UNIVERSIDADE FEDERAL DE GOIÁS (UFG)
INSTITUTO DE MATEMÁTICA E ESTATÍSTICA (IME)
PROGRAMA DE MESTRADO PROFISSIONAL EM MATEMÁTICA EM REDE NACIONAL (PROFMAT)

GREGÓRIO PEREIRA DE QUEIROZ NETO

NÚMEROS CONSTRUTÍVEIS UMA PROPOSTA DE SEU ENSINO PARA O NOVO ENSINO MÉDIO

GOIÂNIA
2023

UNIVERSIDADE FEDERAL DE GOIÁS
INSTITUTO DE MATEMÁTICA E ESTATÍSTICA

TERMO DE CIÊNCIA E DE AUTORIZAÇÃO (TECA) PARA DISPONIBILIZAR VERSÕES ELETRÔNICAS DE TESES

E DISSERTAÇÕES NA BIBLIOTECA DIGITAL DA UFG

Na qualidade de titular dos direitos de autor, autorizo a Universidade Federal de Goiás (UFG) a disponibilizar, gratuitamente, por meio da Biblioteca Digital de Teses e Dissertações (BDTD/UFG), regulamentada pela Resolução CEPEC nº 832/2007, sem ressarcimento dos direitos autorais, de acordo com a Lei 9.610/98, 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 e Dissertações disponibilizado na BDTD/UFG é de responsabilidade exclusiva do autor. Ao encaminhar o produto final, o 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

[x] Dissertação [ ] Tese [ ] Outro*:_____

*No caso de mestrado/doutorado profissional, indique o formato do Trabalho de Conclusão de Curso, permitido no documento de área, correspondente ao programa de pós-graduação, orientado pela legislação vigente da CAPES.

Exemplos: Estudo de caso ou Revisão sistemática ou outros formatos.

2. Nome completo do autor

Gregório Pereira de Queiroz Neto

3. Título do trabalho

Números construtíveis e uma proposta de seu ensino para o novo ensino médio

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.

Obs. Este termo deverá ser assinado no SEI pelo orientador e pelo autor.

GREGÓRIO PEREIRA DE QUEIROZ NETO

Números construtíveis e uma proposta de seu ensino para o novo ensino médio

Dissertação apresentada ao Programa de Pós–Graduação do Mestrado Profissional em Matemática em Rede Nacional, do Instituto de Matemática e Estatística(IME), da Universidade Federal de Goiás(UFG), como requisito para obtenção do título de Mestre em Matemática.

Área de concentração: Matemática do Ensino Básico.

Orientador: Prof. Dr. Paulo Henrique de Azevedo Rodrigues

Goiânia
2023

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

Neto, Gregório Pereira de Queiroz
Números construtíveis e uma proposta de seu ensino para o novo ensino médio [manuscrito] / Gregório Pereira de Queiroz Neto. - 2023.
LXXXVII, 87 f.: il.

Orientador: Prof. Dr. Paulo Henrique de Azevedo Rodrigues.
Dissertação (Mestrado) - Universidade Federal de Goiás, Instituto de Matemática e Estatística (IME), Programa de Pós-Graduação em Ensino na Educação Básica (Profissional), Goiânia, 2023.
Bibliografia. Apêndice.

1. Construção com régua e compasso. 2. Números construtíveis. 3. Polinômios e construção. I. Rodrigues, Paulo Henrique de Azevedo , orient. II. Título.

CDU 51:37

UNIVERSIDADE FEDERAL DE GOIÁS

INSTITUTO DE MATEMÁTICA E ESTATÍSTICA

ATA DE DEFESA DE DISSERTAÇÃO

Ata nº **07** da sessão de Defesa de Dissertação de **Gregório Pereira de Queiroz Neto**, que confere o título de Mestre em Matemática, na área de concentração em **Matemática do Ensino Básico**.

Aos trinta dias do mês de junho de dois mil e vinte e três, a partir das 15h, no Auditório do IME, realizou-se a sessão pública de defesa de dissertação intitulada **"Números construtíveis e uma proposta de seu ensino para o novo ensino médio"**. Os trabalhos foram instalados pelo orientador, Professor Doutor Paulo Henrique de Azevedo Rodrigues (IME/UFG) com a participação dos demais membros da Banca Examinadora: Professor Doutor Marcelo Almeida de Souza (IME/UFG) e membro titular externo, José Éder Salvador de Vasconcelos (IFG). Durante a arguição os membros da banca **não fizeram** sugestão de alteração do título do trabalho. A Banca Examinadora reuniu-se em sessão secreta a fim de concluir o julgamento da Dissertação, tendo sido o candidato **aprovado** pelos seus membros. Proclamados os resultados pelo Professor Doutor Paulo Henrique de Azevedo Rodrigues, Presidente da Banca Examinadora, foram encerrados os trabalhos e, para constar, lavrou-se a presente ata que é assinada pelos Membros da Banca Examinadora, aos trinta dias do mês de junho de dois mil e vinte e três.

TÍTULO SUGERIDO PELA BANCA

Documento assinado eletronicamente por **Paulo Henrique De Azevedo Rodrigues**, **Professor do Magistério Superior**, em 10/07/2023, às 17:03, conforme horário oficial de Brasília, com fundamento no § 3º do art. 4º do Decreto nº 10.543, de 13 de novembro de 2020.

Documento assinado eletronicamente por **JOSÉ EDER SALVADOR DE VASCONCELOS**, **Usuário Externo**, em 10/07/2023, às 18:52, conforme horário oficial de Brasília, com fundamento no § 3º do art. 4º do Decreto nº 10.543, de 13 de novembro de 2020.

Documento assinado eletronicamente por **Marcelo Almeida De Souza**, **Professor do Magistério Superior**, em 13/07/2023, às 10:09, conforme horário oficial de Brasília, com fundamento no § 3º do art. 4º do Decreto nº 10.543, de 13 de novembro de 2020.

A autenticidade deste documento pode ser conferida no site https://sei.ufg.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **3823758** e o código CRC **20F1F0BF**.

Referência: Processo nº 23070.033888/2023-33 SEI nº 3823758

Dedico este trabalho a Deus que tem me proporcionado saúde e mantido minha mente e coração no lugar certo.

Agradecimentos

Agradeço primeiramente a Deus que esteve me abençoando e dando paciência e saúde em todo este tempo de curso.

Agradeço em especial a minha mãe que sempre me apoiou incondicionalmente a estudar e mesmo diante das dificuldades não mediu esforços para proporcionar tudo que possível e necessário fosse.

Agradeço também em especial a minha hoje esposa, que no início do processo era namorada e aceitou se casar mesmo com todas as dificuldades, sabendo que seriam tempos em que a prioridade eram os estudos e que sempre esteve ao meu lado me apoiando e dando todo suporte necessário, tanto psicológico quanto físico de continuar e continuar bem.

Agradeço a meu colega de estudo Charlles que caminhou comigo os anos de mestrado juntos com dedicação e parceria, se tornando um amigo do peito.

Agradeço ao meu orientador Paulo que sempre me apoiou e nos momentos necessários me tranquilizou e deu todo o suporte intelectual de construir este trabalho.

Agradeço também a toda minha família que esteve me incentivando e entendendo todos os finais de semana e datas comemorativas que não participei para me dedicar a este curso de mestrado.

Quer ser vencedor? tenha história de vencedor.

João Lopes Cardoso Filho,
Professor universitário.

Resumo

Neto, Gregório Pereira de Queiroz. **Números construtíveis e uma proposta de seu ensino para o novo ensino médio**. Goiânia, 2023. 87p. Dissertação de Mestrado. Instituto de Matemática e Estatística, Universidade Federal de Goiás.

Este trabalho apresenta uma introdução a teoria dos corpos com ênfase nas extensões de corpos e aborda também de forma introdutória os polinômios. Apresentamos ainda a teoria de números construtíveis usando apenas régua não graduada e compasso. Finalmente, é apresentada a proposta de aplicação.

Palavras–chave

Construção com régua e compasso, números construtíveis, Polinômios e construção.

Abstract

Neto, Gregório Pereira de Queiroz. **Buildable numbers and a teaching proposal for the new high school**. Goiânia, 2023. 87p. MSc. Dissertation. Instituto de Matemática e Estatística, Universidade Federal de Goiás.

This work presents an introduction to the theory of bodies with emphasis on extensions of fields and also approaches polynomials in an introductory way. we present yet the theory of constructible numbers using only unmarked ruler and compass. Finally, the application proposal is presented.

Keywords

Construction with ruler and compass, constructible numbers, Polynomials and construction.

Sumário

Introdução

As construções geométricas são citadas pela primeira vez nos três primeiros capítulos de "Os Elementos"publicados por Euclides, onde ele cita as três operações básicas para construções permitidas em geometria. As quais são: Traçar uma reta a partir de dois pontos diferentes, prolongar um segmento de reta ilimitadamente segundo uma reta e descrever um círculo com qualquer raio e ponto como centro. Porém, em sua obra ele não comenta como as construções devem ser feitas. Por exemplo, existe o método que usa régua não graduada e compasso apenas, que é o método abordado neste trabalho e é tradicionalmente atribuído a partir de Platão (390 a.c).[Nobre 1995] Esse método será discutido e desenvolvido ao longo texto.

Embora os gregos tenham chegado muito perto de alcançar todas as construções possíveis usando apenas a régua e o compasso, eles chegaram em alguns problemas relativamente simples que não podem ser resolvidos apenas com essas ferramentas. Usando as ferramentas citadas, os exemplos mais famosos impossíveis são: dividir um ângulo dado em três congruentes, encontrar o lado do cubo cujo volume é o dobro do cubo dado e desenhar um quadrado com a área igual ao círculo dado. Esses fatos são demonstrados no final do Capítulo dois.

A busca da solução destes problemas tem sido objeto de estudos de muitos matemáticos desde então, que com sua engenhosidade e criatividade procuraram outros métodos para sua solução. Nessa busca, só em 1882 foi possível mostrar que encontrar o lado do cubo cujo volume é o dobro do cubo dado e desenhar um quadrado com a área igual ao círculo dado utilizando apenas régua e compasso é impossível. O matemático George Mohr [Nobre 1995], publicou no ano de 1672 um livro intitulado *Euclides Danicus*, que foi encontrado em um sebo em 1928. Nele havia uma conclusão que dizia que o compasso apenas é equivalente a compasso e régua, que era uma discussão sobre os métodos usados em algumas demonstrações até aquele tempo. Mais a frente, em 1822, o matemático Jean Victor Poncelet notou que pontos adicionais de construção são obtidos como a intersecção de duas retas, uma reta e um círculo ou dois círculos. Esse método de construção é o que trata esse trabalho e essas operações aqui são definidas como operações básicas de construção.

