Universidade Federal de Campina Grande
Centro de Ciências e Tecnologia
Unidade Acadêmica de Matemática
Curso de Graduação em Matemática

Números Construtíveis, os Três Problemas Gregos Clássicos e o Fabuloso Teorema de Gauss Sobre Construtibilidade de Polígonos Regulares

por

Renato de Melo Filho

sob orientação de

Prof. Dr. Daniel Cordeiro de Morais Filho

Campina Grande - PB
junho de 2016

Universidade Federal de Campina Grande
Centro de Ciências e Tecnologia
Unidade Acadêmica de Matemática
Curso de Graduação em Matemática

Renato de Melo Filho

Números Construtíveis, os Três Problemas Gregos Clássicos e o Fabuloso Teorema de Gauss Sobre Construtibilidade de Polígonos Regulares

Trabalho apresentado ao Curso de Graduação em Matemática da Universidade Federal de Campina Grande como requisito para a obtenção do título de Bacharel em matemática.

Orientador: Prof. Dr. Daniel Cordeiro de Morais Filho

Campina Grande - PB, junho de 2016
Curso de Matemática, modalidade Bacharelado

Números Construtíveis, os Três Problemas Gregos Clássicos e o Fabuloso Teorema de Gauss Sobre Construtibilidade de Polígonos Regulares

Renato de Melo Filho

Trabalho de conclusão de curso defendido e aprovado em 03 de junho de 2016, pela Comissão Examinadora constituída pelos professores:

Prof. Dr. Daniel Cordeiro de Morais Filho
Orientador

Prof. Dr. Antônio Perreira Brandão Júnior
Examinador

Prof. Dr. Vandenberg Lopes Vieira
Examinador

com nota igual a 9,5.

Dedicatória

Ao nosso Senhor Jesus Cristo.

Agradecimentos

Agradeço sempre a Deus pelo dom da vida e saúde, com os quais pude realizar este trabalho, além da esperança que diariamente me alimenta, que um dia O verei face a face, e O conhecerei como também sou conhecido. Grato pela manifestação da Misericórdia de Deus, o nosso Senhor Jesus Cristo.

Sou grato a Deus pela família que ele me deu, meu pai, minha mãe e meus irmãos.

Agradeço a minha mãe Maria do Socorro que sempre me deu suporte e me ensinou a face prática do amor. Agradeço ao meu irmão Robson de Mélo, que sempre me ajudou e esteve presente em todos os tipos de situações.

Agradeço a minha namorada Bruna Melo do Nascimento por suportar minhas decisões pacientemente e tentar sempre me ajudar a manter o foco, além de ser a pessoa com quem eu sempre contava para relaxar dos "aperreios" acadêmicos.

Sou grato a Deus por todo o ambiente de trabalho que Ele me proporcionou, incluindo professores e funcionários do departamento de matemática da UFCG, e os colegas de curso.

Agradeço ao professor Daniel pela tutoria do PET-Matemática-UFCG. Ele certamente cumpriu o papel de tutor com cada aluno que passou por este grupo maravilhoso. Deste modo, minha gratidão é por todas as habilidades profissionais que nos foram ensinadas pelo atencioso cuidado que o professor Daniel tinha por cada um de nós. Ainda agradeço-o pela orientação deste trabalho: o seu norte foi imprescindível para esta realização.

Agradeço ao professor José de Arimatéia Fernandes, não apenas pelos dois ótimos anos de iniciação científica pelo projeto PICME, mas porque ele foi a pessoa que me inspirou a cursar matemática. Desde os tempos quando eu estudava no ensino fundamental, o professor Arimatéia já me inspirava ensinando-me rudimentos técnicos da preparação olímpica. Enfim, creio que

as palavras são insuficientes para expressar minha gratidão e admiração pelo professor. Que Deus o retribua todo o bem que me fez.

Agradeço ao professor Antônio Pereira Brandão Júnior por ter aceito participar da banca avaliativa deste trabalho. Porém agradeço-lhe ainda mais pela sua disponibilidade perene em ajudar-nos e seu exemplo, que me ensinou que um professor pode sim ser amigável e gentil com os alunos sem perder nenhuma qualidade acadêmica.

Agradeço aos professores Vandenberg Lopes Vieira e Marco Aurélio Soares Souto por terem gentilmente disponibilizado o seu tempo para abrilhantarem, com suas correções, este trabalho.

Agradeço a todos os professores que fizeram parte da minha história acadêmica no ensino básico e na universidade. Certamente esta realização é fruto do esforço de muita gente.

Agradeço a todos os colegas com os quais compartilhei momentos de alegria, prazer, empolgação, mas também dúvidas e sofrimento, não apenas acadêmico. Particularmente, todos os amigos e colegas que conheci através do grupo PET: Felipe Barbosa Cavalcante, Matheus Cunha Motta, Tiago Alves de Sousa, Weslley Ferreira da Silva, Geovany Fernandes Patricio, Arthur Cavalcante Cunha, Thiago Felipe da Silva, André Felipe Araújo Ramalho, Daniela da Silva Enéas, Emanuel Carlos Albuquerque Alves, Juliérika Veras Fernandes, Lucas da Silva, Lucas Siebra Rocha, Lorynne de Sousa Santos, Ismael Sandro da Silva, Fábio Monteiro da Silva, Caio Antony de Matos Andrade e a saudosa memória de Juarez Cavalcante Brito Júnior e alguns que conheci em outras ocasiões: Francimário Medeiros, Camila Paulino, Ygor Torquato, Matheus Carvalho Nóbrega, Daniel Barbosa de Oliveira, Bruna Emanuelly P. Lucena, Laise Dias Alves Araújo e Wellington Leonardo.

Resumo

Quais são os polígonos regulares construtíveis com régua e compasso? Os problemas de construtibilidade estão presentes em toda a história da matemática. Particularmente, este problema de caracterização dos polígonos regulares contrutíveis foi resolvido por Gauss no século XIX. Nos propusemos neste trabalho a estudar o teorema que caracteriza os polígonos regulares contrutíveis, sua demonstração e os assuntos que a embasam: corpos, extensões de corpos, polinômios, extensões de números construtíveis e alguns princípios da Teoria de Galois, com o propósito de adquirirmos familiaridade com todas as ferramentas utilizadas na demonstração do teorema. Também nos propusemos a apresentar os três problemas gregos clássicos pela sua importância histórica e proximidade com o tema.

Abstract

What are the constructible regular polygons with ruler and compass? The constructability issues are present throughout the history of mathematics and particularly this polygons characterization problem was solved by Gauss in the nineteenth century. We set out in this work to study the theorem that characterizes the constructible regular polygons, its demonstration and the issues that underlie: Fields, Field extensions, polynomials, extensions of constructible numbers and some principles of Galois theory, for the purpose of acquiring familiarity with all the tools used in the demonstration of the theorem. We also proposed to introduce the three classical Greeks problems because of its historical significance and proximity to our theme.

Sumário

Lista de Figuras

Introdução

Desde tempos imemoriais, a humanidade busca entender os fenômenos naturais e não naturais que nos cercam, seja a chuva que cai a certa periodicidade, sejam as doenças que nos afligem ou ainda a força que nos atrai ao centro da terra. Todos os fenômenos são pensados e simplificados para a nossa compreensão.

A natureza também é cheia de formas distintas: um tronco de árvore tem um formato diferente da sua própria folha; uma gota de água tem o formato diferente de um grão de areia. Um passo importante na compreensão das formas foi a criação de modelos básicos ideais que se assemelhassem às formas encontradas na natureza, e mais, que servissem de padrão (já que são ideais) às próprias criações humanas. O círculo, o quadrado, o triângulo e o hexágono são exemplos destas formas.

Dentre estas figuras planas ideais, umas se destacam em semelhança, pois são formadas apenas de segmentos de retas ligados pelos extremos, os polígonos. Há indícios de que os egípcios antigos já haviam idealizado o triângulo e descoberto algumas de suas propriedades elementares, uma vez que podem ser encontrados papiros com cálculos envolvendo as medidas dos lados de triângulos. Há no Papiro de Rhind (Figura 1), exemplos destes problemas.

Os favos hexagonais de uma colméia são um exemplo que muito se assemelha a uma forma ideal, o hexágono regular. (Figura 2).

Estas formas ideais marcaram o início de uma ciência chamada geometria, que teve seu ápice numa publicação grega de 300 a.C.: Os Elementos, do matemático Euclides de Alexandria.

Tendo em vista a tendência de simplificação de métodos, os gregos criaram regras para o registro das suas ideias, ou seja, delimitaram instrumentos clássicos para a construção das suas figuras geométricas: a régua não graduada e o compasso. A esta altura é razoável perguntar se os instrumentos clássicos para construção geométrica são suficientes para construção exata em um número finito de passos de todas as formas ideais da geometria. A

Figura 1: Papiro de Rhind.

resposta é não, e esta resposta será destacada no capítulo 2.

No que se refere às formas que mencionamos acima, os polígonos, será que, ao menos os regulares (aqueles que possuem lados de igual medida e ângulos internos congruentes) podem ser construídos pela régua não graduada e o compasso? Se não, quais são possíveis?

A resposta é que não é possível construir todos os polígonos regulares (também forneceremos um exemplo no capítulo 2), mas o matemático e físico alemão Johann Carl Friedrich Gauss (1777 - 1855) foi bem mais além e publicou na sua "Disquisitiones Arithmeticae" , [8], uma condição necessária e suficiente para a construtibilidade por régua e compasso de um n-ágono regular. Nosso objetivo é, portanto, estudar este teorema e demonstrá-lo, além de estudar toda a álgebra necessária para tal.

O teorema segue:

Teorema *(Caracterização dos Polígonos Regulares Construtíveis). Seja n um número natural. Uma condição necessária e suficiente para que o n-*

Figura 2: Favos Hexagonais de uma Colméia.

ágono regular seja construtível por régua e compasso é que n seja da forma

$$n = 2^r p_1 \cdots p_s,$$

onde $r, s \in \mathbb{N} \cup \{0\}$ *e* $p_1, \cdots, p_s$ *são primos distintos da forma*

$$p_i = 2^{2^{r_i}} + 1,$$

com $r_i \in \mathbb{N} \cup \{0\}$.

Fizemos uma pesquisa bibliográfica tendo como base principal [14], sempre com [6] e [12] à mão. Devemos prestar os devidos créditos ao texto introdutório para este assunto, [13], que nos serviu de norte na primeira parte das apresentações do projeto de pesquisa e que nos rendeu bastante familiaridade com o tema. Para os fatos históricos, utilizamos os clássicos de história da matemática [1] e [5], além de pesquisas *on line*.

Para compreendermos a demonstração do teorema, que é o nosso objetivo, precisamos estudar alguns princípios elementares de álgebra, como a definição de corpos, subcorpos, extensões de corpos, além de algebricidade

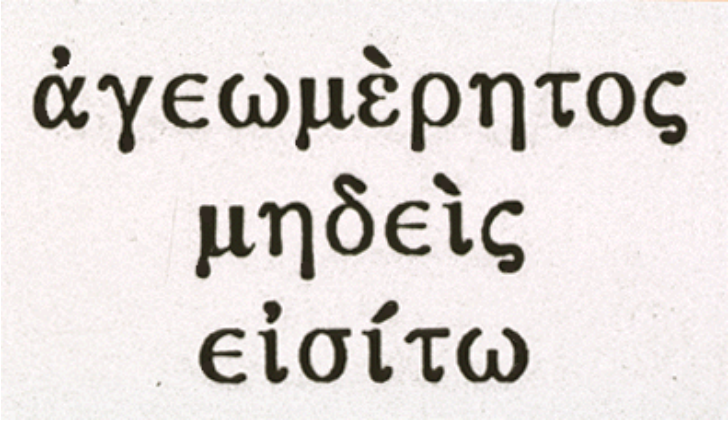
ou transcendentalidade de extensões de corpos. Também abordamos o corpo dos números construtíveis e algumas importantes propriedades algébricas de seus elementos. Isto será feito no primeiro capítulo.

Trouxemos a resposta para a dúvida se todos os números são construtíveis no segundo capítulo, onde mostramos quatro situações em que as medidas são impossíveis de se construir apenas com régua não graduada e compasso com um número finito de passos. Além disso, estas situações são clássicas e possuem uma história respeitável entre os matemáticos.

No terceiro capítulo tratamos sobre os princípios elementares da teoria de Galois que nos são úteis. Este capítulo contém as definições e algumas proposições de K-automorfismos de corpos, decomposição de polinômios e corpos de decomposição, além de extensões normais e separáveis e o teorema fundamental da teoria de Galois.

Por fim, há o quarto capítulo com algumas proposições utilizadas como lemas no nosso teorema principal e, enfim, o teorema de Gauss sobre construtibilidade de polígonos regulares e sua demonstração.

Todas as imagens usadas neste trabalho são de domínio público, exceto se mencionarmos a licença.



"Que não entrem os não iniciados em geometria."

Inscrição no pórtico da Academia de Platão, em Atenas.

Capítulo 1

Alguns Princípios Algébricos

Iniciamos nosso trabalho com algumas definições de conceitos algébricos básicos para o entendimento posterior dos temas matemáticos utilizados na demonstração do nosso teorema principal.

Na primeira seção apresentamos os conceitos mais recorrentes do nosso trabalho, que são corpos e extensões de corpos. Em seguida, na segunda seção, apresentamos os polinômios e algumas proposições sobre polinômios. O resultado mais importante desta seção é, de longe, o critério de irredutibilidade de Eisenstein, crucial para a demonstração do Teorema Principal. Na terceira seção definimos os conceitos de algebricidade e finitude de uma extensão de corpos, além de enunciarmos algumas proposições sobre estes conceitos.

O nosso assunto principal é sobre construção com régua e compasso, por isso, na quarta e quinta seções tratamos de números construtíveis, mais especificamente, mostramos que o conjunto dos números construtíveis é um subcorpo do corpo dos números reais e uma extensão algébrica de $\mathbb{Q}$, como será definido posteriormente.

1.1 Corpos e Extensões de Corpos

Definição 1.1. *Seja K um conjunto munido de duas operações, chamadas adição " $+$ " e multiplicação " $\cdot$ ". Diremos que K é um* ***corpo*** *sempre que forem satisfeitas as seguintes propriedades:*

- *Associatividade da adição e da multiplicação:* $(x+y)+z = x+(y+z)$ *e* $(x \cdot y) \cdot z = x \cdot (y \cdot z)$, $\forall\ x,\ y,\ z \in K$;
- *Comutatividade da adição e da multiplicação:* $x + y = y + x$ *e* $x \cdot y = y \cdot x, \forall\ x, y \in K$;
- *Existência de elementos neutros da adição e da multiplicação:* $\exists\ 0,\ 1 \in K$ *(com* $1 \neq 0$*) tais que* $x + 0 = x$, $\forall\ x \in K$ *e* $y \cdot 1 = y$, $\forall\ y \in K$;
- *Existência de oposto de todo elemento de K, ou seja,* $\exists\ -x \in K$ *tal que* $x + (-x) = 0$ *e existência de inverso de todo elemento não nulo de K, ou seja,* $\exists\ x^{-1} \in K$ *tal que* $x \cdot x^{-1} = 1$;
- *Distributividade da multiplicação em relação à adição, isto é,* $x \cdot (y + z) = x \cdot y + x \cdot z$, $\forall\ x,\ y,\ z \in K$.

Chamaremos o elemento neutro da adição 0 de " zero " e o elemento neutro da multiplicação 1 de " um " ou " unidade ".

Citaremos algumas propriedades básicas dos corpos, cujas demonstrações podem ser encontradas em [6] e [12].

1. Os elementos neutros da adição e da multiplicação são únicos;
2. O simétrico e o inverso de um elemento são únicos;
3. Para todo $x \in K$, temos $x \cdot 0 = 0$.

Definição 1.2. *Seja P um subconjunto de um corpo K. Diremos que P é* ***subcorpo*** *de K sempre que o conjunto P for fechado em relação às operações*

de adição e de multiplicação e, além disso, quando P satisfizer à definição de corpo com as operações de adição e multiplicação induzidas em P pelas operações definidas em K.

Exemplo 1.1.

a) $\mathbb{Q}$ *é subcorpo de* $\mathbb{R}$*, que é subcorpo de* $\mathbb{C}$;

b) $\mathbb{Z}$ *e* $\mathbb{R}\setminus\mathbb{Q}$ *não são corpos, uma vez que em* $\mathbb{Z}$ *não há inversos para todos os elementos não nulos e* $1 \notin \mathbb{R} \setminus \mathbb{Q}$.

Traremos a seguir uma caracterização de subcorpos que é mais prática do que a definição 1.2. Trata-se de uma simplificação dos critérios de verificação para determinar se um subconjunto de um corpo é um subcorpo.

Utilizaremos daqui em diante, para representar o produto de dois elementos x e y de um corpo, o símbolo xy (sem o ponto), em vez de $x \cdot y$, mas, em virtude do estilo, em algumas ocasiões manteremos a notação original.

Proposição 1.1. *Sejam K um corpo e P um subconjunto de K. Então P é um subcorpo de K se, e somente se, as seguintes condições forem verificadas:*

(1) 0 *e* $1 \in P$*;*

(2) Para todos $x, y \in P$*, temos* $x - y$ *e* $xy \in P$*;*

(3) Se $x \in P \setminus \{0\}$*, então* $x^{-1} \in P$.

Demonstração. Suponhamos que as condições sejam satisfeitas para um subconjunto $P \subset K$.

Pela condição (2), P é fechado em relação à multiplicação. Como, por (1), temos $0 \in P$, dados $x, y \in P$, por (2) segue que $0 - x = -x \in P$. E mais, $y - (-x) = y + x \in P$, significando que P é fechado à adição.

Como, para qualquer $x \in P$, temos $-x \in P$, todo elemento de P possui oposto em P e, por (3), todo elemento não nulo de P possui inverso em P.

Todos os elementos de P também pertencem a K, então a associatividade e a comutatividade da adição e da multiplicação, além da distributividade

da multiplicação em relação à adição de elementos de P são propriedades válidas para o conjunto P.

Assim, $P \subset K$ é um corpo com relação às operações " $+$ " e " $\cdot$ ".

Reciprocamente, suponhamos que P seja um subcorpo de K. Tomemos $x \in P \setminus \{0\}$, temos $x - x = 0 \in P$ e $x \cdot x^{-1} = 1 \in P$. Pela propriedade básica de corpos de número 1, estes elementos neutros são os mesmos do corpo K e assim, P satisfaz (1).

Como, $\forall y \in P$, $-y \in P$ então $x - y \in P$ e $xy \in P$, mostrando que P cumpre (2).

Por fim, como P é um corpo em si, então $x^{-1} \in P$, ou seja, P cumpre a condição (3).

Q.E.D.

Definiremos extensões de corpos e discutiremos a sua algebricidade: conceitos centrais e necessários posteriormente para entendermos as ferramentas usadas na demonstração do nosso teorema principal.

Definição 1.3. *Dados um corpo L e um subcorpo $K \subset L$, diremos que L é uma **extensão** de K e denotaremos este fato por $L : K$.*

Definição 1.4. *Seja $L : K$ uma extensão de corpos. Diremos que a extensão é **simples** se existir $t \in L$ tal que $L = K(t)$, onde $K(t)$ é o menor subcorpo de L que contém K e $\{t\}$.*

Exemplo 1.2. *O corpo dos números complexos $\mathbb{C}$ é visto como uma extensão simples dos números reais, pois $\mathbb{C} = \mathbb{R}(i)$.*

Proposição 1.2. *Sejam $K \subset \mathbb{R}$ um subcorpo e w um elemento positivo de K tal que $\sqrt{w} \notin K$. Então $K(\sqrt{w})$ é o corpo cujos elementos são da forma $x + y\sqrt{w}$, onde x e y são elementos de K.*

Demonstração. Seja $M = \{x + y\sqrt{w}; x \text{ e } y \in K\}$. Mostremos que $M = K(\sqrt{w})$ pela dupla inclusão.

