UNIVERSIDADE FEDERAL DE CATALÃO
INSTITUTO DE MATEMÁTICA E TECNOLOGIA
CURSO DE MATEMÁTICA

WESLEY SILVA DE ANDRADE

ESTUDO SOBRE EXTENSÕES DE CORPOS: JUSTIFICANDO IMPOSSIBILIDADES DE CONSTRUÇÕES COM RÉGUA E COMPASSO

Catalão, Goiás
2026

Wesley Silva de Andrade

ESTUDO SOBRE EXTENSÕES DE CORPOS: JUSTIFICANDO IMPOSSIBILIDADES DE CONSTRUÇÕES COM RÉGUA E COMPASSO

Monografia apresentada ao curso de Matemática do Instituto de Matemática e Tecnologia da Universidade Federal de Catalão, como parte dos requisitos para conclusão do curso de Matemática - Licenciatura.

Professor orientador: Prof. Dr. Porfírio Azevedo dos Santos Junior

Catalão, Goiás
2026

UNIVERSIDADE FEDERAL DE CATALÃO

INSTITUTO DE MATEMÁTICA E TECNOLOGIA

Av. Dr. Lamartine Pinto de Avelar, número 1120, - Bairro Setor Universitário, Catalão/GO, CEP 75704-020
Telefone: - - https://www.ufcat.edu.br

TERMO DE CIÊNCIA E DE AUTORIZAÇÃO (TECA)

TERMO DE CIÊNCIA E DE AUTORIZAÇÃO (TECA) PARA DISPONIBILIZAR VERSÕES ELETRÔNICAS DE TESES, DISSERTAÇÕES E TRABALHOS DE CONCLUSÃO DE CURSO NO REPOSITÓRIO INSTITUCIONAL DA UNIVERSIDADE FEDERAL DE CATALÃO (UFCAT)

Na qualidade de titular dos diretos de autor, autorizo a Universidade Federal de Catalão (UFCAT) a disponibilizar, gratuitamente, por meio do Repositório Institucional da Universidade Federal de Catalão (RI/UFCAT), sem ressarcimento dos direitos autorais, de acordo com a Lei 9610/98, o documento conforme permissões assinaladas abaixo, para fins de leitura, impressão e/ou download, a título de divulgação da produção científica brasileira, a partir desta data.

O conteúdo das Teses, Dissertações e Trabalhos de Conclusão de Curso disponibilizado no RI/UFCAT é de responsabilidade exclusiva do autor. Ao encaminhar o produto final, o(a) autor(a) e o(a) orientador(a) firmam o compromisso de que o trabalho não contém nenhuma violação de quaisquer direitos autorais ou outro direito de terceiros.

1. Identificação do material bibliográfico: Trabalho de Conclusão de Curso

2. Nome completo do autor: Wesley Silva de Andrade

Nome completo do(a) orientador(a): Porfírio Azevedo dos Santos Júnior

3. Título do trabalho

ESTUDO SOBRE EXTENSÕES DE CORPOS: Justificando Impossibilidades de Construções com Régua e Compasso.

4. Informações de acesso ao documento (este campo deve ser preenchido pelo orientador)

Concorda com a liberação total do documento: [X] SIM [ ] NÃO[1]

[1] Neste caso o documento será embargado por até um ano a partir da data de defesa. Após esse período, a possível disponibilização ocorrerá apenas mediante:

a) consulta ao(à) autor(a) e ao(à) orientador(a);

b) novo Termo de Ciência e de Autorização (TECA) assinado e inserido no arquivo da tese ou dissertação.

O documento não será disponibilizado durante o período de embargo.

Casos de embargo:

- Solicitação de registro de patente;
- Submissão de artigo em revista científica;
- Publicação como capítulo de livro;
- Publicação da dissertação/tese em livro.

Documento assinado digitalmente
gov.br
PORFIRIO AZEVEDO DOS SANTOS JUNIOR
Data: 30/03/2026 12:22:56-0300
Verifique em https://validar.iti.gov.br

Documento assinado digitalmente
gov.br
WESLEY SILVA DE ANDRADE
Data: 30/03/2026 13:07:54-0300
Verifique em https://validar.iti.gov.br

Ficha de identificação da obra elaborada pelo autor, através do
Programa de Geração Automática do Sistema de Bibliotecas da UFCAT.

Andrade , Wesley Silva de
ESTUDO SOBRE EXTENSÕES DE CORPOS: JUSTIFICANDO IMPOSSIBILIDADES DE CONSTRUÇÕES COM RÉGUA E COMPASSO / Wesley Silva de Andrade . - 2026.
61, f.

Orientador: Prof. Porfírio Azevedo dos Santos Junior .
Trabalho de Conclusão de Curso (Graduação) - Universidade Federal de Catalão, Instituto de Matemática e Tecnologia, Matemática, Catalão, 2026.
Apêndice.
Inclui símbolos, lista de figuras.

1. Extensões de corpos. 2. Duplicação do cubo . 3. Quadratura da circunferência . 4. Trissecção do ângulo . I. Junior , Porfírio Azevedo dos Santos , orient. II. Título.

CDU 51

UNIVERSIDADE FEDERAL DE CATALÃO

INSTITUTO DE MATEMÁTICA E TECNOLOGIA

ATA DA SESSÃO PÚBLICA DE DEFESA DE TRABALHO DE CONCLUSÃO DE CURSO PARA OBTENÇÃO DO TÍTULO DE LICENCIADO EM MATEMÁTICA, A QUE SE SUBMETEU O ALUNO WESLEY SILVA DE ANDRADE, ORIENTADO PELO PROF. DR. PORFÍRIO AZEVEDO DOS SANTOS JÚNIOR.

Aos vinte dias do mês de fevereiro do ano de dois mil e vinte e seis, às nove horas e trinta minutos, na sala dois do bloco J da Universidade Federal de Catalão, reuniu-se a Comissão Examinadora da defesa em epígrafe indicada pela Direção do Instituto de Matemática e Tecnologia, composta pelos: Presidente e Orientador Prof. Dr. Porfírio Azevedo dos Santos Júnior, Prof. Dr. Fernando Kennedy da Silva e Profa. Dra. Luciana Vale Silva Rabelo, para analisar o trabalho do candidato Wesley Silva de Andrade**,** apresentado sob o título "ESTUDO SOBRE EXTENSÕES DE CORPOS: JUSTIFICANDO IMPOSSIBILIDADES DE CONSTRUÇÕES COM RÉGUA E COMPASSO". O Presidente declarou abertos os trabalhos, a seguir o candidato apresentou o seu trabalho e foi arguido pela Comissão Examinadora. Terminada a exposição e a arguição, a Comissão reuniu-se e deliberou pelo seguinte resultado: **APROVADO CONDICIONALMENTE** ao atendimento das alterações sugeridas pela Comissão Examinadora, com nota 9,5 (nove vírgula cinco pontos).

Para fazer jus ao título de Licenciado em Matemática, a versão final do Trabalho de Conclusão de Curso, considerada Aprovada Condicionalmente, deverá ser entregue à professora da disciplina até o dia vinte e três de fevereiro de dois mil e vinte e seis.

Nada mais havendo a tratar, o Senhor Presidente declara a sessão encerrada, sendo a ata assinada pelos(as) Senhores(as) Membros da Comissão Examinadora.

Documento assinado eletronicamente por **PORFIRIO AZEVEDO DOS SANTOS JUNIOR**, **Professor(a) do Magistério Superior**, em 24/02/2026, às 20:03, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 8.539, de 8 de outubro de 2015.

Documento assinado eletronicamente por **LUCIANA VALE SILVA RABELO**, **Professor(a) do Magistério Superior**, em 24/02/2026, às 20:26, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 8.539, de 8 de outubro de 2015.

Documento assinado eletronicamente por **FERNANDO KENNEDY DA SILVA**, **Professor(a) do**

Magistério Superior, em 25/02/2026, às 18:04, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 8.539, de 8 de outubro de 2015.

A autenticidade deste documento pode ser conferida no site https://sei.ufcat.edu.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **0289260** e o código CRC **F560FD13**.

Referência: Processo nº 23852.006202/2025-04 SEI nº 0289260

AGRADECIMENTOS

Agradeço aos meus familiares, professores e amigos. Em especial, ao meu pai, à minha mãe, aos meus irmãos e ao meu orientador.

RESUMO

Esse trabalho busca realizar um estudo de maneira detalhada sobre a teoria de extensões de corpos, buscando ferramentas para justificar de forma algébrica as impossibilidades das construções por meio de régua e compasso dos três problemas grego clássicos: Um quadrado de área igual à um circulo dado, um cubo com o dobro de volume de um cubo dado e a terça parte de um ângulo a partir de um ângulo dado. Para tanto, necessitamos explorar conceitos, proposições, teoremas e exemplos relacionados abordando à teoria de extesões de corpos e as construções com régua e compasso.

Palavras-chave: Extensões de corpos. Duplicação do cubo. Quadratura da circunferência. Trissecção do ângulo.

ABSTRACT

This work aims to conduct a detailed study on the theory of field extensions, seeking tools to algebraically justify the impossibility of performing, with ruler and compass, the constructions involved in the three classical Greek problems: constructing a square with the same area as a given circle, constructing a cube with twice the volume of a given cube, and trisecting a given angle. To this end, we need to explore concepts, propositions, theorems, and related examples concerning the theory of field extensions and ruler-and-compass constructions.

Keywords: Field Extensions. Doubling the Cube. Squaring the Circle. Angle Trisection.

Sumário

Introdução

A escolha desse tema ocorreu durante a disciplina de Pesquisa em Educação Matemática, considerando o meu interesse em ingressar no mestrado em Matemática Pura. A partir disso, meu orientador me recomendou diversas leituras para que eu pudesse encontrar algo que despertasse minha atenção. Das variadas recomendações feitas, estava lá os três problemas clássicos da geometria, no qual, me intrigaram bastante, especialmente quanto ao motivo de ser impossível, utilizando apenas régua e compasso, realizar as seguintes construções: Um quadrado de área igual à um circulo dado, um cubo com o dobro de volume de um cubo dado e a terça parte de um ângulo a partir de um ângulo dado.

Esses três problemas, apesar de serem simples de enunciar, ocuparam muitos anos da história da Matemática até serem resolvidos e, nesse processo, muita Matemática foi revelada. Por exemplo, conta a lenda que o problema da duplicação do cubo surgiu em 429 a.C., quando os atenienses foram ao oráculo de Apolo, na ilha de Delos, pedindo uma graça para que acabasse com uma peste que devastava a cidade. O oráculo, então, exigiu que fosse construído outro altar com o dobro do volume do primeiro, que tinha o formato de um cubo. Os atenienses, acreditando resolver a questão, simplesmente dobraram o comprimento da aresta inicial, mas acabaram obtendo um altar com oito vezes o volume do primeiro. Como consequência, a peste continuou a devastar a cidade.

Todos esse problemas surge ainda na Grécia antiga, mas vieram a ser resolvidos apenas entre os séculos XVIII e XIX, com o desenvolvimento da álgebra moderna. Para esse texto, exploraremos dos conceitos necessários e suficientes para justificar tais impossibilidades de construções geométricas.

Para isso, o texto se encontra organizado da seguinte maneira, o capítulo 1 conta com os conceitos preliminares de álgebra, como por exemplo, anel, corpo, polinômios e números complexos que serão de grande importância para esse estudo.

O capítulo dois tem como objetivo explorar o conceito de anel de polinômios, isso a partir de proposições e teoremas importantes com exemplos.

No capítulo três será apresentado à teoria de extensões de corpos, que tem papel fundamental para a compreensão das impossibilidades mencionadas.

No capítulo quatro, é voltado às construções envolvendo régua e compasso. Nesse capítulo iremos entender as limitações de tais construções, e com isso finalizar apresentando o porquê de ser impossível realizar certas construções.

Para o último capítulo, foi elaborada uma sequência didática envolvendo construções geométricas por meio da ferramenta GeoGebra.

1 Conceitos preliminares de álgebra

Antes de darmos início à teoria de extensão de corpos, iremos relembrar alguns conceitos básicos de álgebra. Desse modo, serão apresentadas algumas definições e variados exemplos para facilitar a compreensão do texto.

1.1 Anéis e corpos, definições e exemplos.

Definição 1.1 *Seja A um conjunto não vazio. Uma operação "$\circledast$"(binária) para A é uma função*

$$f : A \times A \to A$$

$$(x, y) \mapsto x \circledast y$$

Ou seja, para todos x e $y \in A$, $x \circledast y$ também está em A.

Exemplo 1.1: A adição usual no conjunto dos naturais $\mathbb{N}$ é um exemplo de operação binária em $\mathbb{N}$, pois somando dois números naturais resulta em um número natural.

Exemplo 1.2: O mesmo não ocorre para a subtração em $\mathbb{N}$, pois existem 5 e 7 que pertencem a $\mathbb{N}$, e quando subtraímos, $5 - 7 = -2$, que não pertence a $\mathbb{N}$.

Definição 1.2 *Sejam A um conjunto não vazio e $\oplus$, $\otimes$ operações para A, chamadas de adição e multiplicação. Uma terna $(A, \oplus, \otimes)$ é dita Anel quando obedece às seguintes propriedades para $a, b, c, x, y, z \in A$:*

(A.1) $(x \oplus y) \oplus z = x \oplus (y \oplus z)$ *(Associatividade para a adição)*

(A.2) $x \oplus y = y \oplus x$; *(Comutatividade para a adição)*

(A.3) $\exists e \in A$ *tal que* $x \oplus e = x = e \oplus x$, $\forall x \in A$; *(Existência de elemento neutro para a adição)*

(A.4) $\forall x \in A \ \exists a \in A$ *tal que* $x \oplus a = e = a \oplus x$; *(Existência de elemento simétrico para a adição)*

(M.1) $(x \otimes y) \otimes z = x \otimes (y \otimes z)$; *(Associatividade para a multiplicação)*

(M.2) $b \otimes (x \oplus y) = (b \otimes x) \oplus (b \otimes y)$ *e* $(x \oplus y) \otimes c = (x \otimes c) \oplus (y \otimes c)$. *(Distribuição com relação à adição)*

Observações: i) O simétrico aditivo de x será denotado por $-x$.
ii) Um anel é sempre uma terna $(A, \oplus, \otimes)$, mas denotaremos apenas por A, as operações somente serão explicitadas quando houver necessidade.

Exemplo 1.3: Os seguintes conjuntos numéricos, $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$ e $\mathbb{C}$ com as operações de adição e multiplicação usuais são exemplos de anéis.

Exemplo 1.4: O conjunto $\mathbb{Q}[\sqrt{2}] = \{a + b\sqrt{2} : a, b \in \mathbb{Q}\}$, com as operações de adição e multiplicação definidas da seguinte maneira,
$+ : (a + b\sqrt{2}), (c + d\sqrt{2}) \to \Big((a + c) + (b + d)\sqrt{2}\Big)$
e
$\cdot : (a + b\sqrt{2}), (c + d\sqrt{2}) \to \Big((ac + 2bd) + (ad + bc)\sqrt{2}\Big)$
é um anel. De fato,

Sejam $x = (a + b\sqrt{2}), y = (c + d\sqrt{2})$ *e* $z = (e + f\sqrt{2})$ *elementos desse conjunto.* Começaremos verificando a associatividade com relação à adição.

$$\begin{aligned}
(x + y) + z &= \Big((a + b\sqrt{2}) + (c + d\sqrt{2})\Big) + (e + f\sqrt{2}) \\
&= \Big((a + c) + (b + d)\sqrt{2}\Big) + (e + f\sqrt{2}) \\
&= \Big((a + c) + e\Big) + \Big((b + d) + f\Big)\sqrt{2} \\
\text{(Pela associatividade dos racionais)} \quad &= \Big(a + (c + e)\Big) + \Big(b + (d + f)\Big)\sqrt{2} \\
&= (a + b\sqrt{2}) + \Big((c + e) + (d + f)\sqrt{2}\Big) \\
&= (a + b\sqrt{2}) + \Big((c + d\sqrt{2}) + (e + f\sqrt{2})\Big) \\
&= x + (y + z)
\end{aligned}$$

Portanto, vale a associatividade para adição. Agora, veremos a comutatividade.

$$\begin{aligned}
x + y &= (a + b\sqrt{2}) + (c + d\sqrt{2}) \\
&= (a + c) + (b + d)\sqrt{2} \\
&= (c + a) + (d + b)\sqrt{2} \\
&= (c + d\sqrt{2}) + (a + b\sqrt{2}) = y + x
\end{aligned}$$

Logo, os elementos desse conjunto são comutativos com relação à adição. Agora veremos se esse conjunto possui elemento neutro para adição.

$$(a + b\sqrt{2}) + (c + d\sqrt{2}) = a + b\sqrt{2}$$

$$\iff (a + c) + (b + d)\sqrt{2} = a + b\sqrt{2}$$

$$\iff \begin{cases} a + c = a \\ b + c = b \end{cases} \Rightarrow c = 0 \text{ e } d = 0$$

Com isso, o elemento neutro da adição nesse conjunto é $0 + 0\sqrt{2}$. Agora, iremos verificar a existência de elemento inverso aditivo.

$$
\begin{aligned}
&(a+b\sqrt{2})+(c+d\sqrt{2})=0+0\sqrt{2}\\
\iff &(a+c)+(b+d)\sqrt{2}=0+0\sqrt{2}\\
\iff &\begin{cases} a+c=0 \\ b+d=0 \end{cases} \quad \Rightarrow c=-a \ e \ d=-b
\end{aligned}
$$

Logo, dado $a+b\sqrt{2}$ o seu inverso da adição nesse conjunto é $-a-b\sqrt{2}$. Agora, iremos verificar as propriedades com relação à multiplicação. Começaremos pela associatividade e, para isso, veremos se o lado esquerdo da igualdade $(x\cdot y)\cdot z = x\cdot(y\cdot z)$ é igual ao lado direito.

$$
\begin{aligned}
(x\cdot y)\cdot z &= \Big((a+b\sqrt{2})\cdot(c+d\sqrt{2})\Big)\cdot(e+f\sqrt{2})\\
&= \Big((ac+2bd)+(ad+bc)\sqrt{2}\Big)\cdot(e+f\sqrt{2})\\
&= (ac+2bd)e+(ac+2bd)f\sqrt{2}+(ad+bc)e\sqrt{2}+2(ad+bc)f\\
&= (ace+2bde+2adf+2bcf)+(acf+2bdf+ade+bce)\sqrt{2}\\
x\cdot(y\cdot z) &= (a+b\sqrt{2})\cdot\Big((c+d\sqrt{2})\cdot(e+f\sqrt{2})\Big)\\
&= (a+b\sqrt{2})\cdot\Big((ce+2df)+(cf+de)\sqrt{2}\Big)\\
&= a(ce+2df)+a(cf+de)\sqrt{2}+b(ce+2df)\sqrt{2}+2b(cf+de)\\
&= (ace+2bde+2adf+2bcf)+(acf+2bdf+ade+bce)\sqrt{2}
\end{aligned}
$$

Como o lado esquerdo é igual ao direito, vale a associatividade para a multiplicação. Em seguida, daremos sequência à verificação da distributividade da multiplicação com relação à adição.

$$
\begin{aligned}
x\cdot(y+z) &= (a+b\sqrt{2})\cdot\Big((c+d\sqrt{2})+(e+f\sqrt{2})\Big)\\
&= (a+b\sqrt{2})\Big((c+e)+(d+f)\sqrt{2}\Big)\\
&= a(c+e)+a(d+f)\sqrt{2}+b(c+e)\sqrt{2}+2b(d+f)\\
&= \Big((ac+2bd)+(ad+bc)\sqrt{2}\Big)+\Big((ae+2bf)+(af+be)\sqrt{2}\Big)\\
&= \Big((a+b\sqrt{2})\cdot(c+d\sqrt{2})\Big)+\Big((a+b\sqrt{2})\cdot(e+f\sqrt{2})\Big)\\
&= xy+xz
\end{aligned}
$$

Da mesma maneira, mostra-se que $(x+y)z = xz+yz$. Portanto, vale a distributividade da multiplicação com relação à adição. Logo, esse conjunto com essas operações definidas é um anel.