As construções geométricas usadas pelos gregos antigos eram uma ferra-

menta para resolução de algumas equações até grau três. E com essas construções não conseguiram resolver os problemas clássicos o que culminou na busca de outros tipos de resolução, e diversos matemáticos ajudaram a concluir a partir da teoria das equações polinomiais que eles não tem solução [Gonçalves 1979].

Diferente dos gregos, os hindus em sua procura por soluções de equações usavam métodos aritméticos, métodos esses que foram aperfeiçoados pelos Árabes. Vale destacar a Fórmula de Bhákara de uma equação do segundo grau. Mais adiante, por volta do século XVI em batalhas de matemática, onde essas batalhas eram proposições de problemas ou equações para o adversário resolver. Nelas, destacam-se dois matemáticos italianos, conhecidos como Cardano e Tartáglia. Que em meio a essas batalhas encontraram soluções gerais para equações de terceiro grau lidando apenas com operações analíticas, que se dão a partir da redução de cada equação para equações do tipo $x^3 + px = q$.

Este trabalho é dividido em três capítulos, onde é desenvolvido a teoria de construções geométricas e apresentada uma proposta de aplicação desta teoria para alunos do ensino médio. Essa proposta se dá por meio da construção de um material básico que pode servir como uma fonte de pesquisa para professores do ensino médio. Ele também pode servir como uma trilha de ensino em forma de um itinerário de aprofundamento na área de matemática e suas tecnologias, ou mesmo como um minicurso para discentes de licenciatura matemática. O desenvolvimento do material é feito no terceiro capítulo, dividido em oito partes. Essas partes sugerem a ordem cronológica a ser seguida e mistura os números construtíveis com a teoria de polinômios e suas raízes. Esse material pode ser tratado também como uma tentativa de aplicação e integração da geometria com a álgebra no ensino médio em um contexto que não é visto nas literaturas mais comuns do ensino médio.

Já no primeiro capítulo, é apresentada a teoria dos corpos e das suas extensões. Algumas das demonstrações são omitidas dado o objetivo principal do trabalho que é estudar os números construtíveis. Esse capítulo é uma introdução teórica para o segundo capítulo e trás definições e proposições importantes usadas em demonstrações do capítulo dois ou mesmo em demonstrações do próprio capítulo. Nele ainda, é apresentado a teoria dos polinômios de maneira objetiva e simples diferente do modo apresentado no capítulo três.

No segundo capítulo, são apresentadas as definições de construções e operações básicas de construção. Contém o principal objetivo do trabalho que é construir ou garantir a construção de números sem a necessidade dos passos construtivos. É seguido uma ordem cronológica para chegar no último teorema que dá uma garantia de quando um número real pode ser construído. Terminamos mostrando a impossibilidade da construção dos três problemas clássicos das construções geométricas,

que são a trissecção do ângulo, a quadratura do círculo e a duplicação do cubo. Em termos de ensino médio ou ensino básico da educação, o capítulo dois serve como fonte de teoria e pesquisa para professores.

CAPÍTULO 1

Introdução à corpos

Nesse primeiro capítulo são apresentadas algumas definições e proposições sobre anéis, corpos, polinômios e extensões de corpos. Esse capítulo é uma base teórica para o próximo capítulo que trata da construção de números reais.

1.1 Corpos

A seguir é apresentada a definição de corpo e alguns exemplos de corpos, teoremas e proposições que seguem uma ordem lógica de afirmações que são de grande valia no decorrer do desenvolvimento teórico. Basicamente um conjunto que possui a estrutura de corpo deve conter as 10 propriedades abaixo citadas e para a adição e multiplicação definida para elementos desse conjunto.

Definição 1.1. Seja A um conjunto não vazio que possui duas operações, que são chamadas de adição e multiplicação em A e denotadas por $+$ e $\cdot$. Diz-se que $(A, +, \cdot)$ é um corpo com adição $+$ e multiplicação $\cdot$, se as propriedades enumeradas a seguir forem satisfeitas para quaisquer $a, b, c \in A$.

(1) Associatividade da adição: $(a + b) + c = a + (b + c)$
(2) Existência de elemento neutro para a soma: Existe 0 pertencente à A tal que $a + 0 = 0 + a = a$.
(3) Existência do inverso aditivo: $\forall\ x \in A$ existe $y \in A$, denotado por $y = -x$ tal que, $x + y = y + x = 0$.
(4) Comutatividade da soma: $a + b = b + a$.
(5) Associatividade do produto: $(a \cdot b) \cdot c = a \cdot (b \cdot c)$.
(6) Distributividade à esquerda e à direita: $a \cdot (b+c) = a \cdot b + a \cdot c$ e $(a+b) \cdot c = a \cdot c + b \cdot c$.
(7) Unidade do produto: Existe 1 pertencente à A onde $0 \neq 1$, tal que $x \cdot 1 = 1 \cdot x = x$ para todo $x \in A$.
(8) Comutativo para o produto: Para todo $x, y \in A$ tem-se $x \cdot y = y \cdot x$.
(9) Possui inverso multiplicativo: Para todo $x \in A,\ x \neq 0$, existe $y \in A$ tal que $x \cdot y = y \cdot x = 1$.

Observação 1. Aqui são apresentadas algumas definições sobre as propriedades acima enunciadas, assim se $(A, +, \cdot)$ satisfaz as 6 primeiras propriedades diz-se que é um anel. Se $(A, +, \cdot)$ satisfaz as sete primeiras propriedades diz-se que é um anel com unidade. Se $(A, +, \cdot)$ satisfaz as 8 primeiras propriedades diz-se que é um anel comutativo e por fim se $(A, +, \cdot)$ satisfaz as 8 primeiras propriedades e ainda, dados $x, y \in A$, tais que $x \cdot y = 0$ então $x = 0$ ou $y = 0$, diz-se que é um anel sem divisores de zero, em outras palavras, diz-se que $(A, +, \cdot)$ é um domínio de integridade.

Exemplo 1.2. Observe que o conjunto $\mathbb{Q} = \left\{ \frac{p}{q} \mid p, q \in \mathbb{Z} \; com \; q \neq 0 \right\}$ dos números racionais é um corpo. Para mostrar essa afirmação, inicialmente defina as operações de soma e produto. Dados dois números racionais $x = \dfrac{a}{b}$ e $y = \dfrac{c}{d}$ com $c, d \neq 0$ quaisquer. Defina soma de x e y por

$$+ =: x + y = \frac{a}{b} + \frac{c}{d} = \frac{a \cdot d + b \cdot c}{b \cdot d}$$

e o produto de x e y por

$$\cdot =: x \cdot y = \frac{a}{b} \cdot \frac{c}{d} = \frac{a \cdot c}{b \cdot d}.$$

Note que tanto a soma como o produto estão bem definidas, pois a soma e o produto de números inteiros continua sendo um número inteiro, e nos denominadores o produto de números inteiros diferentes de zero é também diferente de zero. Logo, com estas operações o conjunto $\mathbb{Q}$ é fechado para a soma e para o produto. Agora, observe a demonstração das propriedades que o tornam um corpo. Considere para as demonstrações a seguir os números $x = \dfrac{a}{b}$, $y = \dfrac{c}{d}$, $z = \dfrac{e}{f} \in \mathbb{Q}$, daí

(1) É associativo para a soma. De fato,

$$\begin{aligned}
x + (y + z) &= \frac{a}{b} + \left(\frac{c}{d} + \frac{e}{f} \right) \\
&= \frac{a}{b} + \frac{cf + de}{df} \\
&= \frac{adf + b \cdot (cf + de)}{b \cdot (df)} \\
&= \frac{adf + bcf + bde}{bdf} \\
&= \frac{(ad + bc)f + bde}{(bd) \cdot f} \\
&= \frac{ad + bc}{bd} + \frac{e}{f} \\
&= \left(\frac{a}{b} + \frac{c}{d} \right) + \frac{e}{f} \\
&= (x + y) + z.
\end{aligned}$$

Perceba que tanto a propriedade distributiva quanto a propriedade associatividade é válida para números inteiros. Usando essa afirmação, a primeira propriedade está satisfeita.

(2) Existência do elemento neutro para adição. Basta então tomar $\overline{0} = \dfrac{0}{1}$ e daí

$$\overline{0} + x = \frac{0}{1} + \frac{a}{b} = \frac{0 \cdot b + 1 \cdot a}{1 \cdot b} = \frac{a}{b} = x$$

e

$$x + \overline{0} = \frac{a}{b} + \frac{0}{1} = \frac{a \cdot 1 + b \cdot 0}{b \cdot 1} = \frac{a}{b} = x.$$

Logo, $\forall\ x \in \mathbb{Q}$ tem-se $x + 0 = 0 + x = x$ como se queria demonstrar.

(3) Existência do inverso aditivo. Considere $\forall\ x = \dfrac{a}{b} \in \mathbb{Q}$ seu inverso aditivo por $w = -x = -\dfrac{a}{b} = \dfrac{(-a)}{b} = \dfrac{a}{(-b)} \in \mathbb{Q}$, tais que

$$x + w = x + (-x) = \frac{a}{b} + \left(\frac{-a}{b}\right) = \frac{ab + (-a)b}{b \cdot b} = \frac{ab - ab}{b^2} = \frac{0}{b^2} = 0$$

e

$$w + x = \frac{-a}{b} + \frac{a}{b} = \frac{(-a) \cdot b + a \cdot b}{b \cdot b} = \frac{-ab + ab}{b^2} = \frac{0}{b^2} = 0.$$

Logo, $x + w = w + x = 0$ como se queria demonstrar.

(4) Comutatividade para a adição, sejam $x, y \in \mathbb{Q}$ quaisquer, então

$$x + y = \frac{a}{b} + \frac{c}{d} = \frac{a \cdot d + b \cdot c}{b \cdot d} = \frac{d \cdot a + c \cdot b}{d \cdot b} = \frac{c}{d} + \frac{a}{b} = y + x.$$

Como se queria demonstrar.

(5) Associatividade do produto. Basta usar a associatividade do produto nos números inteiros, tal que

$$x \cdot (y \cdot z) = \frac{a}{b} \cdot \left(\frac{c}{d} \cdot \frac{e}{f}\right) = \frac{a}{b} \cdot \left(\frac{ce}{df}\right) = \frac{ace}{bdf} = \left(\frac{ac}{bd}\right) \cdot \frac{e}{f} = (x \cdot y) \cdot z.$$

Como se queria demonstrar.

