$ um polinômio pertencente a $\mathbb{Z}[x]$, $n \geq 1$. Se existe um inteiro primo p tal que:*

i) p *não divide* a_n

ii) p *divide* a_0, a_1, a_2, $\cdots$, a_{n-1}

iii) p^2 *não divide* a_0

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

Demonstração. De acordo com o lema de Gauss, é suficiente mostrar que $p(x)$ é irredutível sobre $\mathbb{Z}$. Suponha que $p(x) = p_1(x) \cdot p_2(x)$, em que $p_1(x)$ e $p_2(x)$ pertencem a $\mathbb{Z}[x]$ e $1 \leq \partial p_1(x) \leq \partial p_2(x) \leq \partial p(x) = n$.

$p_1(x) = b_{n_1}x^{n_1} + b_{n_1-1}x^{n_1-1} + \cdots b_2x^2 + b_1x + b_0$ pertencente a $\mathbb{Z}[x]$ e $\partial p_1(x) = n_1$

$p_2(x) = c_{n_2}x^{n_2} + c_{n_2-1}x^{n_2-1} + \cdots c_2x^2 + c_1x + c_0$ pertencente a $\mathbb{Z}[x]$ e $\partial p_2(x) = n_2$

Assim, temos $n = n_1 + n_2$.

Note que $a_0 = b_0 \cdot c_0$ e como p é um primo tal que p divide a_0 segue que p divide b_0 ou p divide c_0. Mas, por hipótese, p^2 não divide a_0 e segue que p divide apenas um dos inteiros b_0 e c_0. Considere, sem perda de generalidade, que p divide b_0 e p não divide c_0.

Note que $a_n = b_{n_1} \cdot c_{n_2}$ é o coeficiente de $x^n = x^{n_1+n_2}$ e p não divide b_{n_1} e p divide b_0. Seja b_i o primeiro coeficiente de $p_1(x)$ tal que p não divide b_i.

Assim, temos $a_i = b_0 \cdot c_i + b_1 \cdot c_{i-1} + \cdots + b_i \cdot c_0$ e como p divide b_0, b_1, $\cdots$, b_{i-1}, p não divide b_i e c_0, segue que p não divide a_i o que significa $i = n$. Mas, isso é uma contradição pois $1 \leq i \leq n_1 < n$. ■

A seguir mostramos alguns exemplos de polinômios irredutíveis sobre $\mathbb{Q}$.

Exemplo 12. Se $p(x) = x^5 + 6x + 14$, podemos aplicar o teste de Eisenstein para o primo $p = 2$ e constatar facilmente que $p(x)$ é irredutível sobre $\mathbb{Q}$.

Exemplo 13. Seja $p(x) = x^n - p$ um polinômio de grau $n \geq 1$, em que p é um primo qualquer. Podemos aplicar o teste de Eisenstein para o próprio primo p e concluir facilmente que $p(x)$ é irredutível sobre $\mathbb{Q}$.

No exemplo a seguir, usaremos o seguinte fato: Sejam $\mathbb{K}$ um corpo e $\mathbb{K}[x]$ o conjunto dos polinômios com coeficientes pertencentes a $\mathbb{K}$. Se $k \in \mathbb{K}$ e $p(x) \in \mathbb{K}[x]$, então $p(x)$ é irredutível sobre $\mathbb{K}$ se, e somente se, $f(x + k)$ é irredutível sobre $\mathbb{K}$.

Exemplo 14. Seja $p(x) = x^{p-1} + x^{p-2} + \cdots + x^2 + x + 1$ um polinômio, em que p é um primo positivo. Mostraremos que $p(x)$ é irredutível sobre $\mathbb{Q}$. Note que não podemos aplicar o teste

de Eisenstein, mas sabemos que, pelo argumento anterior, $p(x)$ será irredutível sobre $\mathbb{Q}$ se $p(x+1)$ for irredutível sobre $\mathbb{Q}$. Após desenvolver $p(x+1) = (x+1)^{p-1} + (x+1)^{p-2} + \cdots + (x+1)^2 + (x+1) + 1$ aplicamos o teste de Eisenstein para o próprio primo p e verificamos que $p(x)$ é irredutível sobre $\mathbb{Q}$.

A proposição a seguir nos fornece mais um critério de irredutibilidade sobre $\mathbb{Q}$

Proposição 3.1.3. *Sejam p um primo positivo e $\mathbb{Z}_p = \{\overline{0}, \overline{1}, \overline{2}, \cdots, \overline{p-1}\}$ o corpo contendo p elementos. Se $p(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_2 x^2 + a_1 x + a_0$ pertence a $\mathbb{Z}[x]$, defina o polinômio $\overline{p}(x)$ pertencente a $\mathbb{Z}_p[x]$ da seguinte forma:*

$$\overline{p}(x) = \overline{a_n}x^n + \overline{a_{n-1}}x^{n-1} + \cdots + \overline{a_2}x^2 + \overline{a_1}x + \overline{a_0},$$

em que $\overline{a_i} = a_i + p\mathbb{Z}$ é a classe de equivalência, módulo p, cujo representante é $a_i \in \mathbb{Z}$. Se p não divide a_n e $\overline{p}(x)$ é irredutível sobre $\mathbb{Z}_p$, então $p(x)$ é irredutível sobre $\mathbb{Q}$.

Demonstração. Sejam $p(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_2 x^2 + a_1 x + a_0$ um polinômio de grau n e p um primo tal que p não divide a_n. Suponha que $p(x)$ pertence a $\mathbb{Z}[x]$ e é redutível sobre $\mathbb{Q}$. Segue do lema de Gauss que existem $f(x) = b_m x^m + b_{m-1}x^{m-1} + \cdots + b_2 x^2 + b_1 x + b_0$ de grau m, com $1 \leq m < n$, e $g(x) = c_k x^k + c_{k-1}x^{k-1} + \cdots + c_2 x^2 + c_1 x + c_0$ de grau k, com $1 \leq k < n$, tais que $p(x) = f(x) \cdot g(x)$. Assim, temos $\overline{p}(x) = \overline{f}(x) \cdot \overline{g}(x)$, em que $\overline{f}(x)$ e $\overline{g}(x)$ pertencem a $\mathbb{Z}_p[x]$. E, como $a_n = b_m \cdot c_k$ e p não divide a_n, segue que p não divide b_m e nem c_k, logo $b_m \neq \overline{0}$ e $c_k \neq \overline{0}$, isto é, o grau de $\overline{f}(x)$ é m e o grau de $\overline{g}(x)$ é k. Portanto, $\overline{p}(x)$ é redutível sobre $\mathbb{Z}_p$. ■

Exemplo 15. Considere $p(x) = x^4 + 15x^3 + 10x^2 + 25x + 22$ em $\mathbb{Z}[x]$. Mostraremos que $p(x)$ é irredutível sobre $\mathbb{Q}$. Para isso, considere $p = 5$ e $\mathbb{Z}_5 = \{\overline{0},\ \overline{1},\ \overline{2},\ \overline{3},\ \overline{4}\}$. Assim, temos $\overline{p}(x) = x^4 + \overline{2}$ em $\mathbb{Z}_5[x]$. Como 5 não divide 1, pela proposição anterior basta mostrar que $\overline{p}(x) = x^4 + \overline{2}$ é irredutível sobre $\mathbb{Z}_5$. Note que $\overline{p}(x) = x^4 + \overline{2}$ não possui raízes em $\mathbb{Z}_5$. Logo, a única maneira de fatoramos $\overline{p}(x) = x^4 + \overline{2}$ seria $\overline{p}(x) = x^4 + \overline{2} = (a_1x^2 + b_1x + c_1)(a_2x^2 + b_2x + c_2)$, em que a_1, b_1, c_1, a_2, b_2, c_2 pertencentes a $\mathbb{Z}_5 = \{\overline{0},\ \overline{1},\ \overline{2},\ \overline{3},\ \overline{4}\}$. Entretanto, podemos verificar facilmente que essa fatoração é impossível. Portanto, $p(x) = x^4 + 15x^3 + 10x^2 + 25x + 22$ é irredutível sobre $\mathbb{Q}$.

4 A CONSTRUTIBILIDADE DO PENTÁGONO E DO HEPTADECÁGONO REGULARES E A NÃO CONSTRUTIBILIDADE DO HEPTÁGONO E DO ENEÁGONO REGULARES

Iniciaremos este capítulo mostrando quando as raízes de uma equação cúbica são construtíveis por meio de régua e compasso. Em seguida provaremos a impossibilidade de resolver dois dos três problemas clássicos de construção deixados sem solução pelos gregos. Finalizando, mostraremos a não construtibilidade do heptátono e do eneágono regulares e a construtibilidade do pentágono e do heptadecágono regulares.

4.1 EQUAÇÕES CÚBICAS IRREDUTÍVEIS

Uma equação cúbica, com coeficientes racionais, é dita irredutível sobre $\mathbb{Q}$ se não tem nenhuma raiz racional. A seguir mostraremos que se uma equação cúbica é irredutível sobre $\mathbb{Q}$ suas raízes não são construtíveis por régua e compasso.