Definição 1.3 *Seja A um anel. Se, para todos os elementos de A, vale a propriedade adicional*

$$x \otimes y = y \otimes x$$

A é dito anel comutativo.

Exemplo 1.5: Considere o conjunto $n\mathbb{Z} = \{n \cdot x : x \in \mathbb{Z}\}$. Esse conjunto, com as operações de adição e multiplicação de $\mathbb{Z}$, é um anel comutativo.

Exemplo 1.6: O conjunto $\mathbb{Q}[\sqrt{2}]$ com as operações definidas no exemplo 1.4, é um anel comutativo. De fato,

Sejam $x, y \in \mathbb{Q}[\sqrt{2}]$

$$\begin{aligned} x \cdot y &= (a + b\sqrt{2}) \cdot (c + d\sqrt{2}) \\ &= (ac + 2bd) + (ad + bc)\sqrt{2} \\ &= (ca + 2db) + (da + cb)\sqrt{2} \\ &= (c + d\sqrt{2}) \cdot (a + b\sqrt{2}) \\ &= y \cdot x \end{aligned}$$

Logo, é válida a comutatividade para a multiplicação.

Exemplo 1.7: De modo geral, o anel das matrizes não é um anel comutativo.

Definição 1.4 *Seja A um anel. Se existe 1_A pertencente a A tal que*

$$x \otimes 1_A = 1_A \otimes x = x, \ \forall x \in A$$

A é dito anel com unidade.

Exemplo 1.8: O conjunto $\mathbb{Q}[\sqrt{2}]$, com as operações definidas possui unidade. De fato,

Sejam $x, y \in \mathbb{Q}[\sqrt{2}]$

$$\begin{aligned} & x \cdot y = (a + b\sqrt{2}) \cdot (c + d\sqrt{2}) = a + b\sqrt{2} \\ \iff & (ac + 2bd) + (ad + bc)\sqrt{2} = a + b\sqrt{2} \\ \iff & \begin{cases} ac + 2bd = a \\ ad + bc = b \end{cases} \end{aligned}$$

Iremos separar em alguns casos. Primeiro iremos considerar $a \neq 0$.

$$\overset{\text{(Multiplicando a primeira linha por } \frac{b}{a})}{\iff} \begin{cases} bc + \frac{2b^2d}{a} = b \\ ad + bc = b \end{cases}$$

$$\begin{cases} c = 1 - \frac{2bd}{a} \\ ad + bc = b \end{cases} \overset{\text{(Substituindo c na segunda eq.)}}{\iff} \begin{cases} c = 1 - \frac{2bd}{a} \\ ad + b - \frac{2b^2d}{a} = b \end{cases}$$

$$\iff \begin{cases} c = 1 - \frac{2bd}{a} \\ d(a - \frac{2b^2}{a}) = 0 \end{cases} \overset{\text{(Do fato de todos esses números serem racionais)}}{\Rightarrow} d = 0 \ ou \ a - \frac{2b^2}{a} = 0$$

$\Rightarrow a^2 = 2b^2$, Como todos os números são racionais, $d = 0$.

Substituindo d na primeira equação, obtém-se $c = 1$. Agora, considerando $a = 0$ e como b é um elemento qualquer dado, segue rapidamente que $c = 1, d = 0$. Desse modo, o elemento neutro da multiplicação nesse conjunto é $1 + 0\sqrt{2}$.

Definição 1.5 *Seja D um anel comutativo e com unidade. Se, em D, vale a seguinte propriedade adicional*

$$x \otimes y = 0 \Rightarrow x = 0 \ ou \ y = 0$$

D é dito anel de integridade ou domínio de integridade.

Exemplo 1.9: O conjunto $\mathbb{Q}[\sqrt{2}]$, com as operações definidas é um domínio de integridade. De fato,

Sejam $x, y \in \mathbb{Q}[\sqrt{2}]$

$$\begin{aligned} x \cdot y = 0 &\Rightarrow (a + b\sqrt{2}) \cdot (c + d\sqrt{2}) = 0 + 0\sqrt{2} \\ &\Rightarrow (ac + 2bd) + (ad + bc)\sqrt{2} = 0 + 0\sqrt{2} \\ &\iff \begin{cases} ac + 2bd = 0 \\ ad + bc = 0 \end{cases} \end{aligned}$$

Vamos separar em alguns casos, primeiro iremos considerar $a \neq 0$

$$\overset{\text{(Multiplicando a primeira linha por b/a)}}{\Rightarrow} \begin{cases} bc + \frac{2b^2d}{a} = 0 \\ ad + bc = 0 \end{cases}$$

$$\Rightarrow \begin{cases} c = -\frac{2bd}{a} \\ ad + bc = 0 \end{cases} \Rightarrow \begin{cases} c = -\frac{2bd}{a} \\ ad - \frac{2b^2d}{a} = 0 \end{cases}$$

Resolvendo a segunda linha, $d(a - \frac{2b^2}{a}) = 0 \Rightarrow d = 0 \ ou \ a - \frac{2b^2}{a} = 0 \Rightarrow a^2 = 2b^2 \Rightarrow a = \pm b\sqrt{2}$

E isso é uma contradição. Portanto, $d = 0$ e, consequentemente, $c = 0$. Agora, iremos considerar $a = 0$. Segue então, $\begin{cases} 2bd = 0 \\ bc = 0 \end{cases}$, supondo $b \neq 0$, segue $c = d = 0$.

Agora, se $b = 0$, não há nada ser feito, pois estamos na situação em que $a = 0$. Sem perda de generalidade, se $c \neq 0$, o argumento vale de forma similar, considerando $c = 0$, também pode ser feito o mesmo. Portanto, se $(a + b\sqrt{2})(c + d\sqrt{2}) = 0 + 0\sqrt{2}$, então $a + b\sqrt{2} = 0 + 0\sqrt{2}$ *ou* $c + d\sqrt{2} = 0 + 0\sqrt{2}$ como queríamos. Fica mostrado, então, que de fato esse conjunto não possui divisores de zero. Logo, esse conjunto, com as operações definidas, é um domínio de integridade.

Exemplo 1.10: O anel $\mathbb{Z}_6$ não é um domínio de integridade, pois existem os elementos $\overline{2}$ *e* $\overline{3}$, tais que $\overline{2} \cdot \overline{3} = 0$.

Definição 1.6 *Seja A um anel. Um subconjunto B de A é dito subanel de A quando*

(i) $\forall a, b \in B \Rightarrow a \oplus b \in B$

(ii) $\forall a, b \in B \Rightarrow a \otimes b \in B$

Proposição 1.1 *Sejam A um anel e B um subconjunto não vazio de A. Então, B é um subanel de A se, e somente, se $a - b,\ ab \in B$, sempre que $a, b \in B$.*

Demonstração. $\Rightarrow$ Se B é um subanel de A, então, evidentemente, temos que $a-b \in B$ e $ab \in B$, para todos $a, b \in B$.

$\Leftarrow$ Observe que, se $x \in B$, então temos $-x \in B$, pois $-x = 0 - x$. Isso significa que, dados $x, y \in B$, temos $x + y = x - (-y) \in B$ e, portanto, B é fechado para a adição. Pela própria hipótese, B já é fechado para a multiplicação.

Como as propriedades associativa, comutativa e distributivas são hereditárias, segue imediatamente que B é um subanel de A.

■

Exemplo 1.11: $\mathbb{Z}[\sqrt{2}] = \{a + b\sqrt{2} : a, b \in \mathbb{Z}\}$ é um subanel de $\mathbb{Q}[\sqrt{2}]$. De fato,

Sejam $x, y \in \mathbb{Z}[\sqrt{2}]$

$$x - y = (a + b\sqrt{2}) - (c + d\sqrt{2}) = (a - c) + (b - d)\sqrt{2} \in \mathbb{Z}[\sqrt{2}]$$
$$x.y = (a + b\sqrt{2}).(c + d\sqrt{2}) = (ac + 2bd) + (ad + bc)\sqrt{2} \in \mathbb{Z}[\sqrt{2}]$$

Logo, $\mathbb{Z}[\sqrt{2}]$ é um subanel de $\mathbb{Q}[\sqrt{2}]$.

Definição 1.7 *Seja K um domínio de integridade. Se todos os elementos de K possuem inverso multiplicativo, isto é,*

$$\forall x \in K\ \exists\ y \in K \text{ tal que } x \otimes y = 1_K$$

K é dito corpo.

Exemplo 1.12: O domínio de integridade apresentado no exemplo 1.9 é um corpo. Para isso, será necessário e suficiente mostrar que, qualquer que seja o elemento $a + b\sqrt{2} \neq 0 + 0\sqrt{2}$ dado, ele possui inverso multiplicativo. De fato,

Sejam x,y $\in \mathbb{Q}[\sqrt{2}]$

$$
\begin{aligned}
& x \cdot y = 1 \Longleftrightarrow (a + b\sqrt{2}) \cdot (c + d\sqrt{2}) \\
& = 1 + 0\sqrt{2} \Longleftrightarrow (ac + 2bd) + (ad + bc)\sqrt{2} \\
& = 1 + 0\sqrt{2} \\
& \Longleftrightarrow \begin{cases} ac + 2bd = 1 \\ ad + bc = 0 \end{cases} \\
& \overset{\text{(Multiplicando a primeira linha por b/a)}}{\Longleftrightarrow} \begin{cases} cb + \frac{2b^2 d}{a} = \frac{b}{a} \\ ad + bc = 0 \end{cases} \\
& \Longleftrightarrow \begin{cases} c = \frac{1}{a} - \frac{2bd}{a} \\ ad + bc = 0 \end{cases} \quad \Longleftrightarrow \begin{cases} c = \frac{1}{a} - \frac{2bd}{a} \\ ad + \frac{b}{a} - \frac{2b^2 d}{a} = 0 \end{cases}
\end{aligned}
$$

Resolvendo a segunda linha, $d(a - \frac{2b^2}{a}) = -\frac{b}{a} \Rightarrow d = \frac{-b}{a^2 - 2b^2}$.

Com isso, $c = \frac{a}{a^2 - 2b^2}$. Dessa forma, qualquer que seja o elemento $(a + b\sqrt{2})$ dado, existe o elemento $\left((\frac{a}{a^2 - 2b^2}) + (\frac{-b}{a^2 - 2b^2})\sqrt{2} \right)$ que é o seu inverso multiplicativo. Nas contas que foram feitas, foi considerado $a \neq 0$, para $a = 0$, o resultado é de fácil verificação. Portanto, o conjunto $\mathbb{Q}[\sqrt{2}]$ com as operações definidas, possui estrutura de corpo.

Definição 1.8 *Seja K um corpo. Um subconjunto L de K é dito subcorpo de K quando L possui estrutura de corpo com relação às operações de K.*

Exemplo 1.13: $\mathbb{R}$ é um subcorpo de $\mathbb{C}$.

Definição 1.9 *Seja A um anel. Um subanel $I \subset A$ chama-se ideal em A se, $\forall x \in I$ e $\forall a \in A$ tem-se*

$$ax \in I \text{ e } xa \in I$$

.

Teorema 1.1 *Seja A um anel. Se, em um subconjunto $I \subset A, I \neq \emptyset$, tem-se:*

(i) $\forall x, y \in I \Rightarrow x - y \in I$;

(ii) $\forall x \in I$ *e* $\forall a \in A \Rightarrow ax$ *e* $xa \in I$.

Então I é um ideal de A.

Demonstração. Imediato a definição.

■

Exemplo 1.14: No anel $\mathbb{Z}$, qualquer que seja o subconjunto $n\mathbb{Z}$, para $n \in \mathbb{Z}$, é um ideal de $\mathbb{Z}$.

Definição 1.10 *Sejam $(A, +, \cdot)$ e $(B, \oplus, \otimes)$ anéis. Uma função $f : A \to B$ é dita um homomorfismo de A em B se satisfaz às seguintes condições:*

(i) $f(x + y) = f(x) \oplus f(y), \forall x, y \in A$

(ii) $f(x \cdot y) = f(x) \otimes f(y), \forall, x, y \in A$

Se $f : A \to B$ é um homomorfismo bijetivo, então f é um isomorfismo de A *em* B.

Os homomorfismos de A *em* A são ditos endomorfismos, e o conjunto de todos os isomorfismos de A *em* A são ditos automorfismos. Denotam-se, respctivamente, $End(A)$ *e* $Aut(A)$.

Exemplo 1.15: A função identidade é um automorfismo.

Exemplo 1.16: Considere o conjunto $\mathbb{Z}[\sqrt{p}] = \{a + b\sqrt{p} : a, b \in \mathbb{Z}\}$ com p primo e fixo. O $Aut(\mathbb{Z}[\sqrt{p}]) = \{I_{\mathbb{Z}[\sqrt{p}]}, \sigma\}$, onde,

$$\sigma : \mathbb{Z}[\sqrt{p}] \to \mathbb{Z}[\sqrt{p}]$$
$$\sigma(a + b\sqrt{p}) = a - b\sqrt{p}, \ \forall a.b \in \mathbb{Z}[\sqrt{p}]$$

Vamos mostrar que as funções identidade e sigma são os únicos isomorfismos. Antes de tudo, observe que, se f é um automorfismo de $\mathbb{Z}[\sqrt{p}]$, então $f(1) = 1$, e daí segue que $f(m) = m, \forall m \in \mathbb{Z}$. Portanto,

$$f(a + b\sqrt{p}) = a + bf(\sqrt{p}), \forall a, b \in \mathbb{Z}$$

Levando em consideração que $(\sqrt{p})^2 = p$, temos $(f(\sqrt{p}))^2 = f(p) = p$. Logo, existem duas possibilidades para $f(\sqrt{p})$ em $\mathbb{Z}[\sqrt{p}]$, $f(\sqrt{p}) = \sqrt{p}$ ou $f(\sqrt{p}) = -\sqrt{p}$. Na primeira, obtemos $f = I_{\mathbb{Z}[\sqrt{p}]}$. Na segunda, obtemos $f(a + b\sqrt{p}) = a - b\sqrt{p}$. Portanto, de fato, os únicos automorfismos de $\mathbb{Z}[\sqrt{p}]$ são a identidade e a função sigma definida.

Definição 1.11 *Sejam A um anel e I um ideal de A. Sobre A, definimos a relação de congruência $(mod\ I)$ para $a, b \in A$,*

$$a \equiv b \ (mod\ I) \iff a - b \in I.$$

Exemplo 1.17: Sejam $3, 5 \in \mathbb{Z}$. 3 e 5 são congruentes *mod* $2\mathbb{Z}$, pois $3 - 5 \in 2\mathbb{Z}$.

Definição 1.12 *Sejam A um anel e I um ideal de A. Denotaremos por $\overline{x} = \{y \in A : y \equiv x(mod\ I)\}$ a qual chamaremos de classe de equivalência do elemento $x \in A$ relativamente à relação $\equiv (mod\ I)$.*

Exemplo 1.18: Considere o anel $\mathbb{Z}$ e o ideal $3\mathbb{Z}$. Na notação apresentada, $\overline{2} = \{..., -4, -1, 2, 5, 8, ...\}$.

Observe que $y \in \overline{x} \iff y - x \in I$ e, por isso, também denotaremos a classe $\overline{x} = x + I = \{x + z : z \in I\}$.

Definição 1.13 *Sejam A um anel e I um ideal de A. Chamaremos de conjunto quociente de A pelo ideal I ao conjunto $A/I = \{\overline{x} = x + I : x \in A\}$*

Exemplo 1.19: O conjunto quociente $\mathbb{Z}/3\mathbb{Z} = \{\overline{0}, \overline{1}, \overline{2}\}$.

Teorema 1.2 *Sejam A e B anéis e $f : A \to B$ um homomorfismo. Então,*

(i) $Im\ f = \{f(a) : a \in A\}$ *é um subanel de B.*

(ii) $N(f) = \{a \in A : f(a) = o_B\}$ *é um ideal de A, e f é injetiva* $\iff N(f) = \{0_A\}$.

(iii) $A/N(f) \cong Im\ f$.

Demonstração. (i) Temos que:

- $0_B = f(0) \in Im\ f$.
- $f(a), f(b) \in Im\ f \Rightarrow f(a) - f(b) = f(a - b) \in Im\ f$.
- $f(a), f(b) \in Im\ f \Rightarrow f(a) \cdot f(b) = f(a \cdot b) \in Im\ f$.

Portanto, de fato, a $Im\ f$ é um subanel de B.

(ii) Vamos provar que o núcleo de A é, de fato, ideal de A. De fato,

- $0 \in N(f),\ pois\ f(0_A) = 0_B$
- $a, b \in N(f) \Rightarrow f(a - b) = f(a) - f(b) = 0_B - 0_B = 0_B$
- Seja $x \in A\ e\ a \in N$ então,

$$f(x \cdot a) = f(x) \cdot f(a) = f(x) \cdot 0_B = 0_B,\ e\ f(a \cdot x) = f(a) \cdot f(x) = 0_B \cdot f(x) = 0_B$$

Ou seja, $ax \in N(f)\ e\ xa \in N(f)$. Assim, $N(f)$ é um ideal de A.

($\Rightarrow$) Se f é injetiva, segue imediatamente que $N(f) = \{0\}$.

($\Leftarrow$) Se $f(x) = f(y), x, y \in A\ e\ N(f) = \{0\}$, segue que, $f(x) - f(y) = 0_B \Rightarrow f(x - y) = 0_B \Rightarrow x - y \in N(f).E\ como\ N(f) = \{0\} \Rightarrow x = y.$

(iii) Vamos começar definindo uma função $F : A/N(f) \to Im\ f\ por :\ F(\overline{x}) = f(x)$. Observe que F está "bem definida"e é bijetiva pois:

$$\overline{x} = \overline{y} \iff x \equiv y(mod N(f)) \iff x - y \in N(f) \iff f(x) - f(y) = 0_B$$
$$\iff F(\overline{x}) = f(x) = f(y) = F(\overline{y}).$$
$$Im\ f = \{F(\overline{x}) : \overline{x} \in A/N(f)\} = \{f(x) : x \in A\} = Im\ f$$

Logo, $A/N(f)$ é isomorfo a $Im\ f$.

■

1.2 Polinômios em uma variável

Nesta seção, abordaremos ideias gerais sobre polinômios.