(6) Distributividade. Sejam $x, y, z \in \mathbb{Q}$ tem-se que

$$x \cdot (y+z) = \frac{a}{b} \cdot \left(\frac{c}{d} + \frac{e}{f}\right) = \frac{a}{b} \cdot \left(\frac{cf + ed}{df}\right) = \frac{acf + aed}{bdf} = \frac{ac}{bd} + \frac{ae}{df} = x \cdot y + x \cdot z$$

e

$$(x + y) \cdot z = \left(\frac{ad + bc}{bd}\right) \cdot \frac{e}{f} = \frac{ade + bce}{bdf} = \frac{ae}{bf} + \frac{ce}{df} = x \cdot z + y \cdot z$$

como se queria demonstrar.

Até aqui já foi provado que o conjunto dos números racionais é um anel, e as próximas propriedades que são demonstradas a seguir mostram que é também um anel comutativo com unidade, chamado de domínio de integridade. E por fim, com a última propriedade demonstrada será um corpo, que é o que o exemplo propõe.

(7) Unidade do produto: Basta escrever $\overline{1} = \dfrac{1}{1}$, daí $\forall\ x \in \mathbb{Q}$ tem-se

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

como se queria demonstrar.

(8) Comutatividade para o produto: sejam $x, y \in \mathbb{Q}$ tais que

$$x \cdot y = \frac{a}{b} \cdot \frac{c}{d} = \frac{a \cdot c}{b \cdot d} = \frac{c \cdot a}{d \cdot b} = \frac{c}{d} \cdot \frac{a}{b} = y \cdot x$$

como se queria demonstrar.

(9) Possui inverso multiplicativo: Considere para qualquer $x = \dfrac{a}{b} \in \mathbb{Q}$ onde $a, b \neq 0$, basta considerar seu inverso multiplicativo por $y = \dfrac{b}{a}$ tal que

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

como se queria demonstrar.

Agora, como todas as propriedades acima foram demonstradas pode-se afirmar a partir desse momento no trabalho que o conjunto dos números racionais é um corpo.

Exemplo 1.3. Outros exemplos de corpos são: O conjunto dos números reais $\mathbb{R}$, o conjunto dos números complexos $\mathbb{C} = \{a + b \cdot i |\ a, b \in \mathbb{R}\ e\ i = \sqrt{-1}\}$ e um outro conjunto que será bastante utilizado durante o trabalho é $\mathbb{Q}[\sqrt{p}] = \{a + b \cdot \sqrt{p} \mid a, b \in \mathbb{Q}\}$ com p um número primo. As demonstrações são deixadas ao leitor e vale destacar que não são difíceis.

Exemplo 1.4. Agora considere o conjunto $\mathbb{Z}[\sqrt{2}] = \{a + b \cdot \sqrt{2} \mid a, b \in \mathbb{Z}\}$. Ele não é um corpo, pois não possui inverso no produto para todos os seus elementos. De fato, considere $x = a + b\sqrt{2}$ o seu inverso no produto seria $\dfrac{1}{x}$ tal que $x \cdot \dfrac{1}{x} = 1$, porém, o número $\dfrac{1}{x} = \dfrac{a}{a^2 - 2b^2} - \dfrac{b}{a^2 - 2b^2}\sqrt{2}$ poderia fazer com que um dos coeficientes não fosse inteiro, como por exemplo, tomando $a = 1$ e $b = 2$ teríamos $-\dfrac{1}{7}$ e $-\dfrac{2}{7}$ que não são inteiros. Daí $\dfrac{1}{x}$ não pertence ao conjunto, concluindo assim a afirmação.

Definição 1.5. Sejam $(A, +, \cdot)$ um anel e B um subconjunto não vazio de A. Diz-se que B é um subanel de A se:

i) B é fechado para as operações do conjunto A de estrutura de anel;
ii) $(B, +, \cdot)$ também é um anel.

Proposição 1.6. Sejam A um anel e B um subconjunto não vazio de A. Então B é subanel de A se, e somente se,

i) $0 \in B$;
ii) $a - b \in B$ para todo $a, b \in B$;
iii) $a \cdot b$ para todo $a, b \in B$.

Demonstração. [Gonçalves 1979]. □

Observação 2. Se um subanel $(B, +, \cdot)$ de um corpo $(K, +, \cdot)$ é também um corpo diz-se que B é um subcorpo de K.

Com o objetivo de construir uma sequência lógica de afirmações, as próximas definições e afirmações mostram que o conjunto quociente é um corpo e para isso são tratados diversos elementos da teoria de anéis.

1.2 Ideais

Definição 1.7. Seja A um anel e seja I um subanel de A. Diz-se que I é um ideal de A se I é um grupo comutativo de A e

$$a \cdot x \in I, \ \forall\ a \in A \ e \ \forall\ x \in I.$$

Caso necessário, é possível definir ideal à esquerda e à direita. Observe:

Diz-se que I é um ideal à esquerda de A se,

$$x \cdot a \in I, \ \forall\ a \in A \ e \ \forall\ x \in I.$$

Ou seja, $A \cdot I \subset I$. Diz-se ainda que J é um ideal à direita se

$$x \cdot a \in J \ \forall\ a \in A \ e \ x \in I$$

Ou seja, $J \cdot A \subset J$.

Exemplo 1.8. Seja o conjunto $M_{2\times 2}(\mathbb{R})$ das matrizes quadradas de ordem 2 e $I = \left\{ \begin{bmatrix} a & 0 \\ b & 0 \end{bmatrix} ; \ a, b \in \mathbb{R} \right\}$. Observe que

$$\begin{bmatrix} x & y \\ z & t \end{bmatrix} \cdot \begin{bmatrix} a & 0 \\ b & 0 \end{bmatrix} = \begin{bmatrix} x \cdot a + y \cdot b & 0 \\ z \cdot a + t \cdot b & 0 \end{bmatrix} \in I.$$

Por outro lado,

$$\begin{bmatrix} a & 0 \\ b & 0 \end{bmatrix} \cdot \begin{bmatrix} x & y \\ z & t \end{bmatrix} = \begin{bmatrix} a \cdot x & a \cdot y \\ b \cdot x & b \cdot y \end{bmatrix} \notin I.$$

Logo I é um ideal a direta de $M_{2\times 2}(\mathbb{R})$. De modo análogo, é fácil mostrar que $J = \left\{ \begin{bmatrix} a & b \\ 0 & 0 \end{bmatrix} ;\ a, b \in \mathbb{R} \right\}$ é um ideal à esquerda de $M_{2\times 2}(\mathbb{R})$.

Exemplo 1.9. Seja o anel $\mathbb{Z}$ e o subanel $2 \cdot \mathbb{Z}$ de $\mathbb{Z}$. Perceba facilmente que $2\mathbb{Z}$ é um ideal de $\mathbb{Z}$.

Observe que analogamente ao exemplo anterior, é possível mostrar que o conjunto é também um ideal à esquerda, e portanto um ideal de $\mathbb{Z}$.

Definição 1.10. Diz-se que I é um ideal maximal se $I \neq A$ e os únicos ideais de A contendo I são o próprio I e A.

Os conjuntos Seja A um anel e $x_1, x_2, ..., x_n \in A$. Observe que o conjunto

$$Ax_1 + Ax_2 + ... + Ax_n = \{a_1x_1 + a_2x_2 + ... + a_nx_n \mid a_i \in A\}$$

é um ideal à esquerda de A, que é chamado de ideal à esquerda gerado por $x_1, x_2, ..., x_n$.

Definição 1.11. Se $J \subset A$ é um ideal bilateral e $x \in A$ é tal que $I = x \cdot A$ e $I = A \cdot x$, então I é gerado à esquerda e a direita por x.

Exemplo 1.12. Se $A = 2\mathbb{Z}$ e $x_1 = 2 \in A$ então o ideal principal $I = Ax_1 = (2\mathbb{Z}) \cdot 2 = 4\mathbb{Z}$ não contém o elemento gerador x_1.

Teorema 1.13. Seja $(K, +, .)$ um anel comutativo com unidade $1 \in K$. Então as condições a seguir são equivalentes.

(i.) K é um corpo;
(ii.) (0) é um ideal maximal de K;
(iii.) Os únicos ideais de K são os triviais;

Demonstração. Inicialmente será mostrado que $(i.) \Rightarrow (ii.)$. Seja K um corpo e J um ideal de K tal que $(0) \subset J \subset K$. Suponha que $J \neq \{0\}$ então vai existir um elemento $a \in J$ diferente de 0. Como K é um corpo por hipótese, existe $b \in K$ tal que $b \cdot a = 1$ e então $1 \in J$ daí segue que $J = K$, desde que $a \cdot 1 = a \in J$, $\forall a \in K$.

$(ii.) \Rightarrow (iii.)$ Se (0) é um ideal maximal de K, por definição os únicos ideais de K contendo (0) são o próprio (0) e K, que por definição são os triviais.

$(iii.) \Rightarrow (i.)$ Para K ser um corpo falta mostrar que para quaisquer $x, y \in K$ não nulos tem-se que $x \cdot y = y \cdot x = 1$. Para isso, seja $a \in K$ um elemento não nulo

e $I = K \cdot a$ o ideal principal de K gerado por a. Perceba que, $a = a \cdot 1 \in I$ e isso diz que $I \neq \{0\}$ e como por hipótese temos que $I = K$ segue que,

$$1 \in K = K \cdot a \Rightarrow \exists\ b \in K \mid b \cdot a = 1$$

o que conclui a demonstração do teorema. □

1.3 Anéis quocientes

Nesta seção alguns passos para a construção dos anéis quocientes são omitidos pois o foco do trabalho é outro e apresentar demonstrações dos resultados não se faz tão essencial. Aqui, considere que A seja um anel qualquer e J um ideal em A. Defina a relação $(\equiv (modJ))$ pondo para quaisquer $x, x' \in A$

$$x \equiv x'(modJ) \Leftrightarrow x - x' \in J.$$

lê-se: x é congruente à x' módulo J. É possível mostrar que essa é uma relação de equivalência e isso é encontrado em [Gonçalves 1979].

Definição 1.14. O conjunto denotado por $\overline{x} = \{y \in A \mid y \equiv x(modJ)\}$ é chamado de classe de equivalência do elemento $x \in A$ relativamente a relação $\equiv (modJ)$.

