UNIVERSIDADE ESTADUAL DO CEARÁ
CENTRO DE CIÊNCIAS E TECNOLOGIAS
MESTRADO PROFISSIONAL EM MATEMÁTICA EM REDE NACIONAL

IAGO DOUGLAS BARROS ARAUJO

O CORPO DOS NÚMEROS CONSTRUTÍVEIS COM RÉGUA E COMPASSO: OS PROBLEMAS CLÁSSICOS DA DUPLICAÇÃO DO CUBO, DA QUADRATURA DO CÍRCULO E DA TRISSECÇÃO DO ÂNGULO.

FORTALEZA – CEARÁ
2024

IAGO DOUGLAS BARROS ARAUJO

O CORPO DOS NÚMEROS CONSTRUTÍVEIS COM RÉGUA E COMPASSO: OS PROBLEMAS CLÁSSICOS DA DUPLICAÇÃO DO CUBO, DA QUADRATURA DO CÍRCULO E DA TRISSECÇÃO DO ÂNGULO.

Dissertação apresentada ao Curso de Mestrado Profissional em Matemática em Rede Nacional do Programa de Pós-Graduação em Matemática do Centro de Ciências e Tecnologias da Universidade Estadual do Ceará, como requisito parcial à obtenção do título de mestre em Matemática em Rede Nacional. Área de Concentração: Ensino de Matemática.

Orientador: Prof. Dr. Tiago Caúla Ribeiro.

FORTALEZA – CEARÁ

2024

Dados Internacionais de Catalogação na Publicação
Universidade Estadual do Ceará
Sistema de Bibliotecas
Gerada automaticamente pelo SidUECE, mediante os dados fornecidos pelo(a)

Araujo, Iago Douglas Barros.
O corpo dos números construtíveis com régua e compasso: os problemas clássicos da duplicação do cubo, da quadratura do círculo e da trissecção do ângulo. [recurso eletrônico] / Iago Douglas Barros Araujo. - 2024.
70 f. : il.

Dissertação (mestrado profissional) - Universidade Estadual do Ceará, Centro de Ciências e Tecnologia, Curso de Mestrado Profissional Em Matemática Rede Nacional, Fortaleza, 2024.
Orientação: Prof. Dr. Tiago Caula Ribeiro.
1. construções geométricas. 2. régua. 3. compasso. 4. duplicação do cubo. 5. quadratura do círculo. 6. trissecção do ângulo. 7. construtível. . I. Título.

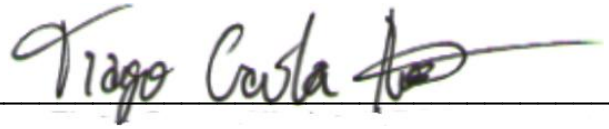
IAGO DOUGLAS BARROS ARAUJO

O CORPO DOS NÚMEROS CONSTRUTÍVEIS COM RÉGUA E COMPASSO: OS PROBLEMAS CLÁSSICOS DA DUPLICAÇÃO DO CUBO, DA QUADRATURA DO CÍRCULO E DA TRISSECÇÃO DO ÂNGULO.

Dissertação apresentada ao Curso de Mestrado Profissional em Matemática em Rede Nacional do Programa de Pós-Graduação em Matemática do Centro de Ciências e Tecnologia da Universidade Estadual do Ceará, como requisito parcial à obtenção do título de mestre em Matemática em Rede Nacional. Área de Concentração: Ensino de Matemática.

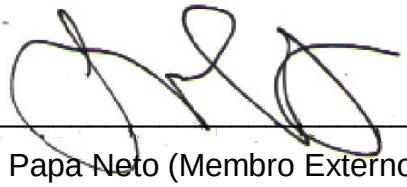
Aprovada em: 10 de dezembro de 2024.

BANCA EXAMINADORA



Prof. Dr. Tiago Caúla Ribeiro (Orientador)

Universidade Estadual do Ceará – UECE



Prof. Dr. Ângelo Papa Neto (Membro Externo ao Programa)

Instituto Federal de Educação, Ciência e Tecnologia do Ceará – IFCE

Prof. Dr. Claudemir Silvino Leandro (Membro Interno ao Programa)

Universidade Estadual do Ceará – UECE

Dedicado aos que tornaram essa jornada possível.

AGRADECIMENTOS

A conclusão desse trabalho só foi possível graças ao apoio e a colaboração da minha família e dos meus grandes amigos. Desde o dia em que aceitei o desafio de cursar o Mestrado e, paralelamente, ter que me dedicar integralmente ao trabalho e à minha família, tive que conviver com a autocobrança e com o receio de não lograr êxito nessa jornada. Por isso, agradeço imensamente aqueles que tornaram possível o alcance dos objetivos por mim estabelecidos.

Agradeço à minha esposa maravilhosa Deyse Correia, meu pai Clealdo, minha mãe Violanda e minha irmã Carol pelo grande apoio durante meus repentinos momentos de apreensão e dúvidas, pelos cuidados e pelas palavras de incentivo.

Ao meu filho amado João Arthur que, muitas vezes, por ter que continuar estudando, não consegui dar a atenção que ele merecia, e com o semblante de tristeza ele simplesmente afirmava: “papai, quero que você seja mestre logo para poder ter tempo de brincar comigo”.

Aos professores da EEM Doutora Aldaci Barbosa que muito me incentivaram ao longo desses dois anos, em especial os grandes amigos Júnior, Kevyn, Raquel, Nágila, Jecson e Ravena que me ajudaram tanto emocionalmente quanto com a elaboração dessa dissertação.

Aos amigos que o PROFMAT me deu a honra de conhecer, em especial ao grande amigo Robério que por vezes me “segurou” para que eu não desistisse do curso, ao Hyderland e ao Felipe por tornarem as aulas bem mais leves, ao amigo de longas datas Kefferson Cartaxo que me ajuda muito desde os tempos de graduação, e aos amigos Valdir, Hélder, Leandro e Leônidas por dividirem esses dois anos comigo.

Aos melhores professores que a matemática me apresentou: Prof. Dr. Ângelo Papa Neto, Prof. Dr. Claudemir Leandro e ao excepcional orientador Prof. Dr. Tiago Caúla Ribeiro que desde o início das orientações me deixou livre para produzir, mas sempre trazia, em seguida, importantes contribuições e dicas valiosíssimas.

“Se você vier me perguntar por onde andei
No tempo em que você sonhava
De olhos abertos, lhe direi
Amigo, eu me desesperava

Sei que assim falando pensas
Que esse desespero é moda em 76
Mas ando mesmo descontente
Desesperadamente, eu grito em português

Tenho vinte e cinco anos
De sonho e de sangue
E de América do Sul
Por força deste destino
Um tango argentino
Me vai bem melhor que um blues”

(A Palo Seco - Belchior)

RESUMO

Nesta pesquisa, abordaremos três problemas da Antiguidade que discorriam sobre construções geométricas utilizando apenas os instrumentos ditos euclidianos, a saber: uma régua sem graduações e um compasso, e que deveriam seguir algumas restrições quanto ao que poderia ser executado com estes instrumentos. Tais problemas, denominados de duplicação do cubo, quadratura do círculo e trissecção do ângulo, ganharam destaque devido ao grande esforço realizado para solucioná-los e a descoberta tardia (mais de 2000 anos depois de seus surgimentos), a partir do aprimoramento da álgebra, de que na verdade eles eram impossíveis de serem solucionados sob as condições de construção impostas. Assim, este trabalho objetiva mostrar, algebricamente, a partir de conceitos relacionados à teoria de corpos, aos polinômios e à álgebra linear, os motivos da impossibilidade da execução dessas três construções. Além disso, definiremos o conceito de número construtível, apresentaremos as regras para construção de números e mostraremos que o conjunto formado por todos os números construtíveis têm estrutura algébrica de corpo. Para alcançarmos estes objetivos, foi realizada uma revisão de literatura que aborda a temática sob diferentes perspectivas, a fim de que fosse possível encontrar uma forma fluida e concisa de apresentar as ideias. Apesar de o trabalho dedicar-se, em boa parte, ao desenvolvimento da álgebra necessária para atingirmos nosso objetivo geral, ao longo do texto destacaremos tópicos relacionados às construções, bem como executaremos, nos apêndices, algumas construções simples. Assim, esperamos que esta pesquisa sirva de fomento aos(as) professores(as) de matemática da Educação Básica a fim de que optem por ministrar suas aulas de geometria plana a partir do suporte das construções geométricas com régua e compasso, podendo assim estimular os estudantes a aprimorar seus conhecimentos geométricos, bem como trabalhar habilidades matemáticas basilares que porventura ainda não tenham sido consolidadas.

Palavras-chave: construções geométricas; régua; compasso; duplicação do cubo; quadratura do círculo; trissecção do ângulo; construtível.

ABSTRACT

In this research, we will examine three problems from antiquity in which geometric constructions were discussed using only the so-called Euclidean instruments: an ungraduated ruler and a compass, and which had to respect certain restrictions on what could be done with these instruments. These problems known as doubling the cube, squaring the circle, and trisecting an angle became famous due to the extensive efforts to solve them. It was only with the advancement of algebra, more than 2,000 years later, that it was discovered they were actually impossible to solve using the allowed construction methods. Therefore, the aim of this paper is to show algebraically, using concepts from field theory, polynomial theory, and linear algebra, why these constructions are impossible to carry out. In addition, we will define the concept of constructible number, present the rules for constructing numbers, and show that the set formed by all constructible numbers has the algebraic structure of a field. To achieve these objectives, we conducted a comprehensive literature review from various perspectives, which facilitated a clear and concise presentation of the ideas. Although much of the work is devoted to developing the algebra needed to achieve our general objective, throughout the text we will highlight topics related to constructions, as well as performing simple constructions. We hope this research will encourage teachers of basic mathematics to incorporate geometric constructions using rulers and compasses into their plane geometry classes, thereby enhancing students' geometric understanding and foundational mathematical skills that may not yet have been consolidated.

Keywords: geometric constructions; ruler; compass; doubling the cube; squaring the circle; trisecting the angle; constructible.

LISTA DE FIGURAS

SUMÁRIO

1 INTRODUÇÃO

A duplicação do cubo, a quadratura do círculo e a trissecção do ângulo eram problemas clássicos da Grécia Antiga que tratavam de construções geométricas, usando como instrumentos básicos apenas uma régua não graduada e um compasso, seguindo algumas regras de construção previamente estabelecidas. Mais detalhadamente, tais problemas referiam-se, respectivamente, a: construir a aresta de um cubo que tem o dobro do volume de um cubo dado, construir um quadrado com área igual à de um círculo dado, e dividir um ângulo arbitrário dado em três partes iguais. Embora existisse a limitação quanto aos instrumentos utilizados, os gregos acreditavam que seria possível resolver esses três problemas, visto a grande quantidade de construções geométricas que, nas mesmas condições, eles conseguiam executar.

Eves (2011, p. 134) entende que a relevância desses problemas "[…] reside no fato de que eles não podem ser resolvidos, a não ser aproximadamente, com régua e compasso, embora esses instrumentos sirvam para a resolução de muitos outros problemas de construção. A busca ingente de soluções para esses problemas influenciou profundamente a geometria grega e levou a muitas descobertas frutíferas, como as secções cônicas, muitas curvas cúbicas e quárticas e várias curvas transcendentes. Um produto muito posterior foi o desenvolvimento de partes da teoria das equações ligadas a domínios de racionalidade, números algébricos e teoria dos grupos. Somente no século XIX, mais de 2000 anos depois de os problemas terem sido concebidos, se estabeleceu a impossibilidade das três construções, sob a limitação autoimposta de se usarem apenas régua e compasso. O grande estímulo ao desenvolvimento da matemática, inclusive para a criação de novas teorias, dado pelos esforços continuados para se resolverem os três famosos problemas da Antiguidade, ilustra o valor heurístico de problemas matemáticos atraentes não resolvidos".

Embora sejam problemas puramente geométricos, foi graças à álgebra que se provou que os esforços em busca de suas soluções eram em vão. Desta forma, o objetivo geral deste trabalho é desenvolver uma álgebra de polinômios que nos permita mostrar a impossibilidade de executar essas três construções. De forma específica, objetivamos: definir o conceito de número construtível, apresentar as regras para construir números, provar que o conjunto formado por todos os números construtíveis têm estrutura algébrica de corpo, e mostrar um importante teorema que

estabeleça uma condição necessária para que um número seja construtível. Com esse teorema, conseguimos provar que, a partir das condições de construção impostas, é impossível duplicar o cubo, quadratar o círculo e trissectar o ângulo.

Este trabalho está dividido da seguinte maneira. Nos capítulos 2 e 3, faremos uma abordagem de alguns conceitos de estruturas algébricas, álgebra linear e da teoria de polinômios, visando ambientar o(a) leitor(a) aos resultados que estão mais alinhados ao nosso objetivo geral. No capítulo 4, desenvolveremos a teoria relacionada às extensões de corpos, aos números algébricos e transcendentes e aos conceitos de adjunção, o que é fundamental para a demonstração do teorema central do trabalho. No capítulo 5, abordaremos todos os tópicos atrelados aos números construtíveis e, aliado ao que foi feito no capítulo 4, mostraremos a impossibilidade da resolução dos três problemas gregos. O capítulo 6 traz a conclusão do trabalho, no qual sugerimos a utilização da temática das construções geométricas como um componente da parte diversificada dos currículos da Educação Básica no Brasil, bem como destacamos a possibilidade de trabalhos futuros. Por fim, apresentaremos, nos apêndices, algumas construções simples, bem como abordaremos brevemente o problema da construtibilidade de polígonos regulares.

Para atingirmos os objetivos estabelecidos, realizamos uma revisão de literatura, onde procuramos sintetizar as ideias necessárias para o desenvolvimento desta pesquisa. A fim de apresentarmos as noções referentes à álgebra linear, nos referenciamos em Boldrini *et al*. (1980) e Hefez; Fernandez (2012). Para abordarmos os conceitos básicos sobre as estruturas algébricas e sobre os polinômios, recorremos a Gonçalves (2017). Para desenvolvermos a parte do trabalho que diz respeito às extensões algébricas e às construções com régua e compasso, incluindo a impossibilidade dos problemas clássicos, nos referenciamos em Gonçalves (2017) e Hefez; Villela (2012). Em alguns casos, fizemos adaptações e complementações às demonstrações fornecidas pelos(as) autores(as) com o intuito de tornar o trabalho o mais completo possível.

As construções geométricas com régua e compasso podem ser utilizadas como uma ferramenta auxiliar no ensino de geometria na Educação Básica. Segundo Wagner (2007, n.p.), os problemas de construção geram motivações, além de serem "[…] intrigantes e frequentemente conduzem à descoberta de novas propriedades. São educativos no sentido que em cada um é necessária uma análise da situação onde se faz o planejamento da construção, seguindo-se a execução dessa

construção, a posterior conclusão sobre o número de soluções distintas e também a compatibilidade dos dados".

Assim, espera-se que o desenvolvimento desta dissertação venha a contribuir com a formação de discentes dos Anos Finais do Ensino Fundamental e do Ensino Médio através da abordagem das construções geométricas com régua e compasso nas aulas de matemática. Acreditamos que este trabalho possa, em linhas gerais, instigar os(as) professores(as) de matemática da Educação Básica a perceberem as construções geométricas como um importante instrumento para colaborar no aprendizado da geometria, tendo em vista o grau de importância que é dado a essa temática ao longo do texto, e a relevância com que a mesma é apresentada durante os capítulos e apêndices desta dissertação.

2 TÓPICOS DE ÁLGEBRA LINEAR

O presente capítulo possui caráter introdutório, no qual serão expostos alguns conceitos acerca dos espaços vetoriais, bem como outras noções relacionadas ao estudo da álgebra linear. Trataremos aqui apenas de alguns tópicos que serão importantes para o desenvolvimento da ideia central do trabalho: as extensões de corpos. A princípio, faremos uma abordagem sobre a estrutura algébrica de corpo, necessária para a definição de espaços vetoriais, e que também terá uma grande importância para o desenvolvimento dos próximos capítulos.

2.1 Corpos

Começaremos esta seção com a definição da estrutura algébrica de anel, para que assim possamos introduzir a ideia de corpo.

Definição 2.1: Seja A um conjunto não vazio sobre o qual definimos duas operações binárias, respectivamente, adição e multiplicação:

$$+ : A \times A \longrightarrow A$$

$$\cdot : A \times A \longrightarrow A$$

A é dito ser um **anel**, e o denotamos por $(A, +, \cdot)$, se as seguintes seis condições forem satisfeitas:

i) A adição é associativa, isto é $a + (b + c) = (a + b) + c$, $\forall\, a, b$ e $c \in A$.

ii) Existe $0 \in A$ tal que $a + 0 = 0 + a = a$, $\forall\, a \in A$. Chamamos 0 de elemento neutro para adição, ou ainda de zero do anel.

iii) Para cada $a \in A$ existe um único $-a \in A$, denominado inverso aditivo de a, tal que $a + (-a) = (-a) + a = 0$.

iv) A adição é comutativa, isto é $a + b = b + a$, $\forall\, a, b \in A$.

v) A multiplicação é associativa, ou seja $a \cdot (b \cdot c) = (a \cdot b) \cdot c$, $\forall\, a, b, c \in A$.

vi) Vale a distributividade da multiplicação em relação à adição, ou seja, quaisquer que sejam $a, b, c \in A$, tem-se:

Distributividade à esquerda: $a \cdot (b + c) = a \cdot b + a \cdot c$

Distributividade à direita: $(b + c) \cdot a = b \cdot a + c \cdot a$

Agora, sendo $(A,\ +,\ \cdot)$ um anel, consideremos as seguintes propriedades:

vii) Existe $1 \in A$, $1 \neq 0$, tal que $a \cdot 1 = 1 \cdot a = a$, $\forall\ a \in A$.
viii) $a \cdot b = b \cdot a$, $\forall\ a, b \in A$.
ix) Para $a, b \in A$, temos que $a \cdot b = 0 \Longrightarrow a = 0$ ou $b = 0$.
x) $\forall\ a \in A$, $a \neq 0$, $\exists\ a^{-1} \in A$ tal que $a \cdot\ a^{-1} = a^{-1} \cdot a = 1$.

Se a propriedade vii) for satisfeita dizemos que A é um **anel com unidade** (denotada por 1_A, ou simplesmente 1). Se a propriedade viii) for satisfeita dizemos que A é um **anel comutativo**. Caso a propriedade ix) seja satisfeita dizemos que A é um **anel sem divisores de zero**. Se $(A,\ +,\ \cdot)$ é um anel comutativo, com unidade e sem divisores de zero, dizemos que A é um **domínio de integridade**. Por fim, se $(A,\ +,\ \cdot)$ é um anel comutativo, com unidade e que satisfaz a propriedade x) dizemos que A é um **corpo**.

Assim, para que um conjunto não vazio A, sobre o qual define-se uma adição e uma multiplicação, seja um corpo é necessário que, além das propriedades de i) a vi) acima listadas sejam satisfeitas, a multiplicação possua elemento neutro (diferente do zero do anel) e seja comutativa, bem como todo elemento (exceto o zero do anel) possua inverso multiplicativo. Quando nos referirmos ao zero do corpo estamos tratando do elemento neutro da adição. Da mesma forma, a unidade do corpo refere-se ao elemento neutro da multiplicação.

Note que $(\mathbb{Z},\ +,\ \cdot)$, $(\mathbb{Q},\ +,\ \cdot)$, $(\mathbb{R},\ +,\ \cdot)$ e $(\mathbb{C},\ +,\ \cdot)$ são anéis com as operações usuais. Esses anéis são chamados, respectivamente, de anel dos números inteiros, anel dos números racionais, anel dos números reais e anel dos números complexos. Além de anéis, $\mathbb{Q}, \mathbb{R}$ e $\mathbb{C}$ são corpos.

Conseguimos demonstrar, sem dificuldades, que todo corpo é um domínio de integridade. Agora, atente-se ao fato de que o anel $\mathbb{Z}$ é um domínio de integridade, mas não é um corpo. Com efeito, apenas os inteiros 1 e -1 satisfazem a propriedade x). Dessa forma, percebemos que nem todo domínio de integridade é um corpo. Ademais, se o domínio de integridade A é finito, temos que A é um corpo.