Definição 1.14 *Seja A um domínio de integridade. Chamaremos de um polinômio sobre A, em uma indeterminada x, a uma expressão formal $p(x) = a_0 + \cdots + a_n x^n + \ldots$, onde $a_i \in A, \forall i \in \mathbb{N}$ e $\exists n \in \mathbb{N}$ tal que $a_j = 0 \forall j \geq n$.*

Dados dois polinômios $p(x) = a_0 + \cdots + a_n x^n + \ldots$ e $g(x) = b_0 + \cdots + b_m x^m + \ldots$ sobre A, a adição e multiplicação entre eles ocorrem da seguinte maneira:

$$+ : \Big((a_0 + \cdots + a_n x^n + \ldots), (b_0 + \cdots + b_m x^m + \ldots)\Big) \mapsto ((a_0 + b_0) + (a_1 + b_1)x + \cdots + (a_i + b_i)x^i + \ldots)$$

$$\cdot : \Big((a_0 + \cdots + a_n x^n + \ldots), (b_0 + \cdots + b_m x^m + \ldots)\Big) \mapsto (c_0 + \cdots + c_i x^i + \ldots)$$

onde $c_m = \sum_{m=i+j} a_i b_j$, $m = 0, 1, 2, \ldots$

Além disso, dois polinômios $p(x) = a_0 + \cdots + a_n x^n + \ldots$, e $g(x) = b_0 + \cdots + b_m x^m + \ldots$ sobre um anel A são iguais apenas quando, $a_i = b_i, \forall i = 0, 1, 2, \ldots$.

Seja A um domínio de integridade. Considere $A[x]$ o conjunto de todos os polinômios sobre A. O conjunto $A[x]$, com as operações definidas acima, possui estrutura de anel e é dito anel de polinômios em uma variável com coeficientes em A.

Exemplo 1.20: Sejam $p(x) = 3 + 11x + 4x^2 + 2x^4$ e $g(x) = -7 + 4x + 6x^3$. A adição desses dois polinômios ocorre da seguinte maneira,

$$p(x) + g(x) = (3-7) + (11+4)x + (4+0)x^2 + (0+6)x^3 + (2+0)x^4 = -3 + 15x + 4x^2 + 6x^3 + 2x^4$$

e a multiplicação,

$$p(x) \cdot g(x) = (3 + 11x + 4x^2 + 2x^4) \cdot (-7 + 4x + 6x^3)$$

$$= (3 \cdot (-7)) + \Big((11 \cdot (-7)) + (3 \cdot 4)\Big)x + \Big((4 \cdot (-7)) + (11 \cdot 4) + (3 \cdot 0)\Big)x^2 + \Big((0 \cdot (-7)) + (4 \cdot 4) + (11 \cdot 0) + (3 \cdot 6)\Big)x^3 + \Big((2 \cdot (-7)) + (0 \cdot 4) + (4 \cdot +0) + (11 \cdot 6) + (3 \cdot 0)\Big)x^4 + \Big((0 \cdot (-7)) + (2 \cdot 4) + (0 \cdot 4) + (4 \cdot 6) + (11 \cdot 0) + (3 \cdot 0)\Big)x^5 + \Big((0 \cdot (-7)) + (0 \cdot 4) + (2 \cdot 0) + (0 \cdot 6) + (4 \cdot 0) +$$

$$(11\cdot 0)+(3\cdot 0)\Big)x^6+\Big((0\cdot(-7))+(0\cdot 4)+(0\cdot 0)+(2\cdot 6)+(0\cdot 0)+(4\cdot 0)+(11\cdot 0)+(3\cdot 0)\Big)x^7$$

$$= -21-65x+16x^2+34x^3+52x^4+32x^5+12x^7$$

Observe, para a multiplicação entre polinômios pode ser aplicado a distributiva como já é conhecido.

Definição 1.15 *Seja $A[x]$ um anel de polinômios. Dado um polinômio $p(x) = a_0 + a_1x... + a_nx^n \in A[x]$ e um elemento u qualquer, define-se $p(u)$ da seguinte maneira: $p(u) = a_0 + a_1u + ... + a_nu^n$.*

Exemplo 1.21: Considere $\mathbb{Q}[x]$ e $p(x) = 2 + x + x^2$. Dado $\sqrt{2}$, temos que $p(\sqrt{2}) = 2 + \sqrt{2} + (\sqrt{2})^2 = 4 + \sqrt{2}$. Perceba que não é necessário que o elemento u pertença ao anel dos coeficientes do polinômio.

Exemplo 1.22: Considere $A[x]$ e $p(x) = a_0 + a_1x + ... + a_nx^n$. Sempre temos $p(x) = (x-u)q(x) + p(u)$ para algum $q(x) \in A[x]$. De fato,

$$\begin{aligned} p(x)-p(u) &= (a_0+a_1x+...+a_nx^n)-(a_0+a_1u+...+a_nu^n) \\ &= a_1(x-u)+a_2(x^2-u^2)+...+a_n(x^n-u^n) \\ &= (x-u)[a_1+a_2(x-u)+...+a_n(x^{n-1}-u^{n-1})] \\ \iff p(x) &= (x-u)q(x)+p(u),\ \textit{onde}\ q(x)=a_1+a_2(x-u)+...+a_n(x^{n-1}-u^{n-1}). \end{aligned}$$

Definição 1.16 *Seja A um anel. Seja $p(x) = a_0+...+a_nx^n, a_n \neq 0$ um polinômio $\in A[x]$. Um número α é dito raiz de $p(x)$ quando $p(\alpha) = 0$.*

Exemplo 1.23: Dado o polinômio $p(x) = 9-x^2$, o número 3 é uma raiz desse polinômio. Observe que um polinômio pode ter mais de uma raiz, por exemplo, nesse caso o número -3, também é uma raiz desse polinômio.

Proposição 1.2 *Se α uma raiz do polinômio $p(x) = a_0 + ... + a_nx^n$, então existe algum $q(x) = b_0 + ... + b_{n-1}x^{n-1}$, tal que, $p(x) = (x-\alpha)q(x)$.*

Demonstração. Imediato ao exemplo 1.20.

■

Exemplo 1.24: Dado o polinômio $p(x) = x^3 - 2x^2 + 3x - 6$ é de fácil verificação que $\alpha = 2$ é uma raiz. De fato, existe o polinômio $q(x) = x^2+3$, tal que, $p(x) = (x-2)(x^2+3)$

1.3 Números complexos

Nessa seção, serão relembradas algumas propriedades a respeito dos números complexos. Não é objetivo deste texto construir formalmente a noção de números

complexos. Para o leitor mais curioso, recomenda-se o livro *A construção dos números*, da coleção Textos Universitários da SBM.

A forma algébrica de um número complexo é $(a + bi)$, tal que $a, b \in \mathbb{R}$ *e* $i^2 = -1$. A adição e a multiplicação dos números complexos ocorrem da seguinte maneira:

$$+ : (a + bi), (c + di) \to (a + c) + (b + d)i$$
$$\cdot : (a + bi), (c + di) \to (ac - bd) + (ad + bc)i$$

Exemplo 1.25: $(3 + 4i) + (5 - 2i) = (3 + 5) + (4 - 2)i = (8 + 2i)$.
Exemplo 1.26: $(2 + 6i) \cdot (5 + 4i) = (2 \cdot 5 - 6 \cdot 4) + (2 \cdot 4 + 6 \cdot 5) = (-14 + 38i)$.

O conjunto dos números complexos, com as operações definidas, possui estrutura de corpo. Para demonstrar isso, procede-se de modo análogo ao exemplo 1.4.

O elemento neutro da adição é $(0+0i)$, e o elemento neutro da multiplicação é $(1+0i)$. Além disso, dado qualquer número complexo $(a + bi)$, o seu inverso multiplicativo é $(\frac{a}{a^2+b^2}) + (\frac{-b}{a^2+b^2})i$.

Definição 1.17 *Seja $\alpha = a + bi$ um número complexo. O número $\overline{\alpha} = a - bi$ é dito conjugado do número α.*

Exemplo 1.27: $z = 3 + 5i \Rightarrow \overline{z} = 3 - 5i$.

Algumas propriedades dos números complexos:

- $z + \overline{z} = (a + bi) + (a - bi) = 2a$
- $z - \overline{z} = (a + bi) - (a - bi) = 2bi$
- $z = \overline{z} \iff z \in \mathbb{R}$
- $\overline{z_1 + z_2} = \overline{z_1} + \overline{z_2}$
- $\overline{z_1 \cdot z_2} = \overline{z_1} \cdot \overline{z_2}$

2 Anéis de polinômios - Definição, exemplos, proposições e teoremas importantes com exemplos

Neste capítulo serão tratados os anéis de polinômios. A fim de simplicidade, definiremos sobre um domínio de integridade.

Definição 2.1 *Sejam A um domínio de integridade e $f(x) = a_0 + a_1x + \cdots + a_nx^n \in A[x]$ com $a_n \neq 0$. Então,*

- *O inteiro n se chama grau de $f(x)$;*
- *O coeficiente a_n se chama coeficiente líder;*
- *Quando o coeficiente líder for igual a 1, o polinômio é dito mônico.*

Exemplo 2.1: Considere o polinômio $f(x) = 3+5x+10x^5+7x^9$. O grau desse polinômio é 9 e o coeficiente líder é 7.

Exemplo 2.2: Considere o polinômio $f(x) = 3+5x+57x^2+x^5$. O grau desse polinômio é 5 e ele é mônico.

Proposição 2.1 *Sejam A um domínio de integridade e $f(x), g(x) \in A[x]$.*

- $grau(f(x) + g(x)) \leq max\{grau(f(x)), grau(g(x))\}$
- $grau(f(x).g(x)) = grau(f(x)) + grau(g(x))$.

Exemplo 2.3: Sendo $f(x) = 1 + x^2, g(x) = 2 + x \in \mathbb{R}[x]$, tem-se que $f(x) + g(x) = 3 + x + x^2$, e nesse caso, o $grau(f(x) + g(x)) = grau(f(x))$.

Exemplo 2.4: Sendo $f(x) = 1 + x^2, g(x) = 2 + x - x^2 \in \mathbb{R}[x]$ o polinômio $f(x) + g(x) = 3 + x$, e nesse caso o $grau(f(x) + g(x)) = 1 < max\{grau(f(x)), grau(g(x))$.

Exemplo 2.5: Sendo $f(x) = 2 + 3x + 4x^2$, $g(x) = 3 + x + 2x^3 \in \mathbb{R}[x]$ o polinômio $f(x)g(x) = 6 + 11x + 15x^2 + 8x^3 + 6x^4 + 8x^5$ e de fato o $grau(f(x).g(x)) = grau(f(x)) + grau(g(x))$.

Definição 2.2 *Seja A um domínio de integridade. Dados dois polinômios $f(x), g(x) \in A[x]$, dizemos que $g(x)$ divide $f(x)$ se houver um polinômio $h(x) \in A[x]$, tal que, $f(x) = g(x)h(x)$. Nesse caso, denota-se $g(x) \mid f(x)$. Caso contrário, é dito que $g(x)$ não divide $f(x)$, e escreve-se $g(x) \nmid f(x)$.*

Exemplo 2.6: Sejam $p(x) = 2x^4 + 3x^3 + x^2$, $g(x) = 2x^3 + x^2 \in \mathbb{Z}[x]$. O polinômio $g(x) \mid p(x)$, pois existe $h(x) = x + 1 \in \mathbb{Z}[x]$ *tal que* $p(x) = g(x)h(x)$.

Teorema 2.1 *Seja $\mathbb{K}$ um corpo. Se $f(x), g(x) \in \mathbb{K}[x]$, então existem únicos $q(x), r(x) \in \mathbb{K}[x]$ tais que:*

$$f(x) = q(x)g(x) + r(x)$$

onde $r(x) = 0$ ou $grau(r(x)) < grau(g(x))$.

Demonstração. Sejam $f(x) = a_0 + \cdots + a_n x^n$ e $g(x) = b_0 + \cdots + b_m x^m$ com $grau(g(x)) = m$.
Se $f(x) = 0$, basta tomar $q(x) = r(x) = 0$. Suponhamos agora $f(x) \neq 0$, assim, $grau(f(x)) = n$, dessa maneira, temos duas situações a analisar: $n < m$ e $n \geq m$. Se $n < m$, basta que $q(x) = 0$, e portanto $f(x) = r(x)$. Resta analisar $n \geq m$. Para isso, definimos o seguinte polinômio: $f_1(x) = f(x) - a_n b_m^{-1} x^{n-m} g(x)$, observe que o $grau(f_1(x)) < grau(f(x)$. Assim, procederemos por indução sobre $grau(f(x))$.
Se $n = 0$, como $n \geq m$ então $m = 0$ e portanto $f(x) = a_0 \neq 0, g(x) = b_0 \neq 0$ e teremos, $f(x) = a_0 b_0^{-1} g(x)$ e basta por $q(x) = a_0 b_0^{-1}$ e $r(x) = 0$.
Pela igualdade $f_1(x) = f(x) - a_n b_m^{-1} x^{n-m} g(x)$ e do fato que $grau(f_1(x)) < grau(f(x))$, temos, pela hipótese de indução, que: $\exists q_1(x), r_1(x)$ tais que:

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

onde $r_1(x) = 0$ ou $grau(r_1(x)) < grau(g(x))$. Daí segue que, $f(x) = (q_1(x) + a_n b_m^{-1} x^{n-m)})g(x) + r_1(x)$ e, portanto, tomando $q(x) = q_1(x) + a_n b_m^{-1} x^{n-m}$ e $r_1(x) = r(x)$, sendo assim, provado a existência dos polinômios $q(x)$ e $r(x)$ tais que $f(x) = q(x)g(x) + r(x)$ e $r(x) = 0$ ou $grau(r(x)) < grau(g(x))$. Resta agora provar a unicidade. Sejam $q_1(x), q_2(x), r_1(x)$ *e* $r_2(x)$ tais que:

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

onde $r_i(x) = 0$ *ou* $grau(r_i(x)) < grau(g(x)), i = 1, 2$.

Daí segue que, $(q_1(x) - q_2(x))g(x) = r_2(x) - r_1(x)$. Observe que, se $q_1(x) \neq q_2(x)$ então o polinômio à esquerda tem grau maior ou igual que $g(x)$, enquanto o grau do polinômio à direita tem grau menor que $g(x)$, o que é uma contradição, logo, $q_1(x) = q_2(x)$ e dai segue que $r_1(x) = r_2(x)$.

■

Proposição 2.2 *Seja* $\mathbb{K}$ *um corpo. Se* $f(x) = a_0 + \cdots + a_n x^n \in \mathbb{K}[x]$ *com* $a_n \neq 0$*, então o número de raízes de* $f(x)$ *em* $\mathbb{K}$ *é no máximo igual a* $grau(f(x)) = n$.

Demonstração. Se $f(x)$ não tiver raízes em $\mathbb{K}$ então a proposição está provada.

Suponhamos que $\alpha \in \mathbb{K}$ seja uma raiz de $f(x)$.

Assim, pela proposição 1.2, temos que existe algum $q(x) \in \mathbb{K}[x]$ tal que $f(x) = q(x)(x - \alpha)$ com $grau\Big(q(x)\Big) = n - 1$.

Como não existe divisores de zero em um corpo, segue que, se $\beta \in \mathbb{K}$ é uma raiz de $f(x)$ então, $f(\beta) = q(\beta)(\beta - \alpha) = 0 \Rightarrow \beta = \alpha$ ou β é também uma raiz de $q(x)$. Assim, as raízes de $f(x)$ são α e as raízes de $q(x)$.

Vamos usar indução sobre $grau\Big(f(x)\Big) = n$.

Ora, se $n = 0$, então $f(x)$ não possuí raízes em $\mathbb{K}$ e, portanto, não há o que demonstrar.

Agora, por indução, $grau\Big(q(x)\Big) < grau\Big(f(x)\Big) = n$, $q(x)$ possui no máximo $grau\Big(q(x)\Big) = n - 1$ raízes em $\mathbb{K}$ e, portanto, $f(x)$ possui no máximo n raízes em $\mathbb{K}$.

■

Exemplo 2.7: O polinômio $f(x) = x^2 - 1 \in \mathbb{R}[x]$ possui duas raízes em $\mathbb{R}[x]$, sendo elas $x = 1$ *e* $x = -1$.

Exemplo 2.8: O polinômio $f(x) = x^3 + 1 \in \mathbb{R}[x]$ possui apenas uma raiz em $\mathbb{R}$, sendo ela $x = -1$. Perceba que, em $\mathbb{C}$, esse polinômio possui outras duas raízes, a saber, $\frac{1+i\sqrt{3}}{2}$ *e* $\frac{1-i\sqrt{3}}{2}$.

Teorema 2.2 *Se $p(x) \in \mathbb{R}[x]$ é um polinômio com grau n, então $p(x)$ possui exatamente n raízes em $\mathbb{C}$.*

Teorema 2.3 *Seja $p(x) = a_0 + ... + a_n x^n \in \mathbb{R}[x]$. Se $z \in \mathbb{C}$ é uma raiz de $p(x)$, então $\overline{z}$ também é raiz de $p(x)$.*

Demonstração. Sejam $z \in \mathbb{C}$ *e* $p(x) = a_0 + ... + a_n x^n \in \mathbb{R}[x]$ *tais que* $p(z) = 0$. Então, levando em consideração as propriedades de números complexos, temos:

$$p(\overline{z}) = a_0 + a_1\overline{z} + ... + a_n\overline{(z^n)} = \overline{a_0} + \overline{a_1}\ \overline{z} + ... + \overline{a_n}\overline{(z^n)} = \overline{a_0 + a_1 z + ... + a_n z^n} = \overline{0} = 0.$$

■

Observação: Todo polinômio $p(x) = a_0 + ... + a_n x^n \in \mathbb{R}[x]$, com n ímpar, possui pelo menos uma raiz real.

Exemplo 2.9: Considere o polinômio $f(x) = 1 - x^3$. Perceba que, $z = \frac{-1+i\sqrt{3}}{2}$ é uma raiz desse polinômio é que o seu conjugado $\overline{z} = \frac{-1-i\sqrt{3}}{2}$ também é raiz desse polinômio.

2.1 Irredutibilidade

Definição 2.3 *Seja K um domínio de integridade. Um polinômio $f(x) \in \mathbb{K}[x]$ é dito irredutível sobre K se, toda vem que $f(x) = g(x)h(x)$, tem-se $g(x) =$ a constante sobre K ou $h(x) = b$ constante sobre K. Se $f(x)$ não for irredutível sobre K, então ele é dito redutível sobre K.*

Observe que os polinômios irredutíveis sobre um domínio K têm papel análogo aos números primos em $\mathbb{Z}$.

Exemplo 2.10: O polinômio $f(x) = x^2 + 4$ é irredutível sobre $\mathbb{R}[x]$. O mesmo polinômio é redutível sobre $\mathbb{C}[x]$, veja, $f(x) = (x - 2i)(x + 2i)$.

Teorema 2.4 *Se $f(x)$ é um polinômio irredutível sobre $\mathbb{Z}[x]$, então $f(x)$ é irredutível sobre $\mathbb{Q}[x]$.*

Demonstração. Suponhamos que $f(x)$ seja irredutível sobre $\mathbb{Z}$, mas que $f(x) = g(x)h(x)$, onde $g(x), h(x) \in \mathbb{Q}[x]$ e $1 \leq grau\Big(g(x)\Big), grau\Big(h(x)\Big) < grau\Big(f(x)\Big)$.