Perceba que $y \in \overline{x}$ acontece se, e somente se, $y - x \in J$ e faz surgir a notação para a classe $\overline{x}$ que é $\overline{x} = x + J = \{x + z \mid z \in J\}$. Pois, se $y - x \in J$, então existe $z \in J$ tal que $y - x = z$. Isto implica que $y = x + z$. Logo, $\bar{x} = \{y \mid y \equiv x(modJ)\} = \{x+z \mid z \in J\} = Z+J$. Assim, finalmente pode-se definir o conjunto quociente de A pelo ideal J sendo o conjunto $A\backslash J = \{\overline{x} = x+J \mid x \in A\}$.

Definição 1.15. Chama-se o conjunto quociente de A pelo ideal J ao conjunto $A/J = \{\bar{x} = x + J \mid x \in A\}$.

Agora que o conjunto quociente de A pelo ideal J está bem definido, são definidas as operações de soma e produto, as quais são fechadas dentro conjunto, porém a demonstração será omitida. Então se $x \equiv x'(modJ)$ e $y \equiv y'(modJ)$ define-se a soma por

$$+ := \ x + y \equiv (x' + y')(modJ).$$

e o produto por

$$\cdot := \ x \cdot y \equiv x' \cdot y'(modJ).$$

Observação 1. Se A for um anel e J um ideal em A com $\overline{x} = \overline{x'}$ e $\overline{y} = \overline{y'}$ então

$$\overline{x + y} = \overline{x' + y'} \ e \ \overline{x \cdot y} = \overline{x' \cdot y'}.$$

Isto é, a classe da soma independe dos representantes das classes das parcelas, e que a classe do produto independe dos representantes das classes dos fatores.

Teorema 1.16. Seja A um anel e J um ideal de A. Se $\overline{x} = x+J$ e $A\backslash J = \{\overline{x} \mid x \in A\}$, então:

(i.) $+ : A\backslash J \times A\backslash J \to A\backslash J$ definida por $(\overline{x}, \overline{y}) \longmapsto \overline{x+y} = \overline{x} + \overline{y}$
e
$\cdot : A\backslash J \times A\backslash J \to A\backslash J$ definida por $(\overline{x}, \overline{y}) \longmapsto \overline{x \cdot y} = \overline{x} \cdot \overline{y}$
definem duas operações em $A\backslash J$;
(ii.) $(A, +, \cdot)$ é um anel chamado quociente de A por J;
(iii.) Se 1 é a unidade de A, então $\overline{1}$ é a unidade de $A\backslash J$;
(iv.) Se A é comutativo, então $A\backslash J$ é comutativo.

Demonstração. [Gonçalves 1979]. □

Teorema 1.17. Seja A um anel comutativo com unidade $1 \in A$ e seja J um ideal de A. Então J é um ideal maximal de A se, e somente se, $A\backslash J$ é um corpo.

Demonstração. [Gonçalves 1979]. □

1.4 homomorfismos de anéis

Definição 1.18. Uma função $f : A \to A'$ diz-se um homomorfismo de A em A' se satisfizer as condições:

(i.) $f(x+y) = f(x) + f(y)$ para todo $x, y \in A$;
(ii.) $f(x \cdot y) = f(x) \cdot f(y)$ para todo $x, y \in A$.

Caso o homomorfismo seja de A em A, diz-se endomorfismo de A e denota-se por $EndA$.

Definição 1.19. Se $f : A \to A'$ é um homomorfismo bijetivo então diz-se que f é um isomorfismo de A em A'. Caso o isomorfismo seja de A no próprio A, diz-se automorfismo de A, denotado por $Aut(A)$ o conjunto de todos os automorfismos de A.

Definição 1.20. Diz-se que dois anéis A e A' são isomorfos, denotados por $A \backsimeq A'$, se existir um isomorfismo de A em A'.

Teorema 1.21. Sejam A e A' anéis e $f : A \to A'$ um homomorfismo. Então,

(i) $f(0_A) = 0'_{A'}$;

(ii) $f(-a) = -f(a)$ para todo $a \in A$;

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

(iv) Se A e A' são corpos então f é a função constante zero ou f é injetiva.

Demonstração. (i) Observe que $0 + 0 = 0 \Rightarrow f(0 + 0) = f(0) + f(0)$, pois é um homomorfismo. Daí, $f(0) = f(0) + f(0)$ e então $f(0) = 0'$.

(ii) Seja $a \in A$, observe que $a + (-a) = 0$, segue do item (i) que

$$\begin{aligned} f(a + (-a)) = f(0) &\Rightarrow f(a) + f(-a) = 0' \\ &\Rightarrow f(-a) = -f(a). \end{aligned}$$

(iii) De $1 \cdot 1 = 1$ segue que $f(1 \cdot 1) = f(1)$ implica que $f(1) \cdot f(1) = f(1)$, daí

$$\begin{aligned} &\Rightarrow f(1)^2 = f(1) \\ &\Rightarrow f(1) \cdot (f(1) - 1') = 0' \\ &\Rightarrow f(1) = 0' \textit{ ou } f(1) = 1'. \end{aligned}$$

Se $f(1) = 0'$ então $f(x) = f(x \cdot 1) = f(x) \cdot f(1) = f(x) \cdot 0' = 0'$. Ou seja, f é a função constante zero.

(iv) Sejam A e A' corpos, suponha que f não é uma função constante zero. Assim, pelo item anterior $f(1) = 1'$. A seguir será mostrado que f é injetiva. Dados $x, y \in A$ onde $f(x) = f(y)$ tem-se que por f ser um homomorfismo, $f(x) - f(y) = f(x - y) = 0'$. Suponha que $x \neq y$, então $x - y \neq 0$ e por A ser um corpo existe $b \in A$ tal que $b \cdot (x - y) = 1$ e daí segue que

$$\begin{aligned} f(b \cdot (x - y)) &= f(1) \\ \Rightarrow f(b) \cdot f(x - y) &= f(1) \\ \Rightarrow 1' &= 0'. \end{aligned}$$

O que é um absurdo, pois $f(1) = 1'$. Concluindo a demonstração.

□

Exemplo 1.22. Seja A um anel qualquer. A função identidade $f : A \to A$ definida por $f(x) = x$ é um isomorfismo. De fato, primeiro observe que é um homomorfismo, pois se

$$f(x + y) = x + y = f(x) + f(y)$$

e

$$f(x \cdot y) = x \cdot y = f(x) \cdot f(y).$$

E como ela é uma função bijetora, é um isomorfismo.

Definição 1.23. Sejam A e A' anéis, $f : A \to A'$ um homomorfismo de A em A'. Chama-se núcleo de f ou Kernel de f o conjunto

$$N(f) = \{a \in A \mid f(a) = 0'\},$$

denotado por $N(f)$ ou $Ker(f)$.

Definição 1.24. Sejam A e A' anéis, $f : A \to A'$ um homomorfismo de A em A'. Chama-se imagem de f ao conjunto

$$Im(f) = \{f(a) \mid a \in A\}.$$

Teorema 1.25. Sejam A e A' anéis e $f : A \to A'$ um homomorfismo. Então,

(i) A imagem de f é um subanel de A';
(ii) O núcleo de f é um ideal de A, e f é injetiva $\Leftrightarrow$ $N(f) = \{0\}$;
(iii) Os anéis $A\backslash N(f)$ e Imf são isomorfos.

Demonstração. [Gonçalves 1979]. □

1.5 Polinômios em uma indeterminada

A fim de usar no próximo capítulo algumas definições, propriedades ou mesmo proposições que envolvem polinômios aqui será feita uma breve revisão.

Definição 1.26. Seja K um corpo. Chama-se polinômio sobre K em uma indeterminada x a uma expressão formal

$$p(x) = a_0 + a_1x + a_2x^2 + ... + a_mx^m + ...$$

onde $a_i \in K$ para todo $i \in \mathbb{N}$, e existe um $n \in \mathbb{N}$ tal que $a_j = 0$ para todos os índices $j \geq n$.

Exemplo 1.27. Observe o polinômio

$$p(x) = 1 - x + x^2 + \frac{2}{3}x^3 + 0x^4 + 0x^5 + ...$$

que é um polinômio na indeterminada x sobre o corpo $\mathbb{Q}$ onde $a_0 = a_2 = 1$, $a_1 = -1$, $a_3 = \frac{2}{3}$ e a partir dos índices maiores ou iguais a 4 todos os coeficientes são nulos.

Definição 1.28. Diz-se que dois polinômios são iguais quando seus coeficientes que estão na mesma posição são todos iguais. Isto é, sejam $p(x) = a_0 + a_1x + a_2x^2 + ... + a_mx^m + ...$ e $q(x) = b_0 + b_1x + b_2x^2 + ... + b_mx^m + ...$ sobre um corpo K são iguais se, e somente se, $a_i = b_i$ em K para todo $i \in \mathbb{N}$.

Definição 1.29. Um polinômio na indeterminada x sobre o corpo K é chamado de identicamente nulo se, e somente se, $a_i = 0$ para todo $i \in \mathbb{N}$ e denota-se $p(x) = 0$. Agora, se $a_0 = a \in K$ e todos os outros índices são nulos diz-se que o polinômio $p(x) = a$ é um polinômio constante, será omitida a parte $0 \cdot x^{n+1} + 0 \cdot x^{n+2} + ...$ quando $a_j = 0$ para todo $j > n$.

Definição 1.30. Seja o polinômio $p(x) = a_0 + a_1x + ... + a_nx^n$ com $a_n \neq 0$ não nulo com coeficientes em K tem que $a_j = 0$ para todo $j > n$ diz-se que o polinômio é de grau n e denota-se $\partial p(x) = n$.

A partir de agora, será denotado por $K[x]$ o conjunto de todos os polinômios sobre o corpo K na indeterminada x. Como se trata de um conjunto, a seguir são definidos as operações de soma e produto. Considere $p(x) = a_0 + a_1x + ... + a_mx^m + ...$ e $q(x) = b_0 + b_1x + ... + b_mx^m + ...$ dois elementos em $K[x]$ tais que a soma é dada por

$$p(x) + q(x) = c_0 + c_1x + ... + c_mx^m + ...$$

onde $c_i = (a_i + b_i) \in K$ e o produto por

$$p(x) \cdot q(x) = c_0 + c_1x + .. + c_mx^m + ...$$

onde $c_0 = a_0b_0,\ c_1 = a_0b_1 + a_1b_0,\ c_2 = a_0b_2 + a_1b_1 + a_2b_0, ..., c_k = a_0b_k + a_1b_{k-1} + ... + a_{k-1}b_1 + a_kb_0$ com $k \in \mathbb{N}$. Essa última, se deve a propriedade distributiva e da multiplicação de potências com a mesma base quando se faz $x^n \cdot x^m = x^{n+m}$.