Por definição $\sqrt{w} \in K(\sqrt{w})$ e $K \subset K(\sqrt{w})$. Pelo fato de $K(\sqrt{w})$ ser um corpo, então, $\forall y \in K \subset K(\sqrt{w})$ temos $y \cdot \sqrt{w} \in K(\sqrt{w})$. Semelhantemente, para todo $x \in K$, temos $x + y\sqrt{w} \in K(\sqrt{w})$. Deste modo, $M \subset K(\sqrt{w})$.

Por outro lado, se tomarmos $y = 0$, notaremos que $K \subset M$. Se tomarmos $x = 0$ e $y = 1$, notaremos que $\sqrt{w} \in M$. Assim, por definição de $K(\sqrt{m})$, temos então que $K(\sqrt{w}) \subset M$.

Pelos dois parágrafos acima, da dupla inclusão obtivemos $M = K(\sqrt{w})$.

Resta apenas mostrarmos que M é um subcorpo de $\mathbb{R}$ e faremos isto utilizando a Proposição 1.1. Primeiramente, podemos fazer $x = 0$ e $y = 0$, obtendo que $0 \in M$. Analogamente, façamos $x = 1$ e $y = 0$, obtendo que $1 \in M$.

Sejam agora $\alpha = x_1 + y_1\sqrt{w}$ e $\beta = x_2 + y_2\sqrt{w}$ elementos de M. Assim,

$$\alpha - \beta = (x_1 + y_1\sqrt{w}) - (x_2 + y_2\sqrt{w}) = (x_1 - x_2) + (y_1 - y_2)\sqrt{w} \in M,$$

e

$$\begin{aligned} \alpha \cdot \beta &= (x_1 + y_1\sqrt{w})(x_2 + y_2\sqrt{w}) \\ &= (x_1x_2 + y_1y_2(\sqrt{w})^2) + (x_1y_2 + y_1x_2)\sqrt{w} \\ &= ((x_1x_2 + y_1y_2w) + (x_1y_2 + y_1x_2)\sqrt{w}) \in M. \end{aligned}$$

Por fim, notemos que para todo $\alpha = x_1 + y_1\sqrt{w} \in M - \{0\}$ temos que $\dfrac{x_1}{x_1^2 - wy_1^2} - \dfrac{y_1}{x_1^2 - wy_1^2}\sqrt{w} \in M$ é tal que

$$\left(x_1 + y_1\sqrt{w}\right) \cdot \left(\frac{x_1}{x_1^2 - wy_1^2} - \frac{y_1}{x_1^2 - wy_1^2}\sqrt{w}\right) = 1.$$

Assim, $K(\sqrt{w})$ é o corpo cujos elementos são da forma $x + y\sqrt{w}$.

Q.E.D.

Exemplo 1.3. $\mathbb{Q}(\sqrt{2}) = \{x + y\sqrt{2}; x, y \in \mathbb{Q}\}$ *é um subcorpo dos números reais e uma extensão simples de* $\mathbb{Q}$. *Assim,* $\mathbb{Q}(\sqrt{2}) : \mathbb{Q}$ *é uma extensão simples de corpos.*

Definição 1.5. *Sejam* $L : K$ *uma extensão de corpos e* u *um elemento de* L. *Diremos que* u *é* ***algébrico*** *sobre* K *sempre que* u *for zero de algum*

polinômio não nulo de $K[x]$. Se u não for algébrico sobre K, diremos que u é ***transcendente*** *sobre K.*

Observação 1.1. *Se existe $f \in K[x]$ não nulo tal que $f(\alpha) = 0$, então existe $g \in K[x]$ mônico com $g(\alpha) = 0$. Para obter este polinômio, basta dividir f pelo coeficiente do termo de maior grau.*

Exemplo 1.4.

a) $\sqrt{2} \in \mathbb{R}$ *é algébrico sobre* $\mathbb{Q}$*, uma vez que é zero do polinômio* $p(x) = x^2 - 2 \in \mathbb{Q}[x]$*.*

b) e *e* π *são números reais transcendentes sobre* $\mathbb{Q}$*. Para uma demonstração da transcendentalidade destes números, veja [12], [6] e [14].*

Definição 1.6. *Dados* $K \subset L \subset M$ *corpos e* $\alpha_1, \alpha_2, \cdots, \alpha_n \in M$ *tal que* $L = K(\alpha_1, \alpha_2, \cdots, \alpha_n)$*, diremos que* L *é* ***gerado*** *a partir de* K *por adjunção de* $\alpha_1, \alpha_2, \cdots, \alpha_n$*.*

Observação 1.2. *Note que na definição 1.6 utilizamos o símbolo* $K(\alpha_1, \cdots, \alpha_n)$ *para representar a extensão simples* $K(\alpha_1, \cdots, \alpha_{n-1})(\alpha_n)$*.*

Exemplo 1.5. *O corpo dos números complexos pode ser visto como o corpo gerado a partir de* $\mathbb{R}$ *por adjunção do elemento* i*.*

1.2 Polinômios

Utilizaremos como notação para o grau de um polinômio f o símbolo ∂f.

Definição 1.7. *Diremos que um polinômio sobre um corpo é* ***redutível*** *sempre que for possível escrevê-lo como um produto de dois outros polinômios sobre este corpo de graus menores (nenhum constante). Do contrário, ele será* ***irredutível*** *sobre o corpo.*

Exemplo 1.6. *No conjunto* $\mathbb{R}[x]$ *de todos os polinômios cujos coeficientes são números reais, todo polinômio de grau* 1 *é irredutível. De fato, seja* $f \in \mathbb{R}[x]$ *tal que* $\partial f = 1$*. sabemos que* f *é da forma*

$$f(x) = ax + b,$$

com $a, b \in \mathbb{R}$ *e* $a \neq 0$*. Sejam* $g, h \in \mathbb{R}[x]$ *tais que* $f = gh$*. Note que se ambos* g *e* h *tiverem grau maior do que ou igual a* 1*,* f *deve ter grau maior do que*

ou igual a 2. *Assim, um deles deve ter grau* 1 *e o outro terá grau* 0, *ou seja, é um polinômio constante. Deste modo,* f *é irredutível.*

Este argumento é o mesmo para qualquer corpo. Se $ab = 0$ então $a = 0$ ou $b = 0$ e assim, para dois polinômios f, g vale a regra $\partial fg = \partial f + \partial g$.

Uma pergunta relevante neste momento é se podemos determinar quando um polinômio é irredutível. Não conhecemos uma maneira geral de determinarmos a irredutibilidade de polinômios para corpos arbitrários, mas referente ao corpo dos números reais, por exemplo, sabemos que todo polinômio de grau 0 ou 1 é irredutível e, além destes, os de grau 2 que não tenham raízes reais. Os demais polinômios são redutíveis. Outro exemplo é o corpo dos números complexos, no qual os polinômios irredutíveis são somente os de grau 1. Estes fatos podem ser encontrados em [6].

Nosso objetivo, porém, nos faz redirecionar a questão a polinômios sobre os racionais e, para este caso, existe o critério de Eisenstein, que nos fornece a garantia de irredutibilidade para uma classe de polinômios que cumprem alguns requisitos. Provamos a seguir um lema atribuído a Gauss que será necessário para a demonstração do critério de Eisentein.

Lema 1.1. *Seja* $f \in \mathbb{Z}[x]$ *um polinômio irredutível sobre* $\mathbb{Z}$. *Se considerarmos* $f \in \mathbb{Q}[x]$, *então* f *é também irredutível sobre* $\mathbb{Q}$.

Demonstração. Seja $f \in \mathbb{Z}[x]$ um polinômio irredutível sobre $\mathbb{Z}$. Suponhamos por absurdo que f seja redutível sobre $\mathbb{Q}$. Assim, $f = g \cdot h$, onde g e h são polinômios sobre $\mathbb{Q}$ de graus menores do que f.

Sendo n o produto dos denominadores dos coeficientes de f e g, podemos reescrever f da seguinte forma

$$nf = g_1 \cdot h_1, \tag{1.1}$$

onde $n \in \mathbb{Z}$, g_1 e h_1 são polinômios sobre $\mathbb{Z}$.

Mostraremos agora que podemos cancelar os fatores primos de n um por um sem sair de $\mathbb{Z}[x]$, o que implicaria um absurdo, pelo fato de f ser irredutível sobre $\mathbb{Z}$.

Sejam p um fator primo da decomposição de n e

$$\begin{aligned} g_1 &= \alpha_r x^r + \alpha_{r-1} x^{r-1} + \cdots + \alpha_1 x + \alpha_0 \\ h_1 &= \beta_s x^s + \beta_{s-1} x^{s-1} + \cdots + \beta_1 x + \beta_0. \end{aligned}$$

Deste modo há três possibilidades: p divide todos os coeficientes α_i, onde $i \in \{0, 1, \cdots, r\}$, p divide todos os coeficientes β_j, com $j \in \{0, 1, \cdots, s\}$ ou não ocorre nenhuma destas possibilidades. Se uma das duas primeiras possibilidades ocorrer, então podemos cancelar p dos dois lados da equação (1.1) como queremos.

Se nenhuma das duas primeiras possibilidades ocorrer, então devem existir i, j mínimos tais que $p \nmid \alpha_i$ e $p \nmid \beta_j$. Sabemos que p divide todos os coeficientes do polinômio $g_1 h_1$, uma vez que igualdade de polinômios é a igualdade de todos os coeficientes na Equação (1.1) e, particularmente, p divide o coeficiente de x^{i+j}, que é

$$(\beta_0 \alpha_{i+j} + \cdots + \beta_{j-1} \alpha_{i+1}) + \beta_j \alpha_i + (\beta_{j+1} \alpha_{i-1} \cdots + \beta_{i+j} \alpha_0). \tag{1.2}$$

Pela minimalidade de i e j, o primo p divide todos as parcelas de (1.2) entre parênteses. Como p divide o coeficiente (1.2), então deveria também dividir a parcela $\beta_j \alpha_i$, uma contradição, já que p não divide nem β_j nem α_i.

Como a terceira possibilidade não ocorre como demonstrado, ocorrerá sempre uma das duas primeiras e, cancelando até o último fator primo de n, chegamos à expressão

$$f = g_m h_m,$$

com $g_m, h_m \in \mathbb{Z}[x], \partial g_m, \partial f_m < \partial f$.

Temos, portanto, uma contradição, pois f é irredutível em $\mathbb{Z}$.

Q.E.D.

Proposição 1.3 (Critério de Irredutibilidade de Eisenstein)**.** *Seja $f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0$ um polinômio cujos coeficientes são números inteiros. Se existir um primo p tal que*

(i) $p \nmid a_n$;

(ii) $p \mid a_i$, *para* $i \in \{0, 1, \cdots, n-1\}$;

(iii) $p^2 \nmid a_0$.

Então f *é irredutível sobre* $\mathbb{Q}$.

Demonstração. Pelo lema 1.1, é suficiente mostrarmos que o polinômio f é irredutível sobre $\mathbb{Z}$.

Suponhamos que f seja redutível em $\mathbb{Z}$, ou seja, $f = gh$, com

$$g(x) = b_r x^r + b_{r-1} x^{r-1} + \cdots + b_1 x + b_0$$

e

$$h(x) = c_s x^s + c_{s-1} x^{s-1} + \cdots + c_1 x + c_0,$$

com $g, h \in \mathbb{Z}[x]$ de graus menores do que f.

Deste modo, $r + s = n$ e também $b_0 \cdot c_0 = a_0$. Por **(ii)**, $p \mid a_0 \Rightarrow p \mid b_0$ ou $p \mid c_0$. Por **(iii)**, $p^2 \nmid a_0 = b_0 c_0$ e assim, p não pode dividir ambos b_0 e c_0. De fato, se dividisse, teríamos

$$p \mid b_0 \text{ e } p \mid c_0 \Rightarrow p^2 \mid b_0 c_0 = a_0,$$

uma contradição.

Suponhamos, então, que $p \mid b_0$ mas $p \nmid c_0$. Se todos os coeficientes de g fossem divisíveis por p, então, particularmente, $a_n = b_n c_n$ seria divisível por p, uma contradição por **(i)**.

Seja b_i o primeiro coeficiente de g não divisível por p, ou seja, i é mínimo tal que $p \nmid b_i$. Sabemos que

$$a_i = b_i c_0 + \cdots + b_0 c_i,$$

onde $i < n$.

Observe que na expressão acima, por **(ii)** p divide a_i. Pela minimalidade de b_i, p divide $b_0, \cdots, b_{i-1}$ mas $p \nmid b_i$. Assim, teríamos p dividindo c_0, uma contradição.

Assim, f é irredutível sobre $\mathbb{Z}$ e, portanto, pelo lema (1.1), sobre $\mathbb{Q}$.

Q.E.D.

Definição 1.8. *Seja $L : K$ uma extensão de corpos e $\alpha \in L$ um elemento algébrico sobre K. Chamaremos de* ***polinômio minimal de*** α ***sobre*** K *o polinômio mônico $m \in K[x]$ de menor grau não nulo tal que $m(\alpha) = 0$.*

Exemplo 1.7. *Consideremos a extensão $\mathbb{R} : \mathbb{Q}$ e o elemento $\sqrt{3} \in \mathbb{R}$. Note que $\sqrt{3}$ é algébrico sobre $\mathbb{Q}$, uma vez que $p(x) = x^3 - 3x$ zera em $x = \sqrt{3}$. Porém, o polinômio minimal de $\sqrt{3}$ sobre $\mathbb{Q}$ é $m(x) = x^2 - 3$, que é mônico e é o de menor grau que zera em $\sqrt{3}$. De fato, supondo que haja um polinômio de grau menor do que 2 tal que $\sqrt{3}$ seja raiz, o grau deste polinômio será zero ou um. Se for zero, então o polinômio é da forma*

$$f(x) = a \text{ com } a \in \mathbb{Q} \text{ e } f(\sqrt{3}) = 0,$$

o que não ocorre, uma vez que isto só ocorreria com o polinômio nulo.

Se o grau for 1, teremos

$$f(x) = ax + b \text{ com } a, b \in \mathbb{Q} \text{ e } f(\sqrt{3}) = 0.$$

Ora, $f(\sqrt{3}) = 0 \Rightarrow a(\sqrt{3}) + b = 0 \Rightarrow \sqrt{3} = \frac{b}{a} \in \mathbb{Q}$, um absurdo, uma vez que $\sqrt{3} \notin \mathbb{Q}$.

Proposição 1.4. *Seja K um corpo. Se um elemento α é algébrico sobre K, então o polinômio minimal de α sobre K é irredutível sobre K e divide todo polinômio sobre K que tenha α como raiz.*

Demonstração. Seja m o polinômio minimal de α sobre K e suponha que existam $f, g \in K[x]$ com $\partial f, \partial g < \partial m$ tais que

$$m = f \cdot g.$$

Ora, $f(\alpha) = 0 \Rightarrow f(\alpha)g(\alpha) = 0$. Como $f(\alpha), g(\alpha) \in K$ e um corpo não possui divisores de zero, então obtemos que

$$f(\alpha) = 0 \text{ ou } g(\alpha) = 0.$$

Como $\partial f < \partial m$ ou $\partial g < \partial m$, chegamos a uma contradição com a minimalidade do grau de m. Deste modo m é irredutível sobre K.

Agora seja $p(x) \in K[x]$ tal que $p(\alpha) = 0$. Então, pelo fato de $K[x]$ ser um domínio euclidiano (como demonstrado em [6]), podemos garantir a existência de $q, r \in K[x]$, com $\partial r < \partial m$ tais que

$$p(x) = m(x)q(x) + r(x).$$

Como α é raiz de m e de p, então

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

Se r não for nulo, então teria α como raiz, uma contradição pelo fato de $\partial r < \partial m$. E, assim, m divide todo polinômio que tenha α como raiz.

Q.E.D.

1.3 Extensões Algébricas e Extensões Finitas

Retomaremos agora o estudo da algebricidade de extensões e introduziremos a noção de grau de uma extensão.

Definição 1.9. *Diremos que uma extensão $L : K$ é **algébrica** sobre K quando todo elemento $u \in L$ for algébrico sobre K. Uma extensão $L : K$ é **transcendente** sobre K se existir algum $u \in L$ tal que u é transcendente sobre K.*

Exemplo 1.8. *A extensão simples $\mathbb{Q}(\pi) : \mathbb{Q}$ é transcendente sobre $\mathbb{Q}$, uma vez que $\pi \in \mathbb{Q}(\pi)$ é transcendente sobre $\mathbb{Q}$ (Exemplo 1.4).*

O próximo teorema é necessário para a definição de grau de uma extensão.

Teorema 1.1. *Se $L : K$ é uma extensão, as operações*

$$\begin{aligned} + \quad : L \times L &\to L \\ (x, y) &\mapsto x + y \end{aligned}$$

e

$$\begin{aligned} \cdot \quad : K \times L &\to L \\ (a, x) &\mapsto a \cdot x, \end{aligned}$$

definem uma estrutura de espaço vetorial sobre K.

Demonstração. Todas as condições de espaço vetorial podem ser claramente verificáveis pelo fato de $K \subset L$ e ambos serem corpos. *Q.E.D.*

Definição 1.10 (Grau de um Extensão)**.** *Seja $L : K$ uma extensão de corpos. Chamaremos de* ***grau da extensão*** *$L : K$ à dimensão de L visto como um espaço vetorial sobre K. Denotaremos este grau por $[L : K]$.*

Exemplo 1.9. *Tomemos a extensão $\mathbb{C} : \mathbb{R}$. Se enxergarmos $\mathbb{C}$ como um espaço vetorial sobre $\mathbb{R}$, podemos afirmar que $\beta = \{1, i\}$ é uma base de $\mathbb{C}$. De fato, pois β gera $\mathbb{C}$, uma vez que todo número complexo é da forma $x \cdot 1 + y \cdot i$, com $x, y \in \mathbb{R}$. Por fim, temos que β é um conjunto linearmente independente:*

$$x \cdot 1 + y \cdot i = 0 \Leftrightarrow x = 0 \text{ e } y = 0,$$

ou seja, β é uma base para $\mathbb{C}$ sobre $\mathbb{R}$.

Ora, se β é base de $\mathbb{C}$, então $dim_{\mathbb{R}}\mathbb{C} = 2$ e, deste modo, $[\mathbb{C} : \mathbb{R}] = 2$.

Teorema 1.2. *Sejam K, L e M corpos tais que $K \subseteq L \subseteq M$. Então*

$$[M : K] = [M : L][L : K].$$

Demonstração. Seja $(\alpha_i)_{i\in I}$ uma base de L visto como um espaço vetorial sobre K e seja $(\beta_j)_{j\in J}$ uma base de M visto como espaço vetorial sobre L.

Para todo $i \in I$ e $j \in J$, temos $\alpha_i \in L$ e $\beta_j \in M$. Para mostrarmos a tese do teorema, basta mostrar que $(\alpha_i\beta_j)_{i\in I,j\in J}$ é uma base para M sobre K.