Claramente, existe m tal que $mf(x) = g_1(x)h_1(x)$, onde $g_1(x), h_1(x) \in \mathbb{Z}[x]$.

Assim temos,

$$g_1(x) = a_0 + ... + a_s x^s,\ a_i \in \mathbb{Z}$$
$$h_1(x) = b_0 + ... + b_r x^r,\ b_j \in \mathbb{Z}$$

Suponhamos agora que $p \mid m$, p primo. Vamos provar que, $p \mid a_i \forall i \in \{1, ..., s\}$ ou $p \mid b_j \forall j \in \{1, ..., r\}$.

De fato, se $\exists i \in \{1, ..., s\}$ e $\exists j \in \{1, ..., r\}$ tais que $p \nmid i$ e $p \nmid j$.

Como $p \mid m$, temos que p divide o coeficiente de x^{i+j} do polinômio $mf(x) = g_1(x)h_1(x)$, isto é, $p \mid (b_0 a_{i+j} + ... + b_{i+j} a_0)$.

Pela escolha de i e j, temos que p divide cada parcela de, exceto $b_j a_i$, do coeficiente x^{i+j} de $g_1(x)h_1(x)$.

Como p divide toda a expressão, segue também que $p \mid a_i b_j$ e, como p é primo, temos que $p \mid a_i$ ou $p \mid b_j$, que é uma contradição.

Assim, se p é primo e $p \mid m$, então $p \mid a_i \forall i \in \{1, ..., s\}$ ou $p \mid b_j \forall j \in \{1, ..., r\}$.

Sem perda de generalidade, suponhamos que $p \mid a_i \forall i \in \{1, ..., s\}$.

Assim, $g_1(x) = pg_2(x)$, com $g_2(x) \in \mathbb{Z}[x]$, e $m = pm_1$. Temos, então,

$$pm_1 f(x) = pg_2(x)h_1(x)$$
$$m_1 f(x) = g_2(x)h_1(x).$$

Como o número de fatores primos de m é finito, prosseguindo o raciocínio chegaremos que:

$$f(x) = g^*(x)h^*(x)\ onde,\ g^*(x), h^*(x) \in \mathbb{Z}[x].$$

Com isso, temos que $g^*(x)$ e $h^*(x)$ são múltiplos racionais de $g(x)$ e $h(x)$, respectivamente, contradizendo a irredutibilidade de $f(x)$ sobre $\mathbb{Z}$.

■

Teorema 2.5 *Seja $f(x) = a_0 + ... + a_n, a_n \neq 0 \in \mathbb{Q}[x]$. Se existe um número primo p tal que,*
(i) $p \mid a_0, ..., a_{n-1}$
(ii) $p \nmid a_n,\ e\ p^2 \nmid a_0$
então $f(x)$ é irredutível sobre $\mathbb{Q}[x]$.

Demonstração. Pelo teorema anterior, é suficiente provar que $f(x)$ é irredutível em $\mathbb{Z}$. Suponhamos, por contradição, que

$$f(x) = g(x)h(x),\ g(x), h(x) \in \mathbb{Z}[x]$$
$$e\ 1 \leq grau\Big(g(x)\Big), grau\Big(h(x)\Big) < grau\Big(f(x)\Big) = n$$

Seja,

$$g(x) = b_0 + ... + b_r x^r \in \mathbb{Z}[x],\ grau\Big(g(x)\Big) = r$$
$$h(x) = c_0 + ... + c_s x^s \in \mathbb{Z}[x],\ grau\Big(h(x)\Big) = s$$

Assim,$n = r + s$.

Agora, $b_0 c_0 = a_0$, desse modo, $p \mid b_0$ ou $p \mid c_0$ e como $p^2 \nmid a_0$ segue que, p dividi apenas um dos dois inteiro b_0, c_0. Vamos admitir, sem perda de generalidade, que $p \mid b_0$ e $p \nmid c_0$.

Dessa forma, $a_n = b_r c_s$ é o coeficiente de $x^n = x^{r+s}$ e, portanto, $p \nmid b_r$ e $p \nmid b_0$. Seja b_i o primeiro coeficiente que p não divide.

Agora, $a_i = b_0 c_i + ... + b_i c_0$ e, como $p \mid b_0, ..., b_{i-1}, p \nmid b_i$ e $p \nmid c_0 \Rightarrow p \nmid a_i \Rightarrow i = n$ o que é um absurdo, pois, $1 \leq i \leq r < n$.

■

Exemplo 2.11: O polinômio $p(x) = 2 + 4x + 6x^2 + 18x^5 + 7x^{10}$ é irredutível sobre $\mathbb{Q}$, pois *existe* 2 que é primo, tal que, divide todos os coeficientes de $p(x)$, exceto o coeficiente líder, e $2^2 \nmid 2$.

Proposição 2.3 *Seja p um número primo e seja $\mathbb{Z}_p = \{\overline{0}, ..., \overline{p-1}\}$ o corpo contendo p elementos. Se $f(x) = a_0 + ... + a_n x^n \in \mathbb{Z}[x]$ vamos definir $\overline{f}(x) \in \mathbb{Z}_p[x]$ da seguinte maneira:*

$$\overline{f}(x) = \overline{a} + ... + \overline{a_n} x^n$$

Onde $\overline{a_i} = a_i + p\mathbb{Z}$ é a classe de equivalência módulo p, cujo representante é $a_i \in \mathbb{Z}$. Então,

$$\phi : \mathbb{Z}[x] \to \mathbb{Z}_p[x]$$
$$f(x) \mapsto \overline{f}(x)$$

define um homomorfismo sobre $\mathbb{Z}[x]$ sobre o domínio $\mathbb{Z}_p[x]$. Se $p \nmid a_n$ e $\overline{f}(x)$ é irredutível sobre $\mathbb{Z}_p$, então $f(x)$ é irredutível sobre $\mathbb{Q}$.

Demonstração. Iremos provar usando a contrapositiva.

Suponhamos $f(x) = a_0 + ... + a_n x^n \in \mathbb{Z}[x]$ seja redutível sobre $\mathbb{Q}$, com $grau\Big(f(x)\Big) = n$, e que $p \nmid a_n$, onde p é primo. Então, sabemos que

$$\exists g(x) = b_0 + ... + b_s x^s \in \mathbb{Z}[x],\ com\ grau\Big(g(x)\Big) = s$$
$$\exists h(x) = c_0 + ... + c_r x^r \in \mathbb{Z}[x],\ com\ grau\Big(h(x)\Big) = r$$

Com $1 \leq s \leq r < n$, tais que, $f(x) = g(x)h(x)$.

Das definições apresentadas segue que:

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

onde $\overline{h}(x), \overline{g}(x) \in \mathbb{Z}_p[x]$.

Mais ainda, como $a_n = b_r c_s$ e $p \nmid a_n$, segue que, $p \nmid b_r$ e $p \nmid c_s$, logo, o $grau\Big(\overline{g}(x)\Big) = s$ e $grau\Big(\overline{h}(x)\Big) = r$. Portanto, $\overline{f}(x)$ é redutível sobre $\mathbb{Z}_p[x]$.

■

Exemplo 2.12: Vamos mostrar que o polinômio $p(x) = x^4 + x^3 + x^2 + x + 1$ é irredutível sobre os racionais. Antes de tudo, perceba que o teorema 2.5 não se aplica a esse polinômio.

Agora, considere $p = 3$. Vamos reduzir esse polinômio a $\mathbb{Z}_3[x]$, isto é, $\overline{p}(x) = x^4 + x^3 + x^2 + x + 1$, supondo que $\overline{p}(x)$ seja redutível em $\mathbb{Z}_3[x]$, existem apenas duas possibilidades, sendo elas o produto de um polinômio $\overline{h}(x)$ com grau$\Big(h(x)\Big) = 1$ por um outro polinômio $\overline{g}(x)$ com grau$\Big(g(x)\Big) = 3$, ou o produto de dois polinômio $\overline{h}(x)$ e $\overline{g}(x)$ com grau 2.

A primeira opção é de fácil verificação quanto à sua impossibilidade, pois nenhum elemento de $\mathbb{Z}_3$ é raiz de $\overline{p}(x)$, e fatorar por um polinômio de grau um é equivalente a fatorar por uma raiz.

Para a segunda opção, é necessário realizar a seguinte verificação:

$x^4 + x^3 + x^2 + x + 1 = (ax^2 + bx + c)(a'x^2 + b'x + c') \iff aa'x^4 + (ab' + ba')x^3 + (ac' + bb' + ca')x^2 + (bc' + cb')x + cc' = x^4 + x^3 + x^2 + x + 1 \iff$

$$\begin{cases} aa' = 1 \\ ab' + ba' = 1 \\ ac' + bb' + ca' = 1 \\ bc' + cb' = 1 \\ cc' = 1 \end{cases}$$

Da primeira e última linha, temos algumas possibilidades que são $a = a' = 1$, $a = a' = 2$, $c = c' = 1$ e $c = c' = 2$.

Fazendo, $a = a' = c = c' = 1$, isso implica em $b = b' = 2$, ou $b = 1\ e\ b' = 0$, para a segunda e quarta linha, e isso leva a um absurdo para a terceira linha, no primeiro caso $0 = 1$ e no segundo $2 = 1$.

Agora, $a = a' = 1\ e\ c = c' = 2$, isso implica em valores diferentes para $b\ e\ b'$ na segunda e quarta linha.

E por fim, $a = a' = c = c' = 2$, isso implica em $b = b' = 1$, ou $b = 2$ *e* $b' = 0$ para a segunda e quarta linha, e isso, leva a um absurdo para a terceira linha, no primeiro caso $0 = 1$ e no segundo $2 = 1$.

Logo, como $\overline{p}(x)$ é irredutível em $\mathbb{Z}_3[x]$, então $p(x)$ é irredutível sobre os racionais.

3 Extensões finitas:

Definição 3.1 *Dado dois corpos* $\mathbb{K}$ *e* $\mathbb{L}$*, diremos que* $\mathbb{L}$ *é uma extensão de* $\mathbb{K}$*, quando* $\mathbb{K}$ *for um subcorpo de* $\mathbb{L}$*. Iremos usar a seguinte notação* $\mathbb{L} \supset \mathbb{K}$*.*

Exemplo 3.1: $\mathbb{Q}[\sqrt{2}]$ é uma extensão de $\mathbb{Q}$.

Definição 3.2 *Um elemento* $\alpha \in \mathbb{L}$ *é dito álgebrico sobre* $\mathbb{K}$*, se houver um polinômio* $p(x) \in \mathbb{K}[x]$*, tal que,* $p(\alpha) = 0$*. Um elemento* α *é dito transcendental se ele não for álgebrico.*

Exemplo 3.2: A constante $i \in \mathbb{C}$ é álgebrica sobre $\mathbb{R}$, pois existe $p(x) = x^2 + 1 \in \mathbb{R}[x]$, tal que, $p(i) = 0$.

Exemplo 3.3: Os números "e, π"são exemplos de elementos transcendentais sobre $\mathbb{Q}$, pois não existe $p(x) \in \mathbb{Q}[x]$, tal que, $p(e) = 0, p(\pi) = 0$. Não iremos demonstrar esse fato, mas usaremos ele futuramente.

Definição 3.3 *Se para todo* $\alpha \in \mathbb{L} \supset \mathbb{K}$ *ele for álgebrico sobre* $\mathbb{K}$ *então a extensão* $\mathbb{L} \supset \mathbb{K}$ *é dita álgebrica.*

Exemplo 3.4: A extensão $\mathbb{Q}[\sqrt{2}] \supset \mathbb{Q}$ é álgebrica, pois qualquer que seja o elemento $a + b\sqrt{2} \in \mathbb{Q}[\sqrt{2}]$ ele é raiz do polinômio $p(x) = x^2 - 2ax + a^2 - 2b^2 \in \mathbb{Q}[x]$.

Definição 3.4 *Seja* $\alpha \in \mathbb{L} \supset \mathbb{K}$*. Definiremos* $\mathbb{K}[\alpha] = \{f(\alpha) : f(x) \in \mathbb{K}[x]\}$*.*

Exemplo 3.5: Seja $i \in \mathbb{C} \supset \mathbb{R}$, vamos mostrar que $\mathbb{R}[i] = \mathbb{C} = \{a + bi : a, b \in \mathbb{R}\}$. De fato, por definição temos que $\mathbb{R}[i] = \{f(i) : f(x) \in \mathbb{R}[x]\}$. Agora se $f(x) \in \mathbb{R}[x]$, segue pelo algoritmo da divisão que existem $q(x), r(x) \in \mathbb{R}[x]$ tais que $f(x) = q(x)(x^2+1)+r(x)$, onde $r(x) = a + bx, a, b \in \mathbb{R}$, e dai vem que $f(i) = q(i)(i^2 + 1) + r(i) = a + bi$.

Definição 3.5 *Sejam* $\alpha \in \mathbb{L}$ *algébrico sobre* $\mathbb{K}$*, e* $p(x) \in \mathbb{K}[x]$ *mônico, e de menor grau tal que,* $p(\alpha) = 0$*. Segue que,* $p(x)$ *é o único polinômio mônico e irredutível sobre* $\mathbb{K}[x]$*, tal que,* $p(\alpha) = 0$*. Esse polinômio será denotado por* $irr(\alpha, \mathbb{K})$*.*

Exemplo 3.6: Seja $i \in \mathbb{C} \supset \mathbb{R}$. Na notação apresentada temos que $irr(i, \mathbb{R}) = x^2 + 1$.

Proposição 3.1 *Sejam* $\mathbb{L} \supset \mathbb{K}$ *uma extensão de corpo, e* $\alpha \in \mathbb{L}$ *algébrico sobre* $\mathbb{K}$*. Se o grau do polinômio* $irr(\alpha, \mathbb{K})$ *é* n*, então*

a) $\forall f(x) \in \mathbb{K}[x]$*,* $f(\alpha)$ *pode ser expresso de modo único na forma* $f(\alpha) = a_0 + a_1\alpha + ... + a_{n-1}\alpha^{n-1}, a_i \in \mathbb{K}$*.*

b) $\mathbb{K}[\alpha] = \{a_0 + ... + a_{n-1}\alpha^{n-1}\}$ *é um subcorpo de* $\mathbb{L}$ *que contém* $\mathbb{K}$*.*

Demonstração. Seja $p(x) = irr(x, \mathbb{K})$. Por hipótese o grau de $p(x)$ é igual a n.

(a) Se $f(x) \in \mathbb{K}[x]$ então pelo algoritmo da divisão $\exists q(x), r(x) \in \mathbb{K}[x]$ tais que: $f(x) = q(x)p(x) + r(x)$, onde $r(x) = 0$, *ou* $grau(r(x)) < grau(p(x))$. Dessa forma $r(x) = a_0 + ... + a_{n-1}x^{n-1}, a_i \in \mathbb{K}, i = 0, 1, ..., n-1$. Dai temos que,

$$f(\alpha) = q(\alpha)p(\alpha) + r(\alpha) = r(\alpha) = a_0 + ... + a_{n-1}\alpha^{n-1}$$

Para demonstrar a unicidade temos que: se $f(\alpha) = a_0 + ... + a_{n-1}\alpha^{n-1} = b_0 + ... + b_{n-1}\alpha^{n-1}, a_i, b_i, \in \mathbb{K}, \forall i \in \{0, 1, ..., n-1\}$ segue imediato que o polinômio $q(x) \in \mathbb{K}[x]$ onde, $q(\alpha) = 0$, como $irr(\alpha, \mathbb{K}) = n$, segue que, $q(x) = 0$, e com isso, $a_i = b_i, \forall i \in \{0, 1, ..., n-1\}$.
(b) Consequência direta do item a.

■

Exemplo 3.7: Seja $\mathbb{C} \supset \mathbb{Q}$. Temos que $\sqrt[3]{2} \in \mathbb{C}$ é algébrico sobre $\mathbb{Q}$, pois existe $p(x) = x^3 - 2 \in \mathbb{Q}[x]$, tal que, $p(\sqrt[3]{2}) = 0$. Então pela proposição apresentada, $\mathbb{Q}[\sqrt[3]{2}] = a + b\sqrt[3]{2} + c(\sqrt[3]{2})^2; a, b, c \in \mathbb{Q}$.

Exemplo 3.8: Seja $\mathbb{C} \supset \mathbb{Q}[\sqrt{2}]$. Temos que $\sqrt{3} \in \mathbb{C}$ é algébrico sobre $\mathbb{Q}[\sqrt{2}]$, pois existe $p(x) = x^2 - 3 \in \mathbb{Q}[\sqrt{2}][x]$, tal que, $p(\sqrt{3}) = 0$. Então pela proposição apresentada, $\mathbb{Q}[\sqrt{2}, \sqrt{3}] = a + b\sqrt{3}; a, b \in \mathbb{Q}\sqrt{2}$. Isto é,

$$\begin{aligned} a + b\sqrt{3} &= (a_1 + a_2\sqrt{2}) + (a_3 + a_4\sqrt{2})\sqrt{3} \\ &= (a_1 + a_2\sqrt{2}) + (a_3\sqrt{3} + a_4\sqrt{2}\sqrt{3}) \\ &= a_1 + a_2\sqrt{2} + a_3\sqrt{3} + a_4\sqrt{6},\ a_1, a_2, a_3, a_4 \in \mathbb{Q} \end{aligned}$$

Teorema 3.1 *Se $\alpha \in \mathbb{L} \supset \mathbb{K}$ e se $\Psi : \mathbb{K}[x] \to \mathbb{L}$ é definida por $\Psi(f(x)) = f(\alpha)$, então Ψ é um homomorfismo tal que.*

i) $Im\Psi = \mathbb{K}[\alpha],\ \mathbb{L} \supset \mathbb{K}[\alpha] \supset \mathbb{K}$.

ii) α *é transcendental sobre* $\mathbb{K} \iff N(\Psi) = 0$.

iii) Se α *é álgebrico sobre* $\mathbb{K}$ *e* $p(x) = irr(\alpha, \mathbb{K})$, *então* $N(\Psi) = \mathbb{K}[x] \cdot p(x)$ *é um ideial maximal de* $\mathbb{K}[x]$.

iv) $\mathbb{K}[x]/N(\psi) \cong \mathbb{K}[\alpha]$.

Exemplo 3.9: Do exemplo 3.2, e pelos itens iii e iv desse teorema temos que, $\mathbb{R}[x]/\mathbb{R}[x](x^2 + 1) \cong \mathbb{C}$.

Considere a extensão de corpos $\mathbb{L} \supset \mathbb{K}$, ela pode ser vista como um espaço vetorial sobre o corpo $\mathbb{K}$, a partir das seguintes operações:

$$\mathbb{L} \times \mathbb{L} \to \mathbb{L}\ e\ \mathbb{K} \times \mathbb{L} \to \mathbb{L}$$

$$(u, v) \mapsto (u + v)\ (\lambda, u) \mapsto \lambda u$$

A verificação é imediato ao fato de $\mathbb{K}$ ser subcorpo de $\mathbb{L}$.