Por fim, afirmamos que se A é um domínio de integridade, então todo elemento não nulo de A é regular para a multiplicação (ser regular significa obedecer à lei do cancelamento). De fato, sejam $a, b, c \in A,\ a \neq 0$. Suponha $ab = ac$. Assim, temos:

$$ab = ac \implies ab - ac = 0 \implies a(b - c) = 0\,.$$

Ora, A não possui divisores de zero, então, como $a \neq 0$, temos que $b - c = 0$. Daí segue que $b = c$.

2.2 Espaços vetoriais

Definição 2.2: Seja K um corpo e V um conjunto não vazio. Dizemos que V é um **espaço vetorial** sobre K, e seus elementos serão chamados de vetores, se V possuir duas operações, uma adição $(+)$ e uma multiplicação por escalar $(\cdot)$:

$$+ : V \times V \longrightarrow V$$
$$\cdot : K \times V \longrightarrow V$$

tais que as seguintes condições sejam satisfeitas:

i) $u + (v + w) = (u + v) + w$, $\forall\, u, v$ e $w \in V$.

ii) $u + v = v + u$, $\forall\, u$ e $v \in V$.

iii) Existe $\vec{0} \in V$, chamado de vetor nulo, tal que $v + \vec{0} = \vec{0} + v = v$, $\forall\, v \in V$.

iv) Para cada $v \in V$, existe um elemento $-v \in V$, chamado vetor oposto de v, tal que $v + (-v) = (-v) + v = \vec{0}$.

v) $a(u + v) = au + av$, $\forall\, a \in K$ e $u, v \in V$.

vi) $(a + b)v = av + bv$, $\forall\, a, b \in K$ e $v \in V$.

vii) $(ab)v = a(bv)$, $\forall\, a, b \in K$ e $v \in V$.

viii) Sendo 1 a unidade de K, temos que $1v = v$, $\forall\, v \in V$.

Os elementos do corpo K são chamados de escalares. Se na definição acima, considerarmos números reais como escalares, então V será chamado de espaço vetorial real. No caso em que os escalares são números complexos, V é dito ser um espaço vetorial complexo.

Exemplo 2.1: Todo corpo é um espaço vetorial sobre si mesmo. Além disso, $\mathbb{R}$ e $\mathbb{C}$ são espaços vetoriais sobre o corpo $\mathbb{Q}$. Ademais, $\mathbb{C}$ é um espaço vetorial sobre $\mathbb{R}$.

Exemplo 2.2: O conjunto das n-uplas de números reais $\mathbb{R}^n = \{(x_1, x_2, \cdots, x_n);\ x_i \in \mathbb{R}\}$ é um espaço vetorial sobre $\mathbb{R}$. As operações de adição de vetores e multiplicação por

escalares são definidas da seguinte forma: sendo $u = (x_1, x_2, \cdots, x_n)$ e $v = (y_1, y_2, \cdots, y_n)$ elementos de $\mathbb{R}^n$, e $\alpha \in \mathbb{R}$, então $u + v = (x_1 + y_1, x_2 + y_2, \cdots, x_n + y_n)$ e $\alpha u = (\alpha x_1, \alpha x_2, \cdots, \alpha x_n)$. Nesse caso, a n-upla $(0,0,\cdots,0)$ é o vetor nulo e o vetor oposto de $u = (x_1, x_2, \cdots, x_n)$ é o vetor $-u = (-x_1, -x_2, \cdots, -x_n)$.

2.3 Subespaços vetoriais

Em algumas situações, é necessário identificar, dentro de um espaço vetorial V, subconjuntos W que, com as mesmas operações de adição em V e de multiplicação de vetores de V por escalares, também sejam espaços vetoriais. Tais conjuntos são denominados subespaços vetoriais de V.

Definição 2.3: Dado um espaço vetorial V sobre um corpo K, dizemos que um subconjunto $W \neq \emptyset$ é um **subespaço vetorial** de V se as seguintes condições são satisfeitas:

i) $u + v \in W$, $\forall\, u, v \in W$

ii) $\alpha u \in W$, $\forall\, u \in W$ e $\alpha \in K$.

Exemplo 2.3: De forma imediata temos que todo espaço vetorial V contém pelo menos dois subespaços, a saber: o próprio V e o espaço formado apenas pelo vetor nulo de V.

Exemplo 2.4: Como caso particular do exemplo 2.2 temos que $V = \mathbb{R}^5$ é um espaço vetorial sobre $\mathbb{R}$. Seja W o conjunto dos vetores de $\mathbb{R}^5$ cuja primeira coordenada é nula, isto é $W = \{(0, x_2, x_3, x_4, x_5);\ x_i \in \mathbb{R}\}$. Note que, tomando $u = (0, x_2, x_3, x_4, x_5)$ e $v = (0, y_2, y_3, y_4, y_5)$ elementos de W, e $\alpha \in \mathbb{R}$. Então,

i) $u + v = (0,\ x_2 + y_2,\ x_3 + y_3,\ x_4 + y_4,\ x_5 + y_5) \in W$.

ii) $\alpha u = (0, \alpha x_2, \alpha x_3, \alpha x_4, \alpha x_5) \in W$.

Logo, W é um subespaço vetorial de V.

2.4. Dependência e independência linear

Uma importante característica de um espaço vetorial é a possibilidade de obtermos novos vetores a partir de vetores dados. Nesta seção trataremos deste fato, o que nos conduz a abordar duas definições relevantes, quais sejam: vetores linearmente independentes e vetores linearmente dependentes.

Definição 2.4: Seja V um espaço vetorial sobre um corpo K. Considere $v_1, v_2, \cdots, v_n$ vetores de V. Diremos que o vetor $v \in V$ é uma **combinação linear** de $v_1, v_2, \cdots, v_n$ se existirem $\alpha_1, \alpha_2, \cdots, \alpha_n \in K$ tais que $v = \alpha_1 v_1 + \alpha_2 v_2 + \cdots + \alpha_n v_n$.

Definição 2.5: Seja X o subconjunto de um espaço vetorial V, formado pelos vetores $v_1, v_2, \cdots, v_n$. O conjunto W de todos os vetores v de V que são dados como combinação linear dos vetores $v_1, v_2, \cdots, v_n$ é chamado de **subespaço gerado** por X, que denotaremos por $W = [v_1, v_2, \cdots, v_n]$.

Proposição 2.1: Nas notações da definição 2.5 temos que W é um subespaço de V.

Demonstração: Com efeito, sejam $u, w \in W$ e $\alpha, \alpha_1, \alpha_2, \cdots, \alpha_n, \beta_1, \beta_2, \cdots, \beta_n \in K$ tais que $u = \alpha_1 v_1 + \alpha_2 v_2 + \cdots + \alpha_n v_n$ e $w = \beta_1 v_1 + \beta_2 v_2 + \cdots + \beta_n v_n$. Note que,

i) $u + w = \alpha_1 v_1 + \alpha_2 v_2 + \cdots + \alpha_n v_n + \beta_1 v_1 + \beta_2 v_2 + \cdots + \beta_n v_n = (\alpha_1 + \beta_1)v_1 + (\alpha_2 + \beta_2)v_2 + \cdots + (\alpha_n + \beta_n)v_n$.

ii) $\alpha u = \alpha(\alpha_1 v_1 + \alpha_2 v_2 + \cdots + \alpha_n v_n) = (\alpha\alpha_1)v_1 + (\alpha\alpha_2)v_2 + \cdots + (\alpha\alpha_n)v_n$.

As igualdades obtidas em i) e ii) seguem do fato de V ser um espaço vetorial sobre K. Como K é fechado para as operações que o dotam da estrutura de corpo, temos que a somas e os produtos dos parênteses são elementos de K. Logo, $u + w$ e αu são elementos de W e, assim, pela definição 2.3, W é um subespaço de V. ∎

Definição 2.6: Considere $v_1, v_2, \cdots, v_n$ vetores de um espaço vetorial V definido sobre K, e $\alpha_1, \alpha_2, \cdots, \alpha_n \in K$. Dizemos que o conjunto $\{v_1, v_2, \cdots, v_n\}$ é **linearmente independente (LI)** se $\alpha_1 v_1 + \alpha_2 v_2 + \cdots + \alpha_n v_n = \vec{0} \Longrightarrow \alpha_1 = \alpha_2 = \cdots = \alpha_n = 0$. Caso exista algum $\alpha_i \neq 0$ dizemos que $\{v_1, v_2, \cdots, v_n\}$ é um conjunto **linearmente**

dependente (LD). Podemos também, no caso de $\{v_1, v_2, \cdots, v_n\}$ ser LI (ou LD), dizer que os vetores que o compõe são LI (ou LD).

Exemplo 2.5: Os vetores do $\mathbb{R}^3$, $(1,0,0)$, $(0,1,0)$ e $(0,0,1)$ são linearmente independentes. De fato, sendo α_1, α_2 e α_3 números reais, temos que:

$$\alpha_1(1,0,0) + \alpha_2(0,1,0) + \alpha_3(0,0,1) = (0,0,0) \Longrightarrow (\alpha_1, \alpha_2, \alpha_3) = (0,0,0) \Longrightarrow$$
$$\Longrightarrow \alpha_1 = \alpha_2 = \alpha_3 = 0\,.$$

Exemplo 2.6: O conjunto $\{1, \sqrt{3}\} \subset \mathbb{R}$ é LI sobre $\mathbb{Q}$, mas é LD sobre $\mathbb{R}$. Com efeito, $(-3) \cdot 1 + \sqrt{3} \cdot \sqrt{3} = 0$, mas

$$a \cdot 1 + b \cdot \sqrt{3} = 0 \text{ com } a, b \in \mathbb{Q} \Longrightarrow a = b = 0.$$

Caso contrário, teríamos $\sqrt{3} = -\frac{a}{b} \in \mathbb{Q}$.

2.5. Bases e dimensão

Suponha que estejamos interessados em encontrar, em um espaço vetorial V, um conjunto finito de vetores, de tal maneira que qualquer outro vetor de V seja dado por uma combinação linear destes. Além disso, queremos que todos os vetores desse conjunto finito sejam, de fato, necessários para gerar V. Veremos que tal conjunto é denominado de base do espaço vetorial V.

Definição 2.7: Seja $\{v_1, v_2, \cdots, v_n\}$ um conjunto de vetores de um espaço vetorial V. Diremos que tal conjunto é uma **base** de V se as seguintes condições forem verificadas:

i) $\{v_1, v_2, \cdots, v_n\}$ é LI

ii) $V = [v_1, v_2, \cdots, v_n]$.

Exemplo 2.7: Considere o espaço vetorial real $\mathbb{R}^3$. Assim, $\{(1,0,0), (0,1,0), (0,0,1)\}$ é uma base de $\mathbb{R}^3$, chamada de base canônica de $\mathbb{R}^3$. De fato, pelo exemplo 2.5, esse conjunto é LI. Além disso, é de fácil verificação que para todo $(x,y,z) \in \mathbb{R}^3$, temos que $(x,y,z) = x(1,0,0) + y(0,1,0) + z(0,0,1)$. Logo, $\mathbb{R}^3 = [(1,0,0), (0,1,0), (0,0,1)]$.

Salientamos que nem sempre a base de um espaço vetorial é um conjunto finito. Boldrini *et al*. (1980, p.117) destaca que "[…] isto acontece principalmente quando trabalhamos com espaços de funções. Nestes casos precisaremos de um conjunto infinito de vetores para gerar o espaço. Isto não quer dizer que estamos trabalhando com combinações lineares infinitas, mas sim, que cada vetor do espaço é uma combinação linear finita daquela "base infinita". Ou seja, para cada vetor, podemos escolher uma quantidade finita de vetores da "base" para, com eles, escrever o vetor dado".

O exemplo que segue ilustra a afirmação feita anteriormente sobre espaços vetoriais que não admitem base finita.

Exemplo 2.8: Consideremos o conjunto $\mathbb{R}^{\infty}$ cujos elementos são as sequências infinitas $u = (\alpha_1, \alpha_2, \cdots, \alpha_n, \cdots)$ e $v = (\beta_1, \beta_2, \cdots, \beta_n, \cdots)$ de números reais. $\mathbb{R}^{\infty}$ com as operações semelhantes às que definimos para o $\mathbb{R}^n$, no exemplo 2.2, é um espaço vetorial sobre $\mathbb{R}$. Agora, consideremos o conjunto $\mathbb{R}^{(\infty)}$, subespaço de $\mathbb{R}^{\infty}$, formado pelas sequências $w = (x_1, x_2, \cdots, x_n, \cdots)$ que tem apenas um número finito de termos x_n diferentes de zero. Consideremos o conjunto $X = \{e_1, \cdots, e_n, \cdots\} \subset \mathbb{R}^{\infty}$, onde $e_n = (0, \ldots, 0, 1, 0, \ldots)$ é a sequência infinita cujo n −ésimo termo é 1 e os demais são iguais a zero. Note que X é uma base de $\mathbb{R}^{(\infty)}$. Ademais, essa base não é finita.

Definição 2.8: Seja V um espaço vetorial sobre K. Se V admite uma base finita, então chamamos de **dimensão** de V, e denotamos por $dim_K V$, o número de elementos de tal base. Caso contrário, dizemos que a dimensão de V é infinita.

Exemplo 2.9: Considerando o espaço vetorial real $V = \mathbb{R}^2$, temos que $\{(1,0), (0,1)\}$ e $\{(1,1), (0,1)\}$ são bases de V. Logo, $dim_{\mathbb{R}} \mathbb{R}^2 = 2$.

Exemplo 2.10: A partir do exemplo 2.7, concluímos que $dim_{\mathbb{R}} \mathbb{R}^3 = 3$. Mais geralmente, $dim_{\mathbb{R}} \mathbb{R}^n = n$.

Para finalizarmos essa seção, apresentaremos alguns resultados que serão necessários para demonstrações apresentadas nos capítulos seguintes.

Seja V um espaço vetorial sobre um corpo K. Vale ressaltar que qualquer base de V tem sempre o mesmo número de elementos, ou seja, em um espaço vetorial de dimensão finita, tal dimensão é única. Além disso, se V tiver dimensão finita, digamos $dim_K V = n$, então qualquer conjunto de vetores de V com mais de n elementos é linearmente dependente. Ademais, afirmamos que o conjunto $\{v_1, v_2, \cdots, v_n\}$ é base de V se, e somente se, todo elemento de V se escreve de forma única como combinação linear dos vetores $v_1, v_2, \cdots, v_n$. Por fim, se W é um subespaço de V, o qual tem dimensão finita, então W também tem dimensão finita e $dim_K W \leq dim_K V$ (com igualdade se, e somente se, $W = V$).

3 CONCEITOS BÁSICOS SOBRE POLINÔMIOS

No próximo capítulo os números algébricos e transcendentes serão abordados com detalhes, visto que são fundamentais para o desenvolvimento da teoria relacionada às construções impossíveis com régua e compasso que destacaremos neste trabalho. Para isso, será importante conhecermos alguns tópicos relacionados aos polinômios. Tendo em vista tal necessidade, desenvolveremos o capítulo que segue. Nem todas as proposições e teoremas serão demonstrados, visto que o nosso interesse com este capítulo é o de utilizar alguns resultados sobre polinômios no desenvolvimento da teoria dos capítulos seguintes, que são mais alinhados ao objetivo principal deste trabalho.

3.1 Definições e exemplos

Definição 3.1: Seja K um corpo qualquer. Considere uma expressão formal do tipo

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

onde $a_i \in K$, $\forall\, i \in \mathbb{N} \cup \{0\}$, e $\exists\, k \in \mathbb{N} \cup \{0\}$ tal que $a_j = 0\ \forall\, j \geq k$. Tal expressão é chamada de **polinômio** sobre K em uma indeterminada x.

Doravante, denotaremos por $K[x]$ o conjunto de todos os polinômios sobre um corpo K, em uma indeterminada x.

Definição 3.2: Dizemos que dois polinômios $p(x) = a_0 + a_1x + \cdots + a_nx^n + \cdots$ e $q(x) = b_0 + b_1x + \cdots + b_mx^m + \cdots$ sobre K são **iguais** se, e somente se, $a_i = b_i$ em K, $\forall\, i \in \mathbb{N} \cup \{0\}$.

Exemplo 3.1: O polinômio $p(x) = 0 + 0x + \cdots + 0x^m + \cdots$ é o **polinômio identicamente nulo** sobre K. Indicaremos tal polinômio por $p(x) = 0$. Assim, um polinômio sobre K da forma $p(x) = a_0 + a_1x + \cdots + a_nx^n + \cdots$ é dito ser identicamente nulo se, e somente se, $a_i = 0,\ \forall\, i \in \mathbb{N} \cup \{0\}$. Vale ressaltar que o símbolo 0 refere-se ao zero do corpo K em questão.

Exemplo 3.2: O polinômio $p(x) = a$, com $a \in K$, é chamado de **polinômio constante**. Nesse caso, temos $p(x) = a_0 + a_1x + \cdots + a_nx^n + \cdots$ onde $a_0 = a$ e $a_i = 0 \; \forall \; i \geq 1$.

Definição 3.3: Seja $p(x) = a_0 + a_1x + \cdots + a_nx^n + \cdots$ um polinômio tal que $a_n \neq 0$ e $a_i = 0 \; \forall \; i > n$. Dizemos que n é o **grau** do polinômio $p(x)$. Nesse caso, denotamos o grau de $p(x)$ por $\partial p(x) = n$. Além disso, podemos indicar o polinômio simplesmente por $p(x) = a_0 + a_1x + \cdots + a_nx^n$. Ademais, a_n é chamado de **coeficiente líder**. Quando $a_n = 1$, dizemos que $p(x)$ é um **polinômio mônico**.

Polinômios constantes tem grau zero. Ademais, não está definido o grau do polinômio identicamente nulo. Note que, podemos interpretar ∂ como uma função do conjunto de todos os polinômios sobre K não nulos, no conjunto $\mathbb{N} \cup \{0\}$. Em símbolos, temos:

$$\begin{aligned} \partial : K[x] - \{0\} &\longrightarrow \mathbb{N} \cup \{0\} \\ p(x) &\longmapsto \partial p(x) \end{aligned}$$

Em $K[x]$ podemos definir as operações de adição e multiplicação como segue.

Definição 3.4: Considere dois elementos de $K[x]$ dados por:

$p(x) = a_0 + a_1x + \cdots + a_nx^n + \cdots$ e $q(x) = b_0 + b_1x + \cdots + b_mx^m + \cdots$

Isso posto, definimos:

i) $p(x) + q(x) = c_0 + \cdots + c_kx^k + \cdots$ onde $c_i = (a_i + b_i) \in K$.

ii) $p(x) \cdot q(x) = c_0 + \cdots + c_kx^k + \cdots$ onde $c_0 = a_0b_0$, $c_1 = a_0b_1 + a_1b_0$,

$c_2 = a_0b_2 + a_1b_1 + a_2b_0, \cdots, c_k = a_0b_k + a_1b_{k-1} + \cdots + a_{k-1}b_1 + a_kb_0, k \in \mathbb{N}$.

A definição de multiplicação dada acima decorre da distributividade e da regra $x^m \cdot x^n = x^{m+n}$, com a convenção de que $x^0 = 1$ e $x^1 = 1$.

A função ∂ definida anteriormente possui as seguintes propriedades:

i) $\partial\big(p(x) + q(x)\big) \leq máx\,\{\partial p(x), \partial q(x)\}$, para todos $p(x)$ e $q(x) \in K[x]$, não nulos, e tais que $p(x) + q(x) \neq 0$.

ii) $\partial\big(p(x) \cdot q(x)\big) = \partial p(x) + \partial q(x)$, para todos $p(x)$ e $q(x) \in K[x]$, não nulos.

Nota: essas propriedades também valem em $D[x]$, sendo D um domínio de integridade.

A partir da definição 3.4 observamos que $(K[x], +, \cdot)$ é um domínio de integridade, onde o zero e a unidade de $K[x]$ são, respectivamente, o polinômio nulo é o polinômio constante igual a 1.