Mostremos primeiro que $(\alpha_i\beta_j)_{i\in I,j\in J}$ é LI. Sejam $k_{ij} \in K$,

$$\sum_{i\in I,j\in J} k_{ij}\alpha_i\beta_j = 0 \Leftrightarrow \sum_{j\in J}\left(\sum_{i\in I} k_{ij}\alpha_i\right)\beta_j = 0.$$

Como $(\beta_j)_{j\in J}$ é LI, então

$$\sum_{j\in J} r_j\beta_j = 0 \Leftrightarrow r_j = 0.$$

Ou seja,

$$\sum_{i\in I} k_{ij}\alpha_i = 0, \forall i \in I.$$

Agora, como $(\alpha_i)_{i\in I}$ é LI, então temos

$$\sum_{i\in I} k_{ij}\alpha_i = 0 \Leftrightarrow k_{ij} = 0, \forall i \in I, j \in J.$$

Finalmente, mostraremos que $(\alpha_i\beta_j)_{i\in I,j\in J}$ gera M sobre K.

Todo elemento $\alpha \in M$ pode ser escrito da seguinte maneira, para certos $m_j \in L$,

$$\alpha = \sum_{j\in J} m_j\beta_j.$$

Semelhantemente, para cada $j \in J$, temos que existem $\lambda_{ij} \in K$, tais que

$$\lambda_j = \sum_{i\in I} \lambda_{ij}\alpha_i.$$

Deste modo, cada elemento α de M pode ser escrito da seguinte forma:

$$\alpha = \sum_{j\in J}\left(\sum_{i\in I}\lambda_{ij}\alpha_i\right)\beta_j = \sum_{i\in I, j\in J}\lambda_{ij}\alpha_i\beta_j.$$

O conjunto $(\alpha_i\beta_j)_{i\in I, j\in J}$ é então uma base para M sobre K e, portanto,

$$[M:K] = [M:L][L:K]$$

.

Q.E.D.

Exemplo 1.10. *Como exemplo de aplicação do teorema acima, determinaremos* $[\mathbb{Q}(\sqrt{2},\sqrt{3}):\mathbb{Q}]$ *e ainda encontraremos uma base seguindo o método da demonstração do teorema.*

Com uma demonstração semelhante à que foi feita para $\mathbb{C}:\mathbb{R}$ *no exemplo 1.9, podemos afirmar que* $\{1,\sqrt{2}\}$ *é uma base para* $\mathbb{Q}(\sqrt{2})$ *sobre* $\mathbb{Q}$ *e que* $\{1,\sqrt{3}\}$ *é uma base para* $\mathbb{Q}(\sqrt{2},\sqrt{3})$ *sobre* $\mathbb{Q}(\sqrt{2})$.

De fato, $X = \{1,\sqrt{3}\}$ *gera* $\mathbb{Q}(\sqrt{2},\sqrt{3})$ *pois todo elemento de* $\mathbb{Q}(\sqrt{2},\sqrt{3})$ *é da forma*

$$\alpha+\beta\sqrt{2}+\gamma\sqrt{3}+\theta\sqrt{6} = \left(\alpha+\beta\sqrt{2}\right)\cdot 1 + \left(\gamma+\theta\sqrt{2}\right)\sqrt{3} \in \mathbb{Q}(\sqrt{2},\sqrt{3})$$

Pois $\alpha+\beta\sqrt{2}, \gamma+\theta\sqrt{2} \in \mathbb{Q}(\sqrt{2})$. *Ou seja,* X *gera* $\mathbb{Q}(\sqrt{2},\sqrt{3})$ *sobre* $\mathbb{Q}(\sqrt{2})$ *e, além disso,* X *é* LI, *uma vez que para* $x, y \in \mathbb{Q}(\sqrt{2})$

$$x\cdot 1 + y\cdot\sqrt{3} = 0 \Leftrightarrow x = 0 \text{ e } y = 0.$$

De fato, lembrando que $x, y \in \mathbb{Q}(\sqrt{2})$, *existem* $\alpha_1, \beta_1, \alpha_2, \beta_2 \in \mathbb{Q}$ *tais que*

$$x = \alpha_1 + \beta_1\sqrt{2} \qquad e \qquad y = \alpha_2 + \beta_2\sqrt{2}.$$

Obtemos

$$\begin{aligned} x \cdot 1 + y \cdot \sqrt{3} = 0 &\Leftrightarrow x = -y\sqrt{3} \\ &\Leftrightarrow \alpha_1 + \beta_1\sqrt{2} = -(\alpha_2 + \beta_2\sqrt{2})\sqrt{3} \\ &\Leftrightarrow \alpha_1 = -(\alpha_2 + \beta_2\sqrt{2})\sqrt{3} - \beta_1\sqrt{2}. \end{aligned}$$

A última equação nos diz que o número racional α_1 é igual a uma soma de produto de números irracionais. Essa igualdade se verificará se, e somente se, $\alpha_2 + \beta_2\sqrt{2} = 0$ e $\beta_1 = 0$, e ainda $\alpha_2 + \beta_2\sqrt{2} = 0$ se, e somente se, $\alpha_2 = 0$ e $\beta_2 = 0$

Assim, $x = y = 0$.

Do teorema 1.2, segue que

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

Também podemos encontrar uma base para o espaço vetorial $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ sobre $\mathbb{Q}$ efetuando a multiplicação de cada elemento de $\{1, \sqrt{2}\}$ por cada elemento de $\{1, \sqrt{3}\}$, como foi feito na demonstração, obtendo a seguinte base

$$\{1, \sqrt{2}, \sqrt{3}, \sqrt{6}\}.$$

Enunciaremos um lema necessário para a demonstração da proposição que o segue. Sua demonstração pode ser encontrada em [14].

Lema 1.2. *Sejam α um elemento algébrico sobre um corpo K, $K(\alpha) : K$ uma extensão simples algébrica e m o polinômio minimal de α sobre K. Todo elemento de $K(\alpha)$ possui uma única expressão na forma $p(\alpha)$, onde p é um polinômio de coeficientes em K e $\partial p < \partial m$.*

Proposição 1.5. *Seja $K(\alpha) : K$ uma extensão simples. Se for transcendente, então $[K(\alpha) : K] = \infty$. Se for algébrica, então $[K(\alpha) : K] = \partial m$, onde m é o polinômio minimal de α sobre K.*

Demonstração. Se $K(\alpha) : K$ é transcendente, então α é um elemento transcendente sobre K (Vide [14]). Notemos que $1, \alpha, \alpha^2, \cdots$ são todos linearmente independentes. De fato, se não fossem, existiriam $\beta_i \in K$ todos não nulos tais que $\beta_0 + \beta_1\alpha + \cdots + \beta_n\alpha^n = 0$ e assim $p(x) = \beta_0 + \beta_1 x + \cdots + \beta_n x^n$ seria uma polinômio não nulo com raiz α, contrariando a sua transcendência. Assim $[K(\alpha) : K] = \infty$.

Para o caso de $K(\alpha) : K$ ser uma extensão simples, chamemos $\partial m = n$ e consideremos os elementos $X = \{1, \alpha, \cdots, \alpha^{n-1}\}$. Pelo lema 1.2, qualquer elemento de $K(\alpha)$ pode ser escrito como combinação dos elementos de X e, portanto, X gera $K(\alpha)$.

Do Lema 1.2 e da unicidade de representação dos elementos do conjunto X, obtemos que X é LI.

Como X é uma base para $K(\alpha)$ sobre K, então $[K(\alpha) : K] = n = \partial m$.

Q.E.D.

Exemplo 1.11. *Podemos utilizar a proposição 1.5 para encontrarmos o grau da extensão $\mathbb{Q}(\sqrt{3}) : \mathbb{Q}$. Já vimos que o polinômio minimal de $\sqrt{3}$ sobre $\mathbb{Q}$ é $m(x) = x^2 - 3$ (exemplo 1.7) e, assim, pela Proposição 1.5 obtemos que $[\mathbb{Q}(\sqrt{3}) : \mathbb{Q}] = \partial m = 2$.*

Definição 1.11. *Diremos que uma extensão de corpos é **finita** quando seu grau for finito.*

Exemplo 1.12. *As extensões do tipo $\mathbb{Q}(\sqrt{s}) : \mathbb{Q}$, onde $s \in \mathbb{C}$ é um elemento algébrico sobre $\mathbb{Q}$, são extensões algébricas e finitas, uma vez que são algébricas simples.*

Observação 1.3. *Pela proposição 1.5, toda extensão simples algébrica é finita, uma vez que existe o polinômio minimal de α.*

Proposição 1.6. *A extensão $L : K$ é finita se, e somente se, $L : K$ é uma extensão algébrica e existe um número finito de elementos $\alpha_1, \alpha_2, \cdots, \alpha_s \in L$ tais que $L = K(\alpha_1, \alpha_2, \cdots, \alpha_s)$.*

Demonstração. Tomaremos como hipótese a segunda parte da equivalência, ou seja, que $L : K$ é uma extensão algébrica e existe um número finito de elementos $\alpha_1, \alpha_2, \cdots, \alpha_s \in L$ tais que $L = K(\alpha_1, \alpha_2, \cdots, \alpha_s)$.

Seguindo a ideia da observação 1.2, L pode ser visto como K adjunto a α_1, depois $K(\alpha_1)$ adjunto a α_2 e assim por diante até $L = K(\alpha_1, \cdots, \alpha_{s-1})(\alpha_s) = K(\alpha_1, \cdots, \alpha_s)$. Em cada etapa do processo descrito podemos calcular o grau da extensão resultante e, pelo teorema 1.2, temos que $L : K$ é uma extensão finita.

Reciprocamente, supondo $L : K$ uma extensão finita, existe uma base $\{\alpha_1, \alpha_2, \cdots, \alpha_s\}$ de L sobre K. Deste modo, $L = K(\alpha_1, \alpha_2, \cdots, \alpha_s)$.

Resta mostrarmos que $L : K$ é algébrica. Seja $n = [L : K]$ e tome $x \in L$. O conjunto $\{1, x, \cdots, x^n\}$ contém $n + 1$ elementos, os quais devem ser LD, uma vez que qualquer conjunto com mais elementos do que uma base será LD. Assim, existem $k_0, k_1, \cdots, k_n \in K$, todos não nulos, tais que

$$k_0 + k_1 x + \cdots + k_n x^n = 0,$$

o que implica que x é algébrico sobre K. Como x é um elemento qualquer de L, então $L : K$ é uma extensão algébrica.

Q.E.D.

Por fim, mostramos um resultado deveras interessante sobre os números complexos algébricos sobre os racionais: eles formam um corpo.

Teorema 1.3. *O conjunto A de todos os números complexos algébricos sobre $\mathbb{Q}$ é um corpo.*

Demonstração. Pela proposição 1.5, para qualquer $\alpha \in A$, temos $[\mathbb{Q}(\alpha) : \mathbb{Q}] < \infty$.

Sejam $\alpha, \beta \in A$. Temos, pelo teorema 1.2,

$$[\mathbb{Q}(\alpha, \beta) : \mathbb{Q}] = [\mathbb{Q}(\alpha, \beta) : \mathbb{Q}(\alpha)][\mathbb{Q}(\alpha) : \mathbb{Q}] < \infty.$$

Como $\mathbb{Q} \subseteq \mathbb{Q}(\alpha + \beta) \subseteq \mathbb{Q}(\alpha, \beta)$ então $[\mathbb{Q}(\alpha + \beta) : \mathbb{Q}] < \infty$.

Semelhantemente,

$$[\mathbb{Q}(\alpha\beta) : \mathbb{Q}] < \infty,$$

uma vez que $\mathbb{Q} \subseteq \mathbb{Q}(\alpha\beta) \subseteq \mathbb{Q}(\alpha, \beta)$ e $\mathbb{Q}(\alpha, \beta) : \mathbb{Q}$ é finito.

Por fim, $\mathbb{Q}(-\alpha) : \mathbb{Q}$ e $\mathbb{Q}(\alpha^{-1}) : \mathbb{Q}$ são finitas pois $\mathbb{Q}(\alpha^{-1}) = \mathbb{Q}(-\alpha) = \mathbb{Q}(\alpha)$.

Provamos que, dado $\alpha \in A \setminus \{0\}$, $-\alpha, \alpha^{-1} \in A$, e assim, $\alpha - \alpha = 0 \in A$ e $\alpha \cdot \alpha^{-1} = \frac{\alpha}{\alpha} = 1 \in A$. Também obtemos que, dados $\alpha, \beta \in A$, tem-se $\alpha - \beta \in A$ e $\alpha\beta \in A$. Da proposição 1.1, resulta que A é um corpo.

Q.E.D.

Definição 1.12. *Diremos que um número algébrico sobre $\mathbb{Q}$ é* ***algébrico****.*

Exemplo 1.13. *Os números $\sqrt{2}$, $\sqrt{3}$, $\sqrt[3]{2}$ e i são algébricos.*

1.4 O Corpo dos Números Construtíveis Por Régua e Compasso

A seguir delimitaremos precisamente o que significa construir números com régua e compasso e, além disso, relacionaremos as medidas de segmentos construídos com números reais.

Definição 1.13. *Diremos que um número real u é* ***construtível*** *quando for a medida de um segmento obtido por meio de um número finito de passos de construção com régua não graduada e compasso.*

Exemplo 1.14. *No início de qualquer construção devemos eleger a medida de um segmento de reta como a unidade. Assim, 1 é construtível.*

Mostraremos agora um método para construção por régua e compasso de todos os números reais da forma $x + y\sqrt{s}$, onde $x, y \in \mathbb{Q}$ e $s \in \mathbb{Q}^+$. Pela proposição 1.2 isto é equivalente a mostrar que os elementos do corpo

$$\mathbb{Q}(\sqrt{s}) = \{x + y\sqrt{s}; x, y \in \mathbb{Q} \text{ e } s \in \mathbb{Q}^+\}$$

são construtíveis.

A Figura 1.1 representa como, a partir da eleição arbitrária de uma unidade u, obter todos os números inteiros e seus opostos. A Figura 1.2 ilustra

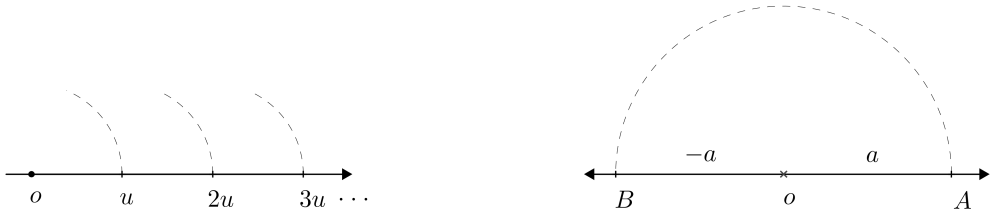


Figura 1.1: Construção dos números inteiros.

como obter a soma e a diferença de dois números construtíveis quaisquer. A

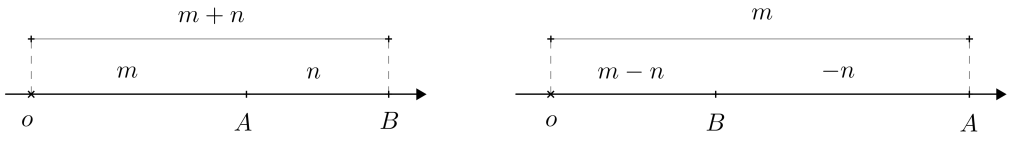


Figura 1.2: Soma e diferença de dois números construtíveis m e n.

Figura 1.3 ilustra o processo para se obter o produto de dois números construtíveis m e n. Primeiro elege-se uma unidade. Marcamos o segmento $\overline{OA}$ de medida n (ou m). Agora traçamos com qualquer ângulo agudo uma reta auxiliar interceptando O e, sobre esta reta, marcamos $\overline{OB}$ de medida m (ou n). Devemos agora traçar $\overline{AC}$ paralela à reta que passa por $\overline{BU}$, passando por A. A partir deste processo, obtivemos $\overline{OC} = m \cdot n$, como justificado na Figura 1.3. O fato do segmento $\overline{OC}$ medir exatamente $m \cdot n$ segue da semelhança entre os triângulos $\triangle OUC$ e $\triangle OAC$.

Os processos de construção para obtermos a reta perpendicular ou a paralela a uma reta dada passando por um ponto são construções elementares que omitimos deste texto. No entanto, ambos, entre outras interessantíssimas construções, podem ser encontrados no clássico [9] ou ainda em [15].

À semelhança do processo descrito anteriormente para obtermos o produto, apresentaremos a construção de $1/n$, onde n é um número construtível

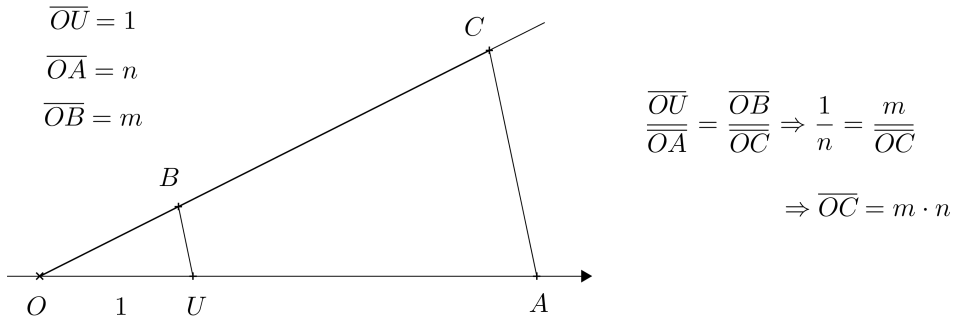


Figura 1.3: Produto de dois números m e n construtíveis.

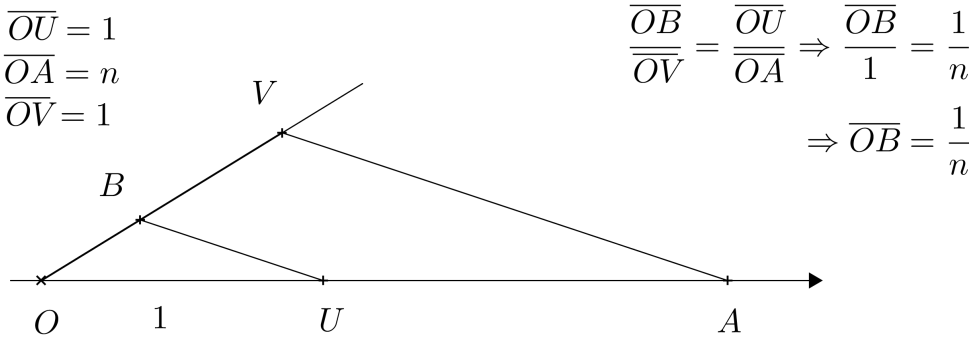


Figura 1.4: Construção do inverso de um número construtível n.

não nulo.

Primeiro elegemos uma medida para a unidade e a marcamos em $\overline{OU}$. Em seguida marcamos $\overline{OA}$ com uma medida n. Agora, com um ângulo agudo traçamos um segmento auxiliar e, sobre ele marcamos $\overline{OV}$ de medida unitária. Por fim traçamos $\overline{BU}$ paralela à reta que passa por $\overline{AV}$ passando por U. Temos que $\overline{OB}$ mede $1/n$. Analogamente à figura 1.3, este resultado segue da semelhança entre os triângulos $\triangle OUB$ e $\triangle OAV$.

Observe que por meio dos procedimentos descritos, é possível construir qualquer número racional.

Portanto, dados dois números construtíveis, sua soma, subtração, produto e quociente (para o denominador não nulo) são números construtíveis.

Exemplo 1.15. *Na Figura 1.5 podemos ver um exemplo de construção do número racional* $2/3$.