Exemplo 1.31. Sejam os polinômios $p(x) = 2x^2 - 2x + 1$ e $q(x) = x + 1$, então

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

$$p(x) - q(x) = (2x^2 - 2x + 1) - (x + 1) = 2x^2 - 3x,$$

e também

$$p(x) \cdot q(x) = (2x^2 - 2x + 1) \cdot (x + 1) = 2x^3 + 2x^2 - 2x^2 - 2x + x + 1 = 2x^3 - x + 1$$

são as operações com os polinômios.

Observe que $(K[x], +, \cdot)$ é um domínio de integridade onde $p(x) = 0$ é o elemento neutro e $p(x) = 1$ é a unidade de $K[x]$. Agora, se D é um domínio de

integridade qualquer, de maneira bem semelhante é possível construir o domínio de integridade $D[x]$ de todos os polinômios na indeterminada x com coeficientes em D.

O próximo teorema apresenta as condições necessárias para efetuar a divisão entre dois polinômios e sua demonstração será omitida, porém uma fonte será indicada.

Teorema 1.32 (Algoritmo da divisão)**.** Sejam $f(x),\ g(x) \in K[x]$ e $g(x) \neq 0$. Então existem únicos $q(x),\ r(x) \in K[x]$ tais que:

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

onde ou $r(x) = 0$ ou $\partial g(x) > \partial r(x)$.

Demonstração. [Gonçalves 1979]. □

Definição 1.33. Seja o polinômio não nulo $p(X) = a_0 + a_1x + ... + a_nx^n$ em $K[x]$ e $\alpha \in K$ tal que $p(\alpha) = a_0 + a_1\alpha + ... + a_n\alpha^n = 0 \in K$ então diz-se que α é uma raiz de $p(x)$ em K.

Definição 1.34. Seja o polinômio não nulo $p(X) = a_0 + a_1x + ... + a_{n-1}x^{n-1} + a_nx^n$ em $K[x]$, se $a_n = 1$ diz-se que o polinômio é mônico e escrito da forma $p(X) = a_0 + a_1x + ... + a_{n-1}x^{n-1} + x^n$.

Proposição 1.35. Seja K um corpo e seja $p(x) = a_0+a_1x+...+a_nx^n$ um polinômio não nulo em $K[x]$ de grau n. Então o número de raízes de $p(x)$ em K é no máximo igual a $n = \partial p(x)$.

Demonstração. [Gonçalves 1979]. □

A seguir é apresentada uma definição bastante usada no desenvolvimento do restante do trabalho que é a de extensão de corpos.

Definição 1.36. seja K é um corpo e se $L \supset K$ é um corpo, diz-se que L é uma extensão de K.

Por exemplo, considere os corpos $\mathbb{R}$ e $\mathbb{C}$ os corpos dos reais e dos complexos respectivamente, como $\mathbb{C} \supset \mathbb{R}$ então $\mathbb{C}$ é uma extensão do corpo $\mathbb{R}$. Um outro exemplo um pouco menos comum mas bastante usado nesse trabalho são os corpos $\mathbb{Q}[\sqrt{2}]$ e $\mathbb{Q}$, onde $\mathbb{Q}[\sqrt{2}] \supset \mathbb{Q}$ e então $\mathbb{Q}[\sqrt{2}]$ é uma extensão do corpo $\mathbb{Q}$.

Caso o objetivo do trabalho fosse fazer uma analogia do conjunto dos polinômios com o conjunto dos números inteiros, então os polinômios irredutíveis que são definidos a seguir fariam o papel dos números primos.

Definição 1.37. Seja $p(x) \in K[x]$ um polinômio tal que $\partial p(x) \geq 1$. Diz-se que o polinômio é irredutível sobre K se toda vez que $p(x) = g(x) \cdot h(x)$, com $g(x),\ h(x) \in K[x]$ tem-se que $g(x) = a$ uma constante em K ou $h(x) = b$ uma constante em K. Se o polinômio não for irredutível chama-se ele de redutível ou fatorável.

Exemplo 1.38. Considere o polinômio $p(x) = x^2 - 2 \in \mathbb{Q}[x]$ que é irredutível sobre o corpo $\mathbb{Q}$ porém, sobre o corpo $\mathbb{R}$ é redutível já que $p(x)$ pode ser escrito em sua forma fatorada como $(x - \sqrt{2}) \cdot (x + \sqrt{2})$.

O exemplo acima mostra que um polinômio pode ser irredutível sobre um corpo K e redutível em uma extensão $L \supset K$, muitas vezes é um trabalho difícil dizer se um polinômio é irredutível sobre um corpo. O próximo teorema apresenta uma breve solução quando se trata do corpo dos racionais e consequentemente para o anel $\mathbb{Z}[x]$.

Proposição 1.39 (Gauss)**.** Seja $p(x) \in \mathbb{Z}[x]$ tal que $p(x)$ é irredutível sobre $\mathbb{Z}$ então $p(x)$ é irredutível sobre $\mathbb{Q}$.

Demonstração. [Gonçalves 1979]. □

Proposição 1.40 (Critério de Einsenstein)**.** seja $p(x) = a_0 + a_1x + ... + a_nx^n$ um polinômio em $\mathbb{Z}[x]$. Suponha que exista um número inteiro e primo p tal que:

(a) p não divide a_n.
(b) p divide $a_0, a_1, ..., a_{n-1}$.
(c) p^2 não divide a_0.

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

Demonstração. [Gonçalves 1979]. □

Exemplo 1.41. Seja o polinômio $p(x) = x^5 + 4x + 10$. Como para $p = 2$ tem-se que $2^2 = 4$ não divide 10, 2 divide 2 e 10, e por fim, 2 não divide 1. Pelo critério Einsenstein tem-se que $p(x)$ é irredutível sobre $\mathbb{Q}$.

Se $u \in K - \{0\}$ e se $p_1(x), p_2(x), ..., p_m(x)$ são polinômios irredutíveis sobre K então todo polinômio $f(x)$ pode ser escrito como

$$f(x) = u \cdot p_1(x) \cdot p_2(x) \cdots p_m(x).$$

Observe que tem-se $f(x) = u$ quando $m = 0$.

Teorema 1.42. Seja K um corpo. Então todo polinômio $f(x) \in K[x] - \{0\}$ pode ser escrito na forma,

$$f(x) = u \cdot p_1(x) \cdots p_m(x)$$

onde $u \in K - \{0\}$ e $p_1(x), p_2(x), ..., p_m(x)$ são polinômios irredutíveis sobre K.

É importante observar que essa expressão é única a menos da constante u e da ordem dos polinômios $p_1(x), ..., p_m(x)$.

Demonstração. [Gonçalves 1979]. □

1.6 Extensões algébricas dos Racionais

Aqui o objetivo da seção é encontrar corpos K de forma que $\mathbb{Q} \subset K \subset \mathbb{R}$ através de um processo que é mostrado abaixo e chamado de adjunção de raízes. Considere a partir de agora K um corpo e $L \supset K$ uma extensão de K.

Definição 1.43. Diz-se que $\alpha \in L$ é algébrico sobre K se existir um polinômio $f(x) \in K[x] - \{0\}$ tal que $f(\alpha) = 0$. Caso contrário, α é transcendente sobre K.

A seguir são apresentados dois exemplos, o primeiro mostra um número algébrico e o segundo mostra um número transcendente, ambos sobre $\mathbb{Q}$.

Exemplo 1.44. Considere o número $\sqrt[3]{3} \in \mathbb{R} \supset \mathbb{Q}$, ele é algébrico sobre $\mathbb{Q}$. De fato, observe que $f(x) = x^3 - 3 \in \mathbb{Q}[x]$ e $f(\sqrt[3]{3}) = (\sqrt[3]{3})^3 - 3 = 3 - 3 = 0$, o que conclui a afirmação.

Exemplo 1.45. O número $\pi \in \mathbb{R} \supset \mathbb{Q}$ é transcendente sobre $\mathbb{Q}$. [Gonçalves 1979].

Observe que caso $\alpha \in K$ onde K é um corpo, então α é algébrico sobre K, pois é raiz do polinômio $f(x) = x - \alpha \in K$. Assim, pode-se afirmar que todo número racional é algébrico sobre $\mathbb{Q}$. Por fim, é possível agora definir o que é um extensão algébrica.

Definição 1.46. Se para todo $\alpha \in L \supset K$ tem-se que α é algébrico sobre K então $L \supset K$ diz-se uma extensão algébrica de K.

Existe uma convenção de nomenclatura que diz que quando o número for algébrico sobre o corpo dos racionais então pronuncia-se apenas que ele é algébrico. E do mesmo jeito, se o número é transcendente sobre os racionais, diz-se apenas que ele é transcendente.

Seja agora $\alpha \in L$ algébrico sobre o corpo K e $p(x)$ um polinômio em $K[x]$, mônico de menor grau tal que $p(\alpha) = 0$. Pela minimalidade do grau do polinômio segue que $p(x)$ é o único polinômio mônico irredutível em $K[x]$ tal que $p(\alpha) = 0$ e ele será denotado por $p(x) = irr(\alpha, K)$.

Exemplo 1.47. Se $\alpha = \sqrt{2} \in \mathbb{R} \supset \mathbb{Q}$, observe que $\mathbb{Q}[\sqrt{2}] = \{f(\sqrt{2}) \mid f(x) \in \mathbb{Q}[x]\}$. De fato, pela definição $\mathbb{Q}[\sqrt{2}] = \{f(\sqrt{2}) \mid f(x) \in \mathbb{Q}[x]\}$. Agora, como $f(x) \in \mathbb{Q}[x]$ pelo algorítmo da divisão existem os polinômios $q(x),\ r(x) \in \mathbb{Q}[x]$ tais que $f(x) = (x^2 - 2) \cdot q(x) + r(x)$ onde $r(x) = 0$ ou $\partial r(x) < 2$. Se $\partial r(x) < 2$ escreve-se $r(x) = a + bx$ com $a, b \in \mathbb{Q}$. Segue daí que

$$\begin{aligned} f(\sqrt{2}) &= ((\sqrt{2})^2 - 2) \cdot q(\sqrt{2}) + r(\sqrt{2}) \\ &= 0 \cdot q(\sqrt{2}) + r(\sqrt{2}) \\ &= r(\sqrt{2}) \\ &= a + b\sqrt{2},\ a, b \in \mathbb{Q}, \end{aligned}$$

como se queria demonstrar.