Note que $K[x]$ não é um corpo. Com efeito, seja $p(x) \neq 0$ um polinômio que possua inverso multiplicativo em $K[x]$. Logo, existe $q(x) \neq 0$ em $K[x]$ tal que $p(x) \cdot q(x) = 1$. Da propriedade ii), anteriormente destacada, segue que $\partial\big(p(x) \cdot q(x)\big) = \partial p(x) + \partial q(x) \Longrightarrow \partial(1) = \partial p(x) + \partial q(x) \Longrightarrow \partial p(x) + \partial q(x) = 0 \Longrightarrow \partial p(x) = 0$. Logo, $p(x)$ é um polinômio constante. Portanto, apenas os polinômio constantes não nulos admitem inverso multiplicativo em $K[x]$.

3.2. O algoritmo da divisão

Seja K um corpo. Provaremos agora um importante teorema sobre a teoria dos polinômios.

Teorema 3.1 (algoritmo da divisão): Sejam $f(x), g(x) \in K[x]$ com $g(x) \neq 0$. Então existem únicos $q(x), r(x) \in K[x]$ tais que $f(x) = q(x) \cdot g(x) + r(x)$, onde teremos $r(x) = 0$ (nesse caso dizemos que $g(x)$ divide $f(x)$) ou $\partial r(x) < \partial g(x)$.

Demonstração: Considere os seguintes polinômios $f(x) = a_0 + a_1x + \cdots + a_nx^n$ e $g(x) = b_0 + b_1x + \cdots + b_mx^m$. Consideremos que, nesse caso, temos $\partial f(x) = n$ e $\partial g(x) = m$. Dividiremos a nossa demonstração em duas partes, a saber: existência e unicidade de $q(x)$ e $r(x)$ em $K[x]$.

i) Existência

Se $f(x) = 0$ basta tomarmos $q(x) = r(x) = 0$. Suponha que $f(x) \neq 0$. Caso tenhamos $n < m$, basta fazermos $q(x) = 0$ e $r(x) = f(x)$. Assim, assumiremos que $n \geq m$. Considere o polinômio $t(x)$ definido da seguinte forma:

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

Note que $\partial t(x) < \partial f(x)$. Nossa prova será por indução sobre n.

Base da indução: Para $n = 0$, do fato de termos $n \geq m$, segue que $m = 0$. Assim, $f(x) = a_0 \neq 0$ e $g(x) = b_0 \neq 0$. Daí, teremos $f(x) = a_0 b_0^{-1} g(x)$ e basta tomar $q(x) = a_0 b_0^{-1}$ e $r(x) = 0$.

Passo indutivo: Pela igualdade $t(x) = f(x) - a_n b_m^{-1} x^{n-m} \cdot g(x)$ e sabendo que $\partial t(x) < \partial f(x) = n$, temos, por hipótese de indução que, existem $q'(x)$ e $r'(x)$ tais que $t(x) = q'(x) \cdot g(x) + r'(x)$, onde $r'(x) = 0$ ou $\partial r'(x) < \partial g(x)$. Daí, segue imediatamente que:

$$f(x) = a_n b_m^{-1} x^{n-m} \cdot g(x) + t(x) = a_n b_m^{-1} x^{n-m} \cdot g(x) + q'(x) \cdot g(x) + r'(x)$$
$$= (q'(x) + a_n b_m^{-1} x^{n-m}) g(x) + r'(x),$$

e, portanto, tomando $q(x) = q'(x) + a_n b_m^{-1} x^{n-m}$ e $r(x) = r'(x)$ fica provada a existência dos polinômios $q(x)$ e $r(x)$ tais que $f(x) = q(x) \cdot g(x) + r(x)$, onde ocorre $r(x) = 0$ ou $\partial r(x) < \partial g(x)$.

ii) Unicidade

Sejam $q_1(x)$, $q_2(x)$, $r_1(x)$ e $r_2(x)$ tais que:

$$f(x) = q_1(x) \cdot g(x) + r_1(x) = q_2(x) \cdot g(x) + r_2(x),$$

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

Daí, segue que $\big(q_1(x) - q_2(x)\big) \cdot g(x) = r_2(x) - r_1(x)$. Ora, se $q_1(x) \neq q_2(x)$, temos que $\partial\big[\big(q_1(x) - q_2(x)\big) \cdot g(x)\big] \geq \partial g(x)$. Por outro lado, $\partial[r_2(x) - r_1(x)] < \partial g(x)$. O que é uma contradição. Logo, $q_1(x) = q_2(x)$ e, assim, $r_1(x) = f(x) - q_1(x) g(x) = f(x) - q_2(x) g(x) = r_2(x)$. ∎

A partir desse teorema podemos provar uma proposição que limita o número de raízes de um polinômio em um corpo. Para tanto, precisamos da definição que segue.

Definição 3.5: Sejam $f(x) = a_0 + a_1 x + \cdots + a_n x^n$ um polinômio não nulo em $K[x]$ e $\alpha \in K$. Dizemos que α é uma **raiz** de $f(x)$ em K se $f(\alpha) = a_0 + a_1 \alpha + \cdots + a_n \alpha^n = 0 \in K$.

Proposição 3.1: Seja K um corpo e $f(x) = a_0 + a_1x + \cdots + a_nx^n$ um polinômio não nulo em $K[x]$ de grau n. Então, o número de raízes de $f(x)$ em K é no máximo igual a n.

Demonstração: Se $f(x)$ não possui raízes em K nada há para demonstrar. Suponhamos, então, que $\alpha \in K$ seja uma raíz de $f(x)$. Como $g(x) = x - \alpha \in K[x]$, podemos usar o algoritmo da divisão. Assim, existem únicos $q(x)$ e $r(x) \in K[x]$ tais que $f(x) = q(x) \cdot (x - \alpha) + r(x)$, onde $r(x) = 0$ ou $\partial r(x) < \partial g(x) = 1$. A única possibilidade é que $r(x)$ seja um polinômio constante e, assim, teremos $r(x) = b$, com $b \in K$. Daí, segue que $f(x) = q(x) \cdot (x - \alpha) + b$, mas como $f(\alpha) = 0$, temos que $0 = 0 + b$, ou seja $r(x) = 0$ e $f(x) = q(x) \cdot (x - \alpha)$, donde concluímos que $\partial q(x) = n - 1$.

Sabemos que todo corpo é um domínio de integridade. Logo, o corpo K em questão, por ser também um domínio de integridade, não possui divisores de zero. Assim, se $\beta \in K$ é uma raíz qualquer de $f(x)$ então, $f(\beta) = (\beta - \alpha) \cdot q(\beta) = 0 \implies \beta = \alpha$ ou β é também uma raíz de $q(x) \in K[x]$. Daí, segue que as raízes de $f(x)$ são α e as raízes de $q(x)$.

Agora, procederemos por indução sobre $\partial f(x) = n$.

Base da indução: Para $n = 0$, $f(x)$ não possui raízes em K e, nesse caso, já vimos que a proposição é válida.

Passo indutivo: Como $\partial q(x) < \partial f(x) = n$, $q(x)$ possui no máximo $\partial q(x) = n - 1$ raízes em K e, portanto, $f(x)$ possui no máximo n raízes em K.

Isso estabelece o passo de indução e, assim, conclui a demonstração. ∎

3.3. Polinômios irredutíveis

Fazendo uma analogia entre os domínios de integridade $K[x]$ e $\mathbb{Z}$, introduziremos, a partir daqui, os polinômios em $K[x]$ que fazem o mesmo papel dos números primos em $\mathbb{Z}$. Esses polinômios serão chamados de polinômios irredutíveis sobre K.

Definição 3.6: Seja $f(x) \in K[x]$ tal que $\partial f(x) \geq 1$. Dizemos que $f(x)$ é um **polinômio irredutível sobre K** se, sempre que $f(x) = g(x) \cdot h(x)$, com $g(x)$ e $h(x) \in K[x]$, então temos $g(x) = a$ ou $h(x) = b$, com a e b elementos de K, ou seja, $g(x)$ é

um polinômio constante em $K[x]$ ou $h(x)$ é um polinômio constante em $K[x]$. Se $f(x)$ for não irredutível sobre K, dizemos que f é **redutível** sobre K.

Exemplo 3.3: Todo polinômio de grau 1 em $K[x]$ é irredutível sobre o corpo K. Note, também, que o polinômio $f(x) = x^2 + 1$ é irredutível sobre o corpo $\mathbb{R}$, porém é redutível sobre $\mathbb{C}$.

3.4. Fatorização única

Agora apresentaremos, sem demonstração, um teorema muito relevante na teoria dos polinômios em uma variável. Novamente trazendo uma analogia com o domínio $\mathbb{Z}$, tal teorema assemelha-se ao que em $\mathbb{Z}$ chamamos de Teorema Fundamental da Aritmética. Aqui, os polinômios irredutíveis fazem o papel que os números primos desempenham no teorema anteriormente mencionado.

Teorema 3.2: Seja K um corpo. Todo polinômio $f(x) \in K[x] - \{0\}$ pode ser escrito na forma $f(x) = a \cdot p_1(x) \cdot p_2(x) \cdot \cdots \cdot p_m(x)$, onde $a \in K - \{0\}$ e $p_1(x)$, $p_2(x)$, $\cdots$, $p_m(x)$ são polinômios irredutíveis, não necessariamente distintos, sobre K. Mais ainda, essa expressão é única a menos da constante a e da ordem dos polinômios $p_1(x), p_2(x), \cdots, p_m(x)$.

3.5. O critério de Eisenstein

A verificação da irredutibilidade de um polinômio sobre um corpo é, em geral, um trabalho complicado. Veremos aqui um teorema que nos garante condições suficientes para que um polinômio $f(x) \in \mathbb{Q}[x]$ seja irredutível sobre $\mathbb{Q}$. Tal teorema é chamado de critério de Eisenstein. A fim de facilitar a prova desse resultado, apresentaremos a proposição a seguir que deve-se a Gauss. Note que, ao enunciarmos a proposição e o teorema anteriormente mencionados, surge uma sutileza que devemos abordar, a saber: até o momento consideramos o conjunto de polinômios $K[x]$ apenas no caso em que K é um corpo, todavia trataremos agora de $\mathbb{Z}[x]$, e sabemos que $\mathbb{Z}$ é um domínio de integridade que não é um corpo. Se D é um domínio de integridade, então de maneira inteiramente análoga à construção de $K[x]$

que é feita quando K é um corpo, consegue-se construir o domínio de integridade $D[x]$ de todos os polinômios na indeterminada x com coeficientes em D. Em particular, $\mathbb{Z}[x]$ é o conjunto de todos os polinômios $p(x) = a_0 + a_1x + \cdots + a_nx^n$, onde $a_i \in \mathbb{Z}$. Vale ressaltar que a Proposição 3.1 continua válida em $D[x]$, sendo D um domínio de integridade.

Nota: Para o Lema e o Teorema a seguir, usaremos a notação $a \mid b$ para indicar que "a é um divisor de b". Caso contrário, diremos que "a não é um divisor de b" e o denotaremos por $a \nmid b$.

Proposição 3.2 (Lema de Gauss): Seja $f(x) \in \mathbb{Z}[x]$ um polinômio irredutível sobre $\mathbb{Z}$. Então, $f(x)$ é irredutível sobre $\mathbb{Q}$.

Demonstração: Vamos demonstrar a contrapositiva, isto é, se $f(x) = q(x) \cdot s(x)$, com $q(x), s(x) \in \mathbb{Q}[x]$, é uma decomposição não trivial de $f(x)$ (ou seja, $\partial q(x) > 0$ e $\partial s(x) > 0$), então existe uma decomposição não trivial $f(x) = p(x) \cdot t(x)$, com $p(x), t(x) \in \mathbb{Z}[x]$. Seja $q(x) = \frac{u_0}{v_0} + \frac{u_1}{v_1}x + \cdots + \frac{u_n}{v_n}x^n$, onde $u_i, v_i \in \mathbb{Z}$ e $mdc(u_i, v_i) = 1$. Se $v = mmc\,(v_0, \cdots, v_n)$ então $q(x) = \frac{1}{v}(u'_0 + u'_1x + \cdots + u'_nx^n)$, onde $u'_i \in \mathbb{Z}$. Se $u = mdc\,(u'_0, u'_1, \cdots, u'_n)$, então $q(x) = \frac{u}{v} \cdot q_0(x)$, onde $q_0(x) \in \mathbb{Z}[x]$ é um polinômio primitivo (isto é, $q_0(x) = a_0 + a_1x + \cdots + a_nx^n$ e $mdc\,(a_0, a_1, \cdots, a_n) = 1$). De modo análogo, podemos escrever $s(x) = \frac{r}{t} \cdot s_0(x)$, onde $r, t \in \mathbb{Z}$, $s_0(x) \in \mathbb{Z}[x]$, com $s_0(x) = b_0 + b_1x + \cdots + b_mx^m$ e $mdc\,(b_0, b_1, \cdots, b_m) = 1$. Agora, $f(x) = q(x) \cdot s(x) = \frac{ur}{vt} \cdot q_0(x) \cdot s_0(x) \Longrightarrow vt \cdot f(x) = ur \cdot q_0(x) \cdot s_0(x)$. Vamos mostrar que o polinômio $q_0(x) \cdot s_0(x)$ também é primitivo, ou seja o mdc dos seus coeficientes é 1. Para isso, basta provar que, se p é primo, então p não divide algum coeficiente de $q_0(x) \cdot s_0(x)$. Como $mdc\,(a_0, a_1, \cdots, a_n) = 1$ e $mdc\,(b_0, b_1, \cdots, b_m) = 1$, um primo p qualquer não divide todos os a_i nem divide todos os b_j. Sejam a_i e b_j os coeficientes com menores índices tais que $p \nmid a_i$ e $p \nmid b_j$. O coeficiente de x^{i+j} em $q_0(x) \cdot s_0(x)$ é

$$c_{i+j} = a_{i+j}b_0 + a_{i+j-1}b_1 + \cdots + a_{i+1}b_{j-1} + a_ib_j + a_{i-1}b_{j+1} + \cdots + a_0b_{i+j} \quad (*).$$

Sabemos que $p \mid a_0$, $p \mid a_1$, $\cdots, p \mid a_{i-1}$ e $p \mid b_0$, $p \mid b_1$, $\cdots, p \mid b_{j-1}$. Se p dividisse c_{i+j}, então, por $(*)$, p necessariamente dividiria $a_i b_j$. Mas, $p \mid a_i b_j \implies p \mid a_i$ ou $p \mid b_j$, pois p é primo, e nenhuma das duas situações ocorre. Assim, se d for o mdc dos coeficientes de $f(x)$, é fácil ver que o mdc dos coeficientes de $vt \cdot f(x)$ é vtd, enquanto o mdc dos coeficientes de $ur \cdot q_0(x) \cdot s_0(x)$ é ur (pois, $q_0(x) \cdot s_0(x)$ é primitivo). Daí, segue que $ur = vtd$ e, portanto, $f(x) = d \cdot q_0(x) \cdot s_0(x) = p(x) \cdot t(x)$, com $p(x) \in \mathbb{Z}[x]$ e $t(x) \in \mathbb{Z}[x]$. ∎

Teorema 3.3 (O critério de Eisenstein): Seja $f(x) = a_0 + a_1 x + \cdots + a_n x^n$ um polinômio em $\mathbb{Z}[x]$. Caso exista um inteiro primo p tal que:

i) $p \nmid a_n$

ii) $p \mid a_0, a_1, \cdots, a_{n-1}$

iii) $p^2 \nmid a_0$

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

Demonstração: A partir da proposição 3.2 é suficiente mostrar que $f(x)$ é irredutível sobre $\mathbb{Z}$. Suponhamos, por absurdo, que $f(x) = g(x) \cdot h(x)$, com $g(x)$ e $h(x) \in \mathbb{Z}[x]$ e $1 \leq \partial g(x), \partial h(x) < \partial f(x) = n$. Considere que:

$$g(x) = b_0 + b_1 x + \cdots + b_r x^r \in \mathbb{Z}[x] \text{ com } \partial g(x) = r \text{ e}$$

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

Assim, $n = r + s$.

Note que, $b_0 \cdot c_0 = a_0$ e assim $p \mid b_0$ ou $p \mid c_0$, pois $p \mid a_0$, e daí, como $p^2 \nmid a_0$, segue que p divide apenas um dos inteiros b_0 e c_0. Admitiremos, sem perda de generalidade, que $p \mid b_0$ e $p \nmid c_0$.

Agora, perceba que $a_n = b_r \cdot c_s$ é o coeficiente de $x^n = x^{r+s}$ e, portanto, temos que $p \nmid b_r$ (pois $p \nmid a_n$) e $p \mid b_0$. Seja b_i o primeiro coeficiente de $g(x)$ tal que $p \nmid b_i$.

Por fim, sendo $a_i = b_0 \cdot c_i + b_1 \cdot c_{i-1} + \cdots + b_i \cdot c_0$ temos que $p \nmid a_i$, pois $p \mid b_0, b_1, \cdots, b_{i-1}$, $p \nmid b_i$ e $p \nmid c_0$. Logo, $i = n$. Absurdo, pois $1 \leq i \leq r < n$.

Logo, $f(x)$ é irredutível sobre $\mathbb{Z}$. Como queríamos demonstrar. ∎

Exemplo 3.4: Seja $f(x) = x^3 + 2x + 10$. Considerando o primo $p = 2$, temos que $2 \nmid 1,\ 2|0,\ 2|2,\ 2|10$ e $4 \nmid 10$. Logo, o critério de Eisenstein garante que $f(x)$ é irredutível sobre $\mathbb{Q}$.

Exemplo 3.5: Seja $f(x) = 3x^5 + 4x + 6$. Sendo $p = 2$, temos que $2 \nmid 3,\ 2|0,\ 2|4,\ 2|6$ e $4 \nmid 6$. Assim, pelo critério de Eisenstein, temos que $f(x)$ é irredutível sobre $\mathbb{Q}$.

Exemplo 3.6: Seja $f(x) = 2x^4 - 12x^3 - 3x^2 + 6x - 6$. Considerando o primo $p = 3$, temos que $3 \nmid 2,\ 3|-12,\ 3|-3,\ 3|6,\ 3|-6$ e $9 \nmid -6$. Assim, pelo critério de Eisenstein, temos que $f(x)$ é irredutível sobre $\mathbb{Q}$.

Exemplo 3.7: Sejam p um número primo qualquer e $p(x) = x^n - p$ um polinômio de grau $n \geq 1$ sobre $\mathbb{Q}$. Claramente, considerando o próprio primo p, podemos aplicar o critério de Eisenstein, e portanto $p(x)$ é irredutível sobre $\mathbb{Q}$.

A partir do exemplo 3.7, conseguimos obter uma conclusão relevante que, apesar de não ser crucial para o desenvolvimento desse trabalho, merece ser destacada. Esse resultado consta na proposição que segue.

Proposição 3.3: Raízes n-ésimas, com $n > 1$, de números primos são irracionais.

Demonstração: Seja p um número primo qualquer. Para $n > 1$, o polinômio dado por $p(x) = x^n - p$ é redutível sobre $\mathbb{R}$. De fato, podemos fazer:

$$p(x) = x^n - p = x^n - \sqrt[n]{p^n} = x^n - \left(\sqrt[n]{p}\right)^n =$$
$$\left(x - \sqrt[n]{p}\right) \cdot (x^{n-1} + x^{n-2} \cdot \sqrt[n]{p} + x^{n-3} \cdot \sqrt[n]{p^2} + \cdots + \sqrt[n]{p^{n-1}}).$$

Supondo que $\sqrt[n]{p}$ é racional, a fatoração obtida anteriormente permite concluir a redutibilidade do polinômio $p(x) = x^n - p$ sobre $\mathbb{Q}$, o que contraria o exemplo 3.7. Assim, concluímos que $\sqrt[n]{p}$ é irracional. ∎

Por fim, apresentaremos uma última proposição a fim de concluir as considerações do capítulo 3 sobre polinômios.

Proposição 3.4: O polinômio $f(x) = x^{p-1} + \cdots + x + 1$ é irredutível sobre $\mathbb{Q}$, se p é primo.