Definição 3.6 *A dimensão $\mathbb{K}$-espaço de $\mathbb{L}$ é denotada por $[\mathbb{L} : \mathbb{K}]$ e é chamada de grau da extensão $\mathbb{L} \supset \mathbb{K}$. Dizemos que $\mathbb{L} \supset \mathbb{K}$ é uma extensão finita quando $[\mathbb{L} : \mathbb{K}] < \infty$.*

Definição 3.7 *Dizemos que os elementos $\beta_0, \beta_1, \ldots, \beta_n \in \mathbb{L}$ formam uma base $\mathbb{L} \supset \mathbb{K}$ quando for uma base $\mathbb{K}$-espaço de $\mathbb{L}$.*

Exemplo 3.10: A extensão $\mathbb{Q}[\sqrt{2}] \supset \mathbb{Q}$ tem grau dois, e uma base para essa extensão é $\{1, \sqrt{2}\}$.

Exemplo 3.11: A extensão $\mathbb{Q}[\sqrt{3}, \sqrt{2}] \supset \mathbb{Q}[\sqrt{2}]$ tem grau dois, e uma base para essa extensão é $\{1, \sqrt{3}\}$.

Exemplo 3.12: A extensão $\mathbb{Q}[\sqrt[3]{2}] \supset \mathbb{Q}$ tem grau três, e uma base para essa extensão é $\{1, \sqrt[3]{2}, (\sqrt[3]{2})^2\}$.

Proposição 3.2 $[\mathbb{L} : \mathbb{K}] = 1 \Longleftrightarrow \mathbb{L} = \mathbb{K}$.

Demonstração. $\Rightarrow$ $\{1\}$ é uma base de $\mathbb{L} \supset \mathbb{K}$, $\alpha \in \mathbb{L} \Rightarrow \alpha = \alpha 1$ para algum α em $\mathbb{K}$, com isso $\alpha = \alpha$.

$\Leftarrow$ Imediato ao fato de $\{1\}$ ser a base de $\mathbb{L} \supset \mathbb{K}$.

■

Proposição 3.3 *Se α é algébrico sobre $\mathbb{K}$, então $[\mathbb{K}(\alpha) : \mathbb{K}]$ é o grau do polinômio $irr(\alpha, \mathbb{K})$.*

Teorema 3.2 *Se $\mathbb{M} \supset \mathbb{L} \supset \mathbb{K}$ então $[\mathbb{M} : \mathbb{K}] = [\mathbb{M} : \mathbb{L}][\mathbb{L} : \mathbb{K}]$.*

Demonstração. Sejam $v_1, ..., v_r$ uma base de $\mathbb{M}$ sobre $\mathbb{L}$ e seja $u_1, ..., u_s$ uma base de $\mathbb{L}$ sobre $\mathbb{K}$. Vamos provar que:

$\beta = \left\{ v_i u_j : \begin{matrix} i = 1, ..., r \\ j = 1, ..., s \end{matrix} \right\}$ é uma base de $\mathbb{M}$ sobre $\mathbb{K}$ e isso demonstra o teorema.

De fato, primeiramente vamos provar que β é um conjunto L.I em $\mathbb{M}$ sobre $\mathbb{K}$.

Se $\alpha_{ij} \in \mathbb{K}, 1 \leq i \leq r, 1 \leq j \leq s$, e $\sum\limits_{i,j} \alpha_{ij} v_i u_j = 0 \Longleftrightarrow (\alpha_{11} u_1 + \alpha_{12} u_2 + ... + \alpha_{1s} u_s) v_1 + ... + \alpha_{r1} u_1 + \alpha_{12} u_2 + ... + \alpha_{rs} u_s) v_r = 0$

Ora como os $u_j' s$ estão em $\mathbb{L}$ segue pela independência linear dos $v_i' s$ em $\mathbb{M}$ sobre $\mathbb{L}$, que:

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

Agora, como os $\alpha'_{ij}s$ estão em $\mathbb{K}$ segue pela independência linear dos $u'_j s$ em $\mathbb{L}$ sobre $\mathbb{K}$ que cada $\alpha'_{ij}s = 0$. Assim, β é L.I de $\mathbb{M}$ sobre $\mathbb{K}$.

Agora, iremos mostrar que β gera a totalidade de $\mathbb{M}$ sobre $\mathbb{K}$. Seja $y \in \mathbb{M}$.

Sendo $v_1, ..., v_r$ uma base de $\mathbb{M}$ sobre $\mathbb{L}$ então existem $\lambda_1, ..., \lambda_r \in \mathbb{L}$, tais que,

$$y = \lambda_1 v_1 + ... + \lambda_r v_r$$

Sendo cada $\lambda_i \in \mathbb{L}$ e $u_1, ..., u_s$ uma base de $\mathbb{L}$ sobre $\mathbb{K}$ então existem $\alpha_{ij} \in \mathbb{K}, 1 \leq i \leq r, 1 \leq j \leq s$, tais que,

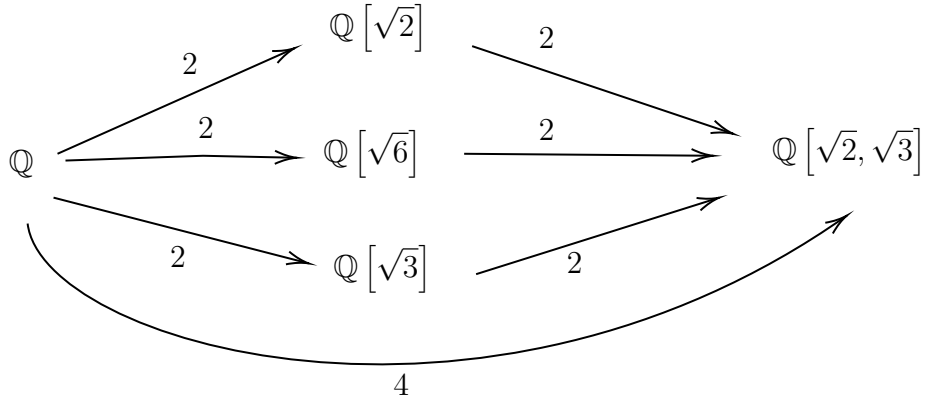
$$\lambda_i = \alpha_{i1} u_1 + ... + \alpha_{is} u_s$$

E dai segue imediatamente que,

$$y = \sum_{i,j} \alpha_{ij} v_i u_j, \alpha_{ij} \in \mathbb{K}.$$

■

Exemplo 3.13: O grau da extensão $\mathbb{Q}[\sqrt{2}, \sqrt{3}] \supset \mathbb{Q}$ é quatro, pois, do teorema 3.2, temos que $\Big[\mathbb{Q}[\sqrt{2}, \sqrt{3}] : \mathbb{Q}\Big] = \Big[\mathbb{Q}[\sqrt{2}, \sqrt{3}] : \mathbb{Q}[\sqrt{2}]\Big]\Big[\mathbb{Q}[\sqrt{2}] : \mathbb{Q}\Big] = \Big[\mathbb{Q}[\sqrt{2}, \sqrt{3}] : \mathbb{Q}[\sqrt{3}]\Big]\Big[\mathbb{Q}[\sqrt{3}] : \mathbb{Q}\Big]$. Perceba que, entre o corpo $\mathbb{Q}$ e $\mathbb{Q}[\sqrt{2}, \sqrt{3}]$ tem mais um corpo além de $\mathbb{Q}[\sqrt{2}]$ e $\mathbb{Q}[\sqrt{2}]$.



Os elementos da base da extensão $\mathbb{Q}[\sqrt{2}, \sqrt{3}] \supset \mathbb{Q}$ são $\{1, \sqrt{2}, \sqrt{3}, \sqrt{6}\}$.

Observações: Se $\mathbb{M} \supset \mathbb{L} \supset \mathbb{K} < \infty$ então $[\mathbb{M} : \mathbb{L}]$ e $[\mathbb{L} : \mathbb{K}]$ dividem $[\mathbb{M} : \mathbb{K}]$. Se $[\mathbb{M} : \mathbb{K}]$ for primo não existe nenhum corpo estritamente entre $\mathbb{M}$ e $\mathbb{K}$.

Corolário 3.1 *Seja $\mathbb{L} \supset \mathbb{K}$ uma extensão de corpo finita de grau n. Seja α um elemento algébrico sobre $\mathbb{K}$. Então, o grau do polinômio $irr(\alpha, \mathbb{K})$ divide n.*

Exemplo 3.14: Todos os polinômios irredutíveis sobre $\mathbb{R}[x]$ possuem grau 1 ou 2. Isso pois, $\mathbb{C} = \mathbb{R}[i]$ como vimos no exemplo 3.5, e portanto todos os elementos de $\mathbb{C}$ são algébricos sobre os $\mathbb{R}$, logo, para cada $\alpha \in \mathbb{C}$ existe um polinômio $irr(\alpha, \mathbb{R})$, e de acordo com o corolário 3.1 $irr(\alpha, \mathbb{R})$ tem que dividir $[\mathbb{C} : \mathbb{R}] = 2$.

4 Construções envolvendo régua e compasso

Nesse capítulo iremos usar da teoria de extensão de corpo para entender de uma maneira algébrica as construções envolvendo régua e compasso. Dessa maneira, será inicialmente apresentado variados exemplos de construções, para assim, ser dado continuidade com teoremas relacionados, e assim, entender quando uma construção é possível ser feita, isso é, quais são os requisitos que elas devem cumprir. E por fim, concluir que de fato é impossível construir com régua e compasso os três problemas clássicos da geometria.

Construções que provaremos ser impossíveis de serem construídas com régua e compasso:

i) Um quadrado de área igual à de um circulo dado;

ii) Um cubo com o dobro do volume de um cubo dado;

iii) Um ângulo igual a um terço de um ângulo dado.

Para isso iremos considerar régua como um objeto sem quaisquer tipos de marcadores, isto é, régua é a ferramenta que liga dois pontos distintos. E o compasso possui a regra de ter a ponta seca e a ponta de grafite colocadas sempre em pontos já "construídos", ou seja, não se pode fazer uma abertura qualquer do compasso. Essa última regra é equivalente a dizer que obrigatoriamente as circunferências devem ter centro em pontos já existentes e também passar por pelo menos um ponto já existente.

Definição 4.1 *Seja $\mathcal{P}$ um subconjunto do $\mathbb{R}^2$ contendo pelo menos dois pontos distintos. Dizemos que uma reta r de $\mathbb{R}^2$ é uma reta em $\mathcal{P}$ se r contém dois pontos distintos em $\mathcal{P}$ e dizemos que uma circunferência c em $\mathbb{R}^2$ é uma circunferência em $\mathcal{P}$ se o centro de c pertence a $\mathcal{P}$ e um ponto de c está em $\mathcal{P}$. Por definição $\mathcal{P}_0 = \{O, U\}$, onde, $O = (0,0)$ e $U = (1,0)$.*

Chamaremos os itens a seguir de operações elementares em $\mathcal{P}$.

(i) Interseção de duas retas em $\mathcal{P}$;

(ii) Interseção de uma reta em $\mathcal{P}$ e uma circunferência em $\mathcal{P}$;

(iii) Interseção de duas circunferências em $\mathcal{P}$.

Um ponto $A \in \mathbb{R}^2$ é dito construível se for possível determinar A a partir dessas operações.

Denotaremos por $< \mathcal{P} >$ o subconjunto dos pontos de $\mathbb{R}^2$ que são construíveis a partir de $\mathcal{P}$.

Exemplo 4.1: $< \mathcal{P}_0 >= \{O, U, A_1, A_2, A_3, A_4\}$. Pois por definição existe a reta que passa por O e U, e também existem as circunferências com centro em U passando por O, e com centro em O passando por U, desse modo, pelas operações (ii) e (iii) os pontos A_1, A_2, A_3 *e* A_4 são construíveis.

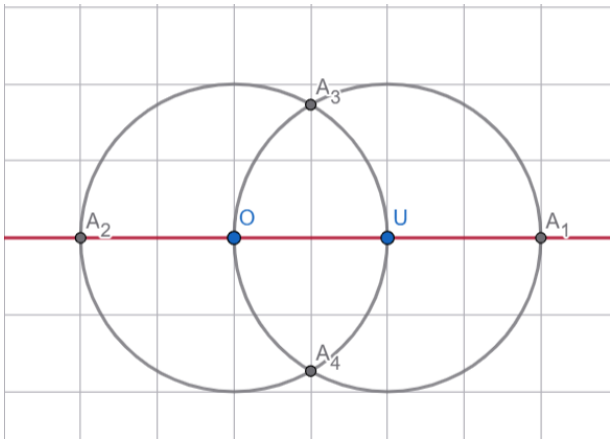


Figura 1: Pontos construíveis a partir de $\mathcal{P}_0$

Agora, seja $\mathcal{P}_0 = \{O, U\}, \mathcal{P}_1 =< \mathcal{P}_0 >, ..., \mathcal{P}_{n+1} =< \mathcal{P}_n >, \forall n \in \mathbb{N}$.
Desse modo, $\mathcal{P}_0 \subset \mathcal{P}_1 \subset ... \subset \mathcal{P}_n \subset \mathcal{P}_{n+1} \subset ... \subset \mathbb{R}^2$.

Perceba que, usando o sistema de coordenadas cartesiana $A_1 = (2, 0)$, $A_2 = (-1, 0)$, $A_3 = (\frac{1}{2}, \frac{\sqrt{3}}{2})$ e $A_4 = (\frac{1}{2}, -\frac{\sqrt{3}}{2})$. Isto é, $\mathcal{P}_1 = \{(0, 0), (1, 0), (-1, 0), (2, 0), (\frac{1}{2}, \frac{\sqrt{3}}{2}), (\frac{1}{2}, -\frac{\sqrt{3}}{2})\}$.

Para melhor ilustração, iremos fazer $\mathcal{P}_2$. Para isso comece fazendo as retas que passam por A_1 *e* A_3, A_1 *e* A_4, A_2 *e* A_3, A_2 *e* A_4, perceba que até o momento nenhum novo ponto foi construído.

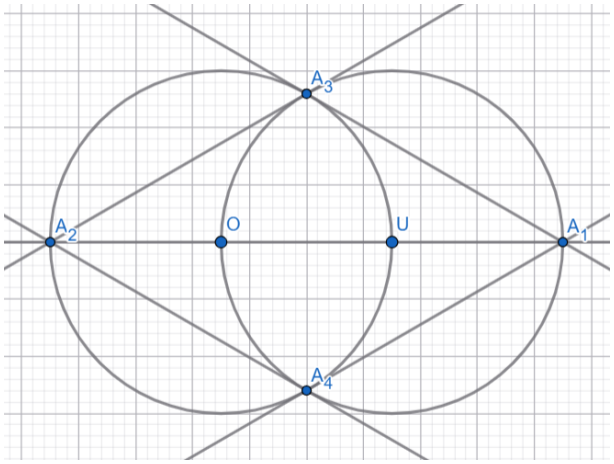


Figura 2: Encontrando $\mathcal{P}_2$

Agora, faça as reta que passam por O *e* A_3, O *e* A_4, U *e* A_3, U *e* A_4, A_3 *e* A_4. Perceba que, ao fazer isso treze novos pontos apareceram.

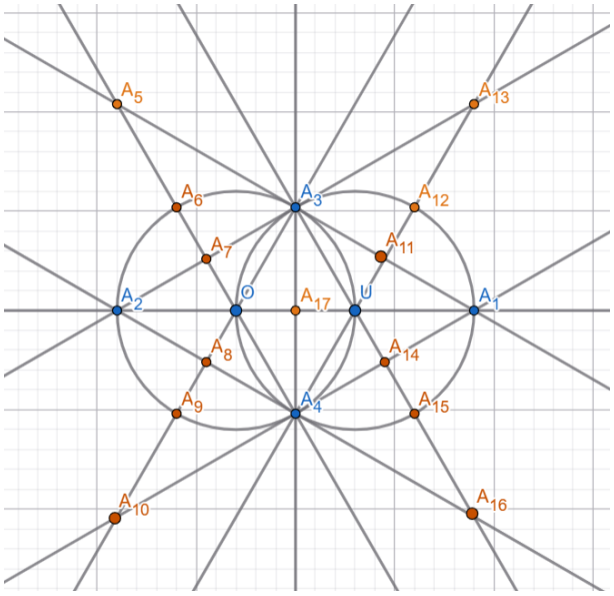


Figura 3: Encontrando $\mathcal{P}_2$

Agora resta fazer todas as circunferências tendo os pontos de $\mathcal{P}_0$ como centro e passando por um outro ponto de $\mathcal{P}_0$.

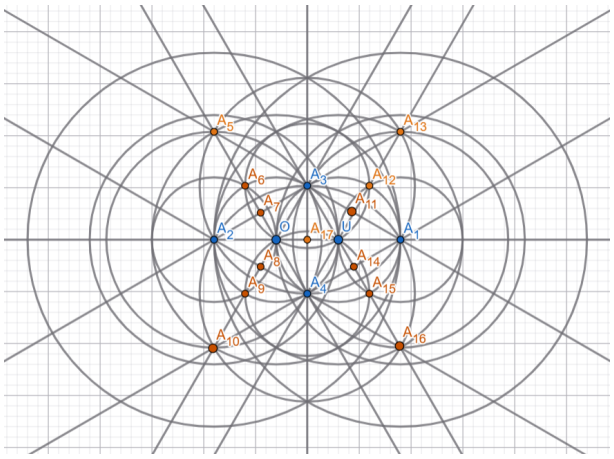


Figura 4: Encontrando $\mathcal{P}_2$

A fim de não poluir a imagem os pontos de interseção não foram marcados, no entanto, cada um deles pertencem a $\mathcal{P}_2$.

Denotaremos por $\mathcal{P}_\infty$ o conjunto de todos os pontos construíveis. Um número real a é dito construível se $(a, 0) \in \mathcal{P}_\infty$. Perceba que o conjunto dos números inteiros são construíveis. Basta fazer circunferências a direita e a esquerda de O.

Proposição 4.1 *Se A e B são pontos distintos construíveis então o ponto médio M do segmento $\overline{AB}$ é construível e as retas perpendiculares a $\overline{AB}$ passando pelos pontos A, B e M também são construíveis.*

Demonstração. Primeira faça a reta que contenha os pontos A, B, chamaremos de reta r. Em seguida faça duas circunferências, uma com o centro em A passando por

B, e a outra com centro em B passando por A. Dessa maneira, teremos quatro novos pontos de interseção, sendo eles, dois das interseção entre as circunferências, chamaremos de C, D, e outros dois das interseção entre circunferência e a reta r, denotaremos por E, F. Fazendo a reta que passa pelos pontos C, D o ponto de interseção dessa reta com a reta r é exatamente o ponto médio entre o segmento $\overline{AB}$, chame de M, e essa reta é também a reta perpendicular de r. Perceba agora que A é ponto médio do segmento $\overline{EB}$ e que B é o ponto médio do segmento $\overline{AF}$, desse modo repita o processo, e terá as retas perpendicular a r passando por A *e* B.