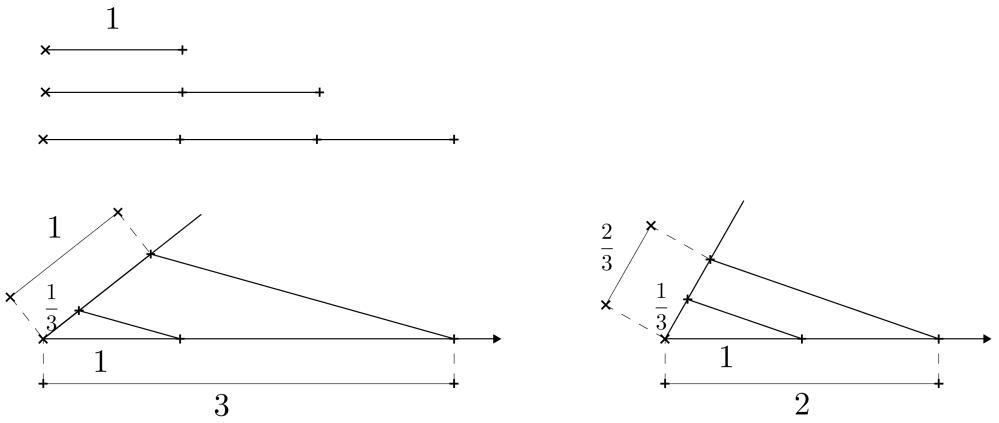


Figura 1.5: Exemplo: A construção de $2/3$.

Para finalizarmos a construção do corpo $\mathbb{Q}(\sqrt{s})$, nos resta apenas construirmos $\sqrt{s}$, onde s é construtível, o que é feito na Figura 1.6.

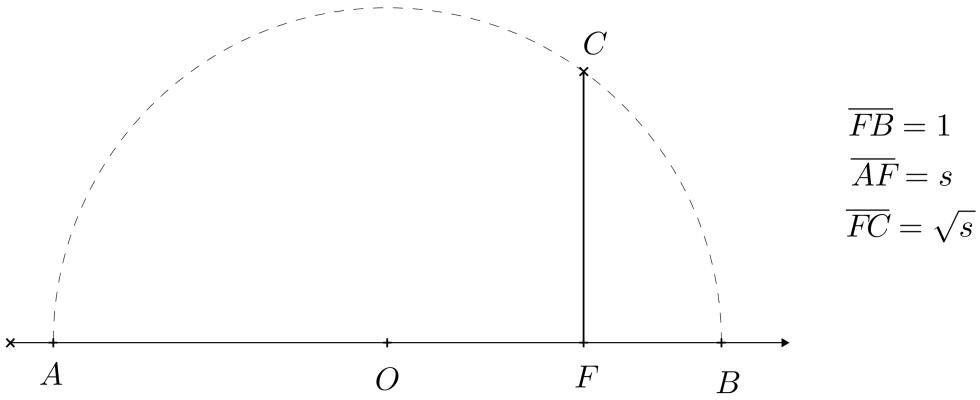


Figura 1.6: Construção da raiz quadrada de um número construtível s.

Provemos que esta construção é válida, ou seja, que o segmento $\overline{FC}$ é realmente $\sqrt{s}$.

Proposição 1.7. *O Segmento* $\overline{FC}$ *na figura 1.6 mede* $\sqrt{s}$.

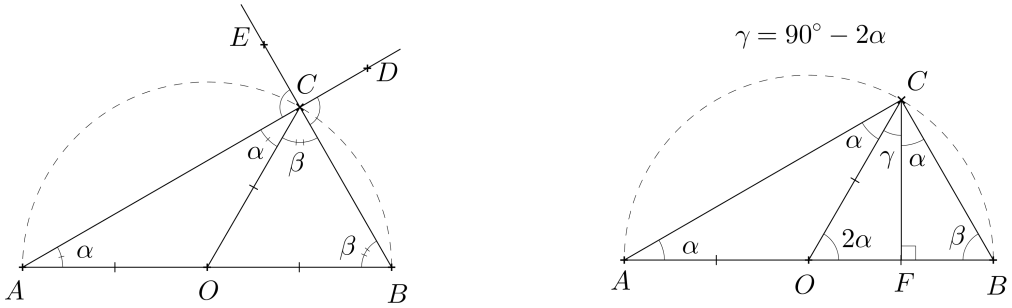


Figura 1.7: Imagem auxiliar para a demonstração da construção de $\sqrt{s}$.

Demonstração. Notemos primeiramente na Figura 1.7 que

$$\overline{AO} = \overline{OB} = \overline{OC},$$

uma vez que são raios de uma mesma circunferência. Por isso os triângulos $\triangle AOC$ e $\triangle COB$ são isósceles de bases $\overline{AC}$ e $\overline{BC}$ respectivamente. Daí obtemos que $O\hat{A}C = O\hat{C}A = \alpha$ e $O\hat{C}B = C\hat{B}O = \beta$ (vide Figura 1.7).

Do teorema do ângulo externo e, por serem opostos pelo vértice, $B\hat{C}D = E\hat{C}A = \alpha + \beta$. Com isto mostramos que o $\triangle ABC$ é retângulo, uma vez que

$$B\hat{C}A + D\hat{C}B = 180^o \Rightarrow 2(\alpha + \beta) = 180^o \Rightarrow 90^o = \alpha + \beta = A\hat{C}B.$$

Também pelo teorema do ângulo externo, $C\hat{O}B = 2\alpha$ e, olhando para o $\triangle OCF$, obtemos

$$90^o + 2\alpha + \gamma = 180^o \Rightarrow \gamma = 90^o - 2\alpha.$$

Ora,

$$90^o = A\hat{C}B = \alpha + \gamma + F\hat{C}B \Rightarrow 90^o = \alpha + 90^o - 2\alpha + F\hat{C}B \Rightarrow F\hat{C}B = \alpha.$$

Deste modo, como $B\hat{F}C = A\hat{F}C = 90^o$ e $F\hat{C}B = F\hat{A}C = \alpha$, então os triângulos $\triangle AFC$ e $\triangle BFC$ são semelhantes.

Finalmente, da semelhança obtemos

$$\frac{\overline{CF}}{\overline{AF}} = \frac{\overline{FB}}{\overline{CF}} \Rightarrow \overline{FC}^2 = \overline{AF} \Rightarrow \overline{CF} = \sqrt{\overline{AF}} = \sqrt{s}.$$

Q.E.D.

Concluímos a demonstração do seguinte teorema:

Teorema 1.4. *Seja s um número construtível. Então os elementos do corpo $\mathbb{Q}(\sqrt{s})$ são construtíveis. Se K é um corpo cujos elementos são construtíveis, então os elementos de $K(\sqrt{s})$ são construtíveis.*

Chamemos agora $\mathbb{Q}$ de K_0 e $\mathbb{Q}(\sqrt{s})$ de K_1. Seja u um elemento positivo de K_1. Através do mesmo processo de construção que utilizamos para raízes de números naturais, podemos construir $\sqrt{u}$, e obteremos assim um novo corpo $K_2 = K_1(\sqrt{u})$. Realizando este processo reiteradamente, obteremos uma cadeia de corpos, onde cada um é extensão simples do anterior:

$$\mathbb{Q} = K_0 \subset K_1 \subset K_2 \subset \cdots \subset K_{i-1} \subset K_i \subset \cdots \subset \mathbb{R}.$$

Pelo teorema 1.4, obtemos que qualquer número real que pertença a um dos corpos da cadeia acima é construtível por régua e compasso. Mostraremos agora que todo número construtível pertence a um destes corpos. Para isto, analisaremos as regras de construção por régua e compasso, ou seja, vamos dissecar o processo e observar o que podemos construir.

A construção por régua e compasso utiliza exclusivamente a seguinte lista de procedimentos elementares:

- Traçar uma reta que passa por dois pontos dados;
- Traçar um arco de circunferência de centro e raio dados.

Podemos escrever os mesmos processos acima listados de uma forma analítica:

- Encontrar a reta cuja equação é $ax + by = c$, onde a, b e c são construtíveis;
- Encontrar a circunferência cuja equação é $(x - a)^2 + (y - b)^2 = r^2$, em que a, b e r são construtíveis.

Podemos ainda afirmar que, com os procedimentos elementares da construção por régua e compasso, determinamos um ponto (ou construímos um ponto) a partir de uma das seguintes maneiras:

1. Intersectando duas retas construtíveis;
2. Intersectando uma reta e um arco de circunferência construtíveis;
3. Intersectando dois arcos de circunferências construtíveis.

Agora, utilizando uma linguagem algébrica, podemos construir um ponto:

a) Resolvendo um sistema linear de duas equações e duas incógnitas do tipo:
$$\begin{cases} ax + by &= c \\ a'x + b'y &= c', \end{cases}$$
onde a, a', b, b', c, e c' são construtíveis;

b) Resolvendo um sistema de duas equações e duas incógnitas, sendo uma do primeiro grau e a outra do segundo grau:
$$\begin{cases} ax + by &= c \\ (x - a')^2 + (y - b')^2 &= r^2, \end{cases}$$
onde a, a', b, b', c, e r são construtíveis;

c) Resolvendo um sistema de duas equações e duas incógnitas, ambas do segundo grau:
$$\begin{cases} (x - a)^2 + (y - b)^2 &= r^2 \\ (x - a')^2 + (y - b')^2 &= r'^2, \end{cases}$$
onde a, a', b, b', r, e r' são construtíveis.

No item (a), que envolve apenas equações do primeiro grau, se a, a', b, b', c, e c' estão em um corpo K, então a solução do sistema também estará em K. Porém, nos itens (b) e (c), estando todos os números em um corpo K, as soluções dos sistemas são números que pertencem a uma extensão $K(\sqrt{s}) : K$, onde $s \in K$. Deste modo, todo número construtível realmente pertence a algum dos corpos

$$\mathbb{Q} = K_0 \subset K_1 \subset K_2 \subset \cdots \subset K_{i-1} \subset K_i \subset \cdots \subset \mathbb{R}, \tag{1.3}$$

onde $K_{i+1} = K_i(\sqrt{s_i})$, com $s_i \in K_i$.

Provamos o seguinte teorema:

Teorema 1.5. *Um número é construtível se, e somente se, pertencer a um dos corpos de uma cadeia*

$$\mathbb{Q} = K_0 \subset K_1 \subset K_2 \subset \cdots \subset K_{i-1} \subset K_i \subset \cdots \subset \mathbb{R}.$$

onde $K_{i+1} = K_i(\sqrt{s_i})$, *com* $s_i \in K_i$.

Proposição 1.8. *O conjunto dos números construtíveis é um corpo e todo número construtível é algébrico.*

Demonstração. Dado um segmento que elegemos com medida 1, a diferença de dois números construtíveis é construtível e, assim, $1 - 1 = 0$ é construtível. Vimos que dados a, b números construtíveis, os números $a - b$ e ab são construtíveis e, se $b \neq 0$, a/b é construtível.

Pela Proposição 1.1, obtemos que o conjunto dos números contrutíveis é um subcorpo do corpo dos números reais.

Tome agora r um número construtível qualquer. Pelo teorema 1.5 temos que ele pertence a um dos corpos de uma cadeia 1.3 e que cada corpo daquela cadeia é obtido pela adjunção de um elemento algébrico ao corpo anterior. Deste modo, cada extensão $K_i : K_{i-1}$ é simples, algébrica e, portanto, finita. Pela Proposição 1.2, a extensão $K_i : \mathbb{Q}$ é finita e gerada pela adjunção de um número finito de elementos algébricos. Da Proposição 1.6 resulta que a

extensão é algébrica e, portanto, r é um número algébrico.

Q.E.D.

1.5 Extensões de Números Construtíveis

Provamos na Seção 1.4 que um número real será construtível se, e somente se, pertencer a um dos corpos de uma cadeia como 1.3 abaixo:

$$\mathbb{Q} = K_0 \subset K_1 \subset K_2 \subset \cdots \subset K_{i-1} \subset K_i \subset \cdots \subset \mathbb{R}.$$

onde $K_{i+1} = K_i(\sqrt{s_i})$, com $s_i \in K_i$.

Associaremos agora a cada estágio da construção de um ponto construtível uma extensão com o corpo dos números racionais adjunto às coordenadas dos pontos construídos nas etapas da construção.

Definição 1.14. *Diremos que um ponto $(x, y) \in \mathbb{R}^2$ é **construtível** quando ambas as coordenadas forem construtíveis.*

Exemplo 1.16. *O ponto $\left(\sqrt{3}-1, 1\right)$ é construtível, uma vez que o número $\sqrt{3}-1$ é construtível, pois*

$$\sqrt{3}-1 \in \mathbb{Q}\left(\sqrt{3}\right) \supset \mathbb{Q}.$$

Como $\mathbb{Q}(\sqrt{3})$ é um dos corpos de uma cadeia como a cadeia 1.3 da seção 1.4, obtemos a construtibilidade de $\sqrt{3}-1$.

Sejam (x, y) as coordenadas de um ponto $p_0 \in \mathbb{R}^2$ dado e $K_0 = \mathbb{Q}(x, y)$ o subcorpo de $\mathbb{R}$ gerado por $\mathbb{Q}$ em adjunção aos elementos x e y.

Se a partir de K_0 conseguirmos obter por régua e compasso um ponto $q_0 = (x_0, y_0)$, então definimos o corpo associado a esta primeira etapa de construção como $K_1 = K_0(x_0, y_0)$.

Podemos, assim, tendo o ponto $p_n = (x_n, y_n)$, definir indutivamente o

corpo $K_n = K_{n-1}(x_n, y_n)$, obtendo uma cadeia

$$K_0 \subseteq K_1 \subseteq \cdots \subseteq K_n \subseteq \mathbb{R}.$$

Lema 1.3. *x_i e y_i são raízes em K_i de polinômios de grau 2 sobre K_{i-1}.*

A demonstração deste lema se baseia no exposto na seção 1.4 sobre a equivalência entre construção com régua e compasso e a resolução de equações do 1º e 2º grau.

Teorema 1.6. *Seja (x, y) um ponto de $\mathbb{R}^2$ construtível a partir de um ponto $p_0 \in \mathbb{R}^2$ e K_0 o subcorpo de $\mathbb{R}$ gerado por $\mathbb{Q}$ e pelas coordenadas de p_0, então os graus das extensões*

$$K_0(x) : K_0 \text{ e } K_0(y) : K_0$$

são potências de 2.

Demonstração. Pelo Lema 1.3 e pela Proposição 1.5, temos

$$[K_{i-1}(x_i) : K_{i-1}] = 1 \text{ ou } 2 \text{ e } [K_{i-1}(y_i) : K_{i-1}] = 1 \text{ ou } 2,$$

assim,

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

Deste modo, $[K_i : K_i - 1]$ é uma potência de 2e, por conseguinte, $[K_i : K_0]$ é também uma potência de 2.

Desde que $[K_i : K_0(x)][K_0(x) : K_0] = [K_i : K_0]$, segue que $[K_0(y) : K_0]$ é uma potência de 2.

Analogamente, mostra-se que $[K_0(y) : K_0]$ também é uma potência de 2.

Q.E.D.

Neste capítulo, vimos algumas definições, exemplos e proposições sobre corpos de uma maneira geral e, mais especificamente, sobre o corpo dos

números construtíveis. No próximo capítulo, veremos quatro importantes exemplos de que nem toda ideia geométrica pode ser representada pelos instrumentos euclidianos.

Capítulo 2

Os Três Problemas Gregos Clássicos e o Heptágono Regular

Acontecimentos políticos e militares do quinto século antes de Cristo, a exemplo da derrota dos persas no início do século, foram de fundamental importância para o florescimento científico em Atenas. O período de paz que seguiu a derrota dos persas atraiu mentes brilhantes a Atenas. Nomes como Anaxágoras (500 a.C. - 428 a.C.), Zenão (cerca de 490 a.C. - 430 a.C.), Parmênides (530 a.C. - 460 a.C.) e Hipócrates (460 a.C. - 370 a.C.) passaram a habitar ou frequentar a cidade que já abrigava Péricles (cerca de 495 a.C. - 429 a.C.) e Sócrates (499 a.C. - 399 a.C.).

O resultado não poderia ser outro: ocorreram muitos avanços científicos tanto de caráter prático quanto idealistas, [1] e, dentre estes, destacam-se os avanços na área da geometria. Mais especificamente, surgiram três problemas que desafiaram os matemáticos durante um período de 2000 anos [5], os chamados três problemas gregos clássicos.

Já citamos na introdução a tendência de tentar representar as ideias geométricas de modo exato apenas com régua e compasso, atitude que foi popularizada de modo oficial por Euclides, nos Elementos. Portanto, passaram

a chamar os instrumentos com as regras já estabelecidas de instrumentos de Euclides.

Um dos pensadores que estavam em Atenas, Anaxágoras, foi preso por impiedade, ao afirmar que o Sol não era um deus, mas apenas uma rocha gigante em chamas. Não puderam, entretanto, prender o seu intelecto que buscou uma maneira de quadrar o círculo [1] e assim relata-se o surgimento de um dos problemas:

- Dado um círculo, é possível construir com os instrumentos euclideanos um quadrado de área igual à do círculo?

Os outros dois problemas têm origens menos confiáveis: temos apenas lendas do seu surgimento. Uma das lendas mais difundidas sobre a duplicação do cubo é que por volta do ano 430 a.C. houve uma peste que devastou a cidade de Atenas, matando aproximadamente um quarto da sua população. Um oráculo do deus Apolo anunciou que a peste, vista como uma maldição dos deuses, poderia ser combatida duplicando o altar de Apolo [1].

Os habitantes de Atenas, tentando obedecer ao decreto anunciado pelo oráculo, dobraram as dimensões do altar, deixando o seu volume oito vezes maior. Os matemáticos notaram a diferença e começaram a pensar o problema nos moldes euclideanos. Esta lenda "explica" o surgimento do problema:

- Dado um cubo, é possível construir um outro cubo com o dobro do seu volume com instrumentos euclideanos?

Neste mesmo período havia um terceiro problema que chamava a atenção dos matemáticos gregos:

- Dado um ângulo qualquer, é possível trissectá-lo por instrumentos euclidianos, ou seja, é possível dividi-lo em três outros ângulos de igual medida?

Estes três problemas já fornecem uma resposta à possibilidade de representar qualquer ideia geométrica utilizando apenas uma régua não graduada e compasso. Eles formam os mais conhecidos contraexemplos a esta possibilidade.

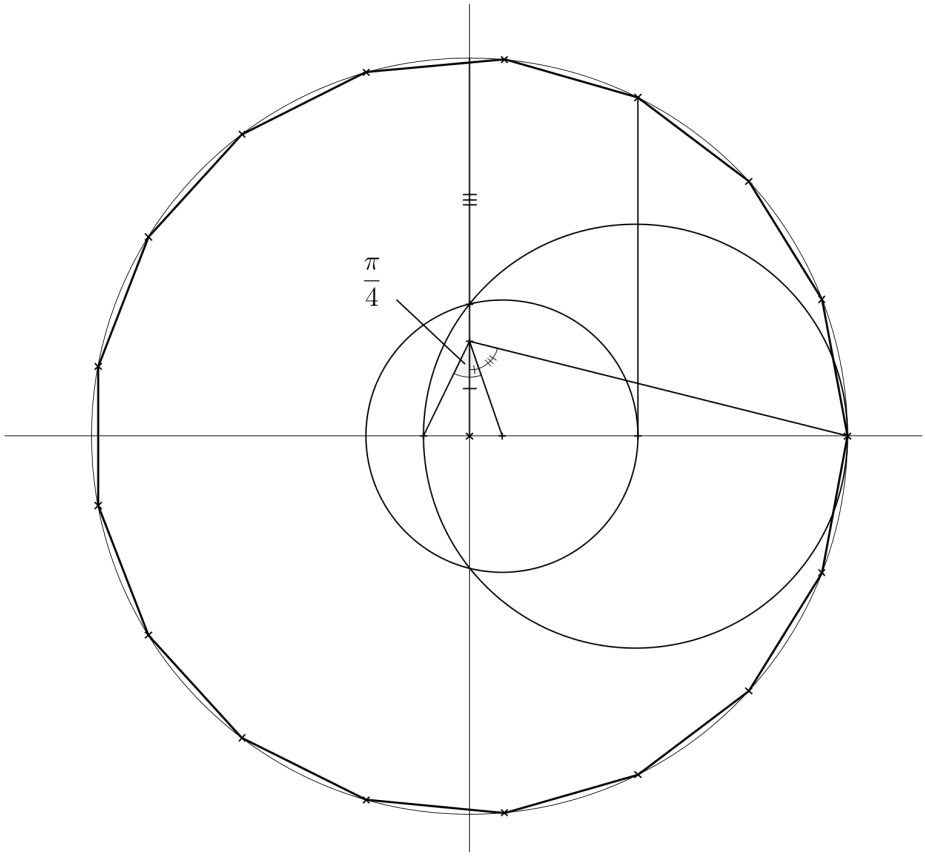


Figura 2.1: Uma Construção do Heptadecágono Regular.