Exemplo 1.48. Se $\alpha = \sqrt[3]{2} \in \mathbb{R} \supset \mathbb{Q}$, observe que $\mathbb{Q}[\sqrt[3]{2}] = \{a + b\sqrt[3]{2} + c(\sqrt[3]{2})^2 \mid a, b, c \in \mathbb{Q}\}$. Por definição tem-se que $\mathbb{Q}[\sqrt[3]{2}] = \{f(\sqrt[3]{2}) \mid f(x) \in \mathbb{Q}[x]\}$ e pelo algoritmo da divisão existem $q(x), r(x) \in \mathbb{Q}[x]$ com $r(x) = 0$ ou $\partial r(x) < 3$. Se $\partial r(x) < 3$ tem -se

$$f(x) = (x^3 - 2) \cdot q(x) + r(x)$$

substituindo $\sqrt[3]{2}$ em x,

$$\begin{aligned} \Rightarrow f(\sqrt[3]{2}) &= ((\sqrt[3]{2})^3 - 2) \cdot q(\sqrt[3]{2}) + r(\sqrt[3]{2}) \\ &= r(\sqrt[3]{2}) \\ &= a + b\sqrt[3]{2} + (\sqrt[3]{2})^2\ a, b \in \mathbb{Q}, \end{aligned}$$

como se queria demonstrar.

Teorema 1.49. Se $\alpha \in L \supset K$ e se $\psi : K[x] \to L$ uma função definida por $\psi(f(x)) = f(\alpha)$ então ψ é um homomorfismo tal que:

(i) $Im\psi = K[\alpha],\ K \subset K[\alpha]\ L$, onde K é um corpo.
(ii) α é transcendente sobre $K \Leftrightarrow N(\psi) = \{0\}$.
(iii) Se α é algébrico sobre K e $p(x) = irr(\alpha, K)$ então $N(\psi) = K[x] = K[x] \cdot p(x)$ é um ideal maximal de $K[x]$.
(iv) $K[x] \backslash N(\psi) \backsimeq K(\alpha)$

Demonstração. Primeiro observe que ψ é um homomorfismo. Com efeito, dados $f(x), g(x) \in K[x]$ tem-se que

$$\psi(f(x) + q(x)) = \psi((f + g)(x)) = (f + g)(\alpha) = f(\alpha) + g(\alpha) = \psi(f(x)) + \psi(g(x))$$

e

$$\psi(f(x)\cdot g(x)) = \psi((f\cdot g)(x)) = (f\cdot g)(\alpha) = f(\alpha)\cdot g(\alpha) = \psi(f(x))\cdot\psi(g(x)).$$

O que conclui a afirmação. Agora, seguem as demonstrações dos itens de (i) a (iv) do teorema.

(i) Observe na definição de ψ que $Im\psi = \{f(\alpha) \mid f(\alpha) = \psi(f(x))\}$, onde $f(x) \in K[x]$. Ou seja, escrito de outra maneira tem-se

$$Im\psi = \{f(\alpha) \mid f(x) \in K[x]\}$$

que é a definição de $K[\alpha]$. Logo, $Im\psi = K[\alpha]$. Agora veja as inclusões. Seja a função identidade $f(a_i) = a_i$ com $a_i \in K$ e $i \in \mathbb{N}$, observe que qualquer $a_i \in K$ também pertence à $K[x]$, logo $K \subset K[x]$.

(ii) Observe que $N(\psi) = \{f(x) \in K[x] \mid \psi(f(x)) = 0\}$, pela hipótese tem-se α transcendente sobre K. Escolha $f(x) \in K[x] - \{0\}$ e daí, $f(\alpha) \neq 0$. Porém, $\psi(f(x)) = f(\alpha) \neq 0$. Logo o único polinômio tal que $\psi(f(x)) = f(\alpha) = 0$ é o próprio polinômio nulo. Portanto, $N(\psi) = \{0\}$. Reciprocamente, suponha que $N(\psi) = \{0\}$. Isto é, $N(\psi) = \{f(x) \in K[x] \mid f(x) = 0'\}$, então para $f(x) \neq 0$ em $K[x]$ tem-se

$$\psi(f(x)) = 0.$$

Como $\psi(f(x)) = f(\alpha) \neq 0$, tem-se que α é transcedente sobre K.

(iii) Como α é algébrico sobre K, então $N(\psi) \neq \{0\}$. Considere $N(\psi) = K[x]\cdot p(x)$ um ideal em $K[x]$. Como $p(x)$ é irredutível sobre K, pelo teorema 1.25 tem-se que $N(\psi) = K[x]\cdot p(x)$ é um ideal maximal em $K[x]$.

(iv) Pelo item (i) desse teorema tem-se $Im\psi = K[\alpha]$ e pelo item (iii) do teorema 1.25 tem-se

$$K[x]\backslash N(\psi) \backsimeq K[\alpha].$$

□

Colorário 1. Seja $\alpha \in L \supset K$. Se α é algébrico sobre K então $K[\alpha]$ é um subcorpo de L que contém K.

Demonstração. Considere $\psi : K[x] \to L$ como no teorema anterior, definida por $\psi(f(x)) = f(\alpha)$. Como α é algébrico sobre K pelo item (iii) do teorema tem-se que $N(\psi) = K[x]\cdot p(x)$ é um ideal maximal e daí $K[x]\backslash N(\psi)$ é um corpo que pelo item (iv) é isomorfo à $K[x]$. Logo, $K[\alpha]$ é um corpo. □

Colorário 2. Seja $\alpha \in L \supset K$. Se α é transcedente sobre K então $K[\alpha]$ é um subdomínio de L isomorfo ao domínio $K[x]$ dos polinômios em uma indeterminada x.

Demonstração. Para mostrar que $K[\alpha]$ é um subdomínio de L, basta que $K[\alpha]$ seja um anel sem divisores de zero. Primeiro, observe que $K[\alpha]$ é um subanel. Considerando $f(\alpha), g(\alpha) \in K[\alpha]$ veja que

i. $f(\alpha) - g(\alpha) = (f - g)(\alpha) \in K[\alpha]$
ii. $f(\alpha) \cdot g(\alpha) = (f \cdot g)(\alpha) \in K[\alpha]$.

Agora, veja que K não possui divisores de zero pois,

$$f(\alpha) \cdot g(\alpha) = 0 \Rightarrow f(\alpha) = 0 \; ou \; g(\alpha) = 0,$$

e pela hipótese, α é transcedente sobre $K[\alpha]$, então $f(\alpha)$ ou $g(\alpha)$ é o polinômio nulo aplicado à α. □

Colorário 3. Se $\alpha, \beta \in L \supset K$ são raízes de um mesmo polinômio irredutível sobre K, então $K[\alpha]$ e $K[\beta]$ são corpos isomorfos.

Demonstração. Como α e β são raízes de polinômios irredutíveis sobre K, então $p(x) = irr(\alpha, K) = irr(\beta, K)$. Pelo item (iii) do teorema anterior obtém-se $J = K[x] \cdot p(x)$ é um ideal maximal de $K[x]$ e pelo item (iv) tem-se

$$K[\alpha] \backsimeq K[x] \backslash J \; e \; K[x] \backslash J \backsimeq K[\beta].$$

Logo $K[\alpha] \backsimeq K[\beta]$ são isomorfos como se queria mostrar. □

Proposição 1.50. Seja $L \supset K$ e $\alpha \in L$ algébrico sobre K. Se o grau do polinômio $irr(\alpha, K)$ é n, então:

(i) Para todo $f(x) \in K[x]$, $f(\alpha)$ pode ser expresso de modo único na forma $f(\alpha) = a_0 + a_1\alpha + ... + a_{n-1}\alpha^{n-1}$ onde $a_i \in K$.
(ii) $K[\alpha] = \{a_0 + a_1\alpha + ... + a_{n-1}\alpha^{n-1} \mid a_i \in K\}$ é um subcorpo de L que contém K.
(iii) Se $K = \mathbb{Z}_p$ então $K[\alpha]$ é um corpo contendo exatamente p^n elementos.

Demonstração. Se $p(x) = irr(\alpha, K)$ onde $\partial p(x) = n$ por hipótese. Existe um polinômio $f(x) \in K[x]$, tal que pelo algoritmo da divisão existem $q(x), r(x) \in K[x]$ de modo que

$$f(x) = p(x) \cdot q(x) + r(x)$$

onde $r(x) = 0$ ou $\partial r(x) < n$. Assim $r(x) = a_0 + a_1x + ... + a_{n-1}x^{n-1}$ onde $a_i \in K$ com $i = 1, ..., n-1$. Agora, aplicando α em $f(x)$ e sabendo que $p(\alpha) = 0$ observa-se

$$\begin{aligned} f(\alpha) &= q(\alpha) \cdot p(\alpha) + r(\alpha) \\ &= q(\alpha) \cdot 0 + r(\alpha) \\ &= r(\alpha) \\ &= a_0 + a_1\alpha + ... + a_{n-1}\alpha^{n-1} \end{aligned}$$

como se queria demonstrar.

(ii) Por definição $K[\alpha] = \{f(\alpha) \mid f(x) \in K[x]\}$, e pelo item (i) dessa proposição $f(\alpha)$ é escrito de maneira única da forma $f(\alpha) = a_0 + a_1\alpha + ... + a_{n-1}\alpha^{n-1}$ onde $a_i \in K$, daí

$$k[\alpha] = \{f(\alpha) \mid f(x) \in K[x]\} = \{a_0 + a_1\alpha + ... + a_{n-1}\alpha^{n-1}\}.$$

Então pelo corolário 1 $K[\alpha]$ é um subcorpo de L que contém K.

(iii) Observe pelos itens anteriores que $\mathbb{Z}_p[\alpha] = \{a_0 + a_1\alpha + ... + a_{n-1}\alpha^{n-1} \mid a_i \in \mathbb{Z}_p\}$. Assim existe correspondência bijetiva entre $\mathbb{Z}_p[\alpha]$ e o conjunto de todas as n-uplas $\{a_0, a_1, ..., a_{n-1}\}$ onde $a_i \in \mathbb{Z}_p = \{\overline{0}, \overline{1}, ..., \overline{p-1}\}$ é isto demonstra este item. □

Exemplo 1.51. Seja $\alpha = \sqrt[n]{p} \in \mathbb{R}$ e n um inteiro maior ou igual à 2. Então α é uma raiz real do polinômio $x^n - p$, que é facilmente mostrado ser irredutível sobre $\mathbb{Q}$ usando o critério de Einsenstein.