Proposição 4.1.1. *Se uma equação cúbica, com coeficientes racionais, é irredutível sobre $\mathbb{Q}$ (não tem raiz racional), então nenhuma de suas raízes é construtível.*

Demonstração. Uma equação cúbica com coeficientes racionais é redutível sobre $\mathbb{Q}$ se tiver pelo menos uma raiz racional. Se a equação não tem raiz racional, diz-se que ela é irredutível sobre $\mathbb{Q}$. Assim, queremos mostrar que nenhuma raiz real de uma equação cúbica irredutível pode ser construtível. Suponha que a equação cúbica $x^3 + px^2 + qx + r = 0$ em que p, q e r são números racionais, não tem raiz racional mas tem uma raiz que é construtível. Seja $\mathbb{K}_0 = \mathbb{Q}$. Existe um menor inteiro positivo i tal que a cúbica tem uma raiz α construtível numa extensão quadrática $\mathbb{K}_i$ com $\mathbb{K}_i = \mathbb{Q}\left(\sqrt{c_1}, \sqrt{c_2}, \cdots, \sqrt{c_i}\right)$. Seja $\mathbb{K}_j = \mathbb{Q}\left(\sqrt{c_1}, \sqrt{c_2}, \cdots, \sqrt{c_j}\right)$ para $j = 1, 2, \cdots, i-1$. Então $\mathbb{K}_j$ é uma extensão quadrática de $\mathbb{K}_{j-1}$ para $j = 1, 2, \cdots, i$, isto é, $\mathbb{K}_j = \mathbb{K}_{j-1}\left(\sqrt{c_j}\right)$. Pela nossa suposição existem a e b pertencentes a $\mathbb{K}_{i-1}$ tal que $\alpha = a + b\sqrt{c_i}$. Note que devemos ter $b \neq 0$, caso contrário a raiz α pertenceria a $\mathbb{K}_{i-1}$ contradizendo a minimalidade de i. Da identidade algébrica $\left(a \pm b\sqrt{c_i}\right)^3 + p\left(a \pm b\sqrt{c_i}\right)^2 + q\left(a \pm b\sqrt{c_i}\right) + r = \left(a^3 + 3ab^2c_i + pa^2 + pb^2c_i + qa + r\right) \pm \left(3a^2b + b^3c_i + 2pab + qb\right)\sqrt{c_i}$ concluímos que $\overline{\alpha} =$

$a - b\sqrt{c_i}$ deve ser uma raiz da cúbica sempre que $\alpha = a + b\sqrt{c_i}$ é uma raiz. Como $b \neq 0$, as raízes α e $\overline{\alpha}$ são distintas. Seja β a terceira raiz da cúbica. Assim, temos $x^3 + px^2 + qx + r = (x - \beta)(x - \alpha)(x - \overline{\alpha})$. Comparando os coeficientes de x^2, temos $p = -\beta - 2a$. Segue que $\beta = -p - 2a$ e β pertence a $\mathbb{K}_{i-1}$. Como β é uma raiz da cúbica e pertence a $\mathbb{K}_{i-1}$, isso contradiz a minimalidade de i. Logo, nossa suposição inicial é falsa. ■

Note que, reciprocamente, se uma equação cúbica com coeficientes racionais tem uma raiz racional α, podemos escrever a equação na forma $(x - \alpha)(x^2 + px + q) = 0$, em que p e q são racionais. Portanto, as raízes desta equação são construtíveis. Resumindo, podemos enunciar a proposição a seguir.

Proposição 4.1.2. *As raízes de uma equação cúbica, com coeficientes racionais, são construtíveis se, e somente se, a equação tem uma raiz racional. Se a equação é irredutível (não tem raiz racional), então nenhuma de suas raízes é construtível.*

Como veremos nas seções seguintes, esta propriedade das equações cúbicas é de fundamental importância na prova da impossibilidade dos problemas da duplicação do cubo, trisecção de um ângulo e a não construtibilidade do heptágono e do eneágono regulares. Para o problema da quadratura do círculo, apenas indicaremos a prova por requerer resultados de natureza diferente. Antes de darmos início a essas seções, mostraremos um resultado que é de grande utilidade no momento de verificar se uma equação polinomial admite raiz racional ou não.

Proposição 4.1.3. *Se uma equação polinomial $a_n x^n + a_{n-1}x^{n-1} + \cdots + a_2 x^2 + a_1 x + a_0 = 0$, em que a_0, a_1, a_2, $\cdots$, a_{n-1}, a_n são todos inteiros, tem uma raiz racional p/q, com p e q inteiros primos entre si, então p divide a_0 e q divide a_n.*

Demonstração. Como p/q é uma raiz da equação, substituindo no lugar do x na equação obtemos

$$a_n \left(\frac{p}{q}\right)^n + a_{n-1}\left(\frac{p}{q}\right)^{n-1} + \cdots + a_2\left(\frac{p}{q}\right)^2 + a_1\left(\frac{p}{q}\right) + a_0 = 0$$

que multiplicando por q^n resulta em

$$a_n p^n + a_{n-1}qp^{n-1} + \cdots + a_2 q^{n-2}p^2 + a_1 q^{n-1}p + a_0 q^n = 0.$$

Como p divide o lado direito da equação e divide todos os termos do lado esquerdo que precede o último, então p deve dividir $a_0 q^n$. Contudo, como p e q são primos entre si, p divide a_0. Do mesmo modo, como q divide todos os termos depois do primeiro e divide o lado direito da equação, q deve dividir $a_n p^n$. Mas, como p e q são primos entre si, q deve dividir a_n. ■

4.2 O PROBLEMA DA DUPLICAÇÃO DO CUBO

O problema da construção de um cubo cujo volume é igual ao dobro do volume de um dado cubo é conhecido como o problema Deliano. D. E. Smith em sua História da Matemática relata a seguinte história com referência a este problema: "... os atenienses apelaram para o oráculo de Delos para saber como eliminar a peste que visitava sua cidade em 430 A.C. Dizem que o oráculo respondeu que eles deveriam dobrar o tamanho do altar de Apolo. Este altar sendo um cubo, o problema era o de sua duplicação ".

O problema de duplicar um cubo cuja aresta é uma unidade de comprimento leva à equação $x^3 = 2$, que é uma equação cúbica irredutível. Pois, pela proposição 4.1.3, se uma das raízes da equação $x^3 - 2 = 0$ fosse racional, seria um dos números -1, 1, -2, 2. Mas nenhum desses números é raiz da equação. Como $x^3 - 2 = 0$ é uma equação cúbica irredutível, suas raízes não são construtíveis e não é possível duplicar o cubo por régua e compasso.

4.3 O PROBLEMA DA TRISSECÇÃO DE UM ÂNGULO

Determinados ângulos podem ser trissectados sem dificuldade. Por exemplo, um ângulo reto pode ser trissectado, pois um ângulo de 30^o pode ser construído com régua e compasso. No entanto, não é possível, usando apenas régua e compasso, construir a terça parte de um ângulo arbitrário.

Provaremos esta afirmação mostrando que um ângulo de 60^o não pode ser trissectado. Para isso, faremos uso da fórmula $cos(3\theta) = 4cos^3\theta - 3cos\theta$ desenvolvida no estudo da trigonometria.

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

$$2cos(3\theta) = 8cos^3\theta - 6cos\theta$$

Fazendo $3\theta = 60^o$ e $2cos20^o = x$, temos:

$$2cos60^o = (2cos20^o)^3 - 3(2cos20^o)$$

$$2 \cdot (1/2) = x^3 - 3x$$

$$x^3 - 3x - 1 = 0$$

Obtemos uma equação cúbica que tem como uma de suas raízes o número $2cos20^o$. Pela proposição 4.1.3, se essa equação cúbica admite raiz racional, essa raiz teria que ser 1 ou -1. Mas, nem 1 e nem -1 são raízes da equação. Segue que $x^3 - 3x - 1 = 0$ é irredutível sobre $\mathbb{Q}$ e suas raízes não são construtíveis. Assim, como $2cos20^o$ não é construtível, temos que $cos20^o$ não é construtível. Já que um ângulo é construtível se, e somente se, seu cosseno é construtível, acabamos de mostrar que um ângulo de 20^o não é construtível e que um ângulo arbitrário não pode ser trissectado por régua e compasso.

4.4 O PROBLEMA DA QUADRATURA DO CÍRCULO

O problema da quadratura do círculo consiste na construção de um quadrado de área igual à área de um círculo de raio unitário. A proposição 2.3.4 indica que π deveria ser algébrico de grau uma potência de 2, isto é, $[\mathbb{Q}(\pi) : \mathbb{Q}] = 2^m$ para algum inteiro $m \geq 0$. De fato, foi provado por Ferdinand von Lindemann, em 1882, que π é transcendental sobre $\mathbb{Q}$, isto é, π não é raiz de nenhum polinômio de coeficientes inteiros, de modo que a quadratura do círculo é impossível. Sua prova é baseada na primeira prova da transcendência de e, $e = \sum_{n=0}^{\infty} \frac{1}{n!}$, que foi criada pelo matemático francês Charles Hermite em 1873. A prova de que π é transcendental pode ser encontrada na referência FIGUEIREDO.

Podemos observar que as soluções dos problemas clássicos de construção apresentadas (trissecção de um ângulo e duplicação de um cubo) dependeram de encontrar polinômios irredutíveis em x tendo o valor 0 para x igual a números que procuramos provar serem não-construtíveis. O resultado de Lindemann mostra que nosso método de solução deve falhar no caso de π. De fato, π satisfaz uma equação "polinomial"de grau infinito, que não é considerada uma equação polinomial.

4.5 A NÃO CONSTRUTIBILIDADE DO HEPTÁGONO E DO ENEÁGONO REGULARES

Os matemáticos gregos e seus sucessores tentaram construir o heptágono (polígono de 7 lados) e o eneágono (polígono de 9 lados) regulares, mas não lograram êxito. Os gregos sabiam construir os polígonos regulares de 3, 4, 5, 6, 8 e 10 lados. Por que não os de 7 ou 9 lados? A resposta a essa pergunta está nas duas seções seguintes.

4.5.1 A não construtibilidade do heptágono regular

Investigaremos agora a não construtibilidade no caso em que o número n de lados é igual a 7. Note que o nosso problema se resume a encontrar o lado x de um heptágono regular inscrito numa circunferência de raio unitário. Sabemos que os vértices do heptágono são determinados pelas raízes da equação $x^7 - 1 = 0$, que são raízes sétima da unidade. As coordenadas dos vértices são as partes real e imaginária desses números complexos. Iniciando com uma das raízes sétima da unidade $\zeta = cos\left(\frac{2\pi}{7}\right) + isen\left(\frac{2\pi}{7}\right)$, temos que o heptágono será construtível se o ponto $\left(cos\frac{2\pi}{7}, sen\frac{2\pi}{7}\right)$ for construtível o que equivale a $cos\frac{2\pi}{7}$ e $sen\frac{2\pi}{7}$ serem construtíveis. Para isso basta que $cos\frac{2\pi}{7}$ seja construtível. Uma das raízes da equação $x^7 - 1 = 0$ é $x = 1$ e as demais são raízes da equação

$$x^6 + x^5 + x^4 + x^3 + x^2 + x + 1 = 0$$

que dividindo por x^3 obtemos

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

que pode ser reorganizada do seguinte modo

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

fazendo uma simples transformação algébrica obtemos

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

daí

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

fazendo $x + \frac{1}{x} = y$, temos

$$y^3 + y^2 - 2y - 1 = 0.$$

Sabemos que x é uma raiz sétima da unidade. Se considerarmos $x = \zeta = cos\left(\frac{2\pi}{7}\right) + isen\left(\frac{2\pi}{7}\right)$, teremos $\frac{1}{x} = \bar{\zeta} = cos\left(\frac{2\pi}{7}\right) - isen\left(\frac{2\pi}{7}\right)$. Assim, temos $y = x + \frac{1}{x} = 2cos\left(\frac{2\pi}{7}\right)$. Note que, se y é construtível, então $cos\left(\frac{2\pi}{7}\right)$ também é construtível, e reciprocamente. Portanto, se pudermos provar que y não é construtível, provaremos ao mesmo tempo que x não é construtível, concluindo que o heptágono não é construtível. Assim, é suficiente mostrar

que a equação cúbica $y^3 + y^2 - 2y - 1 = 0$ não tem raízes racionais. Pela proposição 4.1.3, se esta equação tem raízes racionais elas são 1 e -1, mas nenhum destes números é raiz da equação. Segue que $y^3 + y^2 - 2y - 1 = 0$ é irredutível sobre $\mathbb{Q}$ e suas raízes não são construtíveis.