Além destes três, há ainda outro problema que nos interessa ainda mais por se tratar de construtibilidade de polígonos regulares. Euclides publicou, nos Elementos, a construção de polígonos regulares de três, quatro, cinco, seis e quinze lados, mas nada se sabia sobre a possibilidade de construção do heptágono, do eneágono ou ainda do heptadecágono.

Mostraremos neste capítulo que o heptágono não pode ser construído pelos instrumentos euclideanos.

Segundo alguns historiadores de matemática, [5], Carl Friedrich Gauss

descobriu, aos dezenove anos, que o heptadecágono regular é construtível e este foi o momento em que ele decidiu devotar-se à matemática. Esta descoberta o marcou tão profundamente que ele pediu que em seu túmulo fosse gravado um heptadecágono regular (Figura 2.1).

Para uma demonstração do método de construção do heptadecágono ilustrado na Figura 2.1, visite [16].

Passaremos a expor agora os problemas gregos clássicos e, com ferramentas modernas, demonstrar sua impossibilidade.

2.1 O Problema da Duplicação do Cubo

O primeiro problema de que trataremos é a duplicação do cubo, ou seja, dado um cubo, é possível construir um outro cubo que tenha o dobro do seu volume? Podemos simplificar o problema considerando a aresta do cubo unitária, como na Figura 2.2.

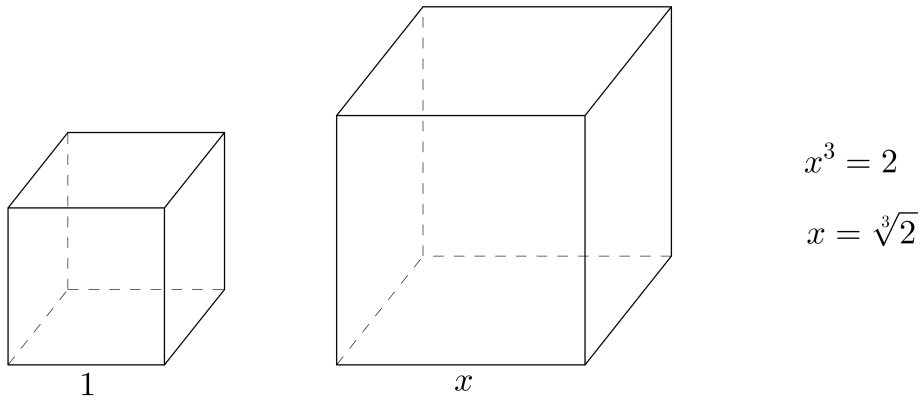


Figura 2.2: A Duplicação do cubo.

Caso a solução fosse possível, o número $\sqrt[3]{2}$ seria construtível. Utilizando o Teorema 1.5, analisaremos se o número $\sqrt[3]{2}$ pertence a algum daqueles corpos na cadeia 1.3. Começando pelo primeiro, mostraremos que $\sqrt[3]{2} \notin \mathbb{Q}$.

Proposição 2.1. *O número $\sqrt[3]{2}$ não pertence ao conjunto dos números racionais.*

Demonstração. Suponhamos que $\sqrt[3]{2} \in \mathbb{Q}$. Logo, existem p, $q \in \mathbb{Z}$ primos entre si tais que

$$\frac{p}{q} = \sqrt[3]{2} \Leftrightarrow p^3 = 2q^3.$$

Isto significa que p^3 é par. Como p^3 é par, temos que p é um número par, então $p^3 = (2r)^3 = 2 \cdot 2^2 \cdot r^3$, para algum $r \in \mathbb{Z}$.

$$2 \cdot 2^2 r^3 = 2 \cdot q^3 \Rightarrow 2^2 r^3 = q^3.$$

Note que na fatoração de q^3 não pode haver 2 pois, se tivesse, q não seria primo com p, uma contradição. Assim $\sqrt[3]{2} \in \mathbb{R} - \mathbb{Q}$.

Q.E.D.

Falta ainda provarmos que $\sqrt[3]{2}$ não é construtível, ou seja, que esse número não se encontra em nenhum dos corpos da cadeia 1.3.

Proposição 2.2. *O número $\sqrt[3]{2}$ não é construtível por régua e compasso.*

Demonstração. Suponha que o polinômio $x^3 = 2 \in \mathbb{Q}[x]$ tenha raiz em algum corpo da cadeia 1.3 e sejam x_1 uma raiz e j o menor índice para o qual

$$x_1 \in K_j = K_{j-1}(\sqrt{w}), \text{ onde } w \in K_{j-1}, \sqrt{w} \notin K_{j-1} \text{ e } w > 0.$$

Nestas condições, temos

$$x_1 = x + y\sqrt{w}, \text{ com } x, y \in K_{j-1},$$

e, deste modo,

$$\begin{aligned} x_1^3 - 2 &= (x + y\sqrt{w})^3 - 2 \\ &= x^3 + 3x^2 y\sqrt{w} + 3xy^2 w + y^3 w\sqrt{w} - 2 \\ &= (x^3 + 3xy^2 w - 2) + (3x^2 y + y^3 w)\sqrt{w} \\ &= p + q\sqrt{w}, \end{aligned}$$

onde $p = x^3 + 3xy^2w - 2$ e $q = 3x^2y + y^3w$, $p, q \in K_{j-1}$.

Seja agora $x_2 = x - y\sqrt{w} \in K_j$. Obtemos também

$$x_2^3 - 2 = x^3 + 3xy^2w) - (3x^2y + y^3w)\sqrt{w} = p - q\sqrt{w}.$$

Ora,

$$x_1^3 - 2 = 0 \Rightarrow p + q\sqrt{w} = 0 \Rightarrow p = q = 0. \tag{2.1}$$

De fato, supondo $q \neq 0$, teríamos $\sqrt{w} = -p/q \in K_{j-1}$, o que não ocorre, já que $\sqrt{w} \notin K_{j-1}$. assim, $q = 0$ e daí $p = 0$.

Deste modo, podemos concluir que $x_2^3 - 2 = p - q\sqrt{w} = 0$ e assim x_2 seria outra raiz real de $x^3 = 2$. Note que $x^3 - 2 = (x - \sqrt[3]{2})(x^2 + \sqrt[3]{2}x + \sqrt[3]{4})$ e que o segundo fator não possui raiz real (o discriminante é $-3\sqrt[3]{4} < 0$), o que significa que $x^3 = 2$ possui apenas uma raiz real. Obtemos que

$$x_1 = x_2 = \sqrt[3]{2} \Rightarrow x + y\sqrt{w} = x - y\sqrt{w} \Rightarrow y = 0 \text{ (pois } w > 0).$$

Neste caso teríamos $\sqrt[3]{2} = x \in K_{j-1}$, o que não ocorre pela nossa hipótese sobre j, uma contradição. Assim, o número $\sqrt[3]{2}$ não pertence a nenhum corpo da cadeia 1.3 e, portanto, não é construtível.

Q.E.D.

Portanto, obtemos que a duplicação do cubo é impossível por régua e compasso.

2.2 O Problema da Trissecção do Ângulo

Apresentamos agora uma proposição que utilizaremos para a demonstração da impossibilidade de trissecção do ângulo.

Proposição 2.3. *Se uma função polinomial do 3º grau com coeficientes racionais não possui raiz racional, então nenhuma de suas raízes pode ser cons-*

truída apenas com régua não graduada e compasso a partir de um segmento unitário.

Demonstração. Seja $f(x)$ uma função polinomial do 3º grau da forma

$$f(x) = r_1x^3 + r_2x^2 + r_1x + r_0,$$

onde r_3, r_2, r_1 e $r_0 \in \mathbb{Q}$ e as raízes de f são x_1, x_2 e $x_3 \notin \mathbb{Q}$.

Suponhamos que pelo menos uma das raízes seja construtível e seja j o menor inteiro tal que K_j da cadeia de extensões 1.3 contenha uma raiz da equação dada. Seja esta raiz x_1, ou seja,

$$x_1 = a + b\sqrt{w}, \text{ com } a, b \in K_{j-1}, w > 0, \sqrt{w} \notin K_{j-1}.$$

Logo,

$$\begin{aligned} f(x_1) &= f(a + b\sqrt{w}) \\ &= r_3(a + b\sqrt{w})^3 + r_2(a + b\sqrt{w})^2 + r_1(a + b\sqrt{w}) + r_0 \\ &= (r_3a^3 + 3r_3ab^2w + r_2a^2 + r_2b^2w + r_1a + r_0) + \\ &\quad (3r_3a^2b + r_3b^3w + 2r_2ab + r_1b)\sqrt{w} \\ &= p + q\sqrt{w}, \end{aligned}$$

onde $p = r_3a^3 + 3r_3ab^2w + r_2a^2 + r_2b^2w + r_1a + r_0$ e $q = 3r_3a^2b + r_3b^3w + 2r_2ab + r_1b$, e, além disso, $p, q \in K_{j-1}$. Como supomos que x_1 é raiz de f, temos

$$0 = f(x_1) = p + q\sqrt{w},$$

e, pela equação 2.1, temos $q = p = 0$.

Por outro lado, temos também que $f(a - b\sqrt{w}) = p - q\sqrt{w} = 0$, o que significa que $a - b\sqrt{w}$ é outra raiz de f.

Já que $w \neq 0$, temos $x_1 \neq x_2$. De fato, se x_1 fosse igual a x_2 teríamos $a + b\sqrt{w} = a - b\sqrt{w} \Rightarrow b = 0 \Rightarrow x_1 = x_2 = a \in K_{j-1}$, uma contradição pelo fato de j ser o menor índice de corpo que contém uma raiz de $f(x)$.

Das relações fundamentais entre os coeficientes e as raízes das equações cúbicas, segue que

$$x_1 + x_2 + x_3 = -\left(\frac{r_2}{r_3}\right) \in \mathbb{Q}.$$

Assim, obtemos

$$\begin{aligned} x_3 &= -\left(\frac{r_2}{r_3}\right) - x_1 - x_2 \\ &= -\left(\frac{r_2}{r_3}\right) - (a + b\sqrt{w}) - (a - b\sqrt{w}) \\ &= -\left(\frac{r_2}{r_3}\right) - 2a \in K_{j-1}, \end{aligned}$$

Uma contradição por j ser o menor índice de corpo da cadeia 1.3 que contém raízes de $f(x)$.

Q.E.D.

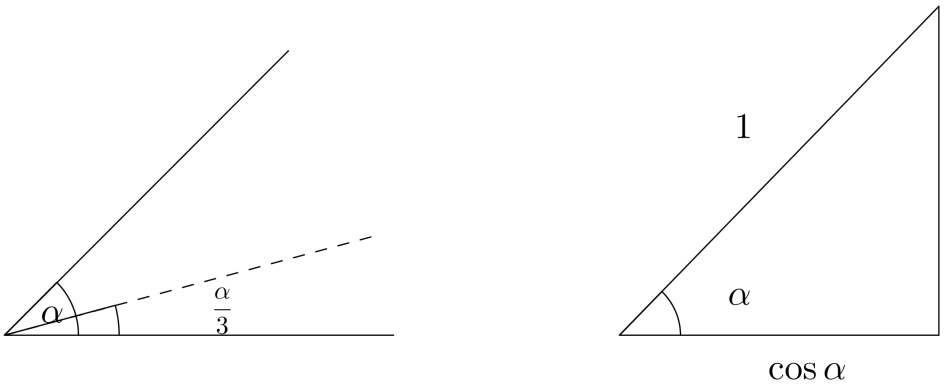


Figura 2.3: A Trissecção do Ângulo e a Relação entre um Ângulo e seu Cosseno.

Agora passaremos ao problema da trissecção do ângulo em si, que consiste em provar que nem todo ângulo pode ser trissectado (dividido em três partes iguais) por régua e compasso.

Notemos primeiramente que alguns ângulos podem ser trivialmente trissectados, como é o caso do ângulo reto: sabemos construir um ângulo de 30^o.

Observemos também, como pode ser visto na Figura 2.3, que a construção de um ângulo α é equivalente à construção de um segmento de comprimento $\cos\alpha$. Deste modo, o problema de trissecção do ângulo estaria resolvido se pudéssemos construir $\cos\alpha/3$, dado que $\cos\alpha$ seja construtível.

Mostraremos a impossibilidade da trissecção do ângulo pela demonstração da impossibilidade de trissecção de 60^o. Ou seja, mostraremos um contra-exemplo, de que 60^o não pode ser trissectado

Antes disto, deduzimos uma identidade trigonométrica que nos será útil:

$$\begin{aligned}\cos 3\beta &= \cos(2\beta+\beta) = \cos 2\beta\cos\beta - \operatorname{sen}2\beta\operatorname{sen}\beta \\ &= (\cos^2\beta - \operatorname{sen}^2\beta)\cos\beta - (2\operatorname{sen}\beta\cos\beta)\operatorname{sen}\beta \\ &= \cos^3\beta - 3\operatorname{sen}^2\beta\cos\beta = \cos^3\beta - 3(1-\cos^2\beta)\cos\beta \\ &= 4\cos^3\beta - 3\cos\beta.\end{aligned}$$

Para $\beta = 20^o$, temos $\cos 60^o = 4\cos^3 20^o - 3\cos 20^o$, ou ainda, $\frac{1}{2} = 4\cos^3 20^o - 3\cos 20^o$. Fazendo $x = 2\cos 20^o$, obtemos

$$x^3 - 3x - 1 = 0. \tag{2.2}$$

Para mostrarmos que $\cos 20^o$ não é construtível, basta mostrarmos que $x = 2\cos 20^o$ não é construtível. Utilizando a Proposição 2.3, mostraremos que a Equação 2.2 não possui nenhuma raiz racional.

Proposição 2.4. *O ângulo de 60^o não pode ser trissectado por régua e compasso.*

Demonstração. Suponhamos por contradição que r/s seja raiz de (2.2) tal que
$r, s \in \mathbb{Z}$, $s \neq 0$ e $\operatorname{mdc}(r,s) = 1$. Deste modo,

$$\frac{r^3}{s^3} - \frac{3r}{s} - 1 = 0 \Rightarrow s^3 = r^3 - 3rs^2 = r(r^2 - 3s^2).$$

Por outro lado,

$$\frac{r^3}{s^3} - \frac{3r}{s} - 1 = 0 \Rightarrow r^3 = s^3 + 3rs^2 = s^2(s + 3r).$$

Assim,

$$s^3 = r(r^2 - 3s^2) \text{ e } r^3 = s^2(s + 3r).$$

Ou seja, s^3 é múltiplo de r e r^3 é múltiplo de s. Como $\text{mdc}(r, s) = 1$, obtemos que 1 e -1 seriam as únicas raízes racionais. Porém, nenhuma delas é raiz da equação (2.2).

Pela Proposição 2.3, as raízes não são construtíveis, ou seja, $\cos 20^o$ não é construtível e, portanto, o ângulo de 60^o não pode ser trissectado por régua e compasso.

Q.E.D.

2.3 O Problema da Quadratura do Círculo

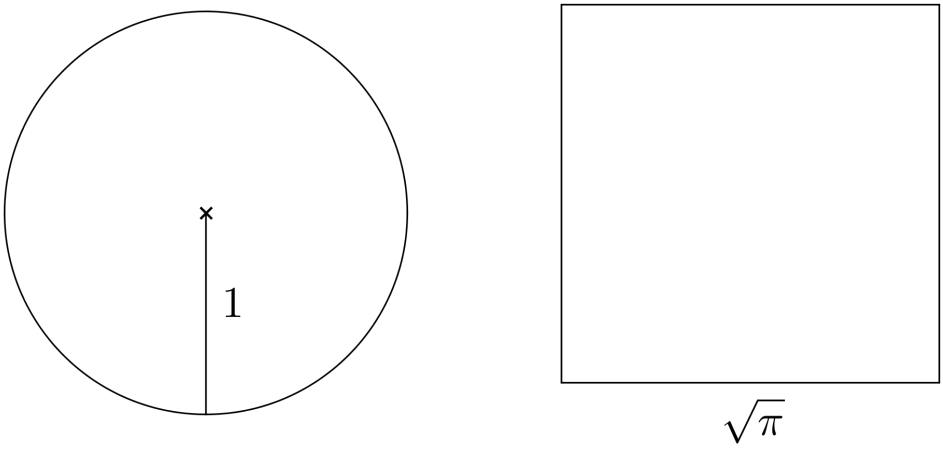


Figura 2.4: A Quadratura do círculo.

O problema da quadratura do círculo consiste em obter por régua e compasso um quadrado de mesma área que um círculo de raio unitário. Note

que este quadrado deverá ter lado de medida $\sqrt{\pi}$ (Figura 2.4). De fato, seja A a área do círculo de raio unitário. Assim,

$$A = \pi,$$

e, sendo l a medida do lado do quadrado, temos

$$l^2 = A = \pi \Rightarrow l = \sqrt{\pi}.$$

Uma condição necessária e suficiente para que o quadrado de mesma área que o círculo unitário seja construtível é que o número $\sqrt{\pi}$ seja construtível, o que não ocorre, pois π é um número transcendente sobre $\mathbb{Q}$, resultado que pode ser visto em [6] e [14]. Como todo número construtível é algébrico (proposição 1.8), então nem π nem $\sqrt{\pi}$ são construtíveis.

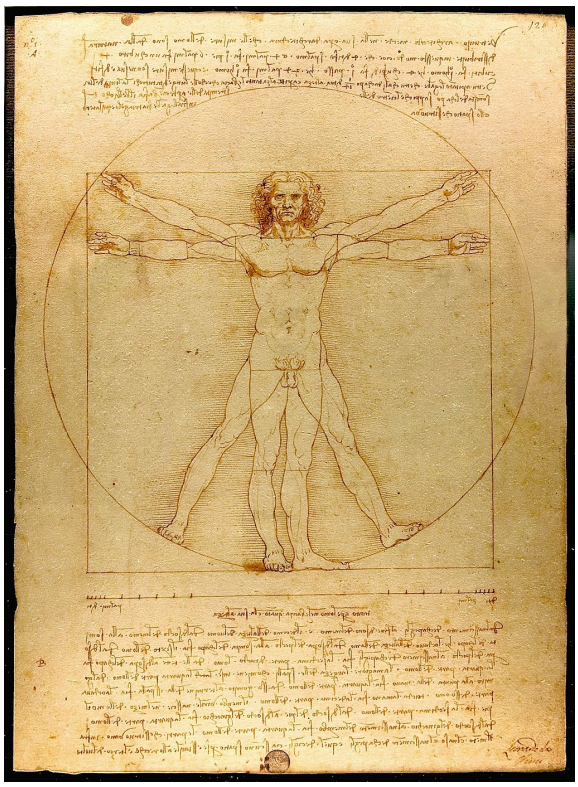


Figura 2.5: L'Uomo Vitruviano

Na época do renascimento, Leonardo da Vinci (1452 - 1519) representou metaforicamente a ideia de que a quadratura do círculo teria solução nas dimensões de um corpo humano ideal [4]. Esta representação é o famoso desenho do homem vitruviano (Figura 2.5).