Demonstração: Faremos a substituição $x = y + 1$. Observe que

$$f(x) \text{ é irredutível em } \mathbb{Q}[x] \Leftrightarrow f(y) \text{ é irredutível em } \mathbb{Q}[y]$$

(basta substituir $y = x - 1$ em qualquer fatoração de $f(y)$).

Agora, escrevendo $f(x) = x^{p-1} + \cdots + x + 1 = \frac{x^p - 1}{x - 1}$, segue da fórmula do desenvolvimento do binômio de Newton que:

$$f(y) = \frac{(y+1)^p - 1}{y} = y^{p-1} + \binom{p}{1} y^{p-2} + \binom{p}{2} y^{p-3} + \cdots + \binom{p}{p-2} y + \binom{p}{p-1}.$$

Para finalizar, do fato de p ser um número primo, temos que p divide $\binom{p}{i}$ para cada $i = 1, \cdots, p-1$. De fato, $\binom{p}{i} = \frac{p!}{i!(p-i)!} \Rightarrow i!\binom{p}{i} = p \cdot (p-1) \cdot \ldots \cdot (p-i+1)$. Logo, p divide $i!\binom{p}{i}$. Como p é primo e não divide $i!$, temos que p divide $\binom{p}{i}$. Ademais, é óbvio que p não divide 1 e que p^2 não divide $\binom{p}{p-1} = p$. Logo, o critério de Eisenstein garante que $f(y)$ é irredutível em $\mathbb{Q}[y]$, ou seja, $f(x)$ é irredutível em $\mathbb{Q}[x]$. ∎

4 EXTENSÕES DE CORPOS

O capítulo que segue será fundamental para que consigamos algebrizar os problemas de construtibilidade com régua e compasso que intitulam este trabalho. A partir daqui desenvolveremos um pouco mais os conceitos relacionados à álgebra dos polinômios, a fim de alcançarmos tal objetivo.

4.1 Definições e exemplos

Começaremos esta seção com a definição de extensão de um corpo, seguida de alguns exemplos. Posteriormente mostraremos alguns resultados sobre extensões, tendo em mente conceitos abordados no capítulo anterior.

Definição 4.1: Sejam $(L, +, \cdot)$ um corpo e K um subconjunto não vazio de L. Dizemos que K é um **subcorpo** de L se as seguintes condições forem satisfeitas:
i) K é fechado para a adição e a multiplicação de L;
ii) Restringindo aos elementos de K as mesmas operações de L, temos que K também é um corpo.

A proposição a seguir, enunciada sem demonstração, será bastante útil para o nosso trabalho posterior de mostrar que o conjunto dos números construtíveis é um corpo.

Proposição 4.1: Sejam $(L, +, \cdot)$ um corpo e K um subconjunto não vazio de L. A fim de que K seja um subcorpo de L é necessário e suficiente que as seguintes condições sejam satisfeitas:
i) O zero e a unidade de L pertençam a K;
ii) $x, y \in K \Longrightarrow x - y \in K$;
iii) $x, y \in K \Longrightarrow xy \in K$;
iv) $0 \neq y \in K \Longrightarrow \frac{1}{y} \in K$.

Exemplo 4.1: $K = \{a + b\sqrt{3} \mid a, b \in \mathbb{Q}\}$ é um subcorpo de $\mathbb{R}$ contendo $\mathbb{Q}$. Com efeito, sendo $x, y \in K$, façamos $x = a + b\sqrt{3}$ e $y = c + d\sqrt{3}$ com $a, b, c, d \in \mathbb{Q}$. Assim, temos:

i) $0 = 0 + 0\sqrt{3}$ e $1 = 1 + 0\sqrt{3}$. Logo, $0, 1 \in K$.

ii) $x - y = (a - c) + (b - d)\sqrt{3}$. Ora, $(a - c), (b - d) \in \mathbb{Q}$. Daí, $x - y \in K$.

iii) $xy = \left(a + b\sqrt{3}\right) \cdot \left(c + d\sqrt{3}\right) = (ac + 3bd) + (ad + bc)\sqrt{3}$. Como temos $(ac + 3bd)$, $(ad + bc) \in \mathbb{Q}$, então $xy \in K$.

iv) Consideremos, agora, $y \neq 0 \in K$ e façamos $y = c + d\sqrt{3}$ com $c, d \in \mathbb{Q}$ ($c \neq 0$ ou $d \neq 0$). Daí, vem:

$$\frac{1}{y} = \frac{1}{c + d\sqrt{3}} = \frac{1}{c + d\sqrt{3}} \cdot \frac{c - d\sqrt{3}}{c - d\sqrt{3}} = \frac{c - d\sqrt{3}}{c^2 - 3d^2} = \frac{c}{c^2 - 3d^2} - \frac{d}{c^2 - 3d^2}\sqrt{3}.$$

Note que $y = 0 \Leftrightarrow c = d = 0$ (caso contrário, teríamos $\sqrt{3} = -\frac{c}{d}$ racional). Daí, como $y \neq 0$, temos que $c^2 - 3d^2 \neq 0$. Logo, $\frac{c}{c^2 - 3d^2}$ e $-\frac{d}{c^2 - 3d^2}$ são racionais e, daí, $\frac{1}{y} \in K$. ∎

Sendo K um subcorpo de L, podemos também dizer que L é uma **extensão** de K. Nesse caso, escrevemos $L \mid K$, ou ainda,

$$\begin{matrix} L \\ | \\ K \end{matrix}$$

Exemplo 4.2: $\mathbb{Q}$ é um subcorpo de $\mathbb{R}$ e $\mathbb{R}$ é subcorpo de $\mathbb{C}$**.** Denotando como extensões de corpos temos $\mathbb{R} \mid \mathbb{Q}$, $\mathbb{C} \mid \mathbb{Q}$ e $\mathbb{C} \mid \mathbb{R}$.

A proposição 3.1 exibia um valor máximo para o número de raízes de um polinômio em um corpo K. Tal valor máximo é o grau do polinômio. Abordaremos, agora, um corolário dessa proposição que garante que o mesmo valor limita o número de raízes de um polinômio em qualquer extensão L de K. Assim, ao estendermos o corpo podemos obter mais raízes de um polinômio, porém esse número de raízes será sempre limitado pelo grau desse polinômio.

Corolário 4.1: Seja $f(x) = a_0 + a_1x + \cdots + a_nx^n$ um polinômio não nulo de grau n em $K[x]$. Então, $f(x)$ possui no máximo n raízes em qualquer extensão L de K.

Demonstração: Note que se $f(x) \in K[x]$ e $K \subset L$, então $f(x) \in L[x]$. O resultado segue da proposição 3.1 aplicada ao corpo L.

Exemplo 4.3: O polinômio $g(x) = x^3 - 2$ não possui raízes em $\mathbb{Q}$**,** possui apenas uma raiz em $\mathbb{R}$ e possui 3 raízes em $\mathbb{C}$**.**

Exemplo 4.4: O polinômio $f(x) = x^2 + 1$ não possui raízes em $\mathbb{R}$ e possui duas raízes em $\mathbb{C}$**.**

Conforme já mencionamos o polinômio $f(x) = x^2 + 1$ é irredutível sobre o corpo $\mathbb{R}$**,** porém é redutível sobre $\mathbb{C}$**.** Dessa forma, um polinômio $f(x) \in K[x]$ pode ser irredutível sobre o corpo K e redutível em uma extensão L de K.

4.2 Grau de uma extensão

Sejam L e K corpos, tais que $L \mid K$. Note que, por L ser um corpo, a adição em L é comutativa, associativa, possui elemento neutro e todo elemento possui inverso aditivo. Além disso, sendo $u, v \in L$ e $a, b \in K$, temos que vale: $a(u + v) = au + av$, $(a + b)v = av + bv$, $(ab)v = a(bv)$ e, sendo 1 a unidade de K, tem-se que $1v = v$. Portanto, L é um espaço vetorial sobre o corpo K. Os conceitos relativos a essa estrutura, abordados no capítulo 2, serão fundamentais para a continuidade do nosso estudo.

Definição 4.2: Consideremos os corpos L e K, tais que $L \mid K$. A dimensão do espaço vetorial L sobre K será chamada de **grau da extensão** e será denotada por $[L : K]$.

Uma extensão $L \mid K$ será dita **finita**, se L como espaço vetorial sobre K tiver dimensão finita, ou seja, se $[L : K] < \infty$. Caso contrário, $L \supset K$ diz-se uma extensão **infinita.**

Exemplo 4.5: Mostramos, no exemplo 4.1, que $K = \{a + b\sqrt{3};\ a, b \in \mathbb{Q}\}$ é um corpo. A extensão $K \mid \mathbb{Q}$ é finita, pois K é um espaço vetorial sobre $\mathbb{Q}$ que admite o conjunto $\{1, \sqrt{3}\}$ como base. Em símbolos, $[K : \mathbb{Q}] = 2$.

Nota: O grau da extensão $\mathbb{C} \mid \mathbb{R}$ é igual a 2.

4.3 Números algébricos, números transcendentes e adjunção

Ao longo desta seção, K representa um corpo e $L \supset K$ uma extensão de K. Começaremos com as definições de número álgébrico e número transcendente, para que posteriormente possamos abordar um processo de obtenção de corpos intermediários entre K e L.

Definição 4.3: Dizemos que $\alpha \in L$ é **algébrico** sobre K se existe $p(x) \in K[x] - \{0\}$ tal que $p(\alpha) = 0$. Caso contrário, dizemos que α é **transcendente** sobre K.

Exemplo 4.6: Se $\alpha \in K$, evidentemente α é algébrico sobre K pois é raiz do polinômio $p(x) = x - \alpha \in K[x]$.

Os elementos algébricos de $\mathbb{C}$ (respectivamente transcendentes) sobre $\mathbb{Q}$ são chamados de números algébricos (respectivamente transcendentes).

Exemplo 4.7: Os elementos $\sqrt{2}$, $\sqrt[3]{2}$ e $\sqrt[4]{2}$ de $\mathbb{C}$ são números algébricos. Com efeito, eles são, respectivamente, raízes dos polinômios $x^2 - 2$, $x^3 - 2$ e $x^4 - 2$ em $\mathbb{Q}[x]$.

Exemplo 4.8: O número π é transcendente. A prova deste fato, realizada em 1882 por Ferdinand von Lindemann, é complicada e, apesar de imprescindível para os nossos objetivos, usa conceitos de diversas áreas da matemática, principalmente de Cálculo Diferencial, conceitos estes não abordados neste trabalho. O número e, base dos logaritmos naturais, também é um número transcendente.

Exemplo 4.9: $a = \sqrt[4]{5 + \sqrt{2}}$ é um número algébrico. De fato, elevando à quarta potência, obtemos $a^4 = 5 + \sqrt{2}$. Agora, elevando a expressão $a^4 - 5 = \sqrt{2}$ ao quadrado, obtemos que $a^8 - 10a^4 + 23 = 0$, o que implica que a é um número algébrico.

Uma maneira de obtermos corpos intermediários entre K e L em uma extenção $L \mid K$ é a partir da noção de adjunção, que definiremos a seguir.

Definição 4.4: Seja $\alpha \in L$. Definimos a **adjunção** de α a K, e denotamos por $K[\alpha]$, o conjunto $K[\alpha] = \{p(\alpha);\ p(x) \in K[x]\}$.

Exemplo 4.10: Seja $\alpha = \sqrt{3} \in L = \mathbb{R} \supset \mathbb{Q} = K$. Mostraremos que $K[\alpha] = \mathbb{Q}[\sqrt{3}] = \{a + b\sqrt{3};\ a, b \in \mathbb{Q}\}$. Com efeito, por definição $\mathbb{Q}[\sqrt{3}] = \{p(\sqrt{3});\ p(x) \in \mathbb{Q}[x]\}$. Assim, sendo $p(x) \in \mathbb{Q}[x]$, segue pelo algoritmo da divisão que existem $q(x), r(x) \in \mathbb{Q}[x]$ tais que $p(x) = q(x)(x^2 - 3) + r(x)$, onde $r(x) = a + bx$, com $a, b \in \mathbb{Q}$. Portanto, $p(\sqrt{3}) = r(\sqrt{3}) = a + b\sqrt{3}$.

4.4 Polinômio mínimo e extensões algébricas

Definição 4.5: Sejam K um corpo, $L \mid K$ uma extensão e $\alpha \in L$ um elemento algébrico sobre K. Definimos o **polinômio mínimo** de α sobre K como sendo o polinômio mônico de menor grau em $K[x]$ que se anula em α.

Exemplo 4.11: O número real $\sqrt{3}$ é algébrico sobre $\mathbb{Q}$ e sobre $\mathbb{R}$, com polinômios mínimos $p(x) = x^2 - 3$ e $q(x) = x - \sqrt{3}$, respectivamente.

Exemplo 4.12: Os números $\sqrt[3]{5}$ e $\sqrt[4]{5}$ são algébricos sobre $\mathbb{Q}$, com polinômios mínimos $p(x) = x^3 - 5$ e $q(x) = x^4 - 5$, respectivamente.

A proposição 4.3 que enunciaremos e demonstraremos a seguir nos fornece uma importante caracterização do polinômio mínimo. Para a sua demonstração, precisaremos da definição 4.6 e da proposição 4.2 que destacaremos a seguir.

Definição 4.6: Um polinômio $p(x) \in A[x]$, onde A é um domínio de integridade, será chamado de **polinômio primo** se, sempre que $p(x)$ dividir um produto de polinômios $g(x)h(x)$, com $g(x)$ e $h(x)$ em $A[x]$, então $p(x)$ divide um dos fatores.

Proposição 4.2: Todo polinômio primo, com coeficientes em um domínio de integridade, é irredutível.

Demonstração: Com efeito, suponhamos que $p(x)$ seja primo e digamos que $p(x) = g(x)h(x)$, com $g(x)$ e $h(x)$ em $A[x]$. Então, $p(x)$ divide $g(x)h(x)$ e, por hipótese, $p(x)$ divide $g(x)$ ou $p(x)$ divide $h(x)$. Suponhamos que $p(x)$ divida $g(x)$ (o outro caso é análogo). Então, $g(x) = p(x)q(x)$ para algum $q(x) \in A[x]$ e, assim, $p(x) = g(x)h(x) = p(x)q(x)h(x)$. Como A é um domínio de integridade, podemos cancelar $p(x)$ obtendo que $1 = q(x)h(x)$. Logo, $h(x) = a \neq 0$, com $a \in A$. Então, $p(x)$ é irredutível. ∎

Proposição 4.3: Sejam K um corpo, $L \mid K$ uma extensão e $\alpha \in L$. Consideremos, ainda, o polinômio $p(x)$ mônico em $K[x]$, tal que $p(\alpha) = 0$. São equivalentes:
i) $p(x)$ é o polinômio mínimo de α.
ii) Se $q(x) \in K[x]$ é tal que $q(\alpha) = 0$, então $p(x)$ divide $q(x)$.
iii) $p(x)$ é irredutível.

Demonstração:
i) ⇒ ii): Suponhamos que $p(x)$ seja o polinômio mínimo de α sobre K. Seja $q(x) \in K[x]$, tal que $q(\alpha) = 0$. Pelo algoritmo da divisão de $q(x)$ por $p(x)$ existem $g(x)$ e $r(x) \in K[x]$ tais que $q(x) = g(x)p(x) + r(x)$, com $r(x) = 0$ ou $\partial r(x) < \partial p(x)$. Assim, temos que $0 = q(\alpha) = g(\alpha) \cdot 0 + r(\alpha) = r(\alpha)$. Ora, $p(x)$ é o polinômio não nulo de menor grau que se anula em α. Logo, $r(x) = 0$ e $p(x)$ divide $q(x)$. ∎

ii) ⇒ iii): A partir da proposição 4.2, como K é um corpo e, consequentemente, um domínio de integridade, basta mostrar que $p(x)$ é primo. Sejam $m(x)$, $g(x) \in K[x]$, tais que $p(x)$ divide $m(x)g(x)$. Então, existe $f(x)$ em $K[x]$, tal que $p(x)f(x) = m(x)g(x)$. Assim, temos que $0 = p(\alpha)f(\alpha) = m(\alpha)g(\alpha) \in L$. Como L é um corpo, temos que L é um domínio de integridade. Logo, $m(\alpha) = 0$ ou $g(\alpha) = 0$. Portanto, por hipótese, $p(x)$ divide $m(x)$ ou $p(x)$ divide $g(x)$. ∎

iii) ⇒ i): Seja $f(x)$ o polinômio mínimo de α sobre K. Suponhamos que $p(x) \in K[x]$ seja mônico e irredutível e $p(\alpha) = 0$. De i) ⇒ ii), concluímos que $f(x)$ divide $p(x)$.

Como os divisores mônicos de $p(x)$ são 1 e $p(x)$, e $f(x) \neq 1$, concluímos que $f(x) = p(x)$. ∎

Seja $p(x)$ o polinômio mínimo de α sobre K. A partir da proposição 4.3, temos que $p(x)$ é o único polinômio mônico irredutível em $K[x]$ que se anula em α, o qual denotaremos por $p(x) = irr(\alpha, K)$.

Proposição 4.4: Sejam K um corpo, $L \mid K$ uma extensão e $\alpha \in L$ um elemento algébrico sobre K. Se o grau de $p(x) = irr(\alpha, K)$ é n, então para todo $g(x) \in K[x]$, $g(\alpha)$ pode ser escrito de modo único como $g(\alpha) = a_0 + a_1\alpha + \cdots + a_{n-1}\alpha^{n-1}$, onde $a_i \in K$.

Demonstração: Seja $p(x) = irr(\alpha, K)$. Sabemos, por hipótese, que o grau de $p(x)$ é igual a n. Se $g(x) \in K[x]$, então pelo algoritmo da divisão existem $q(x), r(x) \in K[x]$ tais que $g(\alpha) = q(\alpha)p(\alpha) + r(\alpha)$, onde $r(x) = 0$ ou $\partial r(x) < \partial p(x)$, digamos, $r(x) = a_0 + a_1x + \cdots + a_{n-1}x^{n-1}$, com $a_i \in K$, $\forall\, i = 0, 1, \cdots, n-1$. Como $p(\alpha) = 0$, segue de $g(\alpha) = q(\alpha)p(\alpha) + r(\alpha)$ que $g(\alpha) = r(\alpha)$. Logo, $g(\alpha) = a_0 + a_1\alpha + \cdots + a_{n-1}\alpha^{n-1}$.

Agora mostraremos a unicidade da escrita. Seja $g(\alpha) = a_0 + a_1\alpha + \cdots + a_{n-1}\alpha^{n-1} = b_0 + b_1\alpha + \cdots + b_{n-1}\alpha^{n-1}$, com $a_i, b_i \in K$, $\forall\, i \in \{0, 1, \cdots, n-1\}$. Daí, segue que o polinômio $t(x) = (a_0 - b_0) + (a_1 - b_1)x + \cdots + (a_{n-1} - b_{n-1})x^{n-1} \in K[x]$ é tal que $t(\alpha) = 0$ e $\partial t(x) < n = \partial(irr(\alpha, K))$. Portanto, $t(x) = 0$, donde segue que $a_i = b_i\ \forall\, i \in \{0, 1, \cdots, n-1\}$. ∎

Nas notações da proposição 4.4, uma consequência desse resultado é que $K[\alpha] = \{a_0 + a_1\alpha + \cdots + a_{n-1}\alpha^{n-1};\ a_i \in K\}$ é um subcorpo de L, com $K \subset K[\alpha] \subset L$. Além disso, é possível mostrar que $K[\alpha]$ é o menor subcorpo de L contendo $K \cup \{\alpha\}$. Isto significa que $K[\alpha]$ é um subcorpo de L tal que se F é um subcorpo de L, com $K \subset F$ e $\alpha \in F$, então $K[\alpha] \subset F$.