4.5.2 A não construtibilidade do eneágono regular

Para o caso do eneágono, sabemos que os vértices são determinados pelas raízes da equação $x^9 - 1 = 0$ que são as raízes nona da unidade. Procedendo como no caso do heptágono, umas das raízes dessa equação é $x = 1$ e as demais são raízes da equação

$$x^8 + x^7 + x^6 + x^5 + x^4 + x^3 + x^2 + x + 1 = 0$$

que tendo grau igual a 2^3 aparenta que suas raízes são construtíveis e, assim, o eneágono regular seria construtível. No entanto, $x^9 - 1$ não é divisível apenas por $x - 1$, é divisível também por $x^3 - 1$. Assim, dividindo $x^9 - 1$ por $x^3 - 1$ obtemos $x^6 + x^3 + 1$. Segue que a equação $x^6 + x^3 + 1 = 0$ tem as mesmas raízes da equação $x^9 - 1 = 0$, exceto as raízes cúbicas da unidade, as quais são construtíveis. Portanto, podemos dividir a equação

$$x^6 + x^3 + 1 = 0$$

por x^3 obtendo

$$x^3 + 1 + \frac{1}{x^3} = 0$$

que reagrupando, temos

$$x^3 + \frac{1}{x^3} + 1 = 0$$

que após algumas transformações algébricas elementares, obtemos

$$\left(x + \frac{1}{x}\right)^3 - 3\left(x + \frac{1}{x}\right) + 1 = 0$$

fazendo $x + \dfrac{1}{x} = y$, temos

$$y^3 - 3y + 1 = 0.$$

que é uma cúbica irredutível sobre $\mathbb{Q}$ e suas raízes não são construtíveis, já que as possíveis raízes racionais seriam 1 e -1, mas nenhum desses números é raiz da cúbica. Logo, o eneágono regular não é construtível.

4.6 A CONSTRUTIBILIDADE DO PENTÁGONO E DO HEPTADECÁGONO REGULARES

4.6.1 A construtibilidade do pentágono regular

Para verificarmos a construtibilidade do pentágono regular utilizaremos a equação $x^5-1=0$, cujas raízes são as raízes quinta da unidade. Iniciando com a raiz $\zeta = cos\left(\frac{2\pi}{5}\right) + isen\left(\frac{2\pi}{5}\right)$, uma das raízes da equação é $x=1$ e as demais são raízes da equação

$$x^4+x^3+x^2+x+1=0$$

que tem grau 2^2 e é irredutível sobre $\mathbb{Q}$. Dividindo a equação

$$x^4+x^3+x^2+x+1=0$$

por x^2, temos

$$x^2+x+1+\frac{1}{x}+\frac{1}{x^2}=0$$

que reagrupando, obtemos

$$x^2+\frac{1}{x^2}+x+\frac{1}{x}+1=0$$

que, após algumas transformações algébricas, obtemos

$$\left(x+\frac{1}{x}\right)^2+\left(x+\frac{1}{x}\right)-1=0$$

fazendo $x+\frac{1}{x}=y$, temos

$$y^2+y-1=0$$

cujas raízes são $y_1=\frac{-1+\sqrt{5}}{2}$ e $y_2=\frac{-1-\sqrt{5}}{2}$ portanto, construtíveis. Se considerarmos $x=\zeta=cos\left(\frac{2\pi}{5}\right)+isen\left(\frac{2\pi}{5}\right)$, teremos $\frac{1}{x}=\overline{\zeta}=cos\left(\frac{2\pi}{5}\right)-isen\left(\frac{2\pi}{5}\right)$. Assim, temos $y_1=2cos\left(\frac{2\pi}{5}\right)$ e como $2cos\left(\frac{2\pi}{5}\right)>0$, concluímos que $y_1=\frac{-1+\sqrt{5}}{2}$. De modo análogo, temos $y_2=2cos\left(\frac{4\pi}{5}\right)$ e como $2cos\left(\frac{4\pi}{5}\right)<0$, concluímos que $y_2=\frac{-1-\sqrt{5}}{2}$. Portanto, $cos\frac{2\pi}{5}=\frac{-1+\sqrt{5}}{4}$ e o pentágono regular é construtível.

4.6.2 A construtibilidade do heptadecágono regular

Nos 2000 anos, entre Euclides e Gauss, nem sequer se imaginava que um polígono regular de 17 lados pudesse ser construtível por régua e compasso. Apesar do fato de que eminentes matemáticos como Fermat e Euler trabalharam no problema da construção dos polígonos regulares por meio de régua e compasso, nenhum progresso adicional foi feito até o final do século XVIII, quando Gauss resolveu o problema completamente em 1796.

Vamos agora descrever o procedimento usado por Gauss na construção do heptadecágono. As raízes n-ésimas da unidade no plano complexo, isto é, as n soluções da equação ciclotômica $x^n - 1 = 0$, são os vértices de um polígono regular de n lados inscrito na circunferência de raio unitário. Se começarmos no vértice $1 = (1, 0)$, podemos mostrar que o próximo vértice do n-ágono regular, no sentido anti-horário, a saber $\zeta = cos\left(\frac{2\pi}{n}\right) + isen\left(\frac{2\pi}{n}\right)$, pode ser construído com régua e compasso, então teremos conseguido provar que o n-ágono regular é construtível.

Gauss, que estava bem familiarizado com a interpretação geométrica de números complexos como pontos no plano - em sua homenagem, às vezes chamamos de plano gaussiano - foi capaz de resolver equações ciclotômicas por meio de radicais. A fim de encontrar valores intermediários adequados, ele primeiro ordenou as raízes n-ésimas da unidade de um modo particular, motivado por seu conhecimento das propriedades de divisibilidade dos inteiros.

Num primeiro momento parece sensato ordenar as raízes de acordo com a sua posição na circunferência, isto é, como visto na figura 31, na ordem 1, ζ, ζ^2, ζ^3, $\cdots$, ζ^{n-1}, em que $\zeta = cos\left(\frac{2\pi}{n}\right) + isen\left(\frac{2\pi}{n}\right)$. No entanto, Gauss percebeu que fazia sentido ordenar as raízes em uma ordem bem diferente, pelo menos no caso em que n é um número primo. Considerando que $\zeta^n = 1$, o valor de ζ^k depende apenas do resto da divisão de k por n. Assim, podemos escolher qualquer ordem dos possíveis restos da divisão por n. Além da ordem 1, 2, 3, $\cdots$, $n - 1$ é possível, no caso em que n é um número primo, obter todos os restos não nulos 1, 2, 3, $\cdots$, $n - 1$ não apenas pela adição repetida de 1, mas pela repetida multiplicaçao por um número g adequado. Assim, obtemos a seguinte ordenação: g^0, g^1, g^2, $\cdots$, g^{n-1}. O resto obtido quando g é dividido por n é chamado de raiz primitiva módulo n.

No caso em que $n = 17$, por exemplo, pode-se escolher $g = 3$. De fato, começando com $g^0 = 1$, $g^1 = 3^1 = 3$, $g^2 = 3^2 = 9$, $g^3 = 3^3 = 27 \equiv 10\ mod\ 17$, $g^4 = 3^4 = 81 \equiv 13\ mod\ 17$. Completamente, obtém-se a seguinte ordenação: 3, 9, 10, 13, 5, 15, 11, 16, 14, 8, 7, 4, 12, 2, 6, 1. Como a lista finaliza em $g^{16} \equiv 1$, poderíamos continuar obtendo $g^{17} \equiv 3$, $g^{18} \equiv 9$, e assim por diante.

No caso de um heptadecágono regular, adotando a ordenação sugerida por Gauss, a lista resultante de raízes da unidade teria a seguinte ordenação: ζ^1, ζ^3, ζ^9, ζ^{10}, ζ^{13}, ζ^5, ζ^{15}, ζ^{11}, ζ^{16}, ζ^{14}, ζ^8, ζ^7, ζ^4, ζ^{12}, ζ^2, ζ^6.

O propósito de Gauss ao ordenar as raízes desse modo era formar somas parciais das raízes da unidade, denominadas períodos, que permitem calcular, passo a passo, as raízes da unidade. Inicialmente começamos com os dois períodos contendo as raízes da unidade que estão em posições ímpares e em posições pares, respectivamente. Essas somas de quatro raízes da unidade são denominadas de períodos de oito membros.

$$\alpha_1 = \zeta^1 + \zeta^9 + \zeta^{13} + \zeta^{15} + \zeta^{16} + \zeta^8 + \zeta^4 + \zeta^2,$$

$$\alpha_2 = \zeta^3 + \zeta^{10} + \zeta^5 + \zeta^{11} + \zeta^{14} + \zeta^7 + \zeta^{12} + \zeta^6.$$

Em seguida, consideram-se os quatro períodos contendo as raízes cujas posições diferem em 4 na lista. Essas somas de quatro raízes da unidade são denominadas de períodos de quatro membros.

$$\beta_1 = \zeta^1 + \zeta^{13} + \zeta^{16} + \zeta^4,$$

$$\beta_2 = \zeta^3 + \zeta^5 + \zeta^{14} + \zeta^{12},$$

$$\beta_3 = \zeta^9 + \zeta^{15} + \zeta^8 + \zeta^2,$$

$$\beta_4 = \zeta^{10} + \zeta^{11} + \zeta^7 + \zeta^6.$$

Finalmente, consideramos os períodos de dois membros, que são as somas das raízes da unidade, contendo as raízes cujas posições diferem em 8 na lista original. Para o que queremos obter, os dois períodos seguintes são suficientes.

$$\gamma_1 = \zeta^1 + \zeta^{16},$$

$$\gamma_2 = \zeta^{13} + \zeta^4.$$

Note que todos os períodos são números reais e têm a propriedade adicional, obtida por essa construção especial, de que cada período pode ser obtido a partir do próximo período mais longo por uma equação quadrática. Para isso, os períodos são colocados em pares, de modo que cada soma e cada produto do par possam ser representados como uma soma de períodos do dobro do comprimento. Vamos ver como isso funciona.