2.4 A Inconstrutibilidade do Heptágono Regular

Alguns polígonos regulares são facilmente construídos, como o triângulo e o quadrado (Figura 2.6). Desde a antiguidade clássica já se conheciam métodos de construção dos polígonos de 3, 4, e 5 lados e destes números vezes potências de dois, como descrito em [1]. Para uma referência de métodos atuais de construção, consulte [9] ou [15].

Note as ausências dos métodos de construção dos polígonos regulares de 7 e 9 lados. Os gregos notaram estas ausências e passaram a buscar métodos para construção destes polígonos, especialmente do heptágono.

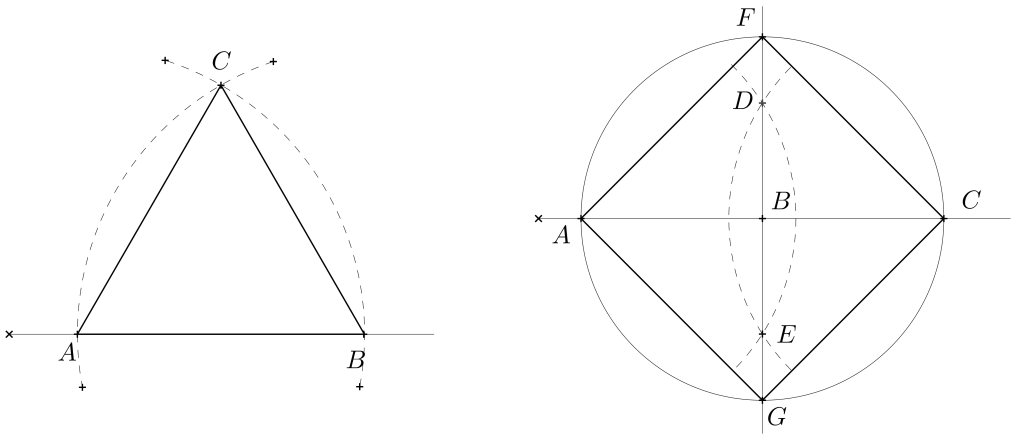


Figura 2.6: Construções do Triângulo Equilátero e do Quadrado.

O problema de inconstrutibilidade do heptágono pode ser visto como uma aplicação particular do teorema de caracterização de polígonos regulares construtíveis, uma vez que trata-se da impossibilidade de construção de um

polígono regular, o de 7 lados.

Os matemáticos tentaram resolver este problema num período de dois mil anos sem, contudo, obterem um método para sua construção. Na verdade, este método não poderia existir pois o heptágono é inconstrutível, o que provaremos nesta seção.

Um princípio importante para ter em mente quando queremos determinar a construtibilidade de polígonos regulares é que a construção do n-ágono regular será possível se, e somente se, a medida do lado do n-ágono regular inscrito em uma circunferência unitária for construtível. Mas isto também equivale à construção do ângulo de medida $2\pi/n$, ou ainda à construção de $\cos 2\pi/n$. A Figura 2.7 ilustra este princípio para o caso do heptágono regular.

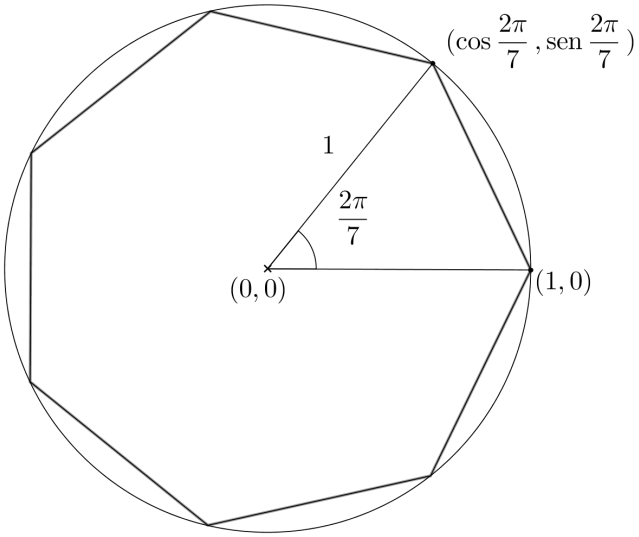


Figura 2.7: O Heptágono Regular.

Agora demonstraremos a impossibilidade de construção do heptágono regular utilizando alguns conhecimentos de números complexos e a proposição 2.3.

Proposição 2.5. *É impossível construir por régua e compasso o heptágono regular.*

Demonstração. Podemos fazer uma associação dos vértices do heptágono regular às sete raízes sétimas da unidade nos números complexos e, desta forma, obtemos uma fórmula para obtenção das raízes:

$$z_n = \cos\frac{2\pi n}{7} + i\,\mathrm{sen}\frac{2\pi n}{7},\ \text{para } n \in \mathbb{N}; n \leq 7.$$

Dentre as raízes acima listadas, apenas $z_0 = 1$ é real.

Observe que

$$z^7 - 1 = (z-1)(z^6 + z^5 + z^4 + z^3 + z^2 + z + 1),$$

e, assim, as seis raízes complexas não reais de $z^7 = 1$ são exatamente as raízes da equação

$$z^6 + z^5 + z^4 + z^3 + z^2 + z + 1 = 0. \tag{2.3}$$

Podemos ainda reescrever a equação (2.3) do seguinte modo:

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

ou ainda

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

Tomando $w = z + \dfrac{1}{z}$, obtemos

$$w^3 + w^2 - 2w - 1 = 0. \tag{2.4}$$

Seja z uma raiz de (2.3), ou seja, $z = \cos\alpha + i\,\mathrm{sen}\alpha$ para $\alpha = \dfrac{2n\pi}{7}$, $n \in$

$\{1, 2, \cdots, 6\}$, então, $w = z + 1/z$ será raiz de (2.4), Note que

$$\begin{aligned} w &= z + \frac{1}{z} = \cos\alpha + i\,\mathrm{sen}\alpha + \frac{1}{\cos\alpha + i\,\mathrm{sen}\alpha} \\ &= \cos\alpha + i\,\mathrm{sen}\alpha + \frac{1}{(\cos\alpha + i\,\mathrm{sen}\alpha)}\frac{(\cos\alpha - i\,\mathrm{sen}\alpha)}{(\cos\alpha - i\,\mathrm{sen}\alpha)} \\ &= \cos\alpha + i\,\mathrm{sen}\alpha + \frac{\cos\alpha - i\,\mathrm{sen}\alpha}{1} \\ &= 2\cos\alpha. \end{aligned}$$

Deste modo, $w = 2\cos\alpha$ será raiz de (2.4).

Note que se mostrarmos que a equação (2.4) não possui nenhuma raiz construtível, então o $\cos\alpha$ não será construtível para nenhum $n = \{1, 2, \cdots, 6\}$. Também, se $\cos\alpha$ não for construtível, então $\mathrm{sen}\alpha$ também não será, já que um seno (ou cosseno) de um ângulo é construtível se, e somente se, o ângulo é construtível.

Verifiquemos agora que a equação (2.4) não possui raízes racionais. Suponhamos, por absurdo, que (2.4) possua uma raiz racional e seja $w = \dfrac{x}{y}$ uma raiz tal que $x, y \in \mathbb{Z}$ e $\mathrm{mdc}(x, y) = 1$. E, assim,

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

Ou ainda,

$$x^3 + x^2y - 2xy^2 - y^3 = 0.$$

Ou seja,

$$x^3 = y(y^2 + 2xy - x^2) \text{ e } y^3 = x(x^2 + xy - 2y^2),$$

donde podemos concluir que x^3 é múltiplo de y e y^3 é múltiplo de x. Como $\mathrm{mdc}(x, y) = 1$, então x e y não possuem fatores comuns, e isso só seria possível se x e y fossem iguais a 1 ou -1.

Neste caso, $w = 1$ ou $w = -1$. Porém, para $w = 1$,

$$1^3 + 1^2 - 2 \cdot 1 - 1 = -1 \neq 0,$$

e para $w = -1$,

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

Nenhum destes números é raiz de (2.4). Portanto, a equação (2.4) não possui raízes racionais. Da proposição 2.3, segue que a medida do lado do heptágono regular não é construtível por régua e compasso.

Q.E.D.

Capítulo 3

Grupos de Galois

Iniciaremos agora a busca pela solução da seguinte questão:

- Quais polígonos regulares são construtíveis?

Já vimos que o heptágono não é construtível (Proposição 2.5) mas, por outro lado, há polígonos regulares construtíveis (Figura 2.6). Será que há alguma propriedade que caracterize todos os polígonos regulares construtíveis? Provaremos que sim de acordo com o nosso teorema principal, que é devido a Gauss:

Teorema *(Caracterização dos Polígonos Regulares Construtíveis). Seja n um número natural. Uma condição necessária e suficiente para que o n-ágono regular seja construtível por régua e compasso é que n seja da forma*

$$n = 2^r p_1 \cdots p_s,$$

onde $r, s \in \mathbb{N} \cup \{0\}$ e $p_1, \cdots, p_s$ são primos distintos da forma

$$p_i = 2^{2^{r_i}} + 1,$$

com $r_i \in \mathbb{N} \cup \{0\}$.

Neste capítulo, apresentaremos mais alguns conceitos necessários para a demonstração do nosso teorema principal que são os relacionados a grupos de Galois de extensões de corpos.

Decidimos agrupar os resultados de decomposição de polinômios e derivada formal, normalidade e separabilidade de extensões de corpos e os rudimentos da teoria de Galois neste capítulo pela ordem mais recorrente de estudo, que também pode ser observada em [12] e [14].

Na última seção, apresentaremos o teorema fundamental da teoria de Galois (teorema 5), cuja demonstração pode ser encontrada em [3], [12] e [14].

3.1 Definição

Definição 3.1. *Dado K um corpo, chamaremos uma função bijetora $f : K \to K$ de* ***automorfismo*** *sempre que, para quaisquer $x, y \in K$, tivermos*

$$f(x+y) = f(x) + f(y) \text{ e } f(xy) = f(x)f(y).$$

Exemplo 3.1. *A função identidade $f(x) = x$ é um automorfismo, seja qual for o corpo.*

Definição 3.2. *Sejam $L : K$ uma extensão de corpos e f um automorfismo de L. Diremos que f é um* ***K-automorfismo*** *de L quando*

$$f(x) = x,$$

para todo $x \in K$.

Exemplo 3.2. *Dados o corpo $\mathbb{C}$ dos números complexos, $z = x + iy$ um número complexo qualquer, com $x, y \in \mathbb{R}$ e a função $f : \mathbb{C} \to \mathbb{C}$ definida por*

$$f(z) = x - iy,$$

que leva um número no seu conjugado complexo. Verifica-se facilmente que

f é um automorfismo de $\mathbb{C}$. Mais ainda, f é um $\mathbb{R}$-automorfismo de $\mathbb{C}$. De fato, uma vez que para todo $z \in \mathbb{R}$ temos $z = x$ e, neste caso,

$$f(z) = x = z.$$

Teorema 3.1. *Se $L : K$ é uma extensão de corpos, então o conjunto de todos os K-automorfismos de L com a operação de composição de funções forma um grupo algébrico.*

Demonstração. Supondo que f e g sejam K-automorfismos de L, mostraremos que $f \circ g$ é também um automorfismo. Sendo $x, y \in L$, temos

$$\begin{aligned}(f \circ g)(x+y) &= f(g(x+y)) \\ &= f(g(x)+g(y)) \\ &= f(g(x))+f(g(y)) \\ &= (f \circ g)(x)+(f \circ g)(y)\end{aligned}$$

e

$$\begin{aligned}(f \circ g)(xy) &= f(g(xy)) \\ &= f(g(x)g(y)) \\ &= f(g(x))f(g(y)) \\ &= (f \circ g)(x)(f \circ g)(y).\end{aligned}$$

Note também que todo $y \in L$ é imagem de algum x por g, uma vez que g é sobrejetivo. Assim, como f também é sobrejetivo, temos, para todo $z \in K$

$$z = f(y) = f(g(x)) = (f \circ g)(x).$$

E, portanto, $(f \circ g)$ é sobrejetiva. Sejam agora $x, y \in K$ tais que $(f \circ g)(x) = (f \circ g)(y)$, ou seja, $f(g(x)) = f(g(y))$. Da injetividade de f segue que $g(x) = g(y)$, e da injetividade de g segue que $x = y$, o que significa

que $(f \circ g)$ é injetiva. Deste modo, mostramos que $(f \circ g)$ é também um automorfismo de L. Mais ainda, uma vez que, para qualquer $x \in K$ temos

$$(f \circ g)(x) = f(g(x)) = f(x) = x,$$

vale que $(f \circ g)$ é um K-automorfismo de L. O elemento neutro deste grupo é a função identidade. De fato, pois, além de ser bijetiva, temos, para quaisquer $x, y \in L$, $i(x + y) = x + y = i(x) + i(y)$ e $i(xy) = xy = i(x)i(y)$, onde i é a função identidade. Para todo automorfismo f de L, existe o inverso f^{-1}, uma vez que f é bijetora, possuindo uma inversa f^{-1} também bijetora. Note que, dados $x, y \in L$, existem $u, v \in L$ tais que $f(u) = x$ e $f(v) = y$. Segue que

$$f^{-1}(x + y) = f^{-1}(f(u) + f(v)) = f^{-1}(f(u + v)) = u + v = f^{-1}(x) + f^{-1}(y)$$

e

$$f^{-1}(xy) = f^{-1}(f(u)f(v)) = f^{-1}(f(uv)) = uv = f^{-1}(x)f^{-1}(y).$$

Também, dado $x \in K$, e lembrando que f é um K-automorfismo, temos

$$f^{-1}(x) = f^{-1}(f(x)) = x$$

e, portanto, f^{-1} é também um K-automorfismo de L. Como a composição de funções é associativa, então o conjunto de todos os K-automorfismos de L é um grupo.

Q.E.D.

Definição 3.3. *Chamaremos de* ***grupo de Galois*** *de uma extensão $L : K$ ao grupo de todos os K-automorfismos de L, com a operação de composição de funções. Denotaremos o grupo de Galois da extensão $L : K$ por $\Gamma(L : K)$.*

Exemplo 3.3. *Voltaremos a abordar a extensão $\mathbb{C} : \mathbb{R}$. Já vimos no exemplo 3.2 um exemplo de $\mathbb{R}$-automorfismo. Agora provaremos que os dois únicos $\mathbb{R}$-automorfismos de $\mathbb{C}$ são a identidade e a função conjugado. Sejam f um*

$\mathbb{R}$-*automorfismo de* $\mathbb{C}$ *e* $j = f(i)$. *Note que*

$$j^2 = f(i) \cdot f(i) = f(i^2) = f(-1) = -1.$$

Assim, $j = i$ *ou* $j = -i$. *Sendo agora* $x, y \in \mathbb{R}$, *segue que*

$$f(x + iy) = f(x) + f(i)f(y) = x + jy,$$

e assim a imagem de um $\mathbb{R}$*-automorfismo pode ter uma das seguintes formas:*

$$\begin{aligned} f_1(x + iy) &= x + iy \text{ ou} \\ f_2(x + iy) &= x - iy. \end{aligned}$$

Ou seja, o grupo $\Gamma(\mathbb{C} : \mathbb{R})$ *consta de apenas dois elementos, a identidade e a função que leva um número complexo no seu conjugado.*

3.2 Decomposição e Derivada Formal de Polinômios

Voltemos agora nossa atenção a conceitos relacionados a polinômios com vistas a apresentarmos a ideia de corpo de decomposição e algumas proposições utilizando derivada formal de um polinômio.

Definição 3.4. *Sejam* K *um corpo e* $f \in K[x]$ *um polinômio. Diremos que* f *é* ***decomposto*** *sobre* K *quando* f *puder ser escrito como um produto de fatores*

$$f(x) = k(x - \alpha_1) \cdots (x - \alpha_n),$$

onde $k, \alpha_1, \cdots, \alpha_n \in K$. *Diremos que um corpo* F *é um* ***corpo de decomposição*** *para o polinômio* $f \in K[x]$ *sempre que* $K \subseteq F$ *e*

(1) f *puder ser decomposto em* $F[x]$;

(2) Se $K \subseteq F' \subseteq F$ *e* f *for decomposto sobre* F', *então* $F = F'$.

Definição 3.5. *Sejam K um corpo e $f \in K[x]$ um polinômio tal que*

$$f(x) = a_0 + a_1x + \cdots + a_nx^n.$$

Diremos que a ***derivada formal*** *de f é o polinômio*

$$Df(x) = a_1 + 2a_2x + \cdots + na_nx^{n-1}.$$

Utilizaremos mais adiante algumas propriedades bastante conhecidas de derivadas, cujas verificações são simples, e podem ser encontradas em [6]. Dados f, g polinômios, valem:

(1) $D(f + g) = Df + Dg$;

(2) $D(fg) = f \cdot Dg + g \cdot Df$;

(3) $D(f \circ g) = Df \circ g \cdot Dg$

Exemplo 3.4. *A derivada formal de um polinômio constante é zero.*

Lema 3.1. *Dados um corpo K e um polinômio não nulo $f \in K[x]$, f possui raízes múltiplas no corpo de decomposição se, e somente se, f e Df possuem um fator comum de grau maior do que ou igual a* 1.

Demonstração. Suponha que f possua raízes múltiplas no corpo de decomposição F. Assim, sobre F,

$$f(x) = (x - \alpha)^2 g(x),$$

para algum $g \in F[x]$ e $\alpha \in F$. Então

$$\begin{aligned} Df(x) &= (x - \alpha)^2 \cdot Dg + 2(x - \alpha) \cdot g \\ &= (x - \alpha)((x - \alpha)Dg + 2g) \end{aligned}$$

e, portanto, f e Df possuem o fator comum $(x - \alpha)$.

Reciprocamente, suponha que f não possua raízes múltiplas. Mostraremos que f e Df são primos entre si em $F[x]$. Se $\partial f = 1$, temos $f(x) = k(x-\alpha)$ e $Df(x) = k$. Neste caso, f e Df não possuem fatores em comum.

Suponha, por hipótese de indução, que g e Dg são primos entre si, para $\partial g < \partial f$ e g sem raizes múltiplas. Seja, agora, $f(x) = (x-\alpha)g(x)$, onde $(x-\alpha) \nmid g(x)$ e $Df(x) = (x-\alpha)Dg + g$. Note que se um fator de g dividir Df, então precisa dividir Dg, já que $(x-\alpha)$ é irredutível. Mas, por hipótese de indução, g e Dg são primos entre si. Note também que, uma vez que $x-\alpha$ não divide g, então não divide $Df(x) = (x-\alpha)Dg + g$. Assim, f e Df são primos entre si, como queríamos demonstrar. A prova segue da contrapositiva do que demonstramos.

Q.E.D.

Proposição 3.1. *Sejam K um corpo de característica zero e L um corpo de decomposição para $x^p - 1$ sobre K, onde p é um número primo. Então o grupo de Galois de $L : K$ é abeliano.*

Demonstração. A derivada de $x^p - 1$ é px^{p-1}. Estes polinômios não contêm fatores em comum, uma vez que a derivada é $p(x-0)^{p-1}$ e $(x-0)$ não divide $x^p - 1$ em um corpo de característica zero. Do lema 3.1 segue que $x^p - 1$ não possui raízes múltiplas em L. Note que as raízes de $x^p - 1$ formam um grupo em relação à multiplicação de elementos do corpo L.