Do exemplo acima tem-se $x^n - p = irr(\alpha, \mathbb{Q})$ e que $\mathbb{Q}[\alpha]$ é um subcorpo de $\mathbb{R}$ contendo $\mathbb{Q}$. Veja mais ainda, $\mathbb{Q}[\alpha] = \{a_0 + a_1\alpha + ... + a_{n-1}\alpha^{n-1} \mid a_i \in \mathbb{Q} \ \ i = 1, ..., n-1\}$. Observe,

$$\begin{aligned} &\mathbb{Q} \subset \mathbb{Q}[\sqrt{2}] = \{a_0 + a_1\sqrt{2} \mid a_0, a_1 \in \mathbb{Q}\} \subset \mathbb{R}. \\ &\mathbb{Q} \subset \mathbb{Q}[\sqrt[3]{2}] = \{a_0 + a_1\sqrt[3]{2} + a_2(\sqrt[3]{2})^2 \mid a_0, a_1, a_2 \in \mathbb{Q}\} \subset \mathbb{R}. \\ &\mathbb{Q} \subset \mathbb{Q}[\sqrt[4]{2}] = \{a_0 + a_1\sqrt[4]{2} + a_2(\sqrt[4]{2})^2 + a_3(\sqrt[4]{2})^3 \mid a_0, a_1, a_2, a_3 \in \mathbb{Q}\} \subset \mathbb{R}. \end{aligned}$$

Observe ainda que se β é uma raiz cúbica complexa de $x^3 - 2$ tal que β não seja um número real. Tem-se que $\mathbb{Q} \subset \mathbb{Q}[\sqrt[3]{2}] \subset \mathbb{R}$ e $\mathbb{Q} \subset \mathbb{Q}[\beta] \subset \mathbb{C}$ e mais que $\mathbb{Q}[\sqrt[3]{2}]$ é um isomorfismo com $\mathbb{Q}[\beta]$, pois $\sqrt[3]{2} \in \mathbb{R}$ e $\beta \in \mathbb{C}$ são raízes do mesmo polinômio irredutível $p(x) = x^3 - 2$ sobre o conjunto dos números racionais.

Seja p é um número primo maior ou igual à 2, defina α_i por $\alpha_i = \sqrt[2^i]{p_i} \in \mathbb{R}$. Agora, observe que α_i é raiz do polinômio $q(x) = x^{2^i} - p$ irredutível pelo critério de Einsienstein sobre $\mathbb{Q}$, para todo $i \in \mathbb{N}$. Por exemplo,

Se $i = 1$ então $\mathbb{Q}[\alpha_1] = \mathbb{Q}[\sqrt{p}] = \{a_0 + a_1\sqrt{p} \mid a_0, a_1 \in \mathbb{Q}\}$.
Se $i = 2$ então $\mathbb{Q}[\alpha_2] = \{a_0 + a_1\sqrt[4]{p} + a_2(\sqrt[4]{p})^2 + a_3(\sqrt[4]{p})^3 \mid a_0, a_1, a_2, a_3 \in \mathbb{Q}\}$,

e assim por diante. Veja que se $a_1 = a_3 = 0$ em $\mathbb{Q}[\alpha_2]$, o conjunto $\mathbb{Q}[\alpha_2]$ descreve todos os elementos de $\mathbb{Q}[\alpha_1]$ e então $\mathbb{Q}[\alpha_1] \subset \mathbb{Q}[\alpha_2]$. Observe ainda que α_i é raiz do polinômio $x^{2^i} - p$ que é irredutível, usado o critério de Einsienstein sobre $\mathbb{Q}$, para todo $i \in \mathbb{N}$.

Assim, tem-se que os corpos $K_i = \mathbb{Q}[\alpha_i]$ onde $\mathbb{Q} \subset K_i \subset \mathbb{R}$ com $i \geq 2$, e ainda

$$\mathbb{Q} = K_0 \subset K_1 \subset K_2 \subset ... \subset K_i \subset ... \subset \mathbb{R}$$

é uma cadeia ascendente de subcorpos de $\mathbb{R}$ e portanto $\bigcup_{i=0}^{\infty} K_i$ é também um subcorpo de $\mathbb{R}$.

1.7 Corpo de decomposição de um polinômio

Inicialmente são discutidas mais algumas propriedades e definições sobre polinômios, agora com coeficientes no conjunto dos números complexos para posteriormente definir o corpo de decomposição.

Se $f(x) \in K[x]$ é um polinômio de grau $n \geq 1$ e $\alpha_1, ..., \alpha_r$ são todas as diferentes raízes no conjunto dos números complexos, então o polinômio pode ser decomposto da seguinte maneira

$$f(x) = c \cdot (x - \alpha_1)^{m_1} ... (x - \alpha_r)^{m_r}$$

em $\mathbb{C}[x]$ onde $c \in \mathbb{C}$ e $r, m_1, ..., m_r$ são números inteiros positivos. O número inteiro m_i chama-se multiplicidade da raiz α_i e se $m_i = 1$ diz-se que α_i é uma raiz simples do polinômio $f(x)$.

Exemplo 1.52. Considere o polinômio $f(x) = x^3 + 5x^2 + 3x - 9$ cuja sua forma fatorada como descrito acima é da forma

$$f(x) = (x - 1) \cdot (x + 3)^2.$$

Observe que a raiz $\alpha_1 = 1$ tem multiplicidade um e a raiz $\alpha_2 = -3$ tem multiplicidade 2.

Definição 1.53. Se $f(x) = a_0 + a_1 x + ... + a_n x^n \in K[x]$, onde $a_i \in K$ define-se a derivada de $f(x)$ por $f'(x) = a_1 + a_2 x + ... + a_n x^{n-1}$.

Observe antes de apresentar um exemplo que se $\partial f(x) \leq 1$ então $\partial f(x) \neq 0$ e que $\partial f(x) = n - 1$.

Exemplo 1.54. Como no exemplo anterior, considera o polinômio $f(x) = x^3 + 5x^2 + 3x - 9$ cuja derivada, usando a definição, é $f'(x) = 3x^2 + 10x + 3$.

Se $f(x),\ g(x) \in K[x]$ e $a \in K$ seguem imediatamente as seguintes regras para derivadas,

(i) $(f(x)+g(x))' = f'(x)+g'(x)$
(ii) $(a \cdot f(x))' = a \cdot f'(x)$
(iii) $(f(x) \cdot g(x))' = f'(x) \cdot g(x) + f(x) \cdot g'(x)$.

Proposição 1.55. Seja $f(x) \in K[x]$, $\partial f(x) = n \geq 1$ e $\alpha \in \mathbb{C}$ uma raiz de $f(x)$. Então α é raiz simples de $f(x)$ se, e somente se, $f(\alpha) = 0$ e $f'(\alpha) \neq 0$.

Demonstração. Se $\alpha \in \mathbb{C}$ é uma raiz de $f(x)$ com multiplicidade $m \geq 1$ então $f(x)$ pode ser fatorado em $\mathbb{C}[x]$ como $f(x) = (x-\alpha)^m \cdot g(x)$ onde $g(x) \in \mathbb{C}[x]$ e $g'(\alpha) \neq 0$. Daí

$$f'(x) = m \cdot (x-\alpha)^{m-1} \cdot g(x) + (x-\alpha)^m \cdot g'(x).$$

Para $m = 1$ (a hipótese ser raiz simples torna m com esse valor), tem-se

$$f(x) = (x-\alpha)^1 \cdot g(x) \Rightarrow f(\alpha) = (\alpha-\alpha) \cdot g(\alpha) \Rightarrow f(\alpha) = 0$$

e usando o regra do produto para derivadas tem-se

$$f'(x) = m \cdot (x-\alpha)^{m-1} \cdot g(x) + (x-\alpha)^m \cdot g'(x),$$

se $m = 1$, segue que

$$\begin{aligned} f'(x) &= g(x) + (x-\alpha) \cdot g'(x) \\ \Rightarrow f'(\alpha) &= g(\alpha) + (\alpha-\alpha) \cdot g'(\alpha) \\ &= g(\alpha) \neq 0. \end{aligned}$$

como se queria mostrar. Agora, reciprocamente se $f(x) = (x-\alpha)^m \cdot g(x)$ e $f'(x) = m \cdot (x-\alpha)^{m-1} \cdot g(x) + (x-\alpha)^m \cdot g'(x)$. Observe que $f'(\alpha) = 0 \Leftrightarrow m \geq 2$, daí considere por exemplo $m = 2$,

$$f'(x) = 2 \cdot (x-\alpha) \cdot g(x) + (x-\alpha)^2 \cdot g'(x)$$

e aí

$$f'(\alpha) = 2 \cdot (\alpha-\alpha) \cdot g(\alpha) + (\alpha-\alpha)^2 \cdot g'(\alpha) = 0.$$

Mas, por hipótese $f'(\alpha) \neq 0$. Logo $m = 1$ implica que α é uma raiz simples. □

Proposição 1.56. Seja $f(x) \in K[x]$, $\partial f(x) = n \geq 1$ e $\alpha \in \mathbb{C}$ uma raiz de $f(x)$. Se $f(x)$ é irredutível sobre K então todas as raízes de $f(x)$ são simples.

Demonstração. Seja $f(x) \in K[x]$ um polinômio irredutível sobre K e $\alpha \in \mathbb{C}$ uma raiz de $f(x)$ cuja sua multiplicidade é m. A seguir será provado que $m = 1$.

Seja $p(x) = irr(\alpha, K)$, pelo algoritmo da divisão existem $q(x), r(x) \in K[x]$ tais que

$$f(x) = p(x) \cdot q(x) + r(x),$$

onde $r(x) = 0$ ou $\partial r(x) < \partial p(x)$.

Como $r(x) = f(x) - p(x) \cdot q(x)$ e pela minimalidade do grau de $p(x) = irr(\alpha, K)$ segue que $r(x) = 0$ e $f(x) = p(x) \cdot q(x)$. Portanto, pela irredutibilidade de $f(x)$, existe $a \in K$ tal que $q(x) = a \in K$ e então $f(x) = a \cdot p(x)$.

Por outro lado, se $m > 1$ a partir da proposição 1.55 que $f'(\alpha) = a \cdot p'(\alpha) = 0$, ou seja, $p'(\alpha) = 0$ o que contradiz a minimalidade de $p(x)$. Assim, $m = 1$ o que conclui a demonstração. □

Definição 1.57. Chama-se Corpo de decomposição de um polinômio $f(x) \in K[x]$ sobre K, que será denotado por $Gal(f, K)$ ao menor subcorpo de $\mathbb{C}$ que contém K e todas as raízes de $f(x)$ em $\mathbb{C}$.

Vale observar acerca da definição acima que esse menor subcorpo existe e é igual à intersecção de todos os subcorpos de $\mathbb{C}$ que contém K e todas as raízes de $f(x)$ em $\mathbb{C}$.