Iniciamos o cálculo com os dois períodos de oito membros α_1 e α_2. Sua soma pode facilmente ser calculada: $\alpha_1+\alpha_2 = \zeta^1+\zeta^2+\zeta^3+\cdots+\zeta^{16} = (1+\zeta^1+\zeta^2+\zeta^3+\cdots+\zeta^{16})-1 = -1$, já que a soma de todas as raízes n-ésimas da unidade é sempre igual a zero. Em contra partida,

determinar os sessenta e quatro produtos em $\alpha_1 \cdot \alpha_2$ é muito trabalhoso, mas elementar. Assim, obtemos $\alpha_1 \cdot \alpha_2 = -4$. Portanto, os dois períodos de oito membros podem ser calculados como soluções da equação quadrática $a^2 + a - 4 = 0$, cujas raízes são $a_1 = \alpha_1 = -\frac{1}{2} + \frac{1}{2}\sqrt{17}$ e $a_2 = \alpha_2 = -\frac{1}{2} - \frac{1}{2}\sqrt{17}$.

Em seguida, usando os dois períodos de oito membros α_1 e α_2, os quatro períodos de quatro membros β_1, β_2, β_3, β_4 podem ser calculados. Omitindo os detalhes, obtemos: $\beta_1 + \beta_3 = \alpha_1$ e $\beta_1 \cdot \beta_3 = -1$, $\beta_2 + \beta_4 = \alpha_2$ e $\beta_2 \cdot \beta_4 = -1$. Esses dois sistemas levam às equações quadráticas $b^2 - \alpha_1 b - 1 = 0$ e $c^2 - \alpha_2 c - 1 = 0$, respectivamente. As duas raízes da primeira equação são $b_1 = \beta_1$ e $b_2 = \beta_3$, enquanto as duas raízes da segunda equação são $c_1 = \beta_2$ e $c_2 = \beta_4$.

Agora, podemos calcular os dois períodos de dois membros γ_1 e γ_2. Mais uma vez, calculamos sua soma $\gamma_1 + \gamma_2 = (\zeta^1 + \zeta^{16}) + (\zeta^{13} + \zeta^4) = \beta_1$ e seu produto $\gamma_1 \cdot \gamma_2 = (\zeta^1 + \zeta^{16}) \cdot (\zeta^{13} + \zeta^4) = \zeta^{14} + \zeta^5 + \zeta^{12} + \zeta^3 = \beta_2$. Esse sistema de equações leva à equação quadrática $d^2 - \beta_1 d + \beta_2 = 0$, cujas raízes são os dois períodos de dois membros $d_1 = \gamma_1$ e $d_2 = \gamma_2$.

Finalmente, podemos calcular a raiz décima sétima da unidade ζ a partir da equação quadrática $e^2 - \gamma_1 e + 1 = 0$, já que $\gamma_1 = \zeta^1 + \zeta^{16}$ e $\zeta^1 \cdot \zeta^{16} = \zeta^{17} = 1$. As raízes dessa equação são $e_1 = \zeta^1$ e $e_2 = \zeta^{16}$.

No entanto, em uma construção geométrica, esta equação quadrática não necessita ser considerada, já que o heptadecágono regular pode ser construído usando um segmento de comprimento $\gamma_1 = 2cos\left(\frac{2\pi}{17}\right)$, uma vez que $\gamma_1 = \zeta^1 + \zeta^{16}$ e $\zeta^{16} = \overline{\zeta^1}$.

Note que, se resolvermos as equações quadráticas que obtivemos uma após a outra e escolhermos as soluções adequadamente, obtemos como resultado $\gamma_1 = 2cos\left(\frac{2\pi}{17}\right) = -\frac{1}{8} + \frac{1}{8}\sqrt{17} + \frac{1}{8}\sqrt{34 - 2\sqrt{17}} + \frac{1}{4}\sqrt{17 + 3\sqrt{17} - \sqrt{34 - 2\sqrt{17}} - 2\sqrt{34 + 2\sqrt{17}}}$.

Note também que essa expressão em raízes quadradas não só mostra ao mesmo tempo que o heptadecágono regular é construtível, mas também indica como tal construção pode ser realizada. A razão disso é que a construtibilidade de um ponto com régua e compasso é equivalente a do ponto que pode ser expresso por números racionais, as quatro operações aritméticas básicas e a obtenção de raízes quadradas.

4.7 EXEMPLO DE UM NÚMERO ALGÉBRICO DE GRAU 4 NÃO CONSTRUTÍVEL POR RÉGUA E COMPASSO

Vamos agora retornar à questão levantada anteriormente. Note que, mesmo o grau da equação ciclotômica

$$x^8 + x^7 + x^6 + x^5 + x^4 + x^3 + x^2 + x + 1 = 0$$

sendo 2^3, nem todas as raízes dessa equação são construtíveis. Nesse momento podemos constatar que isso se deve ao fato de que a equação é redutível sobre $\mathbb{Q}$. Partindo da análise da construção do eneágono regular, concluímos que

$$x^8 + x^7 + x^6 + x^5 + x^4 + x^3 + x^2 + x + 1 = (x^2 + x + 1)(x^6 + x^3 + 1).$$

O problema agora é saber sob qual condição a equação ciclotômica é irredutível ou redutível e qual o seu grau sobre os racionais. Se observarmos os casos do pentágono e do eneágono, em que n é da forma 2^m+1, notamos que, quando n é primo, a construção é possível, quando n é potência de primo ímpar, a construção não é possível. De fato, é possível provar, que se n é um primo da forma $2^m + 1$, a equação ciclotômica tem grau 2^m e é irredutível sobre $\mathbb{Q}$ e, portanto, o polígono regular de n lados é construtível. Caso contrário, se n é primo ímpar, mas não é da forma $2^m + 1$, então a equação ciclotômica é irredutível mas o polígono regular de n lados não é construtível, como provaremos no capítulo seguinte.

Anteriormente, provamos que os números algébricos construtíveis com régua e compasso têm grau uma potência de dois. Contudo, é falso afirmar que todos os números algébricos com grau uma potência de dois são construtíveis. A seguir, daremos exemplo de um número algébrico de grau quatro que não é construtível com régua e compasso.

Seja α uma raiz real de $x^4+2x-2=0$. Se α fosse construtível existiria um β de grau 2 sobre $\mathbb{Q}$ tal que $\mathbb{Q}(\beta)$ é um subcorpo de $\mathbb{Q}(\alpha)$. Assim, α é algébrico de grau 2 sobre $\mathbb{Q}(\beta)$ com um polinômio mínimo $min(\alpha, \mathbb{Q}(\beta)) = x^2 + cx + d$. Dessa forma $x^4 + 2x - 2$ é múltiplo de $x^2 + cx + d$ e temos $x^4 + 2x - 2 = (x^2 + cx + d)(x^2 - cx - 2/d)$ com c, d pertencentes a $\mathbb{Q}(\beta)$. Temos $-2/d + d - c^2 = 0$ e $c(-2/d - d) = 2$. Logo $-2/d + d = c^2$ e $-2/d - d = 2/c$. Segue que $-4/d = c^2 + 2/c$ e $2d = c^2 - 2/c$. Portanto, $-8 = (c^2)^2 - 4/c^2$ e $(c^2)^3 + 8c^2 - 4 = 0$. O polinômio $x^3 + 8x - 4$ é irredutível em $\mathbb{Q}[x]$ e, portanto, não podemos ter c em $\mathbb{Q}(\beta)$. Logo α não é construtível com régua e compasso.

Existe uma caracterização dos números algébricos com grau uma potência de dois que são construtíveis, em termos do corpo de decomposição (menor corpo contendo todas as raízes do polinômio), que enunciamos a seguir:

Teorema 4.7.1. *Um número algébrico é construtível com régua e compasso se, e somente se, o grau do corpo de decomposição do polinômio mínimo do número algébrico é uma potência de dois.*

A prova deste teorema depende de grupos e Teoria de Galois.

4.8 A CONSTRUTIBILIDADE DE UM POLÍGONO REGULAR DE mn LADOS, COM m E n COPRIMOS

Proposição 4.8.1. *Os polígonos regulares de m e n lados, com m e n primos entre si, são construtíveis se, e somente se, o polígono de mn lados é construtível.*

Demonstração. Suponha que os polígonos regulares de m e n lados são construtíveis. Isto significa que os ângulos centrais $\frac{2\pi}{m}$ e $\frac{2\pi}{n}$ são construtíveis. Como $mdc(m,\ n) = 1$, do algoritmo de Euclides, segue que existem inteiros p e q tais que $pm + qn = 1$. Portanto,

$$\frac{2\pi}{mn} = 2\pi\left(\frac{1}{mn}\right) = 2\pi\left(\frac{pm+qn}{mn}\right) = \left(\frac{2\pi}{n}\right)p + \left(\frac{2\pi}{m}\right)q.$$

Assim, o ângulo central $\frac{2\pi}{mn}$ é construtível e, portanto, o polígono regular de mn lados é construtível. Reciprocamente, suponha que um polígono regular de mn lados é construtível. Segue que o ângulo central $\frac{2\pi}{mn}$ é construtível. Assim, ligando os vértices do polígono de mn lados de m em m, obtemos o polígono regular de n lados e ligando os vértices do polígono de mn lados de n em n, obtemos o polígono regular de m lados. Portanto, se o polígono regular de mn lados é construtível, então os polígonos regulares de m e n lados são construtíveis. ■

4.9 A NÃO CONSTRUTIBILIDADE DE UM POLÍGONO REGULAR DE p LADOS EM QUE p NÃO É UM PRIMO DE FERMAT

4.9.1 Primos de Fermat

Como vimos no final do capítulo anterior, um número da forma 2^m+1 pode ser primo ou composto. A seguir obteremos uma caracterização para os primos da forma $2^m + 1$.