De fato, sejam $a, b \in L$ duas raízes de $x^p - 1$, então

$$a^p = 1 \qquad \text{e} \qquad b^p = 1.$$

Temos

- $(a^{-1})^p = (a^p)^{-1} = 1^{-1} = 1$, e
- $(ab)^p = (a^p)(b^p) = 1 \cdot 1 = 1$.

E assim, $(ab)^p - 1 = 0$ e $(a^{-1})^p - 1 = 0$, o que significa que ab e a^{-1} são também raizes de $x^p - 1$. O elemento neutro da multiplicação 1 é raiz do polinômio

e funciona como neutro para o conjunto das raízes. A comutatividade segue da comutatividade da multiplicação de L e, por fim, se a é raiz de $x^p - 1$, então

$$\begin{aligned} a^p = 1 \quad &\Rightarrow \quad \frac{1}{a} = \frac{1}{\sqrt[p]{1}} = \sqrt[p]{\frac{1}{1}} = \sqrt[p]{1} \\ &\Rightarrow \quad \frac{1}{a} = \sqrt[p]{1} \\ &\Rightarrow \quad \left(\frac{1}{a}\right)^p - 1 = 0 \\ &\Rightarrow \quad \frac{1}{a} \text{ é raiz de } x^p - 1. \end{aligned}$$

Deste modo, as raízes de $x^p - 1$ formam um grupo sobre a operação de multiplicação de L.

Como não há raízes múltiplas em L, então a ordem deste grupo é p, e todo grupo de ordem prima é cíclico (vide [6] e [12]).

Seja, então, ϵ uma raiz geradora deste grupo. Assim, $L = K(\epsilon)$, uma vez que, por definição, o corpo de decomposição é o menor corpo que contém as raízes do polinômio e neste caso, seria $L = K(a_0, \cdots, a_p)$, onde $a_0, \cdots, a_p$ são as raízes p-ésimas de 1. Mas, como as raízes formam um grupo cíclico, então existe $\epsilon = a_i$, para algum $i = \{0, \cdots, p\}$, tal que cada a_j é potência de ϵ.

Observe que um K-automorfismo será diferenciado dos outros pelo seu efeito no elemento ϵ, já que todo K-automorfismo leva $\alpha \in K$ em α.

Como são bijeções, os K-automorfismos de L devem permutar as raízes de $x^p - 1$. Assim, todo K-automorfismo é da forma

$$f_j : \epsilon \to \epsilon^j.$$

Sejam agora dois K-automorfismos f_i e f_j. Note que

$$f_i : \epsilon \to \epsilon^i \text{ e } f_j : \epsilon \to \epsilon^j.$$

Mas $(f_i \circ f_j)(\epsilon) = (\epsilon^j)^i = \epsilon^{ji} = \epsilon^{ij} = (\epsilon^i)^j(f_j \circ f_i)(\epsilon)$ implicando que o grupo de Galois de $L : K$ é abeliano.

Q.E.D.

3.3 Extensões normais e extensões separáveis

Definição 3.6. *Diremos que uma extensão $L : K$ é **normal** quando todo polinômio irredutível $f \in K[x]$ que tenha pelo menos uma raiz em L puder ser decomposto em L.*

Exemplo 3.5. *A extensão $\mathbb{C} : \mathbb{R}$ é normal, pois, pelo teorema fundamental da álgebra, todo polinômio de $\mathbb{R}$ pode ser decomposto em $\mathbb{C}$.*

Para demonstrarmos a Proposição 3.2, utilizaremos os dois lemas seguintes sem demonstrá-los. Contudo, suas demonstrações podem ser encontradas em [14].

Lema 3.2. *Sejam $K(\alpha) : K$ e $K(\beta) : K$ extensões algébricas simples tais que α e β possuem o mesmo polinômio minimal m sobre K. Então as duas extensões são isomorfas.*

Lema 3.3. *Sejam $i : K \to K'$ um isomorfismo de corpos, T o corpo de decomposição para o polinômio $f \in K[x]$ e T' o corpo de decomposição para $i(f) \in K'[x]$, onde $i(f)$ é o polinômio de $K'[x]$ cujos coeficientes são as imagens por i dos coeficientes de $f \in K[x]$. Então as extensões $T : K$ e $T' : K'$ são isomorfas.*

Proposição 3.2. *Seja $L : K$ uma extensão de corpos. Se L for um corpo de decomposição para algum polinômio de $K[x]$, então $L : K$ é normal e finita.*

Demonstração. Seja L um corpo de decomposição para algum polinômio $g \in K[x]$. Se $\alpha_1, \cdots, \alpha_n$ são as raízes de g em L, então, do fato de L ser o menor corpo que contém K e as raízes, então $L = K(\alpha_1, \cdots, \alpha_n)$ e assim $L : K$ é uma extensão finita. Resta mostrarmos que é normal.

Seja $f \in K[x]$ um polinômio irredutível que tenha pelo menos uma raiz em L. Devemos mostrar que f pode ser decomposto em L. Seja $M \supseteq L$ o corpo de decomposição para o polinômio $fg \in K[x]$. Suponha β_1 e β_2 raízes de f em M. Temos que

$$M \supseteq L(\beta_1) \supseteq K(\beta_1) \supseteq K \text{ e } M \supseteq L(\beta_2) \supseteq K(\beta_2) \supseteq K$$

e

$$[L(\beta_1) : L][L : K] = [L(\beta_1) : K] = [L(\beta_1) : K(\beta_1)][K(\beta_1) : K] \tag{3.1}$$

$$[L(\beta_2) : L][L : K] = [L(\beta_2) : K] = [L(\beta_2) : K(\beta_2)][K(\beta_2) : K]. \tag{3.2}$$

Pelo Lema 3.2, como β_1 e β_2 são raízes do mesmo polinômio irredutível de $K[x]$, então $[K(\beta_1) : K] = [K(\beta_2) : K]$. Se tomarmos g considerando-o um polinômio de $K(\beta_1)$ (ou $K(\beta_2)$), então $L(\beta_1)$ (ou $L(\beta_2)$) é um corpo de decomposição para g.

Pelo lema 3.3 e pelo fato de β_1 e β_2 serem raízes do mesmo polinômio de $K[x]$, temos

$$L(\beta_1) : K(\beta_1) \simeq L(\beta_2) : K(\beta_2)$$

e, como são isomorfos, possuem o mesmo grau.

Podemos aplicar as nossas considerações na equação 3.1 e na equação 3.2, obtendo

$$[L(\beta_1) : L] = [L(\beta_2) : L].$$

Supondo $\beta_1 \in L$, então $[L(\beta_1) : L] = 1 = [L(\beta_2) : L]$ e assim

$$L(\beta_2) = L.$$

Ou seja, $\beta_2 \in L$ e, portanto, $L : K$ é normal.

Q.E.D.

Definição 3.7. *Dados K um corpo e $f \in K[x]$ um polinômio irredutível, diremos que f é **separável** sobre K quando não possuir raízes múltiplas em*

nenhum corpo de decomposição. Caso contrário, dizemos que f é ***inseparável****.*

Exemplo 3.6. *O polinômio $f(x) = x^2 - x - 3/4 \in \mathbb{Q}[x]$ é separável, uma vez que suas raízes são $3/2$ e $-1/2$, que são distintas.*

Proposição 3.3. *Se K é um corpo de característica zero, então todo polinômio irredutível de $K[x]$ é separável em $K[x]$.*

Demonstração. Do Lema 3.1, obtemos que um polinômio $f \in K[x]$ é inseparável se, e somente se, f e Df possuem um fator comum de grau maior do que ou igual a 1. Do fato que f é irredutível, e, sendo $U(K[x])$ o corpo dos polinômios inversíveis de $K[x]$, ou seja, os polinômios constantes (vide [6]), obtemos o seguinte:

$$f(x) = g(x)h(x) \Leftrightarrow h(x) \in U(K[x]) \Leftrightarrow h(x) = c \in K.$$

Supondo que g seja o fator comum entre f e Df, resulta que $Df(x) = g(x)j(x)$. Disto, obtemos que f divide Df mas, como $\partial Df < \partial f$ então $Df(x) = 0$, uma contradição. Por outro lado, sendo $f(x) = a_0 + \cdots + a_n x^n$, temos

$$Df(x) = a_1 + \cdots + n a_n x^{n-1}.$$

Mas, como Df é o polinômio nulo, então

$$a_1 = 2a_2 = \cdots = n a_n = 0.$$

Do fato que a característica de K é zero, obtemos

$$a_1 = a_2 = \cdots = a_n = 0.$$

Disto resultaria que $f(x) = a_0$, uma contradição com o fato de f ser irredutível e, portanto, não inversível (constante).

Q.E.D.

Semelhantemente ao que fizemos anteriormente, podemos definir, mais geralmente, polinômios, elementos algébricos e extensões algébricas separáveis.

Definição 3.8. *Sejam K um corpo, $f \in K[x]$ um polinômio, $\alpha \in L$ um elemento algébrico sobre K e $L : K$ uma extensão algébrica, diremos que f é* ***separável*** *em $K[x]$ quando todos os seus fatores irredutíveis forem separáveis sobre K. Diremos que α é* ***separável*** *sobre K quando o seu polinômio minimal sobre K for separável sobre K. Por fim, diremos que $L : K$ é uma* ***extensão separável*** *quando todo elemento de L for separável sobre K.*

Exemplo 3.7. *O polinômio $p(x) = x^3 + x \in \mathbb{R}[x]$ é separável sobre $\mathbb{R}$, uma vez que*

$$p(x) = x(x^2 + 1),$$

e ambos os polinômios $q(x) = x^2 + 1$ e $r(x) = x$ são separáveis, pois possuem raízes distintas num corpo de decomposição.

O elemento $\sqrt{2} \in \mathbb{R}$ é algébrico e seu polinômio minimal $p = x^2 - 2$ é separável sobre $\mathbb{Q}$, pois possui duas raízes distintas $\sqrt{2}$ e $-\sqrt{2}$.

3.4 O teorema fundamental da teoria de Galois

Da forma como apresentada, a definição de grupo de Galois não teria tanto impacto se não existisse uma correspondência entre os subgrupos de $\Gamma(L : K)$ e os subcorpos $M \subseteq L$ tais que $K \subseteq M$. Chamaremos esses corpos de corpos intermediários.

Para cada corpo M, podemos associar o grupo $M^* = \Gamma(L : M)$ de todos os M-automorfismos de L. Note que se $M \subseteq N$, então $N^* \subseteq M^*$, uma vez que os N-automorfismos são também M-automorfismos.

Devemos também associar a cada subgrupo H de $\Gamma(L : K)$ o conjunto $H^\dagger$ de todos os elementos $x \in L$ tais que $f(x) = x$, para todo $f \in H$

Lema 3.4. *Se H é um subgrupo de $\Gamma(L:K)$, então $H^\dagger$ é um subcorpo de L que contém K.*

A demonstração deste lema pode ser encontrada em [14].

Definição 3.9. *Diremos que $H^\dagger$ é o* ***corpo fixo*** *de H.*

Temos que se $H \subseteq G \subseteq \Gamma(L:K)$, então $G^\dagger \subseteq H^\dagger$, pois se $x \in G^\dagger$, então $x \in L$ e, particularmente, $f(x) = x$ para qualquer $f \in H$ e, portanto, $x \in H^\dagger$.

Chamaremos o conjunto de corpos intermediários de $\mathcal{F}$ e o conjunto dos subgrupos de Galois de $\mathcal{G}$. Com estas nomenclaturas, temos as seguintes funções:

$$^* : \mathcal{F} \to \mathcal{G} \text{ e}$$

$$^\dagger : \mathcal{G} \to \mathcal{F}.$$

Dadas as definições, apresentaremos o Teorema Fundamental da Teoria de Galois.

Teorema 3.2 (Teorema Fundamental da Teoria de Galois)**.** *Seja $L:K$ uma extensão finita, normal e separável. Então*

1. $|\Gamma(L:K)| = [L:K]$.
2. *As funções * e † são mutuamente inversas e geram uma correspondência bijetiva entre $\mathcal{G}$ e $\mathcal{F}$.*
3. *Dado M um corpo intermediário, temos*

$$[L:M] = |M^*| \text{ e}$$

$$[M:K] = \frac{|\Gamma(L:K)|}{|M^*|}.$$

4. *Um corpo intermediário M é uma extensão normal de K se, e somente se, M^* é um subgrupo normal de G.*

5. *Se um corpo intermediário M é uma extensão normal de K, então $\Gamma(M : K)$ é isomorfo ao grupo quociente*

$$\frac{\Gamma(L : K)}{M^*}.$$

Capítulo 4

Construtibilidade de Polígonos Regulares

Neste capítulo, apresentamos a solução para a nossa principal questão:

- Quais polígonos regulares são construtíveis?

Já vimos exemplos de polígonos regulares construtíveis e inconstrutíveis no Capítulo 2. Agora mostraremos uma regra que caracterizará os números n naturais tais que o n-ágono regular é construtível.

4.1 Preliminares

Nesta seção mostraremos proposições que lidam diretamente com números construtíveis, com vistas a adquirirmos ferramentas para lidar com polígonos regulares que sejam construtíveis.

Enunciaremos um lema de álgebra que nos fornece um resultado sobre p-grupos cuja demonstração pode ser encontrada em [6] ou em [14] e nos será útil na demonstração da Proposição 4.1:

Lema 4.1. *Se G é um p-grupo finito de ordem p^n, com p primo, então G possui uma cadeia de subgrupos normais*

$$G_0 \subseteq G_1 \subseteq \cdots \subseteq G_n$$

tais que $|G_i| = p^i$*, para todo* $i = 0, \cdots, n$.

Proposição 4.1. *Seja* K *um subcorpo de* $\mathbb{R}$*. Se* α *e* β *pertencem a uma extensão normal* $K : \mathbb{Q}$ *tal que* $[K : \mathbb{Q}] = 2^r$*, para algum inteiro* r*, então* (α, β) *é um ponto construtível.*

Demonstração. Pela Proposição 3.3, a extensão $K : \mathbb{Q}$ é separável. Seja $G := \Gamma(K : \mathbb{Q})$. Pelo primeiro item do teorema fundamental da teoria de Galois, obtemos

$$|G| = [K : \mathbb{Q}] = 2^r$$

e, deste modo, G é um 2-grupo. Pelo lema 4.1, G possui uma série de subgrupos normais

$$G_0 \subseteq G_1 \subseteq \cdots \subseteq G,$$

tais que $|G_i| = 2^i$, para todo $i = 0, \cdots, n$.

Seja K_i o corpo fixo $G_{r-i}^{\dagger}$. Pela parte 3 do Teorema fundamental da teoria de Galois, temos que

$$\begin{aligned} 2^r &= [K : K_{j+1}][K_{j+1} : K_j][K_j : \mathbb{Q}] \\ &= |G_{r-j-1}|[K_{j+1} : K_j]\frac{2^r}{|G_{r-j}|}. \end{aligned}$$

Como $\dfrac{|G_{r-j-1}|}{|G_{r-j}|} = \dfrac{1}{2}$ então obtemos $[K_{j+1} : K_j] = 2$, para qualquer j. Do Teorema 1.5 resulta a construtibilidade de (α, β).

Q.E.D.

Proposição 4.2. *Seja* n *o número de lados de um polígono regular construtível. Se* $m \in \mathbb{N}$ *divide* n*, então o* m*-ágono regular é construtível.*

Demonstração. Uma vez que m divide n, existe $k \in \mathbb{N}$ tal que

$$n = km.$$

Devemos agora ligar o primeiro vértice do n-ágono ao m-ésimo, depois o m-ésimo ao $2m$-ésimo e assim por diante até ligarmos o $(k-1)m$-ésimo ao km-ésimo, que coincide com o primeiro. Desta forma, construímos o m-ágono regular.

Q.E.D.

Proposição 4.3. *Se m, n são números naturais primos entre si tais que o m-ágono e o n-ágono regulares são construtíveis, então o mn-ágono regular é construtível.*

Demonstração. Sabemos que se m e n são primos entre si, então existem $r, s \in \mathbb{Z}$ tais que

$$rm + sn = 1.$$

Se multiplicarmos ambos os membros da equação por $\dfrac{2\pi}{mn}$, obtemos

$$r\frac{2\pi}{n} + s\frac{2\pi}{m} = \frac{2\pi}{mn},$$

ou seja, uma maneira de se obter o ângulo $\dfrac{2\pi}{mn}$ como combinação linear (com coeficientes inteiros) dos dois ângulos dados $\dfrac{2\pi}{m}$ e $\dfrac{2\pi}{n}$, que são construtíveis.

Q.E.D.

Corolário 4.1. *Seja*

$$n = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$$

onde p_i são primos distintos para $i \in \{1, \cdots, r\}$. Então o n-ágono regular é construtível se, e somente se, cada $p_i^{\alpha_i}$-ágono regular for construtível

Demonstração. Da Proposição 4.2, se o n-ágono regular for construtível, então cada um dos $p_i^{\alpha_i}$-ágonos regulares será construtível.

Reciprocamente, para $i \neq j$ temos $p_i^{\alpha_i}$ e $p_j^{\alpha_j}$ dois a dois relativamente primos. Note que pela proposição 4.3, o $p_1^{\alpha_1} p_2^{\alpha_2}$-ágono é construtível.

Aplicando recursivamente a proposição 4.3 sobre $p_1^{\alpha_1} \cdots p_{s-1}^{\alpha_{s-1}}$ e o $p_s^{\alpha_s}$, que são relativamente primos para todo $s \in \{2, \cdots, r\}$, obtemos o $p_1^{\alpha_1} \cdots p_s^{\alpha_s}$-ágono construtível. Assim, o n-ágono é construtível

Q.E.D.

Lema 4.2. *O 2^n-ágono regular é construtível, para todo $n \in \mathbb{N}$ tal que $n \geq 2$.*

Demonstração. Para $n = 2$, temos o resultado válido, pois o quadrado é construtível.

Suponhamos que o resultado seja válido para algum $k \geq 2$. Uma vez que qualquer ângulo pode ser bissectado, então, bissectando o ângulo formado por dois vértices consecutivos do 2^k-ágono e a origem da circunferência que o circunscreve, obtemos o ângulo formado por dois vértices consecutivos do 2^{k+1}-ágono e a origem da circunferência que o circunscreve.

Deste modo, pelo princípio de indução, o resultado é válido para todo $n \geq 2, n \in \mathbb{N}$.

Q.E.D.

Proposição 4.4. *Sejam p um número primo e n um número natural tais que o p^n-ágono seja construtível e α uma raiz p^n-ésima da unidade nos complexos. Então o grau do polinômio minimal de $\alpha \in \mathbb{Q}[x]$ é uma potência de 2.*

Demonstração. Sejam $x = \cos\frac{2\pi}{p^n}$ e $y = \text{sen}\frac{2\pi}{p^n}$. Uma vez que o p^n-ágono é construtível, ambos x e y são contrutiveis, pois são o cosseno e seno do ângulo formado por dois vértices consecutivos do p^n-ágono e a origem do círculo que o circunscreve e, portanto, construtível (vide Seção 2.2). Pelo teorema 1.6, obtemos que $[\mathbb{Q}(x) : \mathbb{Q}]$ e $[\mathbb{Q}(y) : \mathbb{Q}]$ são potências de dois. Temos também que $\mathbb{Q}(x)(y) = \mathbb{Q}(x, y)$ e, assim, $[\mathbb{Q}(x, y) : \mathbb{Q}(x)][\mathbb{Q}(x) : \mathbb{Q}] = [\mathbb{Q}(x, y) : \mathbb{Q}]$ é uma potência de dois.