A construção da adjunção pode ser iterada, ou seja, sendo $K[\alpha_1] \subset L$ e $\alpha_2 \in L$, podemos formar a adjunção de α_2 a $K[\alpha_1]$ que denotamos por $(K[\alpha_1])[\alpha_2] = K[\alpha_1, \alpha_2]$. Nesse caso, temos que $K \subset K[\alpha_1] \subset K[\alpha_1, \alpha_2] \subset L$. Ademais, podemos, recursivamente, construir, a partir de $K[\alpha_1, \alpha_2, \cdots, \alpha_{n-1}]$, o corpo $K[\alpha_1, \alpha_2, \cdots, \alpha_{n-1}, \alpha_n] = (K[\alpha_1, \alpha_2, \cdots, \alpha_{n-1}])[\alpha_n]$.

Exemplo 4.13: Seja $\alpha = \sqrt[n]{p}$, com $n \in \mathbb{Z}$ $(n \geq 2)$ e p um primo qualquer. Note que α é raiz real do polinômio $p(x) = x^n - p$ que é, conforme exemplo 3.7, irredutível sobre $\mathbb{Q}$. Assim, $p(x) = x^n - p = irr(\alpha, \mathbb{Q})$. Além disso, $\mathbb{Q}[\alpha]$ é um subcorpo de $\mathbb{R}$ contendo $\mathbb{Q}$ e, mais ainda, $\mathbb{Q}[\alpha] = \{a_0 + a_1\alpha + \cdots + a_{n-1}\alpha^{n-1}\ ; a_i \in \mathbb{Q}\}$.

Exemplo 4.14: Diante dos exemplos 4.10 e 4.13, temos que $\mathbb{Q} \subset \mathbb{Q}[\sqrt{3}] = \{a + b\sqrt{3}; a, b \in \mathbb{Q}\} \subset \mathbb{R}$.

O próximo resultado relaciona os graus da extensão $K[\alpha] | K$ e do polinômio mínimo de α sobre K.

Proposição 4.5: Sejam K um corpo, $L \mid K$ uma extensão e $\alpha \in L$ um elemento algébrico sobre K. Se n é o grau de $p(x) = irr(\alpha, K)$, então $[K[\alpha] : K] = n < \infty$ e $\{1, \alpha, \alpha^2, \cdots, \alpha^{n-1}\}$ é uma base de $K[\alpha]$ sobre K.

Demonstração: A proposição 4.4 garante que todo elemento de $K[\alpha]$ pode ser escrito de forma única como combinação linear sobre K de $1, \alpha, \alpha^2, \cdots, \alpha^{n-1}$. Assim, $\{1, \alpha, \alpha^2, \cdots, \alpha^{n-1}\}$ é uma base de $K[\alpha]$ sobre K e isto nos diz que $[K[\alpha] : K] = n$. ∎

O seguinte resultado, conhecido como teorema da torre, aborda sobre a multiplicatividade dos graus em extensões de corpos.

Teorema 4.1 (Teorema da Torre): Sejam F, L e K corpos tais que $F \subset K \subset L$. Se $L \mid K$ e $K \mid F$ são extensões finitas, então a extensão $L \mid F$ é finita e, além disso, $[L : F] = [L : K] \cdot [K : F]$.

Demonstração: Seja $\{a_k\ ; k = 1, \cdots, m\} \subset K$ uma base de $K \mid F$ e seja $\{b_j\ ; j = 1, \cdots, n\} \subset L$ uma base de $L \mid K$. Mostraremos que o conjunto $\{a_k b_j\ ;\ k = 1, \cdots, m$ e $j = 1, \cdots, n\} \subset L$ é uma base de $L \mid F$.

Seja $b \in L$. Como $\{b_j\ ; j = 1, \cdots, n\}$ gera $L \mid K$, existem $x_j \in K$ tais que $b = \sum_{j=1}^{n} x_j b_j$. Como $\{a_k\ ; k = 1, \cdots, m\}$ gera $K \mid F$, então, para cada $x_j \in K$ existem $y_{kj} \in F$ tais que $x_j = \sum_{k=1}^{m} y_{kj}\, a_k$. Daí, vêm:

$$b = \sum_{j=1}^{n} x_j b_j = \sum_{j=1}^{n} \left(\sum_{k=1}^{m} y_{kj}\, a_k \right) b_j = \sum_{j=1}^{n} \left(\sum_{k=1}^{m} y_{kj}\, a_k b_j \right) = \sum_{j=1}^{n} \sum_{k=1}^{m} y_{kj}(a_k b_j),$$

o que mostra que $\{a_k b_j\ ;\ k = 1, \cdots, m$ e $j = 1, \cdots, n\}$ gera $L \mid F$.

Resta mostrar que o conjunto $\{a_k b_j\ ;\ k = 1, \cdots, m$ e $j = 1, \cdots, n\}$ é linearmente independente. Suponhamos que, sendo $y_{kj} \in F$, temos

$$\sum_{j=1}^{n} \sum_{k=1}^{m} y_{kj}(a_k b_j) = 0\,.$$

Então,

$$0 = \sum_{j=1}^{n} \sum_{k=1}^{m} y_{kj}(a_k b_j) = \sum_{j=1}^{n} \left(\sum_{k=1}^{m} y_{kj}\, a_k \right) b_j\,,$$

com $\sum_{k=1}^{m} y_{kj}\, a_k \in K$, para cada j. Como $\{b_j\ ; j = 1, \cdots, n\}$ é linearmente independente sobre K, temos que $\sum_{k=1}^{m} y_{kj}\, a_k = 0$ para todo $j = 1, \cdots, n$, e como $\{a_k\ ; k = 1, \cdots, m\}$ é linearmente independente sobre F, obtemos que $y_{kj} = 0$ para todo $k = 1, \cdots, m$. ∎

Para a demonstração do corolário a seguir basta usarmos o teorema da torre e indução sobre n.

Corolário 4.2: Se $K = K_0 \subset K_1 \subset \cdots \subset K_n = L$ são corpos tais que $[L : K]$ é finito, então $[L : K] = [K_n : K_{n-1}] \cdot [K_{n-1} : K_{n-2}] \cdot \cdots \cdot [K_1 : K_0]$.

A fim de encerrar nossas considerações sobre extensões de corpos, traremos a definição de extensão algébrica, bem como alguns exemplos e uma proposição.

Definição 4.7: Seja K um corpo**.** Uma extensão $L \mid K$ é dita **algébrica**, se todo $\alpha \in L$ é algébrico sobre K.

Exemplo 4.15: A extensão $\mathbb{R} \mid \mathbb{Q}$ não é algébrica, pois π é transcendente sobre $\mathbb{Q}$**.**

Exemplo 4.16: A extensão $\mathbb{C} \mid \mathbb{R}$ é algébrica. Com efeito, se $\alpha = a + bi$, com $a, b \in \mathbb{R}$, então $(\alpha - a)^2 = -b^2 \Rightarrow \alpha^2 - 2a\alpha + a^2 + b^2 = 0$. Daí, α é raiz do polinômio $p(x) = x^2 - 2ax + b^2 + a^2 \in \mathbb{R}[x]$.

Proposição 4.6: Toda extensão finita é algébrica.

Demonstração: Sejam $L \mid K$ uma extensão finita, tal que $[L : K] = m < \infty$, e $\alpha \in L$. Logo, $1, \alpha, \cdots, \alpha^m$ são linearmente dependentes, pois m é o número máximo de elementos de L linearmente independentes sobre K. Assim, existem $a_0, a_1, \cdots, a_m \in K$, não todos nulos, tais que $a_0 + a_1\alpha + \cdots + a_m\alpha^m = 0$. Portanto, α é algébrico sobre K. ∎

5 CONSTRUÇÕES IMPOSSÍVEIS COM RÉGUA E COMPASSO

Chegamos ao capítulo mais importante deste trabalho. Aqui detalharemos como construir números, a partir de dois números assumidos previamente como construtíveis e de operações elementares, com o uso apenas dos instrumentos euclidianos: a régua e o compasso. A régua considerada não possui graduações servindo apenas para unir pontos do plano $\mathbb{R}^2$. Em algumas demonstrações utilizaremos conceitos básicos de geometria euclidiana plana, sendo necessário que o leitor possua certa familiaridade com esses conhecimentos. Além disso, mostraremos que o conjunto dos números construtíveis formam um corpo (mais precisamente, um subcorpo de $\mathbb{R}$). Ademais, tendo em mente a álgebra de polinômios desenvolvida nos capítulos anteriores abordaremos critérios para a construtibilidade de números, o que nos permitirá mostrar a impossibilidade da realização dos problemas gregos clássicos: a duplicação do cubo, a quadratura do círculo e a trissecção do ângulo.

5.1 As regras para a construção de números

Definição 5.1: Consideremos o conjunto $\mathcal{P} \subset \mathbb{R}^2$ contendo pelo menos dois pontos distintos. Uma reta r de $\mathbb{R}^2$ é uma reta em $\mathcal{P}$ se r contém dois pontos distintos de $\mathcal{P}$. Ademais, dizemos que uma circunferência c de $\mathbb{R}^2$ é uma circunferência em $\mathcal{P}$ se o centro de c pertence a $\mathcal{P}$ e um ponto de $\mathcal{P}$ pertence a c.

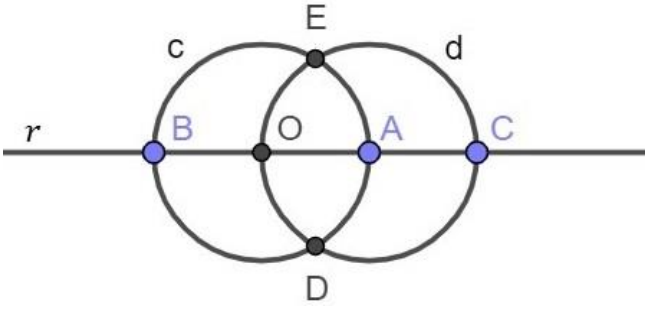
Algumas operações são ditas elementares em $\mathcal{P}$, são elas: interseção de duas retas em $\mathcal{P}$, interseção de uma reta em $\mathcal{P}$ e uma circunferência em $\mathcal{P}$ e, por fim, interseção de duas circunferências em $\mathcal{P}$.

Definição 5.2: Dizemos que $M \in \mathbb{R}^2$ é um **ponto construtível a partir de $\mathcal{P}$** se formos capazes de determinar M a partir de uma das operações elementares em $\mathcal{P}$, anteriormente mencionadas. Denotaremos por $[\mathcal{P}]$ o subconjunto dos pontos de $\mathbb{R}^2$ que são construtíveis a partir de $\mathcal{P}$.

Na busca de obtermos pontos construtíveis a partir de $\mathcal{P}$ não são permitidos: traçar uma circunferência de raio ou centro “arbitrários”, usar graduações previamente preparadas do compasso, tomar sobre uma reta um ponto “arbitrário”, deslizar a régua até uma certa posição, dentre outras ações que não as especificadas nas definições 5.1 e 5.2.

Exemplo 5.1: Seja $\mathcal{P} = \{O, A\} \subset \mathbb{R}^2$, com $O = (0,0)$ e $A = (1,0)$. Nesse caso, temos que $[\mathcal{P}] = \{O, A, B, C, D, E\}$, conforme indica a figura 1 destacada abaixo. A reta r foi obtida unindo os pontos O e A de $\mathcal{P}$, logo r é uma reta de $\mathcal{P}$. A circunferência c foi construída com centro no ponto O e tal que $A \in c$, assim c é uma circunferência de $\mathcal{P}$. Da mesma forma, conclui-se que d é uma circunferência de $\mathcal{P}$ visto que foi construída com centro em A e passando pelo ponto O. A partir das operações elementares em $\mathcal{P}$ obtemos o ponto $B = (-1,0)$ como interseção de r e c, e o ponto $C = (2,0)$ como interseção de r e d. Através de cálculos simples mostra-se que a interseção das circunferências c e d gera os pontos $D = \left(\frac{1}{2}, -\frac{\sqrt{3}}{2}\right)$ e $E = \left(\frac{1}{2}, \frac{\sqrt{3}}{2}\right)$, basta usarmos algumas propriedades dos triângulos equiláteros OAE e OAD.

Figura 1 – Construção de alguns pontos



Fonte: Adaptada de Gonçalves (2017).

Em geral, os pontos $O = (0,0)$ e $A = (1,0)$ são aqueles que assumiremos previamente como sendo elementos de $\mathcal{P}$. Agora, sejam $\mathcal{P}_0 = \{O, A\}$, $\mathcal{P}_1 = [\mathcal{P}_0]$, $\mathcal{P}_2 = [\mathcal{P}_1], \cdots, \mathcal{P}_{n+1} = [\mathcal{P}_n]$, $\forall\, n \in \mathbb{N}$. Assim, temos que:

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

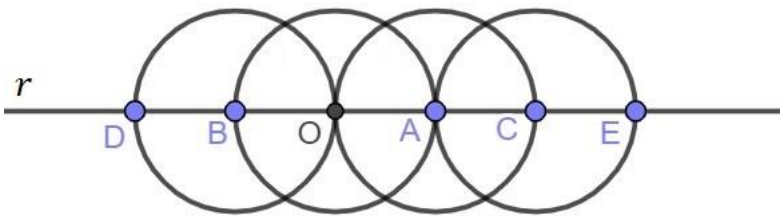
Seja $\mathcal{P}_\infty = \bigcup_{n=0}^{\infty} \mathcal{P}_n$. Note que $\mathcal{P}_\infty$ é infinito embora cada $\mathcal{P}_n$ seja um subconjunto finito do $\mathbb{R}^2$. Além disso, é imediato que $[\mathcal{P}_\infty] = \mathcal{P}_\infty$.

Definição 5.3: Chamamos de **pontos construtíveis** os pontos do plano que pertencem a $\mathcal{P}_\infty$. Da mesma forma, as retas de $\mathcal{P}_\infty$, ou seja, retas que contém dois pontos construtíveis distintos, são chamadas de **retas construtíveis**.

Definição 5.4: Um número real x é dito ser um **número construtível** se o ponto $A(x, 0)$ é construtível.

Diante do exposto até aqui, conseguimos concluir que todo número inteiro é construtível. O que já era esperado, pois partindo dos pontos $O = (0, 0)$ e $A = (1, 0)$ conseguimos construir todos os pontos do tipo $P(a, 0)$ com $a \in \mathbb{Z}$, vide figura 2. De fato, seja r a reta que passa por O e A (logo uma reta construtível). Já vimos que a interseção desta reta com a circunferência centrada em O que passa por A gera o ponto construtível $B = (-1,0)$. Analogamente, a interseção de r com a circunferência centrada em A que passa por O gera o ponto construtível $C = (2,0)$. Continuando o processo, centrando circunferências nos pontos B e C passando, respectivamente, por O e A obtemos os pontos construtíveis $D = (-2, 0)$ e $E = (3,0)$. Basta prosseguir desta forma para obter todos os números inteiros como interseção da reta r com circunferências centradas em pontos anteriormente construídos.

Figura 2 – Construção dos números inteiros



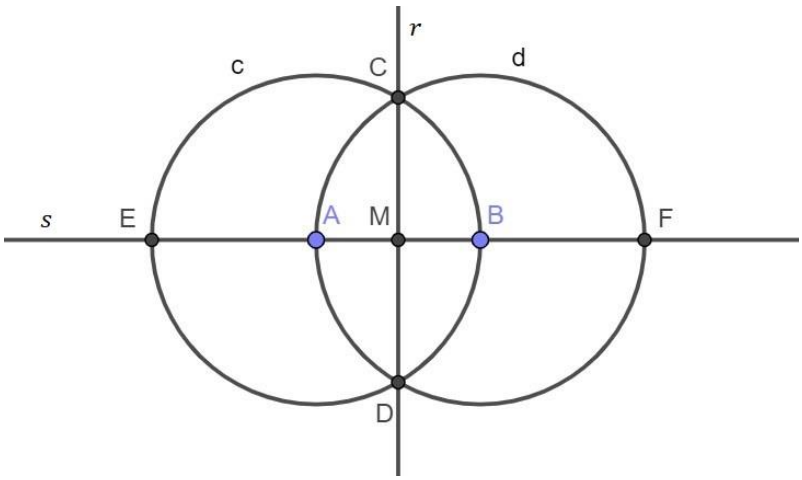
Fonte: Elaborada pelo autor.

Apresentaremos agora algumas proposições que, além de enriquecer a teoria abordada até aqui, serão fundamentais para a demonstração de resultados futuros.

Proposição 5.1: Se A e B são pontos construtíveis distintos, então o ponto médio M do segmento AB é construtível e as retas perpendiculares a AB passando pelos pontos A, B e M também são construtíveis.

Demonstração: Observemos a figura 3. A circunferência c foi construída com centro em A e passando por B, e a circunferência d tem centro em B e passa por A. A reta s é construtível, pois passa pelos pontos A e B. A partir da operação elementar de intersectar circunferências obtem-se os pontos C e D, bem como intersectando a reta s e as circunferências c e d, respectivamente, obtem-se os pontos E e F. A reta r passa pelos pontos C e D sendo, portanto, uma reta construtível.

Figura 3 – Construção da perpendicular



Fonte: Adaptada de Gonçalves (2017).

Sabemos que c e d possuem o mesmo raio, a saber o segmento AB é raio das duas circunferências. Logo, o quadrilátero $ABCD$ possui os quatro lados congruentes, isto é, tal quadrilátero é um losango. Como as diagonais de um losango intersectam-se no ponto médio de ambas, e são perpendiculares, concluímos que a reta r é mediatriz e, portanto, perpendicular ao segmento AB. Assim, como M é obtido pela intersecção de r e s, temos que M é um ponto construtível.

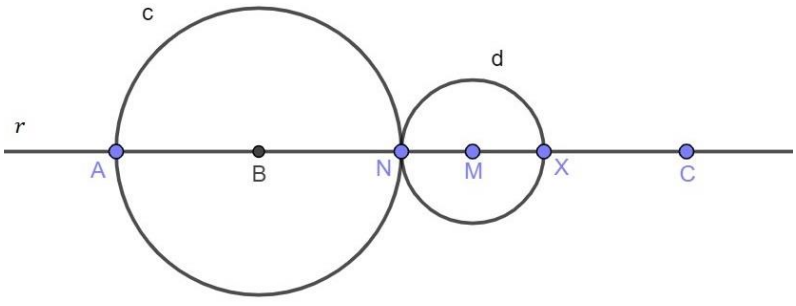
Perceba que A é o ponto médio de EB. Assim, considerando uma circunferência centrada em E e passando por B e outra centrada em B e passando por E, usa-se um raciocínio análogo para mostrar que é construtível a reta perpendicular ao segmento AB passando por A. Da mesma forma, sendo B o ponto

médio de AF, mostra-se que a reta perpendicular ao segmento AB passando por B é também uma reta construtível. ■

Proposição 5.2 (Lema do transporte de segmentos): Sejam A e r, respectivamente, um ponto construtível e uma reta construtível tais que $A \in r$. Se B e C são pontos construtíveis, então existe um ponto construtível X tal que $X \in r$ e os segmentos AX e BC possuem o mesmo comprimento.

Demonstração: A partir de circunferências centradas em B e centradas em A, podemos assumir que A, B e C pertencem a reta r. Considere a figura 4 apresentada abaixo. A circunferência c foi construída com centro em B e passando por A. Seja M o ponto médio de BC e $N \in r$ um ponto construtível tal que $\overline{AB} = \overline{BN}$, ou seja, tais segmentos possuem o mesmo comprimento. Note que a construtibilidade de M segue da proposição 5.1, enquanto que N é construtível por ser obtido pela interseção entre c e r. Considere ainda o ponto $X \in r$ tal que $\overline{NM} = \overline{MX}$. A circunferência d tem centro em M e passa por N. Logo, o ponto X é construtível por ser obtido pela interseção entre d e r. Como M é ponto médio de BC, e $\overline{NM} = \overline{MX}$, então temos que $\overline{AB} = \overline{BN} = \overline{XC}$, e portanto, $\overline{AX} = \overline{BC}$. ■

Figura 4 – Lema do transporte de segmentos

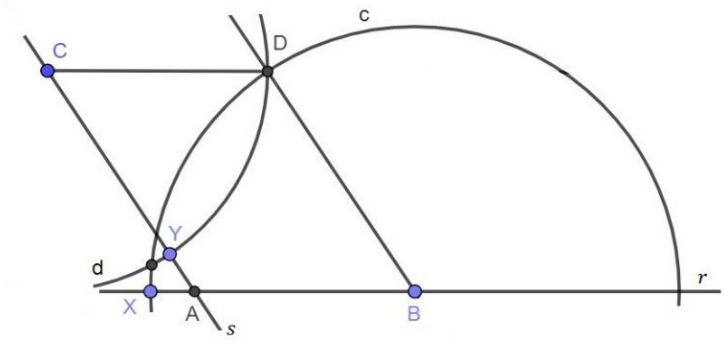


Fonte: Adaptada de Gonçalves (2017).