Proposição 4.9.1. *Considere um inteiro positivo da forma $2^m + 1$ com $m > 0$. Se $2^m + 1$ é primo, então m deve ser da forma 2^k em que k é um inteiro não negativo.*

Demonstração. Suponha, por contradição, que m não é da forma 2^k em que k é um inteiro não negativo. Segue que $m = 2^r \cdot s$, em que s é um inteiro ímpar maior ou igual a 3. Assim, temos

$$2^m + 1 = 2^{2^r \cdot s} + 1 = \left(2^{2^r}\right)^s + 1 = \left(2^{2^r} + 1\right)\left[\left(2^{2^r}\right)^{s-1} - \left(2^{2^r}\right)^{s-2} + \cdots \pm 1\right].$$

Segue que $2^m + 1$ é um número composto. ■

Definição 19. Um número da forma $F_k = 2^{2^k} + 1$ é denominado *número de Fermat.*

Seja $F_k = 2^{2^k} + 1$ com $k = 0, 1, 2, 3, \cdots$. Fermat observou que $F_0 = 2^{2^0} + 1 = 3$, $F_1 = 2^{2^1} + 1 = 5$, $F_2 = 2^{2^2} + 1 = 17$, $F_3 = 2^{2^3} + 1 = 257$, $F_4 = 2^{2^4} + 1 = 65537$ são números primos. Fermat acabou conjecturando que todos os inteiros da forma $F_k = 2^{2^k} + 1$ são números primos. Mais tarde, Euler descobriu que $F_5 = 2^{2^5} + 1$ não é um número primo, mostrando que 641 é um fator de $F_5 = 2^{2^5} + 1$.

$F_5 = 2^{2^5} + 1 = 2^{32} + 1 = 2^{28}\left(5^4 + 2^4\right) - \left(5 \cdot 2^7\right)^4 + 1 = 2^{28} \cdot 641 - \left(640^4 - 1\right) = 641\left[2^{28} - 639\left(640^2 + 1\right)\right]$

Proposição 4.9.2. *Seja p um número primo positivo. Se o polígono regular de p lados é construtível por régua e compasso, então p é um primo de Fermat.*

Demonstração. Suponha que o polígono regular de p lados, p primo, é construtível. Segue que os vértices do polígono são determinados pelas raízes da equação ciclotômica

$$x^p - 1 = 0$$

as quais são raízes p-ésima da unidade. Uma dessas raízes é $x = 1$ e as demais são raízes da equação

$$x^{p-1} + x^{p-2} + \cdots + x^2 + x + 1 = 0.$$

O ponto chave da prova é mostrar que a equação acima é irredutível. Para isso usaremos o teste de Eisenstein, o qual não podemos aplicá-lo diretamente. Contudo, sabemos que se o polinômio $p(x+1)$ for irredutível, então o polinômio $p(x)$ será irredutível. Assim, substituindo o x da equação por $x + 1$ obtemos

$$(x+1)^{p-1} + (x+1)^{p-2} + \cdots + (x+1)^2 + (x+1) + 1 = 0$$

que após desenvolvermos obtemos

$$x^{p-1} + px^{p-2} + \frac{p(p-1)}{1 \cdot 2}x^{p-3} + \cdots + \frac{p(p-1)}{1 \cdot 2} + p = 0.$$

Note que agora podemos aplicar o teste de Eisenstein para o primo p, pois todos os coeficientes da equação, execeto o coeficiente líder, são divisíveis por p e p^2 não divide o termo independente p. Portanto, a equação é irredutível quando p é primo. Segue que o polinômio mínimo de ζ_p é $min(\zeta_p, \mathbb{Q}) = x^{p-1} + x^{p-2} + \cdots + x^2 + x + 1$ cujo grau é igual a $p-1$. Por outro lado, como o polígono regular de p lados é construtível, sabemos que $[\mathbb{Q}(\zeta_p) : \mathbb{Q}] = 2^m$, em que m é um inteiro positivo, que é o grau do polinômio mínimo de ζ_p. Assim, $p - 1 = 2^m$ e $p = 2^m + 1$, isto é, p é um primo de Fermat. ■

4.10 A NÃO CONSTRUTIBILIDADE DE UM POLÍGONO REGULAR DE p^α LADOS COM p PRIMO ÍMPAR

Consideramos agora o caso em que o polígono regular tem p^α lados, em que p é um primo ímpar e α é um inteiro maior que 1.

Proposição 4.10.1. *Se p um número primo ímpar positivo e α um número inteiro positivo maior que 1, então o polígono regular de p^α lados não é construtível por régua e compasso.*

Demonstração. Inicialmente mostraremos que se $p > 2$, o polígono regular com p^2 lados não é construtível. O problema geral estará então resolvido, pois caso o polígono regular de p^α lados fosse construtível o polígono de p^2 também seria: $\frac{2\pi}{p^2} = p^{\alpha-2} \cdot \frac{2\pi}{p^\alpha}$. Iniciando com a equação ciclotômica $\frac{x^{p^2}-1}{x-1} =$ notamos que a mesma admite raízes estranhas ao problema do polígono regular de p lados, isto é, às raízes da equação $\frac{x^p-1}{x-1} = 0$. Suprimindo estas raízes pela divisão, obtemos $\frac{x^{p^2}-1}{x^p-1} = 0$ como equação ciclotômica, a qual pode ser escrita como

$$x^{p(p-1)} + x^{p(p-2)} + \cdots + x^p + 1 = 0.$$

Substituindo x por $x + 1$ obtemos

$$(x+1)^{p(p-1)} + (x+1)^{p(p-2)} + \cdots + (x+1)^p + 1 = 0.$$

Note que o número de termos de equação é p e o termo independente de x, após o desenvolvimento dos binômios, é igual a p. Assim, a equação tomará a forma $x^{p(p-1)} + p \cdot f(x) = 0$ em que $f(x)$ é um polinômio com coeficientes inteiros cujo termo independente é igual a 1. Verificamos facilmente por meio do teste de Eisenstein para o primo p que a equação é irredutível, pois todos os coeficientes da equação, execeto o coeficiente líder, são divisíveis por p e p^2 não divide o termo independente p. Segue que o polinômio mínimo de ζ_{p^2} é

$min(\zeta_{p^2}, \mathbb{Q}) = x^{p(p-1)} + p \cdot f(x) = 0$ em que $f(x)$ é um polinômio com coeficientes inteiros cujo termo independente é igual a 1. Note que o grau de $min(\zeta_{p^2}, \mathbb{Q})$ é igual a $p(p-1)$. Por outro lado, se o polígono regular de p^2 lados fosse construtível, teríamos $[\mathbb{Q}(\zeta_p) : \mathbb{Q}] = 2^m$, em que m é um inteiro positivo, que é o grau do polinômio mínimo de ζ_{p^2}. Assim, $p(p-1) = 2^m$ e teríamos $p = 2$ contrariando o fato que p é um primo ímpar. ■

5 POLÍGONOS CONSTRUTÍVEIS COM RÉGUA E COMPASSO

Trataremos neste capítulo sobre quais polígonos regulares podem ser construídos com régua e compasso apenas. Lembrando que um polígono é regular quando todos os seus lados são congruentes e todos os seus ângulos internos têm a mesma medida. Isso implica que construir um polígono regular de n lados consiste em dividir uma circunferência unitária em n partes iguais ou construir um ângulo central de medida igual a $\frac{2\pi}{n}$, o que equivale a construir o $cos\left(\frac{2\pi}{n}\right)$. Isso motiva a seguinte definição:

Definição 20. Um polígono é construtível se todos os seus vértices são pontos construtíveis do plano, isto é, um polígono regular de n lados é construtível se o ponto $\left(cos\frac{2\pi}{n},\ sen\frac{2\pi}{n}\right)$ é um ponto construtível do plano.

O problema da possibilidade de construção dos polígonos regulares de n lados, por meio de régua e compasso apenas, vem desde a antiguidade. Há muito tempo sabemos a possibilidade de resolvê-lo quando $n = 2^m$, com $(m \geq 2)$, 3, 5 ou o produto de quaisquer dois ou três desses números. A partir disso vinha sendo especulado se para outros valores de n, por exemplo $n = 7$ ou $n = 9$, poderiam ser ou não construídos. Esse problema só veio a ser resolvido por Gauss, em 1796. Nós tratamos estas questões no capítulo quatro.

Em seu *Disquisitiones Arithmeticae*, Gauss ampliou essa lista de números mostrando que a divisão é possível para todo número primo p da forma $p = 2^{2^k} + 1$, mas impossível para todos os outros números primos e todas as potências de primo com expoente maior que um. Se fizermos $k = 0$ e $k = 1$ em $p = 2^{2^k} + 1$, obtemos $p = 3$ e $p = 5$, respectivamente, casos já conhecidos pelos antigos. Para $k = 2$, obtemos $p = 17$, um caso completamente discutido por Gauss e discutido por nós, brevemente, no capítulo anterior. Para $k = 3$, obtemos $p = 257$, que é também um número primo. O polígono regular de 257 lados é construtível. Do mesmo modo para $k = 4$, já que $p = 65537$ é um número primo. Nos casos em que $k = 5$, $k = 6$, $k = 7$ e $k = 8$ não obtemos números primos. A prova de que o grande número correspondente a $k = 8$ não é primo exigiu um grande esforço computacional e foi realizada em 1980. É, portanto, bastante provável que $k = 4$ seja o último número para o qual temos uma solução.

5.1 A FUNÇÃO ϕ DE EULER

A função ϕ de Euler é uma função aritmética que desempenha um papel importante na nossa teoria.