■

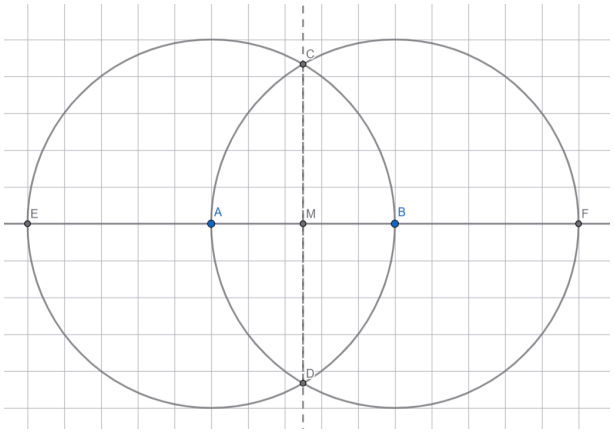


Figura 5: ponto médio M

Em particular, os eixos x, y são construíveis.

Proposição 4.2 *Seja A e r, respectivamente, um ponto construível e uma reta construível tais que $A \in r$. Se B e C são pontos construíveis então existe X tal que $X \in r$ e os segmentos $\overline{AX}$ e $\overline{BC}$ possuem o mesmo tamanho.*

Demonstração. Usando circunferências centradas em A e centradas em B podemos assumir que A, B e C pertencem a reta r, para ilustrar o porque podemos assumir A, B e C na mesma reta, veja a seguinte figura. A distância $\overline{BC} = \overline{BC'} = \overline{B'C''}$, então demonstrar para $\overline{B'C''}$ é o mesmo que para $\overline{BC}$.

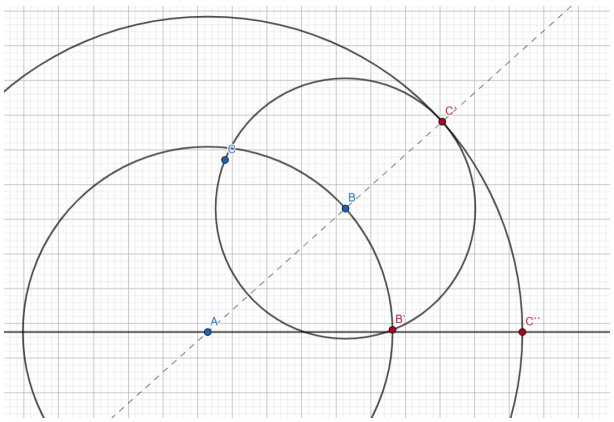


Figura 6: Construção proposição 4.2

Agora, seja M o ponto médio de BC e $N \in r$ um ponto construível tal que $\overline{AB} = \overline{BN}$ (para obter N basta fazer a circunferência centrada em B passando por A). Assim, $A, B, C, M, N \in r$ são pontos construíveis. Seja x o ponto de interseção entre a circunferência com centro em M passando por N e a reta r. Desse modo, $\overline{NM} = \overline{MX}$ e segue imediatamente dessa construção que $\overline{AB} = \overline{BN} = \overline{XC}$ e portanto, $\overline{AX} = \overline{BC}$ como queríamos.

■

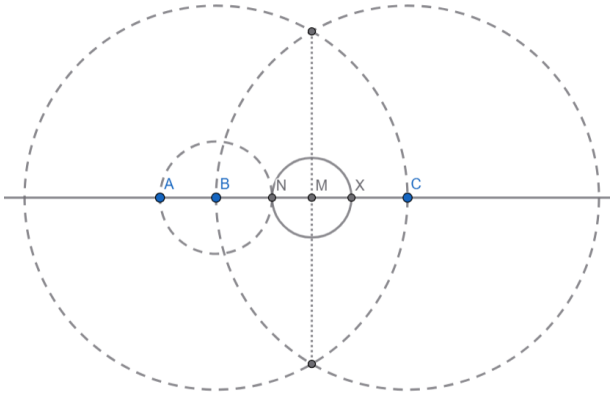


Figura 7: Transferência de segmento

Observe que a proposição 4.2 está garantindo a transferência de segmentos construíveis.

Proposição 4.3 *Sejam A, B e C três pontos construíveis não alinhados. Então existe um ponto D tal que, A, B, C e D formam um paralelogramo. Em particular a reta passando por C paralela ao segmento $\overline{AB}$ é construível.*

Demonstração. Sejam r e s as retas suportes, respectivamente, dos segmentos $\overline{AB}$ e $\overline{CA}$. Aplicando a proposição 4.2 para $B \in r$ encontramos um ponto construível $X \in r$ tal que $\overline{BX} = \overline{AC}$ e aplicando o mesmo resultado para $C \in s$ encontramos um ponto construível $Y \in s$ tal que $\overline{CY} = \overline{AB}$. Agora o ponto D é encontrado, interceptando as circunferências C_1 de centro B passando por X e C_2 de centro C e passando por Y.

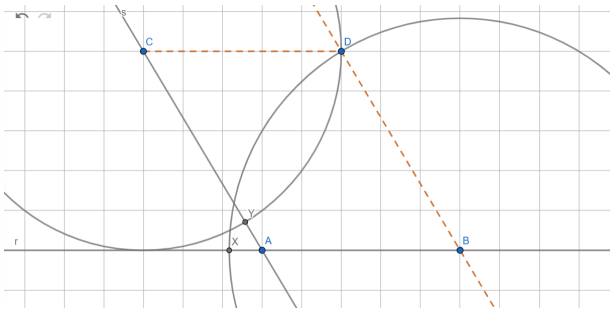


Figura 8: Paralelogramo

■

Proposição 4.4 *Um ponto $A = (a, b) \in \mathbb{R}^2$ é construível se, e somente se, as coordenadas $a, b \in \mathbb{R}^2$ são números construíveis.*

Demonstração. $\Rightarrow$ Seja $A = (a, b)$ um ponto construível e seja M o ponto médio do segmento $\overline{OA}$. Segue imediatamente da geometria elementar que o ponto $A_0 = (a, 0)$ é a interseção a reta $\overleftrightarrow{OU}$ e da circunferência de centro M passando por A como na figura abaixo

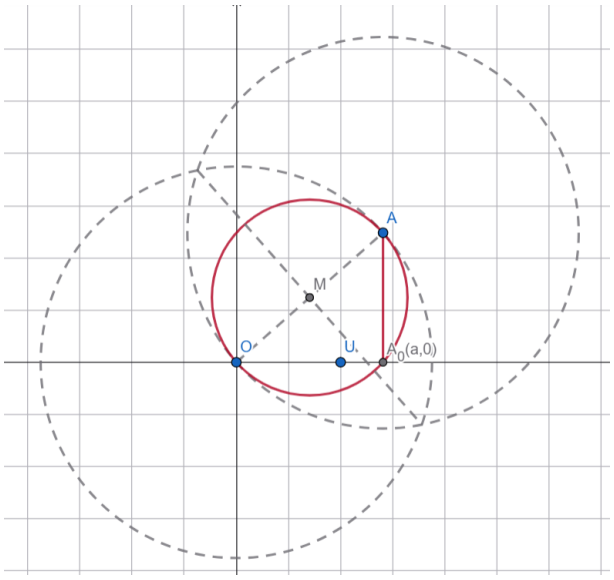


Figura 9: $A_0 = (a, 0)$

Achando o ponto $A_0 = (a, 0)$ pertencente a reta $\overleftrightarrow{OU}$ podemos pela proposição 4.2 encontrar o ponto $B_0 = (b, 0)$ traçando a partir de 0 uma circunferência de raio $\overline{A_0A}$. Portanto, dado um ponto $A = (a, b)$ construível os números a, b são construíveis.
$\Leftarrow$ Reciprocamente suponhamos a, b construíveis, isto é, $(a, 0)$ *e* $(b, 0) \in \mathcal{P}_\infty$. Lembre-se que da proposição 4.1 o eixo y é construível. Logo, dado $(b, 0)$ para obter $(0, b)$ é suficiente fazer uma circunferência centrada em 0 e passando por $(b, 0)$. Como sabemos construir paralelas e perpendiculares segue imediatamente a construção de (a, b) a partir de $(a, 0)$ *e* $(b, 0)$.

■

Teorema 4.1 *O conjunto dos números construíveis $\mathcal{L}_\mathbb{R} = \{\alpha \in \mathbb{R} : \alpha \text{ construtível}\}$ é um subcorpo dos $\mathbb{R}$.*

Demonstração. Sabemos que $\mathcal{L}_\mathbb{R}$ contém $\mathbb{Z}$. Temos que provar que:

- $\alpha, \beta \in \mathcal{L}_\mathbb{R} \Rightarrow \beta - \alpha \in \mathcal{L}_\mathbb{R}$;
- $\alpha, \beta \in \mathcal{L}_\mathbb{R} \Rightarrow \beta.\alpha \in \mathcal{L}_\mathbb{R}$;
- $0 \neq \alpha \in \mathcal{L}_\mathbb{R} \Rightarrow \frac{1}{\alpha} \in \mathcal{L}_\mathbb{R}$.

Vamos assumir sem perda de generalidade $\beta > \alpha > 0$. Sejam $A = (\alpha, 0)$ *e* $B = (\beta, 0)$. Pela proposição 4.2 segue imediatamente que podemos construir X à direita de O tal que $\overline{OX} = \overline{AB}$ e isso demonstra $\beta - \alpha$. Agora seja r uma reta construível como na figura abaixo e sejam $A_1, B_1 \in r$ construídos de modo que $\overline{OA_1} = \overline{OA} = \alpha$ e o segmento $\overline{BB_1}$ seja paralelo ao segmento $\overline{UA_1}$.

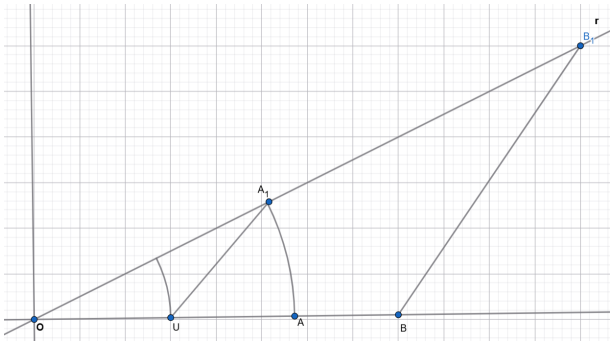


Figura 10: $\alpha.\beta$

Pelo caso ângulo-ângulo os triângulos $\Delta OA_1U \sim \Delta OB_1B$, logo temos que, $\frac{\alpha}{1} = \frac{\overline{OB_1}}{\beta}$ e isso nos diz que $\overline{OB_1} = \alpha\beta$. Na mesma reta r podemos fazer U_1 tal que $\overline{OU_1} = 1$ e também pode ser feito X na reta que contém $\overline{OU}$ de maneira que $\overline{XU_1}$ seja paralela a $\overline{UA_1}$, sendo assim, temos a seguinte semelhança de triângulos $\Delta OU_1X \sim \Delta OA_1U$ (caso ângulo-ângulo), e daí segue imediatamente que, $\overline{OX} = \frac{1}{\alpha}$, como podemos ver na imagem seguinte.

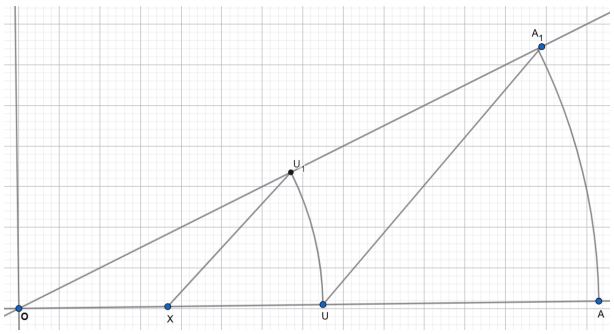


Figura 11: $\frac{1}{\alpha}$

■

Perceba que essa demonstração deixa evidente que o conjunto dos números racionais são construíveis. A pergunta agora é "será que podemos construir números não racionais?", e o próximo teorema mostra que sim, é possível construir números que não são racionais, mais a frente entenderemos quais são possíveis, e quais não são.

Lema 4.1 *Todo triângulo inscrito na circunferência tal que um dos lados coincide com o diâmetro é retângulo.*

Demonstração. A fim de simplicidade, considere uma circunferência de centro na origem e raio r. Portanto, a sua equação é dada por $x^2 + y^2 = r^2$. Considere agora um

triângulo qualquer inscrito nessa circunferência com um dos lados sendo o diâmetro, e os outros lados chame de a e b, como na imagem seguinte:

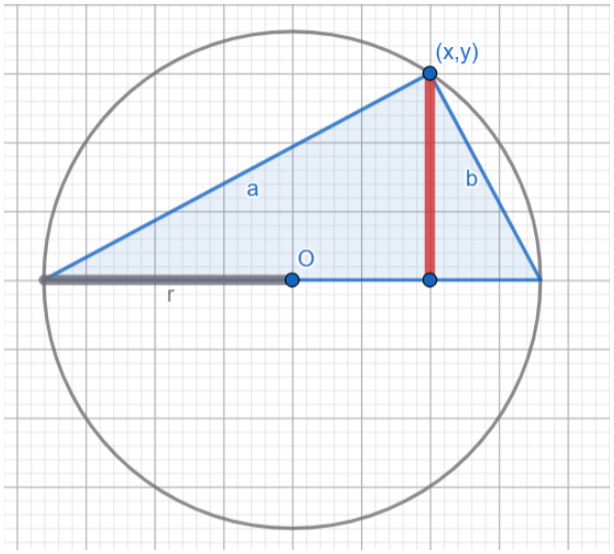


Figura 12: Triângulo inscrito

Veja que $a^2 = y^2 + (r+x)^2$ e $b^2 = y^2 + (r-x)^2$, por tanto,

$$\begin{aligned} a^2 + b^2 &= y^2 + (r+x)^2 + y^2 + (r-x)^2 \\ &= y^2 + r^2 + 2xr + x^2 + r^2 - 2xr + x^2 \\ &= 2y^2 + 2x^2 + 2r^2 = 2(y^2 + x^2) + 2r^2 \\ &2r^2 + 2r^2 = 4r^2 = (2r)^2. \end{aligned}$$

■

Teorema 4.2 *Se $a > 0$ é um número construível então $\sqrt{a}$ é construível.*

Demonstração. Seja a um número construível. Do fato do conjunto dos números construíveis possuir estrutura de corpo, $a + 1$ é um número construível. Considere o segmento de medida $a + 1$, agora pela proposição 4.1 o ponto médio desse segmento pode ser feito. Portanto, a circunferência com diâmetro $a + 1$ é construível. Logo, o triângulo como o da figura seguinte é construível:

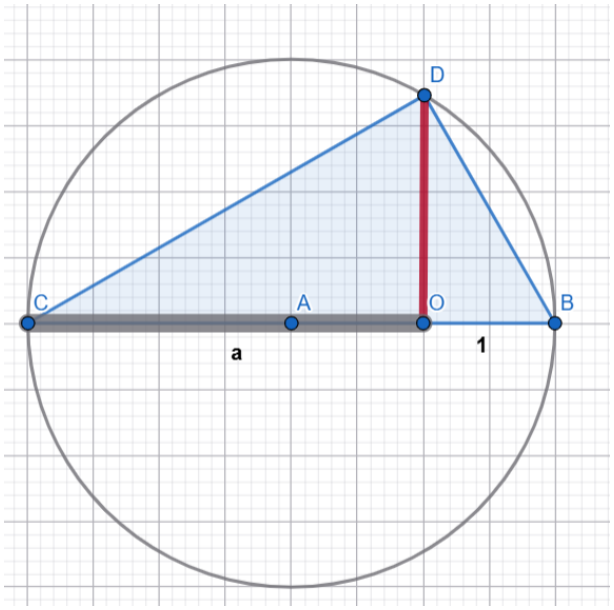


Figura 13: $\sqrt{a}$

Os triângulos $\Delta COD \sim \Delta DOB$. Considere $\overline{DO} = x$, logo, $\frac{a}{x} = \frac{x}{1}$, segue que, o segmento $\overline{DO}$ mede $\sqrt{a}$.

■

Vamos agora entender as limitações das construções envolvendo régua e compasso. Como vimos acima, temos que o conjunto dos números construíveis possui estrutura de corpo, e vimos também que, $\mathcal{P}_0 \subset \mathcal{P}_1 \subset ... \subset \mathcal{P}_n \subset ... \subset \mathbb{R}^2$.

A cada conjunto $\mathcal{P}_n$ de pontos chamaremos por $\mathcal{A}_n$ o conjunto de números das coordenadas em $\mathcal{P}_n$. Dessa maneira, se o ponto $(u, v) \in \mathcal{P}_n$ os números $u, v \in \mathcal{A}_n$.

Exemplo 4.2: Como o conjunto $\mathcal{P}_1 = \{(0,0), (1,0), (-1,0), (2,0), (\frac{1}{2}, \frac{\sqrt{3}}{2}), (\frac{1}{2}, -\frac{\sqrt{3}}{2})\}$, então, $\mathcal{A}_1 = \{0, 1, -1, 2, \frac{1}{2}, \frac{\sqrt{3}}{2}, -\frac{\sqrt{3}}{2}\}$.

Desse modo, é válido a seguinte torre de extensões $\mathbb{Q} \subset \mathbb{Q}[\mathcal{A}_0] \subset \mathbb{Q}[\mathcal{A}_1] \subset ... \subset \mathbb{Q}[\mathcal{A}_n] \subset ... \subset \mathcal{L}_{\mathbb{R}}$. Agora, pelas operações que temos, interseção entre duas retas, interseção de uma reta com uma circunferência e interseção entre duas circunferências, isso equivale a resolver os seguinte sistemas de equação:

Interseção entre duas retas:

$$\begin{cases} ax + by + c = 0 \\ a'x + b'y + c' = 0 \end{cases}$$

Interseção entre uma reta e uma circunferência:

$$\begin{cases} x^2 + y^2 + ax + by + c = 0 \\ a'x + b'y + c' = 0 \end{cases}$$

Interseção entre duas circunferências:

$$\begin{cases} x^2 + y^2 + ax + by + c = 0 \\ x^2 + y^2 + a'x + b'y + c' = 0 \end{cases} \iff \begin{cases} x^2 + y^2 + ax + by + c = 0 \\ (a' - a)x + (b' - b)y + c' - c = 0 \end{cases}$$

Isso significa, que a cada construção equivale a extrair no máximo uma raiz quadrada de um elemento algébrico sobre os racionais. Munido dessas informações e do corolário 3.1, podemos enunciar o seguinte teorema:

Teorema 4.3 *$\mathcal{L}_{\mathbb{R}}$ é uma extensão algébrica dos racionais, tal que, para todo $\alpha \in \mathcal{L}_{\mathbb{R}}$ temos que o grau de $[\mathbb{Q}[\alpha] : \mathbb{Q}]$ é uma potência de 2.*

Demonstração. É bastante provarmos que $\forall \alpha \in \mathcal{L}_{\mathbb{R}}$ tem-se $\Big[\mathbb{Q}[\alpha] : \mathbb{Q}\Big] = 2^r$ para algum $r \in \mathbb{N}$.

De fato, seja $\alpha \in \mathcal{L}_{\mathbb{R}}$. Assim, existe $n \in \mathbb{N}$, tal que, $\alpha \in \mathbb{Q}[\mathcal{A}_n]$.