Proposição 5.3: Sejam A, B e C três pontos construtíveis não alinhados. Então, o único ponto D do plano, tal que A, B, C e D formam um paralelogramo, é construtível. Em particular, a reta passando por C e paralela ao segmento AB é construtível.

Demonstração: Observe a figura 5**.** Consideremos as retas r e s suportes, respectivamente, dos segmentos AB e CA. Aplicando a proposição 5.2 ao ponto $B \in r$, temos que existe um ponto construtível $X \in r$ tal que $\overline{BX} = \overline{AC}$. Mais uma vez pela proposição 5.2, agora aplicada ao ponto $C \in s$, garante-se a existência do ponto construtível $Y \in s$ tal que $\overline{CY} = \overline{AB}$. Considere a circunferência c de centro em B e passando por X, e a circunferência d centrada em C e passando por Y. O ponto D é construtível, pois é obtido pela interseção entre c e d. Note que, por construção, temos $\overline{AB} = \overline{CY} = \overline{CD}$ e $\overline{AC} = \overline{BX} = \overline{BD}$. Logo, o quadrilátero $ABCD$ é um paralelogramo. Em particular, a reta passando por C e paralela ao segmento AB é a reta suporte do segmento CD sendo, portanto, uma reta construtível. ∎

Figura 5 – Construção da paralela

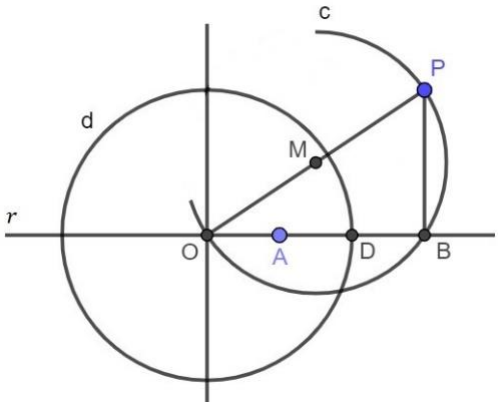


Fonte: Adaptada de Gonçalves (2017).

Proposição 5.4: Um ponto $P = (a, b) \in \mathbb{R}^2$ é construtível se, e somente se, as suas coordenadas $a, b \in \mathbb{R}$ são números construtíveis.

Demonstração: ($\Longrightarrow$) Considere os pontos $O = (0,0)$, $A = (1,0)$ e $P = (a,b) \in \mathbb{R}^2$, onde P é um ponto construtível. Seja M o ponto médio do segmento OP e r a reta suporte do segmento AO. Note que o ponto $B = (a,0)$ é obtido pela interseção entre r e a circunferência c de centro M e que passa por P. Isso decorre do fato do triângulo OPB ser retângulo em B, pois é inscritível em uma semicircunferência de diâmetro OP (veja a figura 6). Um vez obtido o ponto $B = (a,0) \in r$ conseguimos, pela proposição 5.2, determinar o ponto $D = (b,0)$ traçando a circunferência d centrada no ponto $O = (0,0)$ e de raio medindo $\overline{BP}$. Tendo em mente às hipóteses dessa proposição consideraremos o ponto construtível O e a reta construtível r, com $O \in r$, e os pontos construtíveis B e P. Logo, existe o ponto $D \in r$ tal que $\overline{OD} = \overline{BP}$.

Figura 6 – Pontos e coordenadas construtíveis



Fonte: Adaptada de Gonçalves (2017).

($\Longleftarrow$) Suponhamos a e b construtíveis, ou seja, $(a,0)$ e $(b,0)$ são pontos de $\mathcal{P}_\infty$. A reta determinada pelos pontos $O=(0,0)$ e $T=(0,1)$ é construtível. Com efeito, sendo $O(0,0)$ e $A(1,0)$ construtíveis, a proposição 5.1 garante que a reta perpendicular a OA passando por O é construtível. Note que o ponto $T=(0,1)$ pertence a essa reta, pois T é o ponto de interseção entre a referida reta e a circunferência centrada em O que passa por A.

Logo, conseguimos construir $(0,b)$ a partir de $(b,0)$. Assim, pela primeira parte da proposição 5.3, fazendo $D=(a,b)$, segue que é possível construir (a,b) a partir de $(a,0)$ e $(0,b)$. ∎

Diante da proposição 5.4 e do exemplo 5.1 conseguimos concluir que são construtíveis os números reais $-\frac{\sqrt{3}}{2}$, $\frac{1}{2}$ e $\frac{\sqrt{3}}{2}$.

5.2 O corpo dos números construtíveis

Consideremos o conjunto $\mathcal{C}_{\mathbb{R}}=\{a\in\mathbb{R}\,;\,a\ \text{é}\ construtível\}$. A partir da proposição 4.1 mostraremos que $\mathcal{C}_{\mathbb{R}}$ tem estrutura de corpo.

Teorema 5.1: $\mathcal{C}_{\mathbb{R}}=\{a\in\mathbb{R}\,;\,a\ \text{é}\ construtível\}$ é um subcorpo de $\mathbb{R}$ contendo $\mathbb{Q}$.

Demonstração: Já sabemos que $\mathbb{Z}\subset\mathcal{C}_{\mathbb{R}}$. Logo, o zero e a unidade de $\mathbb{R}$ são elementos de $\mathcal{C}_{\mathbb{R}}$. Agora, resta mostrar que:

i) $a,b\in\mathcal{C}_{\mathbb{R}}\implies b-a\in\mathcal{C}_{\mathbb{R}}$

ii) $a, b \in \mathcal{C}_{\mathbb{R}} \implies ab \in \mathcal{C}_{\mathbb{R}}$

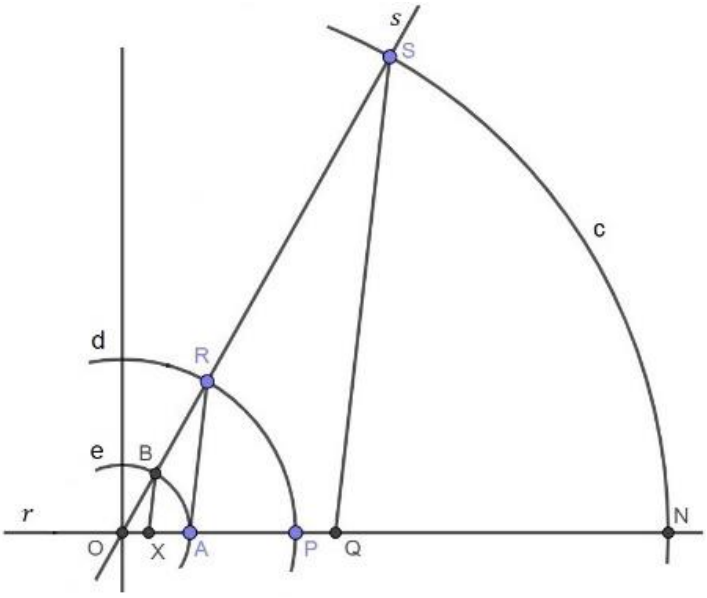
iii) $0 \neq a \in \mathcal{C}_{\mathbb{R}} \implies \frac{1}{a} \in \mathcal{C}_{\mathbb{R}}$.

A fim de provar este teorema, suponhamos, sem perda de generalidade, que tenhamos $b > a > 0$. Assim, temos os pontos construtíveis $P = (a, 0)$ e $Q = (b, 0)$. Considere, ainda, os pontos construtíveis $O = (0, 0)$, $A = (1, 0)$ e a reta r suporte do segmento AO. Note que $P \in r$ e $Q \in r$.

i) Pela proposição 5.2, conseguimos construir um ponto $M \in r$, à direita de O, tal que $\overline{OM} = \overline{PQ}$. Logo, $M = (b - a,\ 0)$ o que mostra que $b - a \in \mathcal{C}_{\mathbb{R}}$. ∎

A figura 7 abaixo auxilia na demonstração dos itens ii) e iii).

Figura 7 – Construção do produto e do inverso multiplicativo



Fonte: Adaptada de Gonçalves (2017).

ii) Observe que existem retas construtíveis passando pelo ponto $O = (0, 0)$, além das retas suportes dos segmentos OA e OT, com $T = (0,1)$. Seja s uma dessas retas. Consideremos os pontos $R, S \in s$ construídos tais que $\overline{OR} = \overline{OP} = a$, e de modo que a reta suporte do segmento SQ seja paralela à reta suporte do segmento AR. Note que os triângulos OAR e OQS são semelhantes. Assim, temos:

$$\frac{\overline{OA}}{\overline{OQ}} = \frac{\overline{OR}}{\overline{OS}} \Longrightarrow \frac{1}{b} = \frac{a}{\overline{OS}} \Longrightarrow \overline{OS} = ab.$$

Seja d a circunferência centrada em O e que passa por P. Tal circunferência é construtível e, consequentemente, o ponto R é construtível pois é interseção de s e d. Assim, como A, R e Q são pontos construtíveis não alinhados, a proposição 5.3 garante que a reta QS é construtível. Dessa forma, obtemos que o ponto S também é construtível, visto que é a interseção de retas construtíveis. Logo, sendo c a circunferência centrada em O que passa por S, temos que o ponto $N(ab, 0)$ é construtível, pois é a interseção de c e r. Portanto, $ab \in \mathcal{C}_{\mathbb{R}}$. ∎

iii) Seja $B \in s$ tal que $\overline{OB} = 1$ e $X \in r$ tal que a reta suporte do segmento BX seja paralela à reta suporte do segmento AR. Assim, os triângulos OXB e OAR são semelhantes. Daí, vêm:

$$\frac{\overline{OX}}{\overline{OA}} = \frac{\overline{OB}}{\overline{OR}} \Longrightarrow \frac{\overline{OX}}{1} = \frac{1}{a} \Longrightarrow \overline{OX} = \frac{1}{a}\ .$$

Ora, com um argumento análogo ao usado na parte ii) da demonstração, mostra-se que $X = \left(\frac{1}{a}, 0\right)$ é um ponto construtível. Portanto, $\frac{1}{a} \in \mathcal{C}_{\mathbb{R}}$. ∎

Por fim, o fato de todo número inteiro ser construtível, aliado a ii) e iii) deste teorema, nos permite concluir que $\mathbb{Q} \subset \mathcal{C}_{\mathbb{R}}$. Com efeito, sendo x e $y \neq 0$ números inteiros, temos que x e $\frac{1}{y}$ são construtíveis, logo o número racional $\frac{x}{y} = x \cdot \frac{1}{y}$ é construtível. ∎

Nota: Diante de algumas ideias até aqui expostas (inclusive a proposição 5.4) temos que $a, b \in \mathcal{C}_{\mathbb{R}} \Leftrightarrow z = a + ib \in \mathcal{P}_{\infty}$. Assim, usando a proposição 4.1, conseguimos mostrar que o conjunto $\mathcal{P}_{\infty}$ dos números complexos construtíveis é um subcorpo de $\mathbb{C}$.

5.3 O critério para construtibilidade de números

Conforme já foi dito, os pontos $O = (0,0)$ e $A = (1,0)$ são aqueles que assumiremos previamente como sendo construtíveis. Além disso, vimos que sendo $\mathcal{P}_0 = \{O, A\},\ \mathcal{P}_1 = [\mathcal{P}_0],\ \mathcal{P}_2 = [\mathcal{P}_1], \cdots, \mathcal{P}_{n+1} = [\mathcal{P}_n],\ \forall\, n \in \mathbb{N}$, temos que:

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

Definição 5.5: Seja $A = (a, b) \in \mathcal{P}_n$. Dizemos que a e b são as coordenadas de A, e denotaremos por $\mathcal{A}_n$ o conjunto das coordenadas de todos os pontos de $\mathcal{P}_n$.

Pela proposição 5.4 sabemos que $\mathcal{A}_n \subset \mathcal{C}_{\mathbb{R}}$, $\forall\, n \in \mathbb{N}$. A partir da noção de adjunção, abordada no capítulo 4, consideremos os seguintes corpos:

$$K_0 = \mathbb{Q},\ K_1 = \mathbb{Q}[\mathcal{A}_1], \cdots,\ K_n = \mathbb{Q}[\mathcal{A}_n], \cdots$$

Como $\mathcal{A}_0 \subset \mathcal{A}_1 \subset \mathcal{A}_2 \subset \cdots \subset \mathcal{A}_n \subset \cdots \subset \mathcal{C}_{\mathbb{R}}$ e $\mathbb{Q} \subset \mathcal{C}_{\mathbb{R}}$, segue das considerações relativas à adjunção que $\mathbb{Q} = K_0 \subset K_1 \subset K_2 \subset \cdots \subset K_n \subset K_{n+1} \subset \cdots \subset \mathcal{C}_{\mathbb{R}}$.

Note que se $\alpha \in \mathcal{C}_{\mathbb{R}}$, então $(\alpha, 0) \in \mathcal{P}_n$ para algum $n \in \mathbb{N}$, isto é, $\alpha \in \mathcal{A}_n$, para algum n, e portanto $\alpha \in K_n$. Assim, concluímos que:

$$K_\infty := \bigcup_{n=0}^{\infty} K_n = \mathcal{C}_{\mathbb{R}}\,.$$

Com essa interpretação de $\mathcal{C}_{\mathbb{R}}$ conseguiremos provar o teorema fundamental desta seção e deste trabalho.

Teorema 5.2: O corpo $\mathcal{C}_{\mathbb{R}}$ é uma extensão algébrica de $\mathbb{Q}$ tal que $\forall\, \alpha \in \mathcal{C}_{\mathbb{R}}$ temos que $[\mathbb{Q}[\alpha] : \mathbb{Q}]$ é uma potência de 2.

Demonstração: Seja $\alpha \in \mathcal{C}_{\mathbb{R}} = \bigcup_{n=0}^{\infty} K_n$. Logo, $\alpha \in K_n = \mathbb{Q}[\mathcal{A}_n]$, para algum $n \in \mathbb{N}$. Assim, $\mathbb{Q} \subset \mathbb{Q}[\alpha] \subset K_n$ e, pelo teorema 4.1, temos que $[K_n : \mathbb{Q}] = [K_n : \mathbb{Q}[\alpha]] \cdot$

$[\mathbb{Q}[\alpha] : \mathbb{Q}]$. Daí concluímos que $[\mathbb{Q}[\alpha] : \mathbb{Q}]$ divide $[K_n : \mathbb{Q}]$. Assim, basta mostrarmos que $[K_n : \mathbb{Q}] = 2^t$, para algum $t \in \mathbb{N}$.

Vamos provar, por indução completa em n, que $[K_n : \mathbb{Q}]$ é uma potência de 2.

Base indução: Se $n = 0$, temos que $K_0 = \mathbb{Q}$ e vale o resultado, pois $[\mathbb{Q} : \mathbb{Q}] = 1 = 2^0$. Se $n = 1$, temos, pelo exemplo 5.1, que $K_1 = \mathbb{Q}[\sqrt{3}]$ e o teorema também é válido, pois os exemplos 4.5 e 4.10 garantem que $\left[\mathbb{Q}[\sqrt{3}] : \mathbb{Q}\right] = 2^1 = 2$.

Passo indutivo: Suponhamos que $[K_i : \mathbb{Q}]$ é uma potência de 2 $\forall\ 0 \leq i < n$, vamos mostrar que $[K_n : \mathbb{Q}]$ é potência de 2. Como $\mathbb{Q} \subset K_{n-1} \subset K_n$, mais uma vez o teorema 4.1 garante que $[K_n : \mathbb{Q}] = [K_n : K_{n-1}] \cdot [K_{n-1} : \mathbb{Q}]$. Como, por hipótese de indução, $[K_{n-1} : \mathbb{Q}]$ é uma potência de 2, então basta provarmos que $[K_n : K_{n-1}]$ também é uma potência de 2.

Seja $L_0 = K_{n-1}$ e $L = K_n$. Sabemos que $L = L_0[\mathcal{A}_n]$. Sendo $\mathcal{A}_n = \{\alpha_1, \cdots, \alpha_k\}$, temos que $L = L_0[\alpha_1, \cdots, \alpha_k]$. Denotemos $L_0 \subset L_1 = L_0[\alpha_1] \subset L_2 = L_1[\alpha_2] \subset \cdots \subset L_i = L_{i-1}[\alpha_i] \subset \cdots \subset L_k = L$. Assim, outra vez pelo teorema 4.1, é bastante mostrarmos que $[L_i : L_{i-1}]$ é potência de 2. Com efeito, mostraremos que $[L_i : L_{i-1}] = 1$ ou 2, com $1 \leq i \leq k$, $L_i = L_{i-1}[\alpha_i]$ e $\alpha_i \in \mathcal{A}_n$. Daí, existe $\beta_i \in \mathcal{A}_n$ tal que $A_i = (\alpha_i, \beta_i) \in \mathcal{P}_n$ ou $B_i = (\beta_i, \alpha_i) \in \mathcal{P}_n$. Suponhamos, sem perda de generalidade, que $A_i = (\alpha_i, \beta_i) \in \mathcal{P}_n$.

Do fato de termos $\mathcal{P}_n = [\mathcal{P}_{n-1}]$ segue que $A_i = (\alpha_i, \beta_i)$ é obtido por uma das três operações elementares em $\mathcal{P}_{n-1}$ que mencionamos no início desta seção. Logo, tendo em mente conhecimentos básicos da geometria analítica sabemos que α_i terá que satisfazer uma equação algébrica de grau menor ou igual a 2 com coeficientes sobre o corpo $K_{n-1} = \mathbb{Q}[\mathcal{A}_{n-1}]$, uma vez que equações de retas tem grau 1 e equações de circunferências tem grau 2.

Assim, como $K_{n-1} = L_0 \subset L_{i-1}$, com $1 \leq i \leq k$, segue α_i é raiz de um polinômio de grau 1 ou 2 sobre o corpo L_{i-1}. Portanto, $[L_i : L_{i-1}] = 1$ ou 2. ∎

Nota: Em parte, a interpretação deste importante teorema é “todo número construtível é algébrico”. A contrapositiva dessa afirmação nos diz que “todo número transcendente não é construtível”.

5.4 A impossibilidade da duplicação do cubo

Conforme já nos foi introduzido, o problema da duplicação do cubo pode ser formulado como abaixo:

"Dada a aresta de um cubo queremos construir, com régua e compasso, a aresta de um cubo que tenha o dobro do volume do cubo cuja aresta é dada".

Analisaremos o caso particular em que a medida da aresta dada é igual a 1. Mostraremos que não existe $\alpha \in \mathcal{C}_{\mathbb{R}}$, tal que o volume do cubo de aresta α seja o dobro do volume do cubo de aresta 1. Ora, $\alpha^3 = 2 \Longrightarrow \alpha = \sqrt[3]{2}$. Assim, pelo exemplo 4.13, temos que $irr(\alpha, \mathbb{Q}) = x^3 - 2$. Logo, da proposição 4.5 segue que $[\mathbb{Q}[\alpha] : \mathbb{Q}] = 3$ e, pelo teorema 5.2, concluímos que α não é construtível. ∎

5.5 A impossibilidade da quadratura do círculo

O problema da quadratura do círculo, o mais famoso dos problemas gregos de construções com régua e compasso, se formula como se segue:

"*Dado um círculo, construir com régua e compasso o lado de um quadrado cuja área seja igual à área do círculo dado".*

Para mostrar que o círculo não é quadrável, analisaremos o caso em que o raio do círculo mede 1. Nesse caso, mostraremos que não existe $\alpha \in \mathcal{C}_{\mathbb{R}}$, tal que a área do quadrado de lado α seja igual a área do círculo de raio 1. Façamos $\alpha^2 = \pi$. Como $\mathcal{C}_{\mathbb{R}}$ tem estrutura de corpo, sabemos que α construtível $\Longrightarrow \alpha^2$ construtível. Um vez que π é transcendente, o teorema 5.2 garante que α^2 não é construtível. Portanto, α não é construtível. ∎

5.6 A impossibilidade da trissecção do ângulo

Trissectar um ângulo, como é bastante intuitivo, significa dividir o ângulo em três ângulos congruentes. O problema da trissecção do ângulo pode ser formulado como segue:

"Dado um ângulo θ, queremos trissectá-lo com régua e compasso".