Definição 21. A função ϕ de Euler é a função $\phi : \mathbb{N} \to \mathbb{N}$ tal que $\phi(n)$ é igual ao número de inteiros positivos menores do que n que são coprimos com n. De outro modo:

$$\phi(n) = \#\{x \in \mathbb{N} : 1 \leq x \leq n \ \ e \ \ mdc(x, n) = 1\}.$$

Proposição 5.1.1. *$\phi(p) = p - 1$ se, e somente se, p é primo.*

Demonstração. Se um inteiro $p > 1$ é primo, então cada um dos inteiros positivos menores que p é coprimo com p. Portanto $\phi(p) = p - 1$. ■

Proposição 5.1.2. *Se p é primo positivo e α é um número inteiro positivo, então $\phi(p^\alpha) = p^\alpha - p^{\alpha-1}$.*

Demonstração. Note que p sendo primo temos que $mdc(m,\ p^\alpha) \neq 1$ se, e somente se, m é um múltiplo de p. Considere a sequência $1, 2, \cdots, p, p+1, \cdots, 2p, \cdots, 3p, \cdots, p^\alpha \cdot p$. Os inteiros que não são coprimos com p^α nesta sequência são $p, 2p, 3p, \cdots, p^{\alpha-1} \cdot p$ dando um total de $p^{\alpha-1}$ números. Assim, os inteiros positivos menores do que p^α e comprimos com p^α são em número de $p^\alpha - p^{\alpha-1}$. ■

Proposição 5.1.3. *Se m e n são inteiros positivos tais que $mdc(m,\ n) = 1$, então $\phi(m \cdot n) = \phi(m) \cdot \phi(n)$.*

Demonstração. A proposição é verdadeira se m ou n é igual a 1, pois

$$\phi(1 \cdot n) = \phi(n) = 1 \cdot \phi(n) = \phi(m) \cdot \phi(n)$$

$$\phi(m \cdot 1) = \phi(m) = \phi(m) \cdot 1 = \phi(m) \cdot \phi(n)$$

Considere m e n maiores do que 1. Considere a tabela a seguir formada pelos inteiros de 1 a $m \cdot n$.

$$\begin{array}{ccccccc} 1 & 2 & \cdots & r & \cdots & m \\ m+1 & m+2 & \cdots & m+r & \cdots & 2m \\ \vdots & \vdots & \vdots & \vdots & & \\ (n-1)m+1 & (n-1)m+2 & \cdots & (n-1)m+r & \cdots & nm \end{array}$$

Como $mdc(a,\ m \cdot n) = 1$ se, e somente se, $mdc(a,\ m) = 1$ e $mdc(a,\ n) = 1$, devemos determinar os inteiros na tabela que são simultaneamente coprimos com m e n, para

determinar os que são coprimos com $m \cdot n$. Se o primeiro elemento de uma coluna não for coprimo com m, então todos os elementos da coluna não são coprimos com m. Portanto, os elementos primos com m estão necessariamente nas colunas restantes e são em número de $\phi(m)$ e é fácil perceber que são coprimos com m todos os elementos destas colunas. Vamos agora determinar quais são os elementos coprimos com n em cada uma destas $\phi(m)$ colunas. Como $mdc(m,\ n) = 1$, a sequência r, $m + r$, $\cdots$, $(n-1)m + r$ forma um sistema completo de restos módulo n. Portanto, $\phi(n)$ destes elementos são coprimos com n. Assim, o número de elementos simultaneamente coprimos com m e n é $\phi(m) \cdot \phi(n)$. ■

Proposição 5.1.4. *Se $n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \cdots \cdot p_r^{\alpha_r}$ com p_1, p_2, $\cdots$, p_r primos distintos e α_1, α_2, $\cdots$, α_r inteiros não negativos, então*

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

Demonstração. Seja $n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \cdots \cdot p_r^{\alpha_r}$ com p_1, p_2, $\cdots$, p_r primos distintos. Segue que $\phi(n) = \phi(p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \cdots \cdot p_r^{\alpha_r})$. Como a função ϕ de Euler é multiplicativa, temos

$$\phi(n) = \phi(p_1^{\alpha_1}) \cdot \phi(p_2^{\alpha_2}) \cdot \cdots \cdot \phi(p_r^{\alpha_r}),$$

já que p_1, p_2, $\cdots$, p_r primos distintos. Assim, temos

$$\phi(n) = (p_1^{\alpha_1} - p_1^{\alpha_1 - 1}) \cdot (p_2^{\alpha_2} - p_2^{\alpha_2 - 1}) \cdot \cdots \cdot (p_r^{\alpha_r} - p_r^{\alpha_r - 1})$$

$$\phi(n) = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \cdots \cdot p_r^{\alpha_r}\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right)\cdots\left(1 - \frac{1}{p_r}\right)$$

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

■

Da proposição anterior, note que se $n \neq 1,\ 2$, então $\phi(n)$ é par. Os números n para os quais $\phi(n) = 2^\alpha$, para algum α inteiro não negativo, são importantíssimos e se relacionam, com a construção dos polígonos regulares por meio de régua e compasso. A proposição a seguir nos dará uma caracterização desses números.

Proposição 5.1.5. *Se $\phi(n) = 2^\alpha$, para algum α inteiro não negativo, então a decomposição de n em fatores primos é dada por $n = 2^\beta \cdot p_1 \cdot p_2 \cdot \cdots \cdot p_r$, com β inteiro não negativo e p_1, p_2, $\cdots$, p_r primos de Fermat distintos.*

Demonstração. Seja $n = q^{\gamma} \cdot p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \cdots \cdot p_r^{\alpha_r}$, com $q, p_1, p_2, \cdots, p_r$ primos distintos, γ inteiro positivo, $\alpha_1, \alpha_2, \cdots, \alpha_r$ inteiros não negativos. Suponha que $2 = q < p_1 < p_2 < \cdots p_r$. Assim, temos:

$$\phi(n) = n\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right)\cdots\left(1 - \frac{1}{p_r}\right) = 2^{\alpha}$$

$$\phi(n) = q^{\gamma} \cdot p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \cdots \cdot p_r^{\alpha_r}\left(1 - \frac{1}{q}\right)\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right)\cdots\left(1 - \frac{1}{p_r}\right) = 2^{\alpha}$$

$$\phi(n) = q^{\gamma-1} \cdot p_1^{\alpha_1-1} \cdot p_2^{\alpha_2-1} \cdot \cdots \cdot p_r^{\alpha_r-1}(q-1)(p_1-1)(p_2-1)\cdots(p_r-1) = 2^{\alpha}$$

Como $p_1, p_2, \cdots, p_r$ são diferentes de 2, devemos ter $\alpha_1 = \alpha_2 = \cdots = \alpha_r = 1$. Além disso, $p_i - 1 = 2^{\beta_i}$ para $i = 1,\ 2,\ \cdots\ r$. Portanto, $p_i = 2^{\beta_i} + 1$ e como p_i é primo, então p_i é primo de Fermat. Assim, fazendo $\gamma = \beta$, temos

$$n = 2^{\beta} \cdot p_1 \cdot p_2 \cdot \cdots \cdot p_r.$$

■

5.2 RAÍZES n-ÉSIMAS DE UM NÚMERO COMPLEXO

Um número complexo z_k é *raiz n-ésima* de um número complexo z se $z_k^n = 1$. Como veremos a seguir, um número complexo $z \neq 0$ admite n raízes distintas.

Considere um número complexo $z \neq 0$ e sua raiz n-ésima z_k na forma trigonométrica:

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

$$z_k = \rho(cos\omega + isen\omega)$$

Utilizando a *fórmula de De Moivre* a equação

$$z_k^n = z$$

assume a seguinte forma:

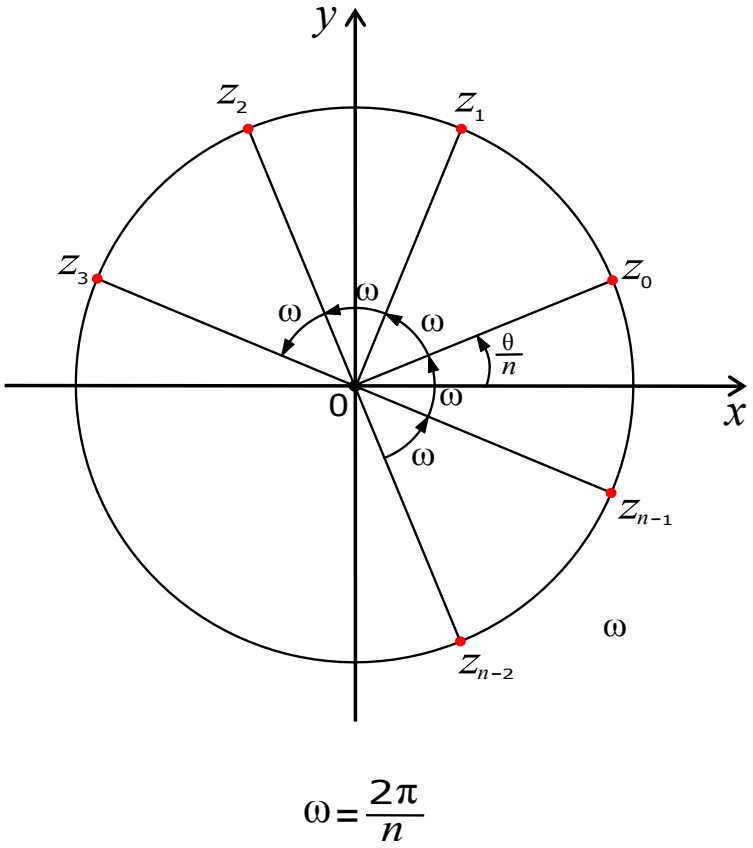
$$\rho^n[cos(n\omega) + isen(n\omega)] = r(cos\theta + isen\theta)$$

Segue que $\rho^n cos(n\omega) = rcos\theta$ e $\rho^n sen(n\omega) = rsen\theta$ que equivalem a $\rho^n = r$ e $n\omega = \theta + 2k\pi$ em que k é um número inteiro. Segue que ρ é a raiz n-ésima positiva de r e assim, temos:

$$z_k = \sqrt[n]{r}\left[cos\left(\frac{\theta}{n} + \frac{2k\pi}{n}\right) + isen\left(\frac{\theta}{n} + \frac{2k\pi}{n}\right)\right]$$

Note que, quando $k = 0, 1, 2, \cdots, n-1$, obtemos n raízes distintas. Qualquer outro valor atribuído a k, diferente dos já assumidos por ele, leva a uma raiz já obtida anteriormente. Concluímos, assim, que um número complexo $z \neq 0$ admite n raízes n-ésimas $z_0, z_1, z_2, \cdots, z_{n-1}$, todas com o mesmo módulo $\rho = \sqrt{r}$ e com argumentos $\varphi_k = \frac{\theta}{n} + \frac{2k\pi}{n}$, $k = 0, 1, 2, \cdots, n-1$.

Figura 33 – Raízes n-ésimas



Fonte: Produzida pelo autor

5.2.1 Raízes n-ésimas da unidade

No caso em que $z = 1$, o ângulo θ assume valor igual a zero e a fórmula da raiz n-ésima fica reduzida a

$$z_k = \left[cos\left(\frac{2k\pi}{n}\right) + isen\left(\frac{2k\pi}{n}\right)\right]$$

que são as *raízes n-ésimas da unidade*. Fazendo

$$\zeta = cos\left(\frac{2\pi}{n}\right) + isen\left(\frac{2\pi}{n}\right)$$

e usando a fórmula de De Moivre, constatamos que as raízes n-ésimas da unidade são dadas por $1, \zeta, \zeta^2, \zeta^3, \cdots, \zeta^{n-1}$.

Note que, representadas no plano complexo, essas raízes são os vértices de um polígono regular de n lados inscrito em uma circunferência de raio 1.