Seja $r \in \mathbb{N}$ tal que $[\mathbb{Q}(x, y) : \mathbb{Q}] = 2^r$, então

$$[\mathbb{Q}(x, y, i) : \mathbb{Q}] = [\mathbb{Q}(x, y)(i) : \mathbb{Q}(x, y)][\mathbb{Q}(x, y) : \mathbb{Q}] = 2 \cdot 2^r = 2^{r+1}.$$

Seja agora $\alpha = e^{\frac{2\pi i}{p^n}} = x + iy$. Note que $\alpha \in \mathbb{Q}(x, y, i) : \mathbb{Q}$ e, assim, $\mathbb{Q}(\alpha) : \mathbb{Q}$ é uma potência de dois. De fato, uma vez que $\mathbb{Q}(\alpha) : \mathbb{Q}$ é subextensão de $\mathbb{Q}(x, y, i) : \mathbb{Q}$.

Portanto, o grau do polinômio minimal de α em $\mathbb{Q}[x]$ é uma potência de 2.

Q.E.D.

O Lema 4.3 a seguir é importante para a demonstração da proposição 4.5 e o encontramos em [7].

Lema 4.3. *Sejam $p, k \in \mathbb{Z}$ números relativamente primos. Então $\binom{p}{k}$ é divisível por k*

Demonstração.

$$\begin{aligned}
\binom{p}{k} &= \frac{p(p-1)\cdots(p-k+1)}{k(k-1)\cdots 1} \\
&= \frac{p}{k}\frac{(p-1)(p-2)\cdots(p-k+1)}{(k-1)(k-2)\cdots 1} \\
&= \frac{p}{k}\binom{p-1}{k-1} \\
&\therefore \\
k\binom{p}{k} &= p\binom{p-1}{k-1}.
\end{aligned}$$

Note que $k\binom{p}{k}$ é divisível por p. Uma vez que p e k são primos entre si, então $\binom{p}{k}$ é divisível por p.

Q.E.D.

Proposição 4.5. *Sejam p um número primo e α uma p-ésima raiz primitiva da unidade em $\mathbb{C}$. O polinômio minimal de $\alpha \in \mathbb{Q}[x]$ é*

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

Demonstração. Temos

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

e, portanto, $f(\alpha) = 0$.

Mostraremos agora que f é irredutível em $\mathbb{Q}[x]$. Seja $x = 1 + t$. Temos $f(x)$ irredutível em $\mathbb{Q}[x]$ se, e somente se, $f(1 + t)$ for irredutível em $\mathbb{Q}[t]$.

Observe que

$$\begin{aligned} f(1+t) &= \frac{(1+t)^p - 1}{t} = \frac{\sum_{k=0}^{p} \binom{p}{k} t^{p-k} - 1}{t} \\ &= \sum_{k=0}^{p} \frac{p!}{k!(p-k)!} t^{p-k-1} - \frac{1}{t} \\ &= t^{p-1} + pt^{p-2} + \frac{p(p-1)}{2!} t^{p-3} + \cdots + \frac{p(p-1)}{2!} t + p + \frac{1}{t} - \frac{1}{t} \\ &= t^{p-1} + p\left(t^{p-2} + \frac{(p-1)}{2!} t^{p-3} + \cdots + \frac{(p-1)}{2!} t + 1\right). \end{aligned}$$

De acordo com o Lema 4.3, todos os coeficientes $\binom{p}{k} = \frac{p!}{k!(p-k)!}$, com $1 \leq k \leq p-1$ são inteiros divisíveis por p, implicando que $g(t) = t^{p-2} + \frac{(p-1)}{2!} t^{p-3} + \cdots + \frac{(p-1)}{2!} t + 1$ pertence a $\mathbb{Z}[t]$. Ou seja,

$$f(1+t) = \frac{(1+t)^p - 1}{t} = t^{p-1} + p \cdot g(t),$$

onde g é um polinômio de $\mathbb{Z}[t]$.

Pelo Critério de Irredutibilidade de Eisenstein, (1.3), $f(1+t)$ é irredutível em $\mathbb{Q}[t]$ e, assim, $f(x)$ é também irredutível em $\mathbb{Q}[x]$.

Portanto, não existe um polinômio de grau menor do que f em $\mathbb{Q}[x]$ que anule α e, portanto, f é o seu polinômio minimal.

Q.E.D.

Proposição 4.6. *Sejam p um número primo e α uma p^2-ésima raiz primitiva da unidade em $\mathbb{C}$. Então o polinômio minimal de α em $\mathbb{Q}[x]$ é*

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

Demonstração. Temos

$$g(x) = \frac{x^{p^2} - 1}{x^p - 1}.$$

Pelo fato de α ser uma raiz primitiva, temos que $\alpha^p - 1 \neq 0$ e, assim, $g(\alpha) = 0$. Mostraremos agora que $g(x) \in \mathbb{Q}[x]$ é irredutível. Semelhantemente ao que fizemos na demonstração da proposição 4.5, façamos $x = 1 + t$ (lembrando que a irredutibilidade de $g(x)$ é equivalente à de $g(1 + t)$), obtendo

$$g(1 + t) = \frac{(1 + t)^{p^2} - 1}{(1 + t)^p - 1}.$$

Podemos utilizar um corolário ao pequeno teorema de Fermat [10] que afirma que, dado p primo,

$$(1 + t)^p \equiv 1 + t^p (\text{mod } p).$$

Deste modo, temos

$$(1 + t)^{p \cdot p} \equiv (1 + t^p)^p \equiv (1 + t^{p^2}) (\text{mod } p).$$

Observe que, em $\mathbb{Z}_p[t]$, vale

$$g(1 + t) = \frac{(1 + t^{p^2}) - 1}{(1 + t^p) - 1} = t^{p(p-1)} \in \mathbb{Z}_p[t].$$

Já em $\mathbb{Z}$, teremos

$$g(1 + t) = t^{p(p-1)} + p(k(t)),$$

onde $k \in \mathbb{Z}[t]$.

Pela expressão alternativa

$$g(1 + t) = (1 + t)^{p(p-1)} + (1 + t)^{p(p-2)} + \cdots + (1 + t)^p + 1,$$

cada expressão $(1 + t)^{py}$ possui termo independente 1. Deste modo, teremos

o termo independente de $g(1+t)$ é igual a p. Pelo critério de irredutibilidade de Eisenstein, $g(1+t)$ é irredutível em $\mathbb{Q}[t]$.

Deste modo, f é o polinômio minimal de α em $\mathbb{Q}[x]$.

Q.E.D.

4.2 Teorema Principal

Chegamos ao ápice do nosso trabalho, onde consideraremos o Teorema que foi proposto por Gauss e cuja recíproca é uma das mais interessantes aplicações da Teoria de Galois.

Este resultado foi reconhecidamente tão importante para Gauss, que a companhia de correios alemã lançou, em homenagem a ele, um selo promocional com seu busto e um heptadecágono, com uma régua e um compasso (Figura 4.1).

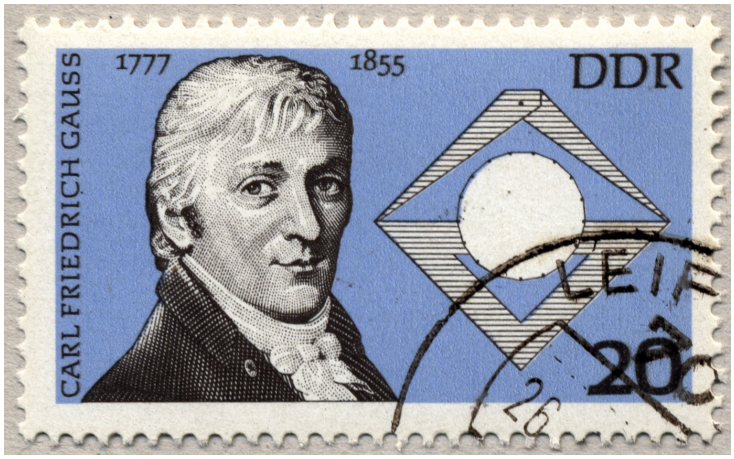


Figura 4.1: Selo Promocional em Homenagem a Gauss

Antes de partirmos para o teorema principal em si, porém, é necessário falarmos sobre a forma dos números que aparecem na caracterização dos polígonos construtíveis,

$$p_i = 2^{2^{r_i}} + 1,$$

com $r_i \in \mathbb{N} \cup \{0\}$.

Estes números são atualmente conhecidos como números de Fermat, mas um dia foram conhecidos como *primos* de Fermat. Este matemático francês brilhante do século XVII contribuiu extensivamente para a teoria dos números e conjecturou que os números dessa forma eram todos primos. O seu pensamento era razoável, pois os números

$$\begin{aligned} p_0 &= 3 \\ p_1 &= 5 \\ p_2 &= 17 \\ p_3 &= 257 \\ p_4 &= 65.537 \end{aligned}$$

são primos. Porém, Euler, outro brilhante matemático, mostrou que $p_5 = 4.294.967.297$ não é primo, derrubando a conjectura de Fermat.

Kraïtchik nos fornece o seguinte argumento da não primalidade de p_5 (encontramos este argumento em [11]):

Observemos que

$$641 = 2^4 + 5^4 = 5 \cdot 2^7 + 1 \Rightarrow 2^4 = 641 - 5^4.$$

Por outro lado,

$$2^{2^5} = 2^{32} = 2^4 \cdot 2^{28} = (641 - 5^4) \cdot 2^{28}.$$

Por fim,

$$(641 - 5^4) \cdot 2^{28} \equiv -5^4 \cdot 2^{28} = -(5 \cdot 2^7)^4 = -(641 - 1)^4 \equiv -1 (\text{mod } 641).$$

Assim, $2^{2^5} - 1 \equiv 0 (\text{mod } 641)$, ou seja, 641 divide 4.294.967.297.

Além dos cinco primeiros, não se conhecem, até esta data, outros números de Fermat que sejam primos. Conhecida a forma dos números que trabalhamos, passaremos ao teorema e objetivo principal deste trabalho.

Teorema *(Caracterização dos Polígonos Regulares Construtíveis). Seja n um número natural. Uma condição necessária e suficiente para que o n-ágono regular seja construtível por régua e compasso é que n seja da forma*

$$n = 2^r p_1 \cdots p_s,$$

onde $r, s \in \mathbb{N} \cup \{0\}$ e $p_1, \cdots, p_s$ são primos distintos da forma

$$p_i = 2^{2^{r_i}} + 1,$$

com $r_i \in \mathbb{N} \cup \{0\}$.

Demonstração. Suponhamos inicialmente que o n-ágono seja construtível. Pelo Teorema Fundamental da Aritmética, temos

$$n = 2^r p_1^{\alpha_1} \cdots p_s^{\alpha_s},$$

com $p_1, \cdots, p_s$ primos ímpares distintos. Do Corolário 4.1 segue que cada $p_i^{\alpha_i}$-ágono regular é construtível.

Provemos primeiramente que $\alpha_i = 1$, para todos $i \in \{1, 2, \cdots, s\}$. Suponhamos, por contradição, que, para algum i, tenhamos $\alpha_i \geq 2$. Da Proposição 4.2 resulta que o p_i^2-ágono regular é construtível.

Por outro lado, da Proposição 4.4 segue que o grau do polinômio minimal em $\mathbb{Q}[x]$ de uma p_i^2-ésima raiz primitiva da unidade em $\mathbb{C}$ é uma potência de 2. Da Proposição 4.6 obteríamos que $p_i(p_i - 1)$ seria uma potência de 2, uma contradição com o fato de p_i ser ímpar. Assim, $\alpha_i = 1, \forall i$, significando que

$$n = 2^r p_1 \cdots p_s.$$

Utilizando as Proposições 4.4 e 4.5, podemos observar que o maior expoente do polinômio $f(x) = x^{p_i-1} + \cdots + x + 1$, que é $p_i - 1$, é uma potência de 2. Seja, então, $s_i \in \mathbb{N}$ tal que

$$p_i - 1 = 2^{s_i}.$$

Queremos mostrar que s_i não possui fatores ímpares na sua decomposição em números primos. Suponha que s_i possua um divisor primo $a > 2$, e seja $b \in \mathbb{N}$ tal que $s_i = ab$. Então,

$$p_i - 1 = 2^{s_i} \Rightarrow p_i = 2^{s_i} + 1 \Rightarrow p_i = (2^b)^a + 1.$$

Agora note que

$$(2^b)^a + 1 = (2^b + 1)((2^b)^{a-1} - (2^b)^{a-2} + \cdots + 1),$$

Neste caso, p_i seria divisível por $(2^b + 1)$, uma contradição com o fato de p_i ser primo, resultando que $s_i = 2^{r_i}$, para algum r_i natural. Assim,

$$p_i = 2^{2^{r_i}} + 1.$$

Reciprocamente, supomos que

$$n = 2^r p_1 \cdots p_s,$$

onde $r, s \in \mathbb{N} \cup \{0\}$ e $p_1, \cdots, p_s$ são primos distintos da forma

$$p_i = 2^{2^{r_i}} + 1,$$

com $r_i \in \mathbb{N} \cup \{0\}$. E devemos mostrar que o n-ágono regular é construtível.

Pelo Lema 4.2, o 2^r-ágono regular é construtível. Pela Proposição 4.3 é suficiente mostrarmos a construtibilidade dos p_i-ágonos regulares para garantirmos a construtibilidade do n-ágono regular.

Seja α uma p_i-ésima raiz primitiva da unidade em $\mathbb{C}$. Pela Proposição 4.5, obtemos que

$$[\mathbb{Q}(\alpha) : \mathbb{Q}] = \partial m_{\alpha,\mathbb{Q}} = p_i - 1 = 2^a,$$

onde $m_{\alpha,\mathbb{Q}}$ é o polinômio minimal de α em $\mathbb{Q}[x]$ e $a \in \mathbb{N}$.

Pela Proposição 4.4, $\mathbb{Q}(\alpha)$ é o corpo de fatoração para $f(x) = x^{p-1} + \cdots + 1 \in \mathbb{Q}[x]$. Pela Proposição 3.2, $\mathbb{Q}(\alpha) : \mathbb{Q}$ é uma extensão normal e, pela proposição 3.3 e como a característica de $\mathbb{Q}$ é zero, é também separável.

Uma vez que $\mathbb{Q}(\alpha)$ é um corpo de decomposição para $x^{p_i} - 1$. Como a característica de $\mathbb{Q}$ é zero, então, da Proposição 3.1, $\Gamma(\mathbb{Q}(\alpha) : \mathbb{Q})$ é abeliano.

Seja $K = \mathbb{R} \cap \mathbb{Q}(\alpha)$. Notemos que

$$\alpha^{-1} = \frac{\cos\frac{2\pi}{p_i} - i\,\mathrm{sen}\frac{2\pi}{p_i}}{\cos^2\frac{2\pi}{p_i} + \mathrm{sen}^2\frac{2\pi}{p_i}} = \cos\frac{2\pi}{p_i} - i\,\mathrm{sen}\frac{2\pi}{p_i} = \overline{\alpha}$$

$$\left(\frac{\alpha + \alpha^{-1}}{2}\right) = \left(\frac{(\cos\frac{2\pi}{p_i} + i\,\mathrm{sen}\frac{2\pi}{p_i}) + (\cos\frac{2\pi}{p_i} - i\,\mathrm{sen}\frac{2\pi}{p_i})}{2}\right) = \cos\frac{2\pi}{p_i} \in K.$$

Uma vez que $\mathbb{Q}(\alpha) \subset \mathbb{C}$, $K \subset \mathbb{R}$, $[\mathbb{C} : \mathbb{R}] = 2$ e $\mathbb{Q}(\alpha) \neq \mathbb{Q}(\alpha) \cap \mathbb{R}$, pois $\alpha \in \mathbb{Q}(\alpha) \setminus (\mathbb{Q}(\alpha) \cap \mathbb{R})$, segue que

$$[\mathbb{Q}(\alpha) : K] = 2.$$

Pelo Teorema Fundamental da Teoria de Galois, (5), obtemos que

$$2 = [\mathbb{Q}(\alpha) : K] = |\Gamma(\mathbb{Q}(\alpha) : K)|,$$

e, como $\Gamma(\mathbb{Q}(\alpha) : \mathbb{Q})$ é abeliano (pela Proposição 3.1), então, $\Gamma(\mathbb{Q}(\alpha) : K)$ é um subgrupo normal de $\Gamma(\mathbb{Q}(\alpha) : \mathbb{Q})$.

Deste modo, como $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 2^a$ e $[\mathbb{Q}(\alpha) : K] = 2$, então $[K : \mathbb{Q}]$ é uma potência de 2 e a extensão é normal.

Portanto, pela Proposição 4.1, obtemos que o ponto $(0, \cos\frac{2\pi}{p_i})$ é construtível e, portanto, o p_i-ágono regular é construtível por régua e compasso, o

que conclui a nossa demonstração.

Q.E.D.

Referências Bibliográficas

[1] BOYER, C. B. *História da Matemática:* Tradução: Elza F. Gomide. São Paulo: Edgard Blücher, 1974.

[2] CHURCHILL, R. V. *Variáveis Complexas e Suas Aplicações:* Tradução: Tadao Yoshioka. São Paulo: McGraw-Hill do Brasil e Editora da Universidade de São Paulo, 1975.

[3] CRUZ, K. B, SHÜTZER, W. *Introdução à Teoria de Galois:* Trabalho de Conclusão de curso. São Carlos: Universidade Federal de São Carlos. 2014. Disponível em http://www.dm.ufscar.br/dm/attachments/article/6/TCCB-Karina_Cruz.pdf Acesso em 22 de Março de 2016

[4] EARLE, J. *Da Vinci Vitruvian Man of Math.* Disponível em http://ed.ted.com/lessons/da-vinci-s-vitruvian-man-of-math-james-earle acesso em 01/05/2016.

[5] EVES, H. *Introdução à História da Matemática:* Tradução: Hygino H. Domingues. Campinas: Editora da Unicamp. 2004.

[6] FRALEIGH, J. B. *A First Course in Abstract Algebra:* 6ª edição. New York: Addison-Wesley, 2000.

[7] FUCHS, D. B, FUCHS, M. B. *The Arithmetic of Binomial Coefficients:* Translation: Ilya Bernstein. Disponível em http://math.ucsd.edu/~lni/math140/Suppl0.pdf. Acesso em 22 de Março de 2016

[8] GAUSS, C. F. *Disquisitiones Arithmeticae:* Yale: University Press, 1966.

[9] GIONGO, A. R. *Curso de Desenho Geométrico:* 24ªedição. São Paulo: Livraria Nobel S.A. 1973.

[10] HEFEZ, A. *Elementos de Aritmética:* 2ª Edição. Rio de Janeiro: SBM, 2011.

[11] PANTOJA, P. H. O. *Números de Fermat:* Revista OIM, número 41. Universidade de Lisboa, Portugal. Disponível em http://www.oei.es/oim/revistaoim/numero41/NUMEROS_DE_FERMAT.pdf/ Acesso em 25/04/2016.

[12] MONTEIRO, L. H. J. *Teoria de Galois:* Poços de Caldas: 7ºColóquio Brasileiro de Matemática, junlho de 1969.

[13] RAMALHO, R. *Tópicos de Ensino de Ciências:* Construções Geométricas com Régua e Compasso. Nº. 1. CECINE. Recife: Universidade Federal de Pernambuco, 1984

[14] STEWART, I. *Galois Theory:* 2ªedição. London: Chapman and Hall, 1973.

[15] WAGNER, E. *Uma Introdução às Construções Geométricas:* Apostila.

[16] WEISSTEIN, E. W. *Heptadecagon:* MathWorld. Disponível em http://mathworld.wolfram.com/Heptadecagon.html acesso em 30/04/2016.