A fim de mostrarmos que não existe uma construção que valha em todos os casos, provaremos a impossibilidade de trissectar o ângulo de medida $\frac{\pi}{3}\ rad$. Antes disso, mostraremos alguns resultados preliminares.

Proposição 5.5: Seja $\theta \in \mathbb{R}$. Assim, $cos\,(3\theta) = 4cos^3\theta - 3cos\theta$.

Demonstração: A partir de alguns conhecimentos de trigonometria, tais quais: soma de arcos, arco duplo e relação fundamental da trigonometria, temos que:

$$\begin{aligned} cos\,(3\theta) = cos(2\theta + \theta) &= cos2\theta cos\theta - sen2\theta sen\theta \\ &= (cos^2\theta - sen^2\theta)cos\theta - (2sen\theta cos\theta)sen\theta \\ &= cos^3\theta - sen^2\theta cos\theta - 2sen^2\theta cos\theta = cos^3\theta - 3sen^2\theta cos\theta \\ &= cos^3\theta - 3(1 - cos^2\theta)cos\theta = cos^3\theta - 3cos\theta + 3cos^3\theta \\ &= 4cos^3\theta - 3cos\theta. \blacksquare \end{aligned}$$

Proposição 5.6: O polinômio $p(x) = 8x^3 - 6x - 1$ é irredutível sobre $\mathbb{Q}$.

Demonstração: A fim de verificar a irredutibilidade de $p(x)$ não conseguimos usar diretamente o critério de Eisenstein, todavia, conforme já comentamos na proposição 3.4, podemos fazer a substituição $x = y - 1$. Nesse caso, temos que

$$p(x) \text{ é irredutível em } \mathbb{Q}[x] \Leftrightarrow p(y) \text{ é irredutível em } \mathbb{Q}[y]$$

(basta substituir $y = x + 1$ em qualquer fatoração de $p(y)$). Assim, temos:

$$p(y) = 8(y-1)^3 - 6(y-1) - 1 = 8(y^3 - 3y^2 + 3y - 1) - 6(y-1) - 1$$
$$= 8y^3 - 24y^2 + 24y - 8 - 6y + 6 - 1 = 8y^3 - 24y^2 + 18y - 3\,.$$

Considerando o primo $p = 3$, temos que $3 \nmid 8,\ 3|-24,\ 3|18,\ 3|-3$ e $9 \nmid -3$. Assim, pelo critério de Eisenstein, temos que $p(y)$ é irredutível em $\mathbb{Q}[y]$. Portanto, $p(x)$ é irredutível sobre $\mathbb{Q}$. ∎

Proposição 5.7: $\alpha = cos\,\frac{\pi}{9}$ não é construtível.

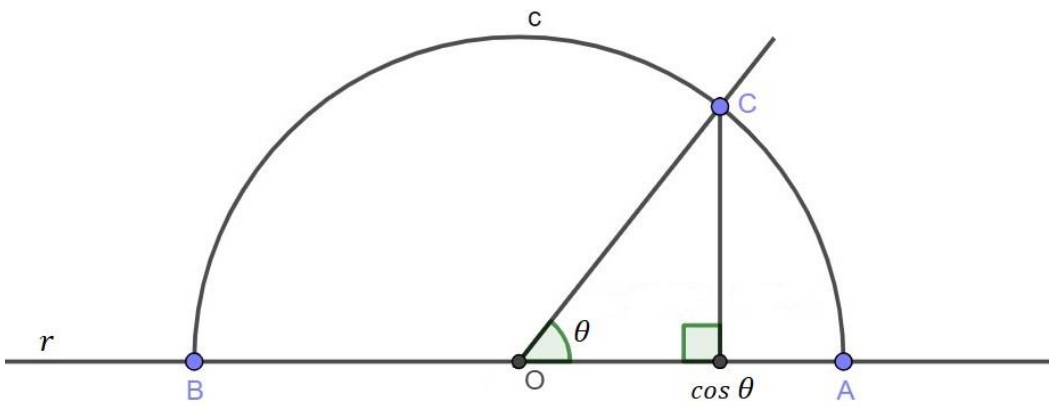
Demonstração: Se $\theta = \frac{\pi}{9}\ rad$, então $3\theta = \frac{\pi}{3}\ rad$. Daí, pela proposição 5.5, temos que:

$$\frac{1}{2} = cos\,3\theta = 4cos^3\theta - 3cos\theta \implies 8cos^3\theta - 6cos\theta - 1 = 0\ .$$

Logo, $\alpha = cos\,\frac{\pi}{9}$ é raiz do polinômio $p(x) = 8x^3 - 6x - 1$. Assim, como o polinômio $p(x) = 8x^3 - 6x - 1$ é irredutível sobre $\mathbb{Q}$, segue da proposição 4.5 que $[\mathbb{Q}[\alpha] : \mathbb{Q}] = 3$ e, pelo teorema 5.2, concluímos que α não é construtível. ∎

Definição 5.6: Um ângulo θ é construtível se, e somente se, seu cosseno for construtível (veja a figura 8, onde $O = (0,0)$ e $A = (1,0)$).

Figura 8 – Definição de ângulo construtível



Fonte: Elaborada pelo autor.

Exemplo 5.2: O ângulo de 60° é construtível, pois $cos\ 60° = \frac{1}{2}$ é racional e, portanto, construtível.

Por fim, mostraremos que não é possível trissectar o ângulo de medida $\frac{\pi}{3}\ rad$. Basta mostrar que $\theta = \frac{\pi}{9}\ rad$ não é construtível. Ora, caso θ fosse construtível, então $\alpha = cos\ \frac{\pi}{9}$ seria construtível, o que contraria a proposição 5.7. ∎

Exemplo 5.3: Note que o ângulo de medida $\theta = \frac{\pi}{2}\ rad$ pode ser trissectado. De fato, $cos\ \frac{\pi}{6} = \frac{\sqrt{3}}{2}$ é construtível. Para ter acesso aos passos necessários para trissectar um ângulo reto com régua e compasso ver o apêndice A.

6 CONSIDERAÇÕES FINAIS

No presente trabalho realizamos uma abordagem sobre três interessantes problemas de construção geométrica concebidos na Grécia Antiga. Por serem intrigantes, estes problemas desafiaram diversas gerações de matemáticos. A grande busca, sem sucesso, para solucioná-los levantou a suspeita de que eram construções impossíveis de serem executadas. Em linhas gerais, nos dedicamos a demonstrar que de fato são problemas impossíveis de serem solucionados, levando em conta as condições impostas de que se deveria usar apenas uma régua não graduada e um compasso, sendo também preestabelecido o que era permitido executar com estes instrumentos.

Acreditamos que os objetivos propostos para este trabalho foram alcançados uma vez que conseguimos desenvolver uma álgebra de polinômios, atrelada à conceitos relativos aos corpos e à álgebra linear, o que tornou possível provar as impossibilidades anteriormente mencionadas. Além disso, pudemos aprofundar os conceitos relativos às construções, destacando o que são pontos e números construtíveis, mostrando alguns importantes resultados sobre ambos, e provando que conseguimos obter um corpo formado por todos os números ditos construtíveis.

Embora o trabalho tenha, em boa parte, versado sobre conceitos algébricos, não tendo se dedicado a realizar as diversas construções possíveis com régua e compasso, acreditamos que esta pesquisa possa estimular os(as) professores(as) a vislumbrarem nas construções geométricas uma ferramenta para suas aulas de geometria plana. Dessa forma, tendo em vista as oportunidades geradas pelo Novo Ensino Médio, acreditamos que as construções geométricas com régua e compasso, além de serem utilizadas nas aulas regulares de matemática, possam também ser pautadas por componentes da parte diversificada dos currículos, sendo ofertadas disciplinas eletivas que tratem da abordagem do aprendizado da geometria plana sob a ótica das construções, envolvendo também a construtibilidade de números. Assim, consideramos que os(as) estudantes estarão tendo contato com uma gama de propriedades das figuras geométricas, bem como buscando aplicar teoremas e relações métricas durante o processo de desenvolvimento das estratégias para realizar tais construções, o que favorece diretamente o processo de aprendizagem.

Tendo em vista estas conclusões, surgem oportunidades para futuros trabalhos. Deixaremos aqui a sugestão de realizar-se uma pesquisa sobre os efeitos

que uma disciplina eletiva que aborde construções geométricas com régua e compasso, desde as mais simples até as mais sofisticadas, pode ter sobre os níveis de aprendizagem dos conceitos geométricos por parte do alunado. Desta forma, teríamos um importante material para subsidiar os(as) docentes de matemática que optarem por ministrar suas aulas sob a perspectiva das construções, bem como contribuiria com a promoção e expansão desta prática de ensino, uma vez que acreditamos que uma pesquisa nestes moldes obteria resultados positivos, a partir das diversas atividades práticas que seriam destinadas aos estudantes.

REFERÊNCIAS BIBLIOGRÁFICAS

BOLDRINI, José Luiz *et al*. **Álgebra linear**. 3. ed. São Paulo: Harper & Row do Brasil, 1980.

EVES, Howard. **Introdução à história da matemática**. 5. ed. Campinas: Editora da Unicamp, 2011.

GONÇALVES, Adilson. **Introdução à álgebra**. 6. ed. Rio de Janeiro: Instituto de Matemática Pura e Aplicada, 2017.

HEFEZ, Abramo; VILLELA, Maria Lúcia Torres. **Polinômios e equações algébricas**. Rio de Janeiro: Sociedade Brasileira de Matemática, 2012.

HEFEZ, Abramo; FERNANDEZ, Cecília de Souza. **Introdução à álgebra linear**. Rio de Janeiro: Sociedade Brasileira de Matemática, 2012.

WAGNER, Eduardo. **Construções geométricas**. 6. ed. Rio de Janeiro: Sociedade Brasileira de Matemática, 2007.

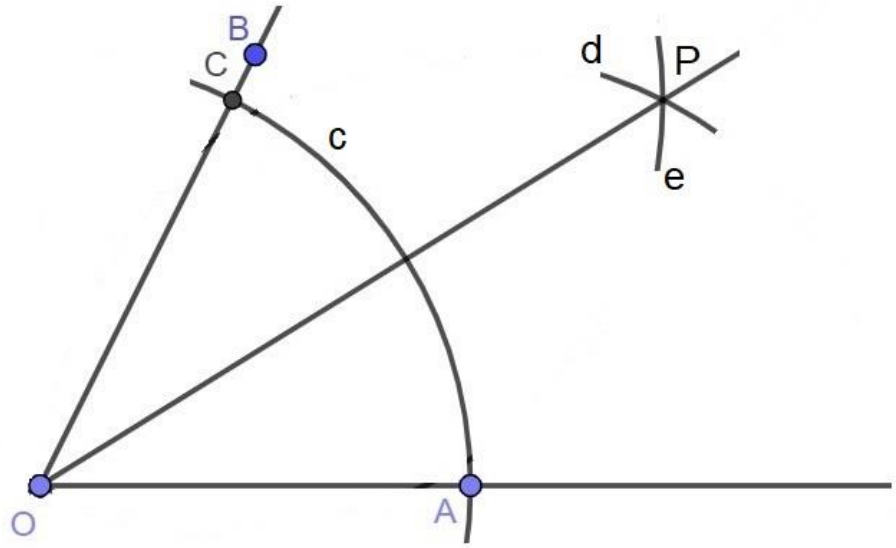
SKOPENKOV, Arkadiy. Yet another proof from The book: the Gauss theorem on regular polygons. **Math.HO**, New York, Cornell University, n. 5, p. 1-5, 2011. https://doi.org/10.48550/arXiv.0908.2029.

APÊNDICE A - SOBRE A TRISSECÇÃO DO ÂNGULO

Tendo em vista o problema da trissecção do ângulo, afirmamos que é possível bissectar qualquer ângulo (dividir esse ângulo em dois ângulos congruentes) utilizando uma régua não graduada e um compasso. De fato, dados três pontos A, B e O, conforme a figura 9, a fim de bissectar o ângulo $A\hat{O}B$, precisamos seguir os seguintes passos:

1. Traça-se uma circunferência c de centro O e que passa pelo ponto A. Suponhamos que essa circunferência intersecta o lado OB do ângulo $A\hat{O}B$ no ponto C.
2. Traçam-se duas circunferências: a circunferência d (com centro em A e que passa pelo ponto O) e a circunferência e (com centro em C e que passa por O) de modo que essas duas circunferências possuam P como um dos pontos de interseção.

Figura 9 – Bissecção do ângulo



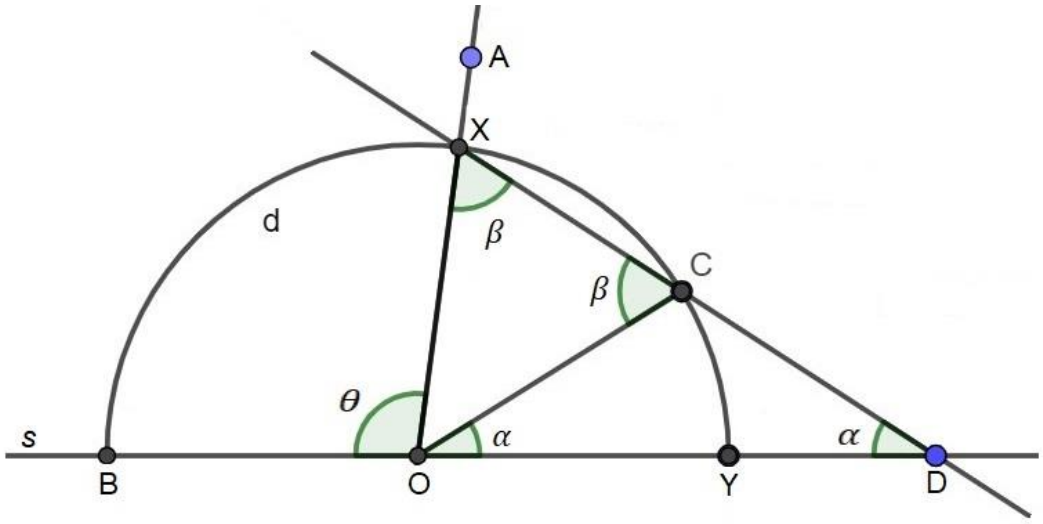
Fonte: Adaptada de Wagner (2007).

A semirreta $\overrightarrow{OP}$ é a bissetriz do ângulo $A\hat{O}B$. Com efeito, por construção, os triângulos OAP e OCP são congruentes (caso lado – lado – lado), pois $\overline{OA} = \overline{OC}$, $\overline{AP} = \overline{CP}$ e OP é lado comum aos dois triângulos. Portanto, $C\hat{O}P = A\hat{O}P$. ∎

Conforme demonstramos no capítulo 5, em geral, não é possível trissectar um ângulo utilizando uma régua não graduada e um compasso, todavia, se considerarmos uma régua com marcas indicando segmentos de comprimento iguais a r, é possivel trissectar um ângulo qualquer de medida θ.

Sejam A, O, X e Y pontos, conforme a figura 10, onde $\overline{OX} = \overline{OY} = r$. Consideremos, ainda, a reta s que passa por O e Y e a circunferência d centrada em O e que passa por X, de tal maneira que $d \cap s = \{B, Y\}$. Seja θ a medida do ângulo $A\hat{O}B$. Mostraremos que é possível marcar os pontos $C \in d$ e $D \in s$ de tal maneira que $\overline{CD} = r$. Com efeito, mantendo uma extremidade da régua no ponto X, temos que a distância entre pontos alinhados com X, um sobre a circunferência d e o outro sobre a reta s, varia de zero (quando esses pontos coincidem com Y) até ∞ (no caso em que a régua passando por X está paralela à reta s). Assim, por continuidade, existem os pontos C e D com a propriedade desejada.

Figura 10 – Trissecção do ângulo com régua graduada



Fonte: Adaptada de Gonçalves (2017).

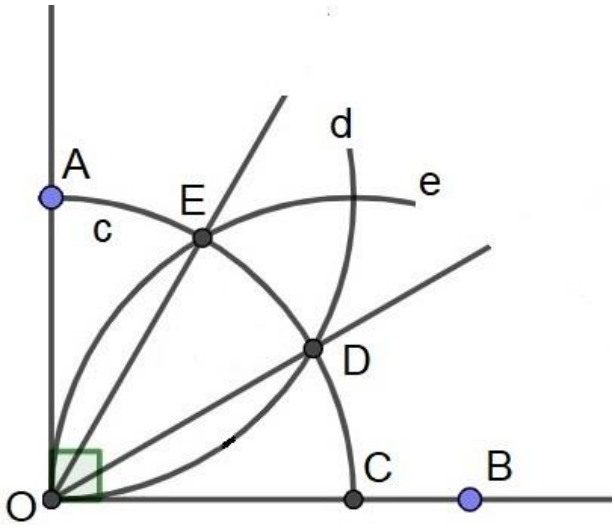
Sejam α e β, respectivamente, as medidas dos ângulos $C\hat{O}Y$ e $O\hat{C}X$. Vamos provar que $\alpha = \frac{\theta}{3}$. De fato, pelo teorema do ângulo externo aplicado aos triângulos XOD e COD, temos, respectivamente, que $\theta = \alpha + \beta$ e $\beta = 2\alpha$. Portanto, $\theta = 3\alpha$. ∎

De acordo com o exemplo 5.3, embora não valha o caso geral, é possível trissectar o ângulo reto usando uma régua não graduada e um compasso. Terminaremos esse apêndice executando essa construção.

Sejam A, B e O pontos, conforme a figura 11, de modo que o ângulo $A\hat{O}B$ seja reto. A fim de trissectar o ângulo $A\hat{O}B$ precisamos seguir os seguintes passos:

1. Traça-se a circunferência c de centro O e que passa por A. Suponha que essa circunferência intersecta o lado OB do ângulo reto no ponto C.
2. Traçam-se duas circunferências: a circunferência d (com centro em A e que passa pelo ponto O) e a circunferência e (com centro em C e que passa por O) de modo que um dos pontos de interseção entre c e d seja D e um dos pontos de interseção entre c e e seja E.

Figura 11 – Trissecção do ângulo reto



Fonte: Elaborada pelo autor.

Afirmamos que as semirretas $\overrightarrow{OD}$ e $\overrightarrow{OE}$ dividem o ângulo reto em três ângulos conguentes. De fato, por construção, temos que $\overline{OA} = \overline{OD} = \overline{AD}$. Logo, o triângulo OAD é equilátero. Assim, o ângulo $A\hat{O}D$ mede 60°. Daí, concluímos que o ângulo $D\hat{O}C$ mede 30°. Analogamente, conseguimos mostrar que o triângulo EOC é equilátero donde concluímos que o ângulo $A\hat{O}E$ mede 30°. Portanto, temos que as medidas dos ângulos $A\hat{O}E$, $E\hat{O}D$ e $D\hat{O}C$ são todas iguais a 30°. ∎

APÊNDICE B - SOBRE A CONSTRUTIBILIDADE DE POLÍGONOS REGULARES

Apresentaremos ao longo deste apêndice resultados importantes sobre a construtibilidade dos polígonos regulares. Para um bom entendimento do que segue, principalmente da demonstração do Teorema de Gauss-Wantzel, é ideal que o leitor domine alguns conceitos sobre o corpo dos números complexos, sobre algumas estruturas algébricas e sobre alguns resultados de aritmética.