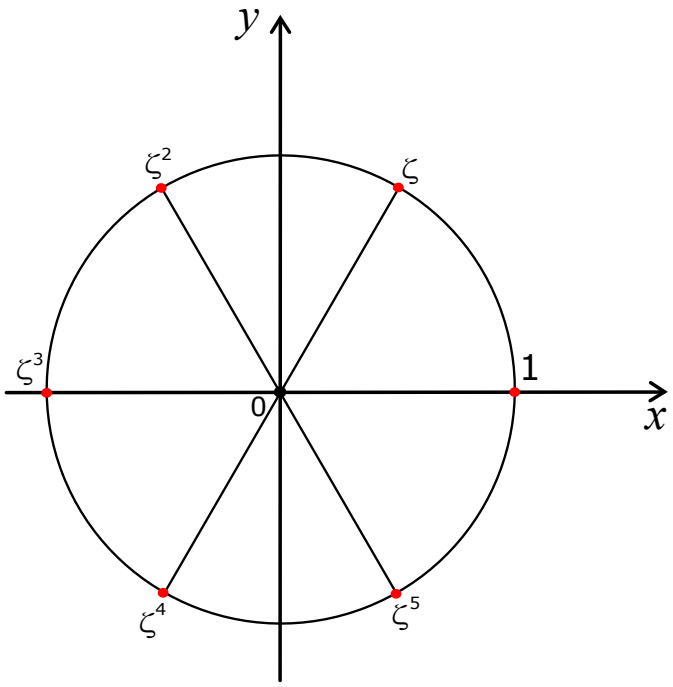
Exemplo 16. A figura a seguir é uma ilustração das raízes da unidade para $n = 6$.

$$\zeta = cos\frac{2\pi}{6} + isen\frac{2\pi}{6}$$

$$\zeta = \frac{1}{2} + \frac{\sqrt{3}}{2}i$$

$$\zeta^2 = -\overline{\zeta},\ \zeta^3 = -1,\ \zeta^4 = -\zeta,\ \zeta^5 = \overline{\zeta}.$$

Figura 34 – Raízes sextas da unidade



Fonte: Produzida pelo autor

A fórmula da raiz n-ésima da unidade pode ser escrita como segue:

$$z_k = \sqrt[n]{r}\left[cos\left(\frac{\theta}{n}+\frac{2k\pi}{n}\right)+isen\left(\frac{\theta}{n}+\frac{2k\pi}{n}\right)\right]$$

$$z_k = \sqrt[n]{r}\left[cos\left(\frac{\theta}{n}\right)+isen\left(\frac{\theta}{n}\right)\right]\left[cos\left(\frac{2k\pi}{n}\right)+isen\left(\frac{2k\pi}{n}\right)\right]$$

$$z_k = \sqrt[n]{r}\left[cos\left(\frac{\theta}{n}\right)+isen\left(\frac{\theta}{n}\right)\right]\left[cos\left(\frac{2\pi}{n}\right)+isen\left(\frac{2\pi}{n}\right)\right]^k$$

$$z_k = \sqrt[n]{r}\left[cos\left(\frac{\theta}{n}\right)+isen\left(\frac{\theta}{n}\right)\right]\cdot\zeta^k, k = 0, 1, 2, \cdots, n-1$$

Essa última igualdade nos diz que *as raízes n-ésimas de um número complexo não nulo podem ser obtidas como o produto de uma de suas raízes particulares,*

$$z_0 = \sqrt[n]{r}\left[cos\left(\frac{\theta}{n}\right)+isen\left(\frac{\theta}{n}\right)\right],$$

pelas raízes n-ésimas da unidade, $1, \zeta, \zeta^2, \cdots, \zeta^{n-1}$.

Exemplo 17. No caso de determinar as raízes cúbicas do número $z = 8$, uma delas é $z_0 = 2$. As raízes cúbicas da unidade são dadas por 1, ω e ω^2 em que

$$\omega = cos\frac{2\pi}{3}+isen\frac{2\pi}{3}$$

$$\omega = -\frac{1}{2}+\frac{\sqrt{3}}{2}i.$$

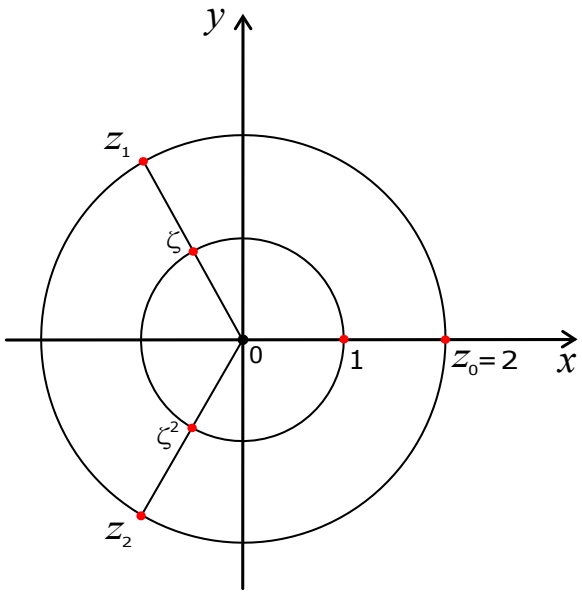
Segue que as raízes cúbicas de 8 são:

$$z_0 = 2\cdot 1 = 2$$

$$z_1 = 2\omega = 2\left(-\frac{1}{2}+\frac{\sqrt{3}}{2}i\right) = -1+\sqrt{3}i$$

$$z_2 = 2\omega^2 = 2\left(-\frac{1}{2}-\frac{\sqrt{3}}{2}i\right) = -1-\sqrt{3}i$$

Figura 35 – Raízes cúbicas do número $z = 8$



Fonte: Produzida pelo autor

5.2.2 Raízes n-ésimas primitivas da unidade

Denomina-se *raiz n-ésima primitiva da unidade* qualquer raiz n-ésima da unidade z tal que n é o menor inteiro positivo tal que $z^n = 1$. É claro que, para dado n,

$$\zeta = cos\left(\frac{2\pi}{n}\right) + isen\left(\frac{2\pi}{n}\right)$$

é raiz primitiva da unidade. Ela é a primeira raiz primitiva que aparece quando percorremos o círculo unitário no sentido anti-horário a partir da unidade real. Porém, ela pode não ser a única raiz primitiva; por exemplo, no caso das raízes cúbicas da unidade, como vimos anteriormente, ζ e ζ^2 são raízes primitivas. Já ζ e ζ^5 são raízes primitivas, mas ζ^2, ζ^3 e ζ^4 não são.

Proposição 5.2.1. *Se ζ é uma raiz n-ésima primitiva da unidade, então as raízes n-ésimas primitivas da unidade são ζ^i com i variando de 1 a n e coprimo com n. O número de raízes n-ésimas primitivas da unidade é igual ao número de naturais de 1 até n que são coprimos com n (ou seja, a função ϕ de Euler de n).*

Demonstração. Sejam i e n coprimos e m o menor inteiro positivo tal que $(\zeta^i)^m = 1$. Então $\zeta^{im} = 1$. Dividindo im por n, obtemos q e r naturais tais que $im = nq + r$ com $0 \leq r < n$ Segue que $\zeta^r = (\zeta^m)^i(\zeta^n)^{-q} = 1$. Portanto, da minimalidade de n temos $r = 0$ e n divide im. Como i e n são coprimos, temos que n divide m. Como $m \leq n$ temos $m = n$. ■

Dado algum i não coprimo com n, é imediato que $(\zeta^i)^{n/mdc(i,n)} = 1$ e, portanto, ζ^i não é raiz n-ésima primitiva da unidade.

5.3 O POLINÔMIO CICLOTÔMICO

O polinômio ciclotômico de ordem n, indica-se por $\Phi_n(x)$, é o polinômio cujas raízes são as raízes primitivas da unidade de ordem n. Note que, se uma raiz n-ésima não primitiva é raiz m-ésima para algum $m < n$, então necessariamente $m|n$. E reciprocamente, se $m|n$, então toda raiz m-ésima ζ da unidade é também raiz n-ésima da unidade, já que $n = km$, com k inteiro, implica $\zeta^n = (\zeta^m)^k = 1$.

Vamos estudar a fatoração do polinômio $x^n - 1$. Considere

$$x^n - 1 = \prod_{\zeta}(x - \zeta),$$

em que o produto é tomado sobre todas as raízes n-ésimas da unidade e agrupe todos os termos pertencentes às raízes da unidade com o mesmo período. Considere

$$\Phi_d(x) = \prod_{perodo(\zeta)=d}(x - \zeta).$$

Então

$$x^n - 1 = \prod_{d|n} \Phi_d(x).$$

Assim, temos

$$\Phi_1(x) = x - 1$$

e

$$\Phi_n(x) = \frac{x^n - 1}{\prod_{d|n\ d<n} \Phi_d(x)}.$$

A partir disso, podemos calcular $\Phi(x)$ recursivamente e vemos que $\Phi_n(x)$ é um polômio em $\mathbb{Q}[x]$, pois dividimos recursivamente por polinômios com coeficientes em $\mathbb{Q}$. Todos os nossos polinômios têm o coeficiente líder 1, de modo que $\Phi_n(x)$ tem coeficientes inteiros.

Desde que $\Phi_1(x) = x - 1$, temos

$$\Phi_2(x) = x + 1,$$

$$\Phi_3(x) = x^2 + x + 1,$$

$$\Phi_4(x) = x^2 + 1,$$

$$\Phi_5(x) = x^4 + x^3 + x^2 + x + 1,$$

$$\Phi_6(x) = x^2 - x + 1,$$

$$\Phi_{12}(x) = x^4 - x^2 + 1,$$

e, em geral, se p é primo, então os únicos d que dividem p são 1 e o próprio p, de modo que

$$x^p - 1 = \Phi_1(x)\Phi_p(x).$$

Assim, temos

$$\Phi_p(x) = \frac{x^p - 1}{x - 1}$$

e

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

Quando n é composto, é mais trabalhoso encontrar o polinômio ciclotômico associado, mas o mesmo pode ser encontrado por meio da fórmula recursiva.

Exemplo 18. Podemos obter $\Phi_6(x)$ a partir de

$$x^6 - 1 = \Phi_1(x)\Phi_2(x)\Phi_3(x)\Phi_6(x).$$

Fatorando $x^6 - 1$, obtemos

$$\begin{aligned} x^6 - 1 &= (x^3 + 1)(x^3 - 1) \\ &= (x + 1)(x^2 - x + 1)(x - 1)(x^2 + x + 1) \\ &= (x - 1)(x + 1)(x^2 + x + 1)(x^2 - x + 1) \end{aligned}$$

Assim, temos $\Phi_6(x) = x^2 - x + 1$.