Como $\Big[\mathbb{Q}[\alpha] : \mathbb{Q}\Big]$ divide $\Big[\mathbb{Q}[\mathcal{A}_n] : \mathbb{Q}\Big]$ é suficiente provarmos que $\Big[\mathbb{Q}[\mathcal{A}_n] : \mathbb{Q}\Big] = 2^s$ para algum $s \in \mathbb{N}$.

Portanto, iremos provar por indução que $\Big[\mathbb{Q}[\mathcal{A}_n] : \mathbb{Q}\Big]$ é uma potência de dois.

Se $n = 1$ temos que,

$$\begin{aligned}\Big[\mathbb{Q}[\mathcal{A}_1] : \mathbb{Q}\Big] &= \Big[\mathbb{Q}[0, 1, -1, 2, \frac{1}{2}, \frac{\sqrt{3}}{2}, -\frac{\sqrt{3}}{2}] : \mathbb{Q}\Big] \\ &= \Big[\mathbb{Q}[\sqrt{3} : \mathbb{Q}\Big] = 2\end{aligned}$$

e o teorema é valido.

Vamos supor por indução que $\Big[\mathbb{Q}[\mathcal{A}_i] : \mathbb{Q}\Big]$ é uma potência de dois $\forall 0 \leq i < n$, e vamos mostrar que $\Big[\mathbb{Q}[\mathcal{A}_n] : \mathbb{Q}\Big]$ é uma potência de dois.

Como $\mathcal{A}_{n-1} \subset \mathcal{A}_n$ $\Big[\mathbb{Q}[\mathcal{A}_n] : \mathbb{Q}\Big] = \Big[\mathbb{Q}[\mathcal{A}_n] : \mathbb{Q}[\mathcal{A}_{n-1}]\Big]\Big[\mathbb{Q}[\mathcal{A}_{n-1}] : \mathbb{Q}\Big]$ é suficiente mostrar que $\Big[\mathbb{Q}[\mathcal{A}_n] : \mathbb{Q}[\mathcal{A}_{n-1}]\Big]$ é uma potência de dois.

Para isso, sejam $\mathbb{L} = \mathbb{Q}[\mathcal{A}_n]$ e $\mathbb{L}_0 = \mathbb{Q}[\mathcal{A}_{n-1}]$. Dessa maneira, se $\mathcal{A}_n = \{\alpha_1, .., \alpha_k\}$ temos então $\mathbb{L} = \mathbb{L}_0[\alpha_1, ..., \alpha_k]$.

A fim de simplicidade iremos fazer o seguinte, $\mathbb{L}_0 \subset \mathbb{L}_1 = \mathbb{L}_0[\alpha_1] \subset .... \subset \mathbb{L}_i = \mathbb{L}_{i-1}[\alpha_i] \subset ... \subset \mathbb{L} = \mathbb{Q}[\mathcal{A}_n]$.

Agora, é suficiente mostrar que $\Big[\mathbb{L}_i : \mathbb{L}_{i-1}\Big]$ é 1 ou 2. Seja $\alpha_i \in \mathbb{L}_i$ como α_i é obtido a parti de uma das três operações definidas, temos então que, α_i é uma raiz de um polinômio de grau no máximo dois sobre $\mathbb{L}_{i-1}$, e isso nos diz que, $\Big[\mathbb{L}_i : \mathbb{L}_{i-1}\Big] = 1$ ou 2.

■

Exemplo 4.3: Dado um quadrado construtível é possível construir um quadrado com o dobro de sua área. Isto pois, dado um quadrado de lado l fazer um quadrado com o dobro de sua área é equivalente a construir um quadrado de lado $l\sqrt{2}$.

Proposição 4.5 *Dado um polígono regular construtível com n lados é sempre possível construir um polígono regular com $2n$ lados.*

De fato, basta fazer a bisseção dos ângulos.

Exemplo 4.4: A partir de um quadrado dado, vamos fazer um octógono. Seja o quadrado da imagem a seguir construtível.

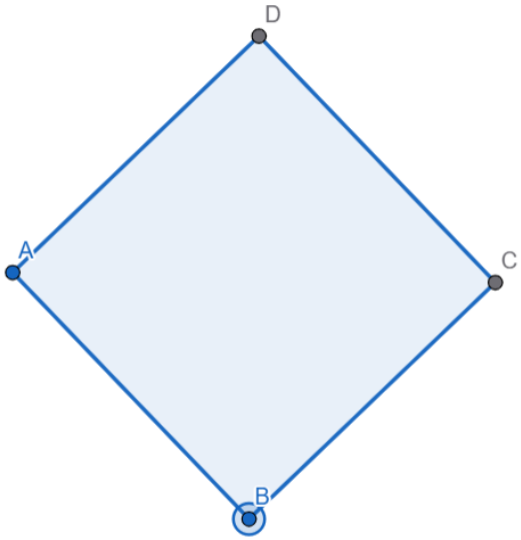


Figura 14: Quadrado

Faça as seguintes bisseções:

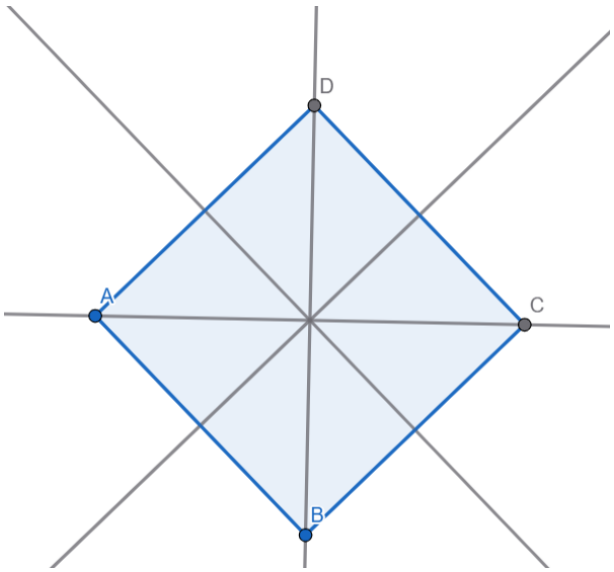


Figura 15: Bisseções

Em seguida, faça uma circunferência de centro no ponto de interseção das bissetrizes e raio maior que o segmento do ponto A ao centro. Com isso, agora basta fazer os segmentos dos pontos de interseção da circunferência e as retas de bisseção. Veja,

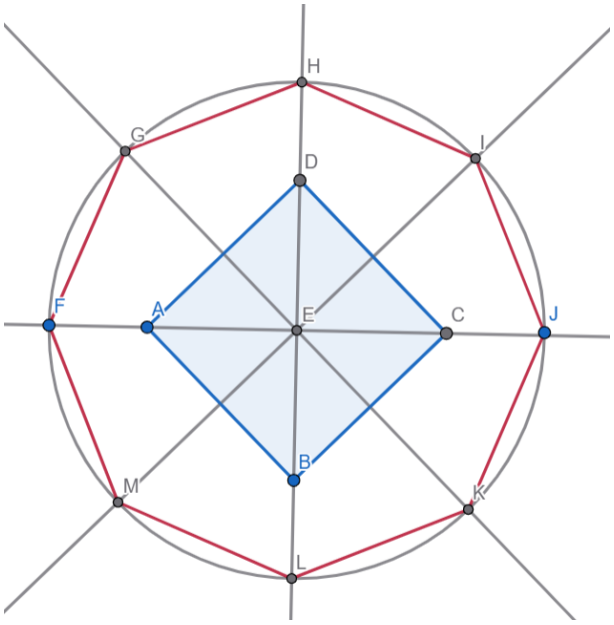


Figura 16: Octágono

Em particular, todos os polígonos com 2^r lados são construtíeis.

Agora iremos resolver os problemas de impossibilidades de construções com régua e compasso.

Problema 1: *Quadratura do circulo.*

É possível, usando apenas régua e compasso, construir um quadrado com a mesma área de um circulo dado?

Isso é equivalente a querer $l^2 = \pi r^2$, onde l^2 é a área do quadrado que gostaríamos de construir, e πr^2 a área do circulo dado.

Portanto, resolver esse problema é o mesmo que construir um segmento $l = r\sqrt{\pi}$, e isso não é possível, pois, como vimos no capítulo anterior, π é transcendente sobre os racionais e, de acordo, com o Teorema 4.3, o conjunto dos números construíveis com régua e compasso forma uma extensão algébrica sobre $\mathbb{Q}$.

Problema 2: *Duplicação do cubo.*

Dado um cubo com aresta l, é possível, usando apenas régua e compasso, obter outro cubo com o dobro de seu volume?

Construir um cubo com o dobro do volume equivale a obter um cubo de volume $2l^3$. Isso implica construir uma aresta de comprimento $l\sqrt[3]{2}$.

Como o polinômio mônico e irredutível de $\sqrt[3]{2}$ sobre $\mathbb{Q}$ é $x^3 - 2$, temos pela Proposição 3.3 que, $[\mathbb{Q}[\sqrt[3]{2}] : \mathbb{Q}] = 3$. Pelo Teorema 4.3, se $\alpha \in \mathcal{L}_{\mathbb{R}}$, então $[\mathbb{Q}[\alpha] : \mathbb{Q}] = 2^r, r \in \mathbb{N}$.

Como 3 não é uma potência de dois, conclui-se que $\sqrt[3]{2}$ não é construível. Logo, o segmento de comprimento $l\sqrt[3]{2}$ não pode ser construído com régua e compasso.

Definição 4.2 *Um ângulo θ é construível se o $\cos\theta \in \mathbb{R}$ é um número construível.*

Problema 3: *Trissecção do ângulo.*

Dado um ângulo qualquer, existe um algoritmo que determine sua terça parte?

Esse problema se resume a exibir um ângulo que não possa ser trissectado com régua e compasso.

Consideremos a tentativa de trissectar o ângulo de 60°. Seja $\alpha = cos(20°)$. Recorde que, $cos(3\theta) = 4cos(\theta)^3 - 3cos(\theta)$. Assim temos, $\frac{1}{2} = 4\alpha^3 - 3\alpha$. Isso equivale a dizer que α é raiz do polinômio $p(x) = 8x^3 - 6x - 1$. Como consequência, α também é raiz do polinômio mônico $g(x) = x^3 - \frac{3}{4}x - \frac{1}{8}$. Ambos os polinômios são irredutível sobre $\mathbb{Q}$. Sendo, $g(x)$ mônico e tendo α como raiz, segue pela Proposição 3.3 que $[\mathbb{Q}[\alpha] : \mathbb{Q}] = Irr(\alpha, \mathbb{Q})$, logo, $[\mathbb{Q}[\alpha] : \mathbb{Q}] = 3 \neq 2^r$. Conclui-se, pelo teorema 4.3, que α não pode ser construído usando apenas régua e compasso.

Considerações finais

Esse trabalho apresentou a interessante maneira de entender construções com régua e compasso por meio da teoria de extensões de corpo. Além disso, forneceu as ferramentas necessárias e suficientes para abordar e justificar a impossibilidade das construções geométricas dos problemas clássicos gregos.

A elaboração deste trabalho possibilitou um maior aprofundamento em tópicos de Álgebra Moderna, contribuindo de maneira significativa para minha preparação com vistas à realização futura de um mestrado em Matemática.

Considerando que estou inserido em um curso de Licenciatura, optei por dedicar o apêndice, com especial satisfação, à apresentação de uma sequência didática, envolvendo construções geométricas, voltada ao Ensino Fundamental.

Apêndice - Sequência didática - Construções geométricas com o Geogebra

Para finalizar esse trabalho, elaboramos a seguinte sequência didática envolvendo construções geométricas com o software geogebra. Levando em consideração que essa SD será para estudantes do 8° ano, iremos abrir mão do rigor das operações definidas para régua e compasso no capítulo anterior.

TURMA: 8° Ano do ensino fundamental.

TEMA CENTRAL: Construções geométricas.

OBJETIVOS:

- Compreender construções geométricas;
- Compreender o que são retas paralelas e perpendiculares;
- Construir ângulos (90°, 60°, 45°, 30°) e polígonos regulares;
- Construir a mediatriz e a bissetriz.

UNIDADE TEMÁTICA: Geometria.

HABILIDADES:

- **(EF06MA21):** Construir retas paralelas e perpendiculares (com réguas, esquadros e softwares).
- **(EF07MA24):** Construir triângulos, reconhecendo condições de existência e a soma dos ângulos internos.
- **(EF08MA15):** Construir mediatriz, bissetriz, ângulos (90°, 60°, 45°, 30°) e polígonos regulares.

RECURSOS DIDÁTICOS: Slides, Geogebra, régua, barbante ou compasso, pincel e quadro.

PROCEDIMENTOS METODOLÓGICOS:

Aula 01: Para melhores resultados, comece essa aula revisando as habilidade EF06MA21 e EF07MA24. Faça isso investigando os conhecimentos dos estudantes da turma, isto é, pergunte se eles sabem o que são retas paralelas e perpendiculares. Em seguida, defina esses objetos no quadro e coloque exemplos.

Dê continuidade perguntando se eles lembram qual é a condição quanto ao tamanho dos segmentos de triângulo para que ele exista, isto é, que dado um triângulo com segmentos medindo a, b e c, deve ser obedecido as seguinte desigualdades:

- $a < b + c$

- $b < a + c$
- $c < a + b$

E que em relação aos ângulos interno, a sua soma sempre deve dar 180°.

Prossiga com variados exemplos, desde, figuras que não são triângulos devido não obedecer as desigualdades ou a soma dos ângulos interno, até a figuras que de fato são triângulos. Nessa parte de revisão, gaste ao máximo 20 minutos.

Agora, continue com a habilidade EF08MA15. Defina o que são mediatriz e bissetriz, em seguida, construa esses objetos usando régua e compasso. Dê continuidade com a construções dos ângulos e finalize a aula 01 com a construção do quadrado.

Aula 02: Para essa aula, será feito a construção de retas paralelas, perpendiculares, a mediatriz e a bissetriz de um ângulo com o software Geogebra. Para isso, assumimos o conhecimento prévio dos estudantes com a ferramenta Geogebra.

Começaremos com a construção de retas paralelas. Para isso, considere uma reta r e um ponto A fora dessa reta, em sequência faça uma circunferência de modo que intercepte a reta em dois pontos, isto é:

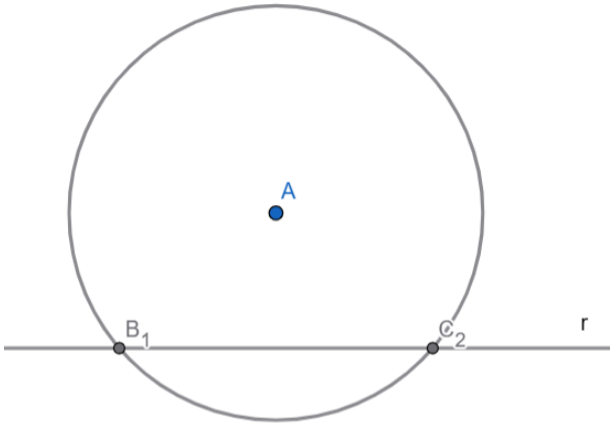


Figura 17: Construção reta perpendicular

Para não cometer erro em encontrar B_1 e C_2 use a ferramenta "Interseção de dois objetos", com isso, clique na reta r e na circunferência.

Agora, use a ferramenta "Compasso", clique nos ponto A e B_1, ao fazer isso você estará determinando a medida do raio do seu compasso, em sequência, faça duas circunferências, uma centrada em B_1 e a outra em C_1, isto é:

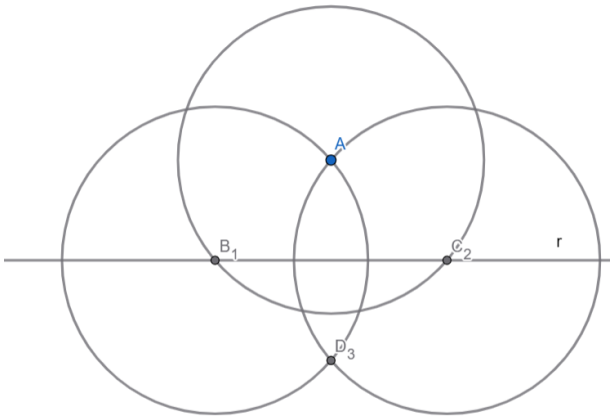


Figura 18: Construção reta perpendicular

A reta que passa por A e D_3 é perpendicular a reta r.

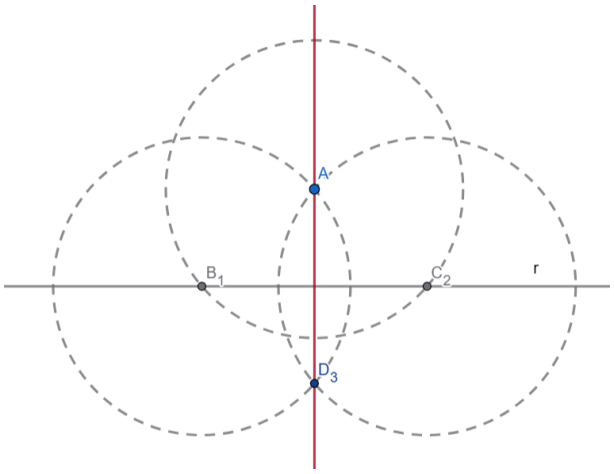


Figura 19: Construção reta paralela

Para fazer a reta paralela a r passando por A, comece fazendo uma circunferência que intercepte a reta r em dois B_1 e C_2 pontos, escolha um deles, sem perca de generalidade, iremos escolher C_2, em seguida faça uma outra circunferência com o auxilio da ferramenta compasso medindo tamanho de A a C_2 e centrada em C_2. isto é,

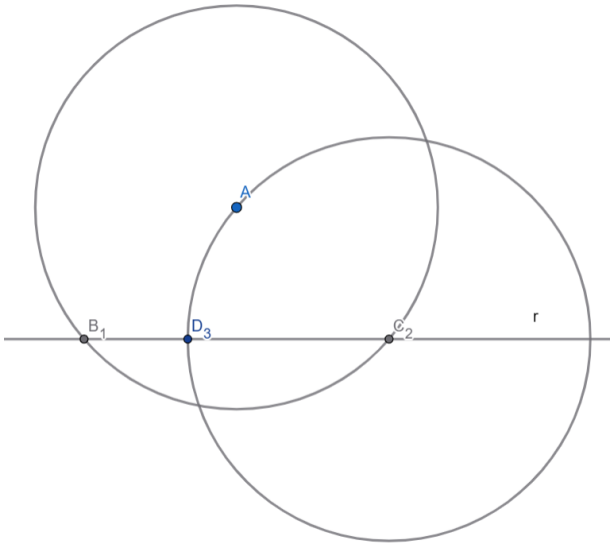


Figura 20: Construção reta paralela

Agora, faça uma outra circunferência centrada em C_2 de raio $\overline{AD_3}$, isto é,

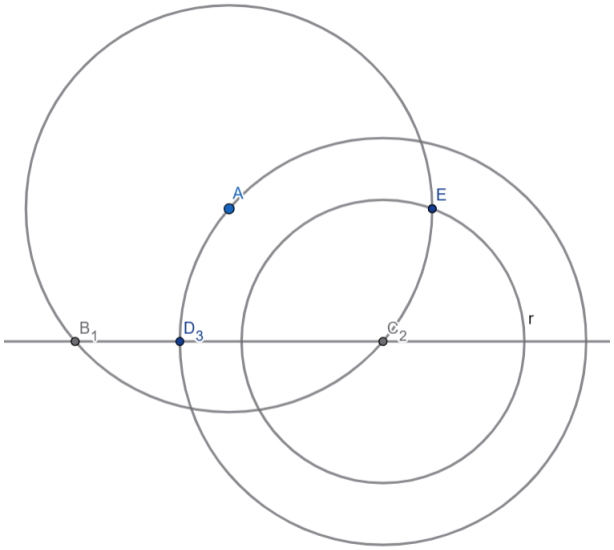


Figura 21: Construção reta paralela

A reta passando por A e E é paralela a reta r.