Um polígono diz-se construtível se todos os seus vértices são pontos construtíveis de $\mathbb{R}^2$. Assim, concluímos que um polígono regular de n lados é construtível se, e somente se, o ponto $A_n = \left(cos\frac{2\pi}{n},\ sen\frac{2\pi}{n}\right)$ é um ponto construtível de $\mathbb{R}^2$. Note que o ponto $A_4 = \left(cos\frac{2\pi}{4},\ sen\frac{2\pi}{4}\right) = \left(cos\frac{\pi}{2},\ sen\frac{\pi}{2}\right) = (0,1)$ é construtível, pois suas coordenadas são números inteiros. Logo, o polígono regular de 4 lados (quadrado) é construtível.

Nota: Inicialmente, perceba que o polígono regular de n lados é construtível se, e somente se, a raíz n –ésima da unidade $\xi_n = e^{\frac{2\pi i}{n}}$ é construtível.

Nota: Os números $F_s = 2^{2^s} + 1$, com $s \in \mathbb{N} \cup \{0\}$, são chamados de **números de Fermat**. Os números de Fermat que são primos são chamamos de **primos de Fermat**. Os únicos primos de Fermat conhecidos são $F_0 = 3$, $F_1 = 5$, $F_2 = 17$, $F_3 = 257$ e $F_4 = 65537$.

Proposição: Valem os seguintes resultados:

i) Todo polígono regular de $n = 2^k$ lados é construtível.

ii) Se um polígono regular de n lados é construtível, então o polígono regular de $2n$ lados também é construtível.

iii) Seja $p \geq 3$ um número primo. Se um polígono regular de p lados é construtível, então existe $s \in \mathbb{N} \cup \{0\}$ tal que $p = 2^{2^s} + 1$. Ou seja, um polígono com um número primo p de lados, que não é primo de Fermat, não é construtível com régua e compasso. Em particular, o heptágono regular não é um polígono construtível.

Demonstração:

As provas de i) e ii) seguem diretamente dos seguintes fatos:

- O quadrado é um polígono construtível;
- É possível bissectar um ângulo qualquer com régua e compasso.

Agora vamos provar iii). Ora, por hipótese, $\left(cos\frac{2\pi}{p},\ sen\frac{2\pi}{p}\right)$ é construtível. Logo, do teorema 5.2, segue que $[\mathbb{Q}[\alpha,\beta]:\mathbb{Q}]=2^m$ onde $\alpha=cos\frac{2\pi}{p}$ e $\beta=\ sen\frac{2\pi}{p}$. Além disso, se $i=\sqrt{-1}$, temos que $[\mathbb{Q}[\alpha,\beta,i]:\mathbb{Q}]=2^{m+1}$ onde $\mathbb{Q}[\alpha,\beta,i]\subset\mathbb{C}$. Assim, concluímos que $\xi_p=\ cos\frac{2\pi}{p}+i\ sen\frac{2\pi}{p}=\ \alpha+i\beta\ \in\ \mathbb{Q}[\alpha,\beta,i]$. Daí, segue que $\mathbb{Q}[\xi_p]\ \subset\mathbb{Q}[\alpha,\beta,i]$ e $[\mathbb{Q}[\xi_p]:\mathbb{Q}]=\ 2^r$ para algum $r\in\mathbb{N}$. Sabemos, pela proposição 3.4, que o polinômio $f(x)=\ x^{p-1}+x^{p-2}+\cdots+x+1$ é irredutível sobre $\mathbb{Q}$. Ademais, não é dificil mostrar que esse polinômio f se anula em $\xi_p=\ cos\frac{2\pi}{p}+i\ sen\frac{2\pi}{p}$. Logo, pela proposição 4.3, temos que $irr(\xi_p,\mathbb{Q})=\ x^{p-1}+\ x^{p-2}+\cdots+x+1$. Daí, da proposição 4.5, segue que $p-1=\ 2^r\Longrightarrow p=\ 2^r+1$. Resta provar que $r=\ 2^s$ para algum $s\in\mathbb{N}$. Suponha que $t>1$ é um fator ímpar de r. Logo, temos que $r=tv$. Daí, segue que

$$p=\ 2^r+1=\ (2^v)^t+1=(2^v+1)((2^v)^{t-1}-\ (2^v)^{t-2}+\ (2^v)^{t-3}-\ \cdots\pm 1),$$

contradizendo o fato de p ser primo. O que finaliza a demonstração. ∎

O teorema a seguir estabelece uma condição necessária e suficiente para que um polígono regular de n lados seja construtível.

Teorema (Gauss-Wantzel): Um polígono regular de n lados é construtível se, e somente se, $n=\ 2^r\cdot\ p_1\cdot\cdots\cdot\ p_k$ onde $r\in\mathbb{N}\cup\{0\}$ e $p_1,\ \cdots,\ p_k$ são distintos primos de Fermat , ou seja cada p_i é um primo ímpar da forma $p_i=\ 2^{2^{s_i}}+1$ com $1\leq i\leq k$ e $s_i\in\mathbb{N}\cup\{0\}$.

Demonstração:

($\Longrightarrow$) Primeiramente, mostraremos que se um polígono regular de n lados é construtível, então n se escreve como produto de uma potência de dois e primos de Fermat distintos. Dividiremos a demonstração da primeira implicação em três passos:

1° passo: mostraremos que o polinômio $f(x) = x^{p(p-1)} + x^{p(p-2)} + \cdots + x^p + 1$, onde p é um número primo, é irredutível em $\mathbb{Q}[x]$.

Essa demonstração segue a mesma ideia da usada nas proposições 3.4 e 5.6, a saber: usaremos o critério de Eisenstein para mostrar que é irredutível o polinômio

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

Note que,

$$(x+1)^{p(p-j)} = ((x+1)^p)^{p-j} = (x^p + 1 + pxg(x))^{p-j} = (x^p+1)^{p-j} + pxg_j(x),$$

onde $xg_j(x)$ é um polinômio de grau menor do que $p(p-j)$, sem termo constante. Logo,

$$\begin{aligned}
(x+1)^{p(p-1)} &= \binom{p-1}{0}x^{p(p-1)} + \binom{p-1}{1}x^{p(p-2)} + \binom{p-1}{2}x^{p(p-3)} + \cdots + \binom{p-1}{p-2}x^p + 1 + pxg_1(x)\\
(x+1)^{p(p-2)} &= \binom{p-2}{0}x^{p(p-2)} + \binom{p-2}{1}x^{p(p-3)} + \cdots + \binom{p-2}{p-3}x^p + 1 + pxg_2(x)\\
(x+1)^{p(p-3)} &= \binom{p-3}{0}x^{p(p-3)} + \cdots + \binom{p-3}{p-4}x^p + 1 + pxg_3(x)\\
&\vdots \qquad\qquad\qquad\qquad\qquad\qquad \vdots\\
(x+1)^p &= \binom{1}{0}x^p + 1 + pxg_{p-1}(x)
\end{aligned}$$

Pela identidade das diagonais do triângulo de Pascal

$$\binom{n}{0} + \binom{n+1}{1} + \cdots + \binom{n+m}{m} = \binom{n+m+1}{m},$$

temos que:

$$\binom{p-1}{1}+\binom{p-2}{0}=\binom{p}{1};$$

$$\binom{p-1}{2}+\binom{p-2}{1}+\binom{p-3}{0}=\binom{p}{2};$$

$$\vdots$$

$$\binom{p-1}{p-2}+\binom{p-2}{p-3}+\cdots+\binom{1}{0}=\binom{p}{p-2};$$

Ora, todos os números binomiais nos segundos membros das igualdades acima são múltiplos de p. Logo, teremos que:

$$f(x+1)=x^{p(p-1)}+p+pxh(x),$$

onde $xh(x)$ é um polinômio de grau menor do que $p(p-1)$, sem termo constante. Portanto, pelo critério de Eisenstein, o polinômio $f(x+1)$ é irredutivel, assim o polinômio $f(x)$ é irredutível em $\mathbb{Q}[x]$. ∎

2° passo: Agora mostraremos que se p é um número primo maior do que 2, então o polígono regular de p^2 lados não é construtível.

Ora, sabemos que uma raiz p^2 – ésima primitiva ξ da unidade é raíz do polinômio

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

que sabemos, pelo 1° passo, ser irredutível em $\mathbb{Q}[x]$. Logo, o grau de ξ sobre $\mathbb{Q}$ é igual a $p(p-1)$, que não é uma potência de 2. ∎

3° passo: Por fim, completaremos a demonstração da referida implicação. Inicialmente, perceba que se um polígono de n lados é construtível, então um polígono de m lados (com m divisor de n) também o é. Consideremos $n=2^r\cdot p_1\cdot\cdots\cdot p_k$, com $p_s>2$ e $s=1,\cdots,k$, a decomposição de n em fatores primos. Se algum dos p_s não for primo de Fermat, o polígono de n lados não é construtível, pois, caso contrário,

o polígono de p_s lados seria construtível (pois p_s é um divisor de n), o que contradiz o item iii) da proposição que provamos neste apêndice. Ademais, os primos dessa fatoração devem ser distintos, pois se tivermos $p_i = p_j$, para algum par de i e j distintos, o polígono de n lados não é construtível, pois, caso contrário, o polígono de p_i^2 lados seria construtível, o que contradiz o resultado obtido no 2° passo. ∎

($\Longleftarrow$) Para a volta, começamos observando que todo polígono regular de $n = 2^k$ lados é construtível (com $k \geq 2$). Além disso, se os polígonos regulares de m e n lados são construtíveis, com m e n primos entre si, então o polígono regular de mn lados é construtível. De fato, a partir de um resultado de aritmética (Teorema de Bachet-Bézout) temos que existem inteiros x e y tais que $mx + ny = 1$. Assim, temos:

$$mx + ny = 1 \implies \frac{x}{n} + \frac{y}{m} = \frac{1}{mn}$$

Daí, sendo $\mathcal{P}_\infty$ o corpo dos números complexos construtíveis, temos que:

$$e^{\frac{2\pi i}{mn}} = \left(e^{2\pi i}\right)^{\frac{x}{n} + \frac{y}{m}} = \left(e^{\frac{2\pi i}{n}}\right)^x \cdot \left(e^{\frac{2\pi i}{m}}\right)^y \in \mathcal{P}_\infty.$$

Para concluir a demonstração do teorema precisamos mostrar que um polígono regular de p lados, onde $p = 2^{2^s} + 1$ com $s \in \mathbb{N} \cup \{0\}$, é construtível. Primeiramente, segue da possibilidade de bissectar um ângulo que $\xi_{p-1} \in \mathcal{P}_\infty$. Seja, g uma raiz primitiva $mod\, p$. Isto posto, definimos, para cada $r = 0, 1, \cdots, p-2$, o seguinte polinômio:

$$T_r(x) := x + {\xi_{p-1}}^r x^g + {\xi_{p-1}}^{2r} x^{g^2} + \cdots + {\xi_{p-1}}^{(p-2)r} x^{g^{p-2}} \in \mathbb{Z}\left[\xi_{p-1}\right][x] \subset \mathcal{P}_\infty$$

Agora, precisamos mostrar três fatos. Por isso, concluiremos nossa demonstração seguindo três passos:

1° passo: Mostraremos que $\xi_p = \frac{T_0(\xi_p) + T_1(\xi_p) + \cdots + T_{p-2}(\xi_p)}{p-1}$. De fato, desenvolvendo as parcelas temos que:

$$T_0(\xi_p) = \xi_p + {\xi_{p-1}}^0 {\xi_p}^g + {\xi_{p-1}}^0 {\xi_p}^{g^2} + \cdots + {\xi_{p-1}}^0 {\xi_p}^{g^{p-2}} = \xi_p + {\xi_p}^g + {\xi_p}^{g^2} + \cdots + {\xi_p}^{g^{p-2}}.$$

$$T_1(\xi_p) = \xi_p + \xi_{p-1}{\xi_p}^g + {\xi_{p-1}}^2 {\xi_p}^{g^2} + \cdots + {\xi_{p-1}}^{p-2} {\xi_p}^{g^{p-2}}.$$

$$T_2(\xi_p) = \xi_p + {\xi_{p-1}}^2 {\xi_p}^g + {\xi_{p-1}}^4 {\xi_p}^{g^2} + \cdots + {\xi_{p-1}}^{(p-2).2} {\xi_p}^{g^{p-2}}.$$

$$\vdots$$

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

Daí, temos que:

$$T_0(\xi_p) + T_1(\xi_p) + \cdots + T_{p-2}(\xi_p) = \xi_p(p-1) + \left({\xi_p}^g + \xi_{p-1}{\xi_p}^g + {\xi_{p-1}}^2 {\xi_p}^g + \cdots + {\xi_{p-1}}^{p-2} {\xi_p}^g\right) + \left({\xi_p}^{g^2} + {\xi_{p-1}}^2 {\xi_p}^{g^2} + {\xi_{p-1}}^4 {\xi_p}^{g^2} + \cdots + {\xi_{p-1}}^{(p-2).2} {\xi_p}^{g^2}\right) + \cdots + \left({\xi_p}^{g^{p-2}} + {\xi_{p-1}}^{p-2} {\xi_p}^{g^{p-2}} + {\xi_{p-1}}^{(p-2).2} {\xi_p}^{g^{p-2}} + \cdots + {\xi_{p-1}}^{(p-2).(p-2)} {\xi_p}^{g^{p-2}}\right).$$

Agora, perceba que ${\xi_p}^g + \xi_{p-1}{\xi_p}^g + {\xi_{p-1}}^2 {\xi_p}^g + \cdots + {\xi_{p-1}}^{p-2} {\xi_p}^g$ é a soma dos $p-1$ primeiros termos de uma progressão geométrica cuja razão é ξ_{p-1}. Logo,

$$\begin{aligned} {\xi_p}^g + \xi_{p-1}{\xi_p}^g + {\xi_{p-1}}^2 {\xi_p}^g + \cdots + {\xi_{p-1}}^{p-2} {\xi_p}^g &= \frac{{\xi_p}^g\left({\xi_{p-1}}^{p-1} - 1\right)}{\xi_{p-1} - 1} \\ &= \frac{{\xi_p}^g\left(\xi_{p-1} - 1\right)\left({\xi_{p-1}}^{p-2} + {\xi_{p-1}}^{p-3} + \cdots + \xi_{p-1} + 1\right)}{\xi_{p-1} - 1} \end{aligned}$$

Ora, ${\xi_{p-1}}^{p-2} + {\xi_{p-1}}^{p-3} + \cdots + \xi_{p-1} + 1 = 0$. Logo, ${\xi_p}^g + \xi_{p-1}{\xi_p}^g + {\xi_{p-1}}^2 {\xi_p}^g + \cdots + {\xi_{p-1}}^{p-2} {\xi_p}^g = 0$.

De maneira análoga, mostra-se que as somas de todos os outros parênteses é zero. Portanto,

$$T_0(\xi_p) + T_1(\xi_p) + \cdots + T_{p-2}(\xi_p) = \xi_p(p-1) \implies \xi_p = \frac{T_0(\xi_p) + T_1(\xi_p) + \cdots + T_{p-2}(\xi_p)}{(p-1)} \blacksquare$$

A partir dessa demonstração, a fim de mostrar que ξ_p é construtível basta provar que $T_r(\xi_p)$ é construtível para todo $r \in \{0, 1, \cdots, p-2\}$.

2° passo: Mostraremos que $T_r(x^g) \equiv {\xi_{p-1}}^{-r} T_r(x) \; mod\; (x^p - 1)$. Com efeito,

$$T_r(x^g) = x^g + {\xi_{p-1}}^{r} x^{g^2} + {\xi_{p-1}}^{2r} x^{g^3} + \cdots + {\xi_{p-1}}^{(p-3)r} x^{g^{p-2}} + {\xi_{p-1}}^{(p-2)r} x^{g^{p-1}}$$

Note que, como g é uma raiz primitiva $mod\; p$, segue do Pequeno Teorema de Fermat que $g^{p-1} \equiv 1 \; mod\; p$. Além disso,

$${\xi_{p-1}}^{-r} T_r(x) = {\xi_{p-1}}^{-r} x + x^g + {\xi_{p-1}}^{r} x^{g^2} + {\xi_{p-1}}^{2r} x^{g^3} + \cdots + {\xi_{p-1}}^{(p-3)r} x^{g^{p-2}}$$

Logo,

$$\begin{aligned} T_r(x^g) - {\xi_{p-1}}^{-r} T_r(x) &= {\xi_{p-1}}^{(p-2)r} x^{g^{p-1}} - {\xi_{p-1}}^{-r} x \\ &= {\xi_{p-1}}^{-r} x \left({\xi_{p-1}}^{(p-1)r} x^{g^{p-1}-1} - 1 \right). \end{aligned}$$

Ora, $g^{p-1} \equiv 1 \; mod\; p \implies g^{p-1} - 1 = pt$, com $t \in \mathbb{Z}$. Ademais, ${\xi_{p-1}}^{(p-1)r} = \left({\xi_{p-1}}^{p-1} \right)^r = 1^r = 1$. Assim, concluímos que

$$T_r(x^g) - {\xi_{p-1}}^{-r} T_r(x) = {\xi_{p-1}}^{-r} x \left(x^{g^{p-1}-1} - 1 \right) = {\xi_{p-1}}^{-r} x \, (x^{pt} - 1) = {\xi_{p-1}}^{-r} x \, ((x^p)^t - 1)$$

Daí, concluímos que $x^p - 1$ divide $T_r(x^g) - {\xi_{p-1}}^{-r} T_r(x)$. ∎

3° passo: Seja $P(x) = a_0 + a_1 x + \cdots + a_{p-1} x^{p-1} \in \mathbb{Z}[\xi_{p-1}][x]$ o resto que $T_r^{p-1}(x)$ deixa na divisão por $x^p - 1$. Mostraremos que $a_1 = a_2 = \cdots = a_{p-1}$. De fato,

$$P(x) \equiv T_r^{p-1}(x) \equiv \left({\xi_{p-1}}^{r} T_r(x^g) \right)^{p-1} \equiv T_r^{p-1}(x^g) \equiv P(x^g) \; mod\; (x^p - 1).$$

Para cada $1 \leq i \leq p-1$, seja $1 \leq j_i \leq p-1$ tal que $gi \equiv j_i \; mod\; p$. Daí, existe $l_i \in \mathbb{Z}$ tal que $gi - j_i = pl_i$. Assim, temos:

$$P(x^g) = a_0 + a_1x^g + a_2x^{2g} + \cdots + a_{p-1}x^{(p-1)g}$$
$$= a_0 + a_1x^{j_1}x^{pl_1} + a_2x^{j_2}x^{pl_2} + \cdots + a_{p-1}x^{j_{p-1}}x^{pl_{p-1}}$$

Ora, $x^p \equiv 1\ mod\ (x^p - 1)$. Logo,

$$P(x^g) = a_0 + a_1x^{j_1}x^{pl_1} + a_2x^{j_2}x^{pl_2} + \cdots + a_{p-1}x^{j_{p-1}}x^{pl_{p-1}}$$
$$\equiv a_0 + a_1x^{j_1} + a_2x^{j_2} + \cdots + a_{p-1}x^{j_{p-1}}\ mod\ (x^p - 1).$$

Assim, $a_1 = a_{g\ mod\ p} = a_{g^2\ mod\ p} = \cdots = a_{g^{p-2}\ mod\ p}$. Como g é raíz primitiva, temos que $a_1 = a_2 = \cdots = a_{p-1}$. ∎

Após esses três passos podemos concluir que:

$$P(\xi_p) = a_0 + a_1(\xi_p + \cdots + {\xi_p}^{p-1})$$

Ora, $\xi_p + \cdots + {\xi_p}^{p-1} = -1$. Logo, $P(\xi_p) = a_0 + a_1(\xi_p + \cdots + {\xi_p}^{p-1}) = a_0 - a_1 \in \mathbb{Z}[\xi_{p-1}] \subset \mathcal{P}_\infty$. Daí, $T_r^{p-1}(\xi_p) = P(\xi_p) \in \mathcal{P}_\infty$. Portanto, $T_r^{2^s}(\xi_p) \in \mathcal{P}_\infty$. O que conclui a demonstração do Teorema de Gauss-Wantzel. ∎