Exemplo 19. Como no exemplo anterior, podemos obter $\Phi_{12}(x)$ a partir de

$$x^{12} - 1 = \Phi_1(x)\Phi_2(x)\Phi_3(x)\Phi_4(x)\Phi_6(x)\Phi_{12}(x).$$

Fatorando $x^{12} - 1$, obtemos

$$\begin{aligned} x^{12} - 1 &= (x^6 + 1)(x^6 - 1) \\ &= [(x^2)^3 + 1](x^3 + 1)(x^3 - 1) \\ &= (x^2 + 1)[(x^2)^2 + x^2 + 1](x + 1)(x^2 - x + 1)(x - 1)(x^2 + x + 1) \\ &= (x^2 + 1)(x^4 + x^2 + 1)(x + 1)(x^2 - x + 1)(x - 1)(x^2 + x + 1) \\ &= (x - 1)(x + 1)(x^2 + x + 1)(x^2 + 1)(x^2 - x + 1)(x^4 - x^2 + 1) \end{aligned}$$

Segue que $\Phi_{12}(x) = x^4 - x^2 + 1$.

O fato interessante é que tais polinômios, assim definidos, têm coeficientes inteiros e são irredutíveis sobre $\mathbb{Q}$. Além disso, de acordo com o teorema a seguir, podemos concluir que o grau do polinômio ciclotômico de ordem n é igual a $\phi(n)$.

Teorema 5.3.1. *Seja n um inteiro positivo. Então $[\mathbb{Q}(\zeta_n) : \mathbb{Q}] = \phi(n)$.*

Demonstração. Seja n um inteiro positivo. O corpo de decomposição do polinômio $x^n - 1$ é $\mathbb{Q}(\zeta_n)$, com ζ_n sendo uma raiz n-ésima primitiva da unidade. Um automorfismo de $\mathbb{Q}(\zeta_n)$ fica definido pela imagem de ζ_n e as possíveis imagens são ζ_n^i com i variando de 1 a n e sendo coprimo com n. Assim, para concluir o teorema, temos que provar que o polinômio mínimo de ζ_n tem as raízes ζ_n^i com i e n coprimos (que são as raízes n-ésimas primitivas da unidade). Seja

$$\Phi_n(x) = \prod_{i=1,\ldots,n \;\; mdc(i,n)=1} (x - \zeta_n^i)$$

Inicialmente, provaremos que $\Phi_n(x)$ tem coeficientes inteiros: a ideia é fatorar $x^n - 1$ como produto dos $\Phi_d(x)$ com d dividindo n, ou seja, que

$$\prod_{d|n} \Phi_d(x) = x^n - 1$$

Para tanto, basta observar que cada raiz n-ésima da unidade é raiz primitiva d-ésima para um único $d|n$. Usando indução, é imediato concluir que $\Phi_n(x)$ tem coeficientes inteiros. Para provar que $\Phi_n(x)$ é irredutível sobre os racionais, precisamos provar que o polinômio mínimo de ζ_n tem as mesmas raízes que $\Phi_n(x)$. Para tanto, seja $f(x)$ o polinômio mínimo de ζ_n; temos que $\Phi_n(x) = f(x)g(x)$ com $g(x)$ com coeficentes inteiros. Suponha, por contradição, que algum ζ_n^i, com i e n coprimos, não é raiz de $f(x)$. Fatorando $i = p_1 ... p_m$, com $p_1, ..., p_m$ primos temos que algum $\zeta_n^{p_i}$ também não é raiz de $f(x)$ pois, se todos o fossem, a associação $\zeta_n \longrightarrow \zeta_n^{p_i}$ definiria um automorfismo de $\mathbb{Q}(\zeta_n)$, e a composição desses automorfirmos seria o definido pela associação $\zeta_n \longrightarrow \zeta_n^i$, que tem como consequência que ζ_n^i seria raiz de $f(x)$ (pois automorfismos enviam raízes do polinômio mínimo em raízes do polinômio mínimo). Podemos supor que existe um primo p tal que ζ_n^p não é raiz de $f(x)$. Observe que ζ_n^p é raiz de $g(x)$ e que ζ_n é raiz de $g(x^p)$. Daí $g(x^p) = f(x)h(x)$. Reduzindo módulo p, obtemos

$$\overline{g(x)^p} = \overline{f(x)h(x)}$$

Segue que as raízes de $\overline{f(x)}$ são também raízes de $\overline{g(x)}$ e, portanto, $\overline{\Phi_n(x)} = \overline{f(x)g(x)}$ teria raízes múltiplas, o que não pode ser porque $\overline{x^n - 1}$ não admite raízes múltiplas, pois p não divide n. ■

Como as raízes de $\Phi_n(x)$ são precisamente as raízes n-ésimas primitivas da unidade, concluímos que o grau de $\Phi_n(x)$ é $\phi(n)$. Assim, pelo teorema anterior, $\Phi_n(x)$ é irredutível sobre $\mathbb{Q}$, e consequentemente $\Phi_n(x) = min(\zeta_n, \mathbb{Q}(x))$.

Teorema 5.3.2 (Gauss)**.** *Se o polígono regular de n lados é construtível, então n se fatora na forma* $n = 2^{\alpha} \cdot_1 \cdot p_2 \cdot \cdots \cdot p_r$ *com* $p_1, p_2, \cdots, p_r$ *primos de Fermat distintos.*

Demonstração. Considere que o polígono regular de n lados é construtível. Isso é equivalente à construtibilidade de ζ_n. Sabemos que, pela proposição 2.3.4 , se ζ_n é construtível, então $[\mathbb{Q}(\zeta_n) : \mathbb{Q}] = 2^m$ para algum inteiro $m \geq 0$. Por outro lado, pelo teorema anterior, $[\mathbb{Q}(\zeta_n) : \mathbb{Q}] = \phi(n)$. Sendo assim, devemos ter $\phi(n) = 2^m$, isto é, $\phi(n)$ deve ser uma potência de 2. Um resultado anterior, deste capítulo, assegura que $n = 2^{\alpha} \cdot_1 \cdot p_2 \cdot \cdots \cdot p_r$ com $p_1, p_2, \cdots, p_r$ primos de Fermat distintos. ■

Enunciaremos a seguir, sem demonstração, a recíproca desse teorema.

Teorema 5.3.3. *Se n é um inteiro da forma* $n = 2^{\alpha} \cdot_1 \cdot p_2 \cdot \cdots \cdot p_r$*, em que* $p_1, p_2, \cdots, p_r$ *são primos de Fermat distintos, então o polígono regular de n lados é construtível.*

A prova desse teorema depende de resultados básicos sobre grupos e de Teoria de Galois.

É bastante difícil determinar todos os valores de n para os quais $\phi(n)$ é uma potência de 2, apesar da resposta está completa num certo sentido. Resumindo, podemos afirmar que sabemos que um polígono regular de n lados é construtível com régua e compasso quando $n = 2^{\alpha} \cdot p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \cdots \cdot p_r^{\alpha_r}$, em que $\alpha \geq 0$ é arbitrário, $p_i = 2^{2^i} + 1$, $i = 0,\ 1,\ 2,\ 3,\ 4$ e $\alpha_i = 0$ ou 1.

A construção do triângulo equilátero, do quadrado e do pentágono regular era conhecida pelos antigos gregos. A construção do heptadecágono regular é uma descoberta de Gauss, e a construção do polígono regular de 257 lados foi obtida por Richelot. Hermes de Lingren fez a construção do polígono regular de 65537 lados.

5.4 CONCLUSÃO

Nos Elementos de Euclides, as únicas construções permitidas são as construções por régua (sem marca) e compasso. Isso nos permite construir a partir de um determinado comprimento todos os múltiplos e submúltiplos, isto é, todos os comprimentos proporcionais a

um determinado comprimento. Isso significa que todos os números racionais podem ser construídos por régua e compasso. Em seguida, usando o fato de que um triângulo inscrito em um círculo que tem um dos lados como um diâmetro é um triângulo retângulo, podemos extrair raízes quadradas de números reais positivos. Afirmamos ao longo dessa dissertação que os problemas clássicos de construção tais como: a quadratura do círculo, a duplicação do cubo e a trissecção de um ângulo não têm solução. É incontestável observar a diferença entre um problema não resolvido e um problema que não tem solução. É certamente difícil trabalhar em um problema não resolvido, na esperança de encontrar uma solução, olhando para o problema de uma maneira particular. No entanto, não é razoável trabalhar em um problema que foi provado não ter solução. Não saber se existe uma solução e saber que não há solução são coisas muito diferentes. A prova da impossibilidade do primeiro problema se baseia na transcendência do número π. Enquanto que as provas da impossibilidade dos dois últimos problemas se baseiam na multiplicatividade dos graus de torres de extensões de corpos. Observamos finalmente que podemos provar a construtibilidade ou não-construtibilidade de polígonos regulares relacionando a multiplicatividade do grau de extensões de corpos e a função ϕ de Euler por meio de resultados de maior complexidade.

Referências Bibliográficas

[1] AABOE, Asger. **Episódios da História Antiga da Matemática**. Tradução de João Bosco Pitombeira de Carvalho. 2. ed. Rio de Janeiro: Sociedade Brasileira de Matemática, 2002.

[2] BOYER, Carl B.. **História da Matemática**. Tradução de Elza F. Gomide. 1. ed. São Paulo: Edgard Blucher, 1974.

[3] EUCLIDES. **Os Elementos/Euclides**. Tradução de Irineu Bicudo. 1. ed. São Paulo: UNESP, 2009.

[4] FIGUEIREDO, Djairo Guedes de. **Números Irracionais e Transcendentes**. 3. ed. Rio de Janeiro: Sociedade Brasileira de Matemática, 2002.

[5] GAUSS, C. F..**Disquisitiones Arithmeticae**. Tradução de Arthur A. Clarke. 1. ed. New Haven: Yale University Press, 1966.

[6] GONÇALVES, Adilson. **Introdução à Álgebra**. 5. ed. Rio de Janeiro: Projeto Euclides, 2003.

[7] HARDY, G. H.; WRIGHT, E. M.. **An Introduction to the Theory of Numbers**. 6. ed. New York: Oxford University Press, 2008.

[8] HEFEZ, Abramo; FERNANDES, Cecília de Souza. **Introdução à Álgebra Linear**. 1. ed. Rio de Janeiro: Sociedade Brasileira de Matemática, 2012.

[9] KAZARINOFF, Nicholas D.. **Ruler and the Round**. 1. ed. New York: Dover, 2003.