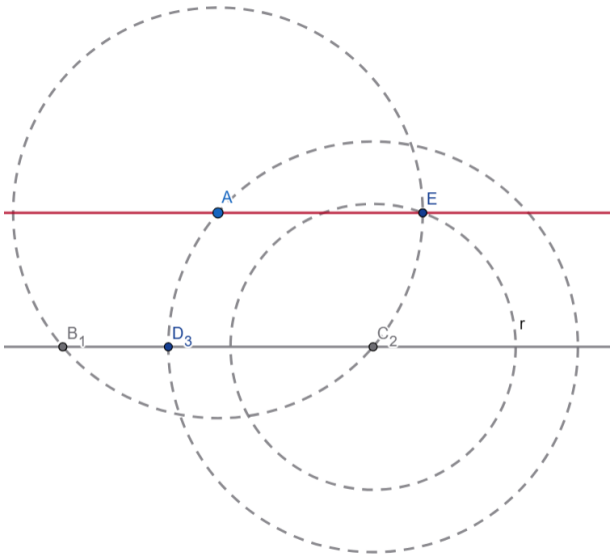


Figura 22: Construção reta paralela

Considere A e B dois pontos dados, para determina a mediatriz do segmento $\overline{AB}$ faça duas circunferências, uma centrada em A passando por B e a outra centrada em B passando por A, isto é,

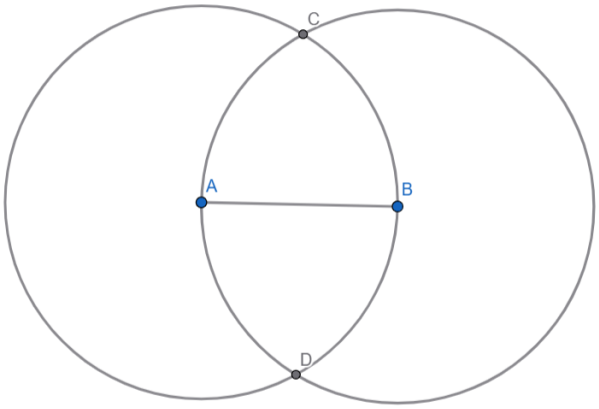


Figura 23: Construção mediatriz

A reta passando por C e D é a mediatriz do segmento $\overline{AB}$.

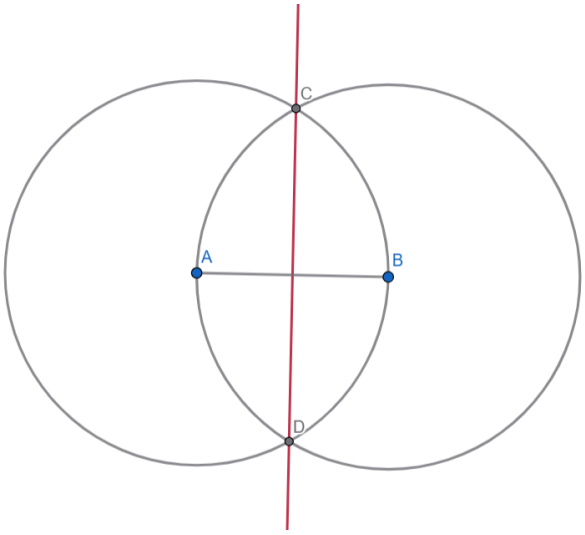


Figura 24: Construção mediatriz

Agora, para finalizar a aula 2, iremos fazer a construção da bissetriz. Para facilitar a visualização, comece com três pontos não alinhados A,B e C, em seguida faça dois segmentos de reta, $\overline{AB}$ e $\overline{BC}$.

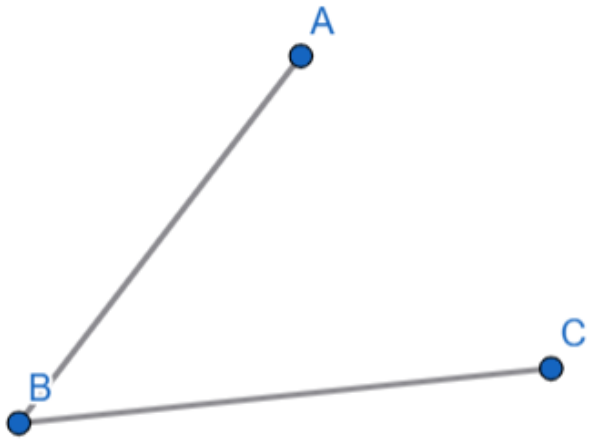


Figura 25: Construção bissetriz

Agora, faça uma circunferência centrada em B.

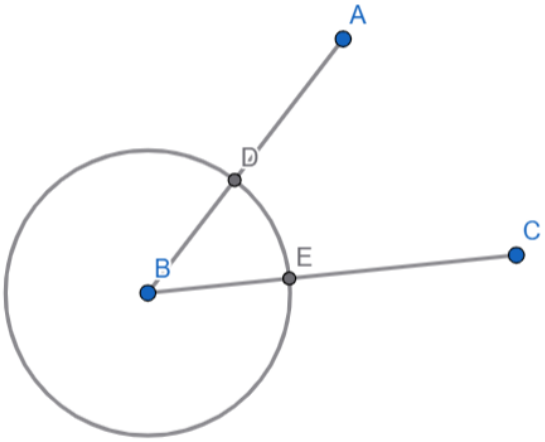


Figura 26: Construção bissetriz

Usando a ferramenta compasso, faça outras duas circunferências com o mesmo raio dessa primeira, um centrada em D e a outra centrada em E.

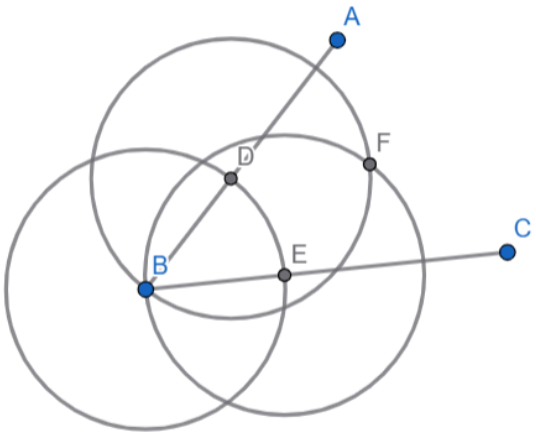


Figura 27: Construção bissetriz

A semirreta de B passando por F e a bissetriz do ângulo dado.

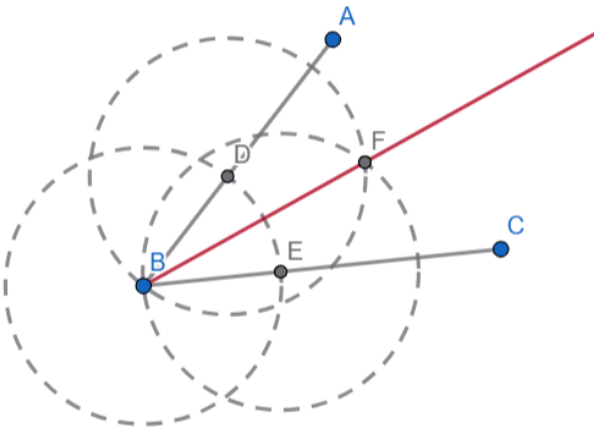


Figura 28: Construção bissetriz

Aula 03:

Para essa aula, será feito a construção de alguns ângulos e polígonos regulares. Como na aula anterior foi ensinado a fazer retas perpendiculares e a construção da bissetriz, peça aos estudantes para que eles façam a construção do ângulo de 90° e 45°.

Em sequência, faremos as construções do ângulo de 60° e do triângulo equilátero:

Comece com um segmento de reta.

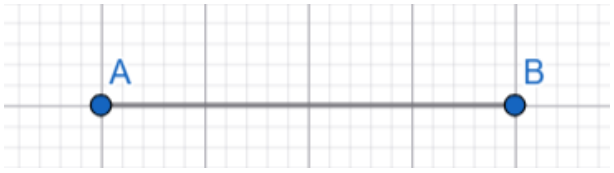


Figura 29: Construção ângulo 60°

Agora, faça duas circunferências uma centrada em A passando por B e a outra centrada em B passando por A.

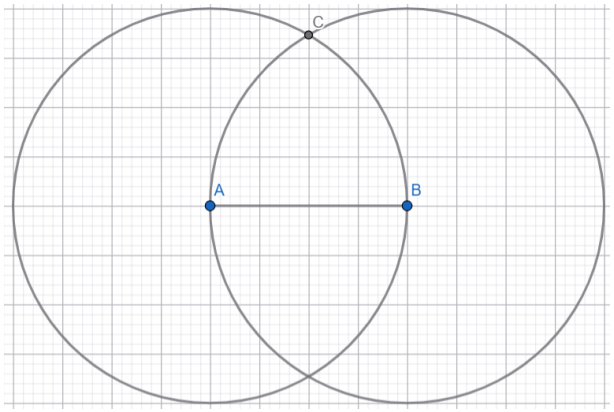


Figura 30: Construção ângulo 60°

Prossiga fazendo o segmento $\overline{AC}$. O ângulo $\angle CAB$ mede 60°.

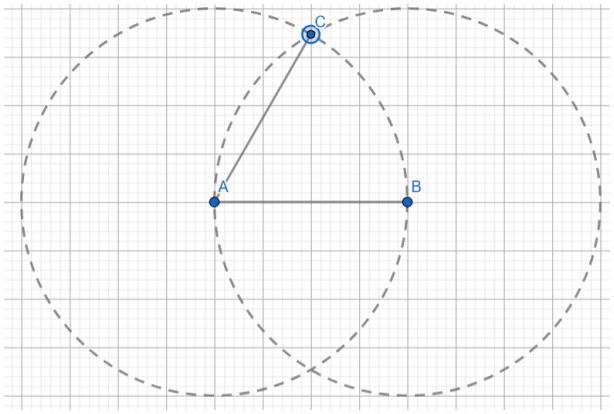


Figura 31: Construção ângulo 60°

Ao fazer o segmento $\overline{BC}$ aparece um triângulo ΔABC, esse triângulo é equilátero.

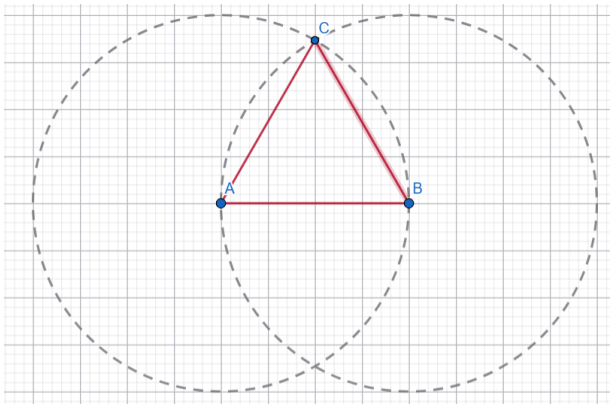


Figura 32: Triângulo equilátero

Agora, faremos um hexágono regular, para isso, comece com uma circunferência e seu diâmetro.

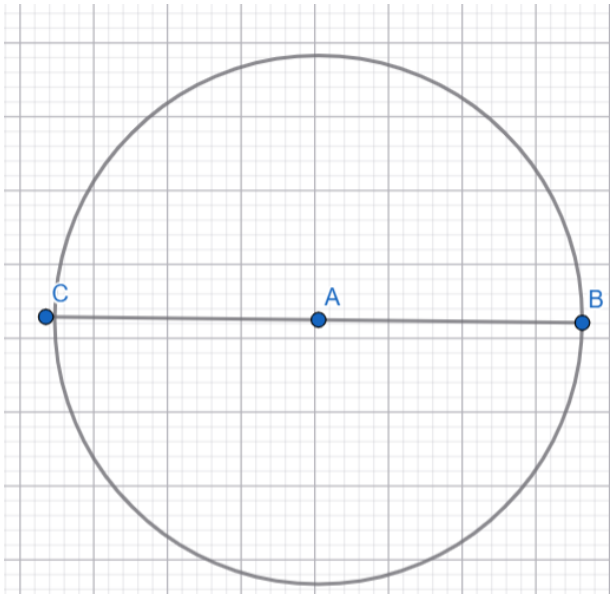


Figura 33: Construção hexágono

Em seguida faça outra duas circunferências, uma com centro em C e passando por A e a outra com o centro em B passando por A.

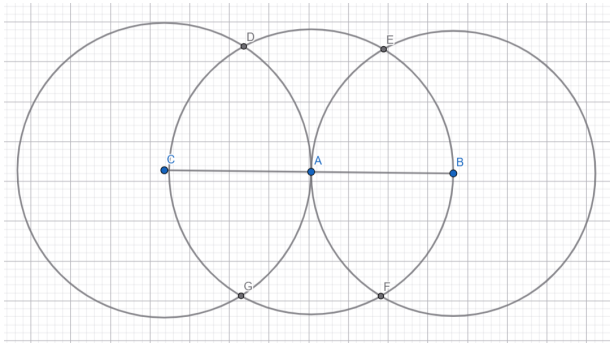


Figura 34: Construção hexágono

Agora, ao fazer os seguimentos $\overline{CD}, \overline{CE}, \overline{EB}, \overline{BF}, \overline{FG}$ *e* $\overline{GC}$, aparecerá o hexágono regular.

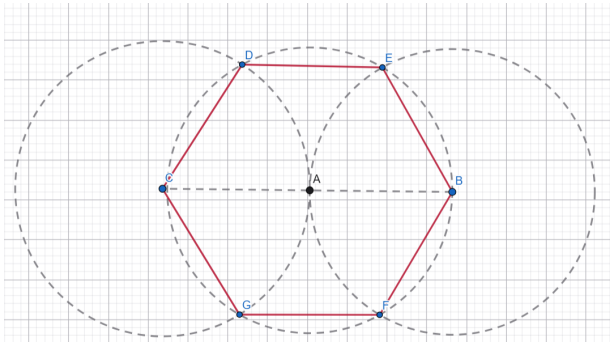


Figura 35: Hexágono regular

Agora faremos o octágono regular. Para isso, comece com uma circunferência com

centro em A e um dos diâmetros $\overline{BC}$. Em sequência use os conhecimentos adquiridos para fazer a mediatriz do segmento $\overline{BC}$. Com isso, terá dois pontos de interseção da reta mediatriz e a circunferência, isto é,

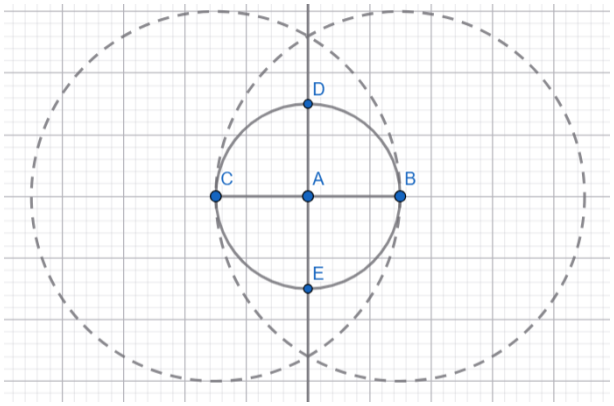


Figura 36: Construção octágono

Continue com a construção das quatro bissetrizes nos ângulos de 90°.

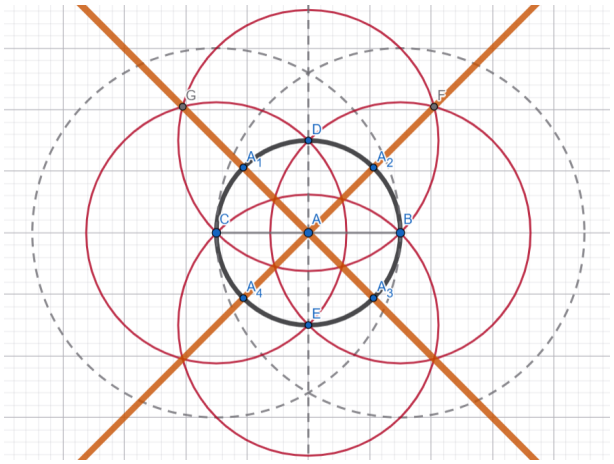


Figura 37: Construção octágono

Finalize fazendo os seguinte segmentos de retas: $\overline{CA_1}, \overline{A_1D}, \overline{DA_2}, \overline{A_2B}, \overline{BA_3}, \overline{A_1E}, \overline{EA_4}$ e $\overline{CA_4}$.

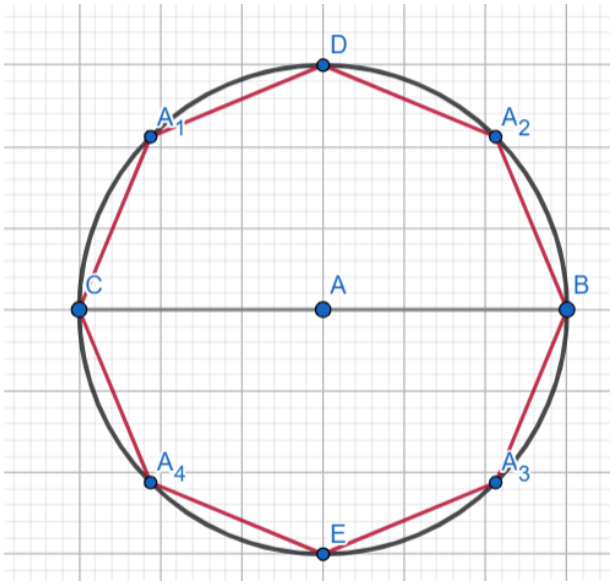


Figura 38: Construção octágono

Referências

CRUZ, Karina Branco da. Introdução à Teoria de Galois. 2014. 117 f. TCC (Graduação) - Curso de Matemática, Universidade Federal de São Carlos, São Carlos, 2014.

DOMINGUES, Hygino H.; IEZZI, Gelson. Álgebra moderna. 4. ed. São Paulo: Atual Editora, 2003.

GONÇALVES, Adilson. Introdução à álgebra. Rio de Janeiro: Projeto Euclidade, 1995.

J.MCCARTHY, Paul. Algebraic extensions of fields. Toronto: General Publishing Company, 1991. 166 p.

ENDLER, Otto. Teoria dos Corpos. Rio de Janeiro: Impa, 1987

WAGNER, Eduardo. Construções Geométricas. 5. ed. Rio de Janeiro: Sociedade Brasileira de Matemática, 2005.