Para facilitar em algumas demonstrações no decorrer do texto é interessante que o conjunto $Gal(f.K)$ seja escrito de uma maneira construtiva. Para isso, sejam $f(x) \in K[x]$ e $\alpha_1, \alpha_2, ..., \alpha_r$ as diferentes raízes de $f(x)$ em $\mathbb{C}$. Considere,

$$K_0 = K \subset K_1 = K[\alpha_1] \subset K_2 = K_1[\alpha_2] \subset ... \subset K_r = K_{r-1}[\alpha_r].$$

Observe que K_i é o menor subcorpo de $\mathbb{C}$ que contém K e $\alpha_1, \alpha_2, ..., \alpha_i$ e então $K_r = K_{r-1}[\alpha_r] = Gal(f, K)$.

Denote $K_r = K[\alpha_1, ..., \alpha_r]$ para se ter $Gal(f, K) = K[\alpha_1, ..., \alpha_r]$. Assim, independente da ordem que a raiz seja escolhida, ainda assim esse processo chamado de *adjunção de raízes* levaria ao conjunto $Gal(f, K)$.

As vezes para se tomar todas as raízes $\alpha_1, ..., \alpha_r$ não será preciso de todas as r etapas. Pode acontecer de uma etapa apenas ser suficiente. Isto é, ao adjuntar uma das raízes, as demais ficam automaticamente incluídas. Observe o exemplo seguinte.

Exemplo 1.58. Sejam $1 = \alpha_0, \alpha_1, ..., \alpha_{n-1}$ as n raízes em $\mathbb{C}$ do polinômio $f(x) = x^n - 1 \in \mathbb{Q}[x]$ onde $n \geq 1$. Defina α por $\alpha = \cos\frac{2\pi}{n} + i \cdot \sin\frac{2\pi}{n}$, então seja

$\alpha_j = \left(\cos\frac{2\pi}{n} + i \cdot \sin\frac{2\pi}{n}\right)^j$ e observe que $\alpha_1^n = \alpha^n = 1$, pois

$$\begin{aligned}
\alpha_1^n &= \left(\cos\frac{2\pi}{n} + i \cdot \sin\frac{2\pi}{n}\right)^n, \\
&= (e^{\frac{2\pi}{n}\cdot i})^n \\
&= e^{\frac{2\pi n}{n}} \\
&= e^{2\pi\cdot i} \\
&= \cos 2\pi + i \cdot \sin 2\pi \\
&= 1,
\end{aligned}$$

onde na segunda igualdade foi usada a Fórmula de Euler para transformar a escrita trigonométrica em uma potência e daí concluir que $\alpha^n = 1$. Observe também que

$$\alpha_j^n = \left(\left(\cos\frac{2\pi}{n} + i \cdot \sin\frac{2\pi}{n}\right)^n\right)^j = 1$$

onde $1 = \alpha_0, \alpha_1, ..., \alpha_{n-1}$ são as n-raízes distintas de f em $\mathbb{C}$ e são todas as raízes de $x^n - 1$. Assim, $\alpha_i = \alpha^i \in \mathbb{Q}[\alpha]$ para todo $i \in \{0, 1, ..., n-1\}$ e portanto $Gal(x^n - 1, \mathbb{Q}) = \mathbb{Q}[\alpha_1]$.

Exemplo 1.59. Para construir o corpo de decomposição do polinômio $f(x) = x^3 - 2 \in \mathbb{Q}[x]$. Observe que $\alpha = \sqrt[3]{2}$ é raiz de $f(x)$, pois $f(\sqrt[3]{2}) = (\sqrt[3]{2})^3 - 2 = 0$. e pelo exemplo anterior tem-se que

$$\begin{aligned}
\beta &= \cos\frac{2\pi}{3} + i \cdot \sin\frac{2\pi}{3} \\
&= \cos 120 + i \cdot \sin 120 \\
&= -\frac{1}{2} + i \cdot \frac{\sqrt{3}}{2}
\end{aligned}$$

é uma raiz complexa de $f(x)$ e portanto seu conjugado $\overline{\beta} = -\frac{1}{2} - i \cdot \frac{\sqrt{3}}{2}$ também é raiz complexa do polinômio. Assim, as três raízes distintas de $f(x) \in \mathbb{Q}[x]$ são α, β e $\overline{\beta}$. Nessa caso são necessárias apenas duas etapas, isto é, $Gal(f, \mathbb{Q}) = \mathbb{Q}[\alpha, \beta, \overline{\beta}] = \mathbb{Q}[\alpha, \beta]$.

Muitas vezes encontrar todas as raízes de um polinômio é complicado e trabalhoso, no exemplo anterior foi visto que nem sempre é preciso de todas as etapas, como feito na construção do corpo de decomposição pelo processo de adjuntar raízes para encontrar o conjunto $Gal(f, K)$. No primeiro exemplo foi preciso apenas uma etapa, mesmo o polinômio tendo n raízes distintas para $n \geq 1$ e no

segundo exemplo, foi preciso apenas de 2 etapas mesmo o polinômio tendo três raízes distintas.

1.8 Grau de uma extensão

Aqui nesta seção são necessários alguns conhecimentos de álgebra linear os quais são deixados a cargo do leitor.

A partir desse momento seja V um espaço vetorial e K um corpo, se V sobre o corpo K possui uma base com n elementos então n é chamado de dimensão de V sobre K e denotado por $[V : K] = n$.

Definição 1.60. Seja K um corpo qualquer. Uma extensão $L \supset K$ diz-se finita se $[L : K] = n < \infty$. Caso contrário $L \subset K$ diz-se uma extensão infinita.

Proposição 1.61. Seja K um corpo e $L \supset K$ uma extensão de K. Se $L \supset K$ é finita então $L \supset K$ é algébrico.

Demonstração. Suponha que $[L : K] = m < \infty$ e $\alpha \in L \supset K$ onde $K[\alpha]$ é um subespaço de L, segue que $[K[\alpha] : K] \leq m < \infty$. Se $[K[\alpha] : K] = n$ então $1, \alpha, \alpha^2, ..., \alpha^n$ são elementos linearmente dependentes, pois n é o número máximo de elementos linearmente dependentes para formar a base, e então existem $a_0, a_1, ..., a_n$ nem todos nulos, tais que

$$a_0 + a_1\alpha + ... + a_n\alpha^n = 0.$$

Isto é, α é um elemento algébrico sobre K, pois, nesse caso basta considerar o polinômio $p(x) = a_0 + a_1x + ... + a_nx^n$. □

Proposição 1.62. Seja K um corpo e $L \supset K$ uma extensão de K. então se $\alpha \in L \supset K$ é um elemento algébrico sobre K e o grau de $irr(\alpha, K) = n$ então $1, \alpha, \alpha^2, ..., \alpha^{n-1}$ é uma base do espaço vetorial $K[\alpha]$ sobre K e $[K[\alpha] : K] = n < \infty$.

Demonstração. Seja $\alpha \in L \supset K$ um elemento algébrico sobre K tal que $\partial(irr(\alpha, K)) = n$. Pela Proposição 1.50 todo elemento pode ser escrito de modo único como combinação linear sobre K dos elementos $1, \alpha, ..., \alpha^{n-1}$. Assim, os elementos formam uma base de $K[\alpha]$ sobre K. Isto é, $[K[\alpha] : K] = n < \infty$. □

Proposição 1.63. Seja K um corpo e $L \supset K$ uma extensão de K. Se $\alpha \in L \supset K$ é um elemento transcedente sobre K então $K[\alpha] \supset K$ é uma extensão infinita.

Demonstração. Se $\alpha \in L \supset K$ é transcedente sobre K, então $K[\alpha]$ não é uma extensão algébrica, pois não existe $f(x) \in K[x]$ tal que $f(\alpha) = 0$. Supondo que

$K[\alpha] \supset K$ seja uma extensão finita, então teria que $K[\alpha] \supset K$ é algébrica pela Proposição 1.61, o que é um absurdo, logo $K[\alpha] \supset K$ é uma extensão infinita. □

Colorário 4. Seja $\alpha \in L \supset K$. Então as seguintes afirmações são equivalentes:

(i) α é algébrico sobre K.
(ii) $[K[\alpha] : K] < \infty$
(iii) $K[\alpha]$ é uma extensão algébrica de K.

Demonstração. Primeiro observe que $(ii) \Rightarrow (i)$ Se $K[\alpha]$ é uma extensão finita sobre K, pela Proposição 1.61 é uma extensão algébrica sobre K. Agora, que $(iii) \Rightarrow (i)$. por definição se $K[\alpha]$ é uma extensão algébrica sobre K então existe $f(x) \in K[x]$ tal que $f(\alpha) = 0$, isto é, α é algébrico sobre K. Por fim, que $(i) \Rightarrow (iii)$ Pela Proposição 1.62 se α é algébrico sobre K então com todas as outras hipóteses satisfeitas tem-se que $[K[\alpha] : K] < \infty$. □

Proposição 1.64. Sejam $M \supset L \supset K$ corpos tais que $[M : L]$ e $[L : K]$ são finitos, então $[M : K]$ é finito e $[M : K] = [M : L] \cdot [L : K]$.

Demonstração. Sejam $v_1, v_2, ..., v_r$ uma base de M e $u_1, u_2, ..., u_s$ uma base de L sobre K. Basta mostrar que

$$\beta = \left\{ v_i \cdot u_j \mid \begin{array}{l} i = 1, ..., r \\ j = 1, ..., s \end{array} \right\}$$

é uma base de M sobre K, isso concluirá a demonstração da afirmação da proposição.

Observe inicialmente que β é um conjunto linearmente independente em M sobre K. Com efeito, se

$$\alpha_{ij} \in K,\ 1 \leq i \leq r,\ 1 \leq j \leq s,\ \sum_{i,j} \alpha_{ij} \cdot v_i \cdot u_j = 0.$$

Essa equação pode ser reescrita da seguinte maneira:

$$(\alpha_{11} \cdot u_1 + \alpha_{12} \cdot u_2 + ... + \alpha_{1s} \cdot u_s) \cdot v_1 + ... + (\alpha_{r1} \cdot u_1 + \alpha_{r2} \cdot u_2 + ... + \alpha_{rs} \cdot u_s) \cdot v_r = 0$$

e como os $u_j's$ estão em L, segue pela independência linear dos $v_j's$ em M sobre L que

$$\begin{array}{c} \alpha_{11} \cdot u_1 + \alpha_{12} u_2 + ... + \alpha_{1s} \cdot u_s = 0 \\ \vdots \\ \alpha_{r1} \cdot u_1 + \alpha_{r1} \cdot u_2 + ... + \alpha_{rs} \cdot u_s = 0 \end{array}$$

como cada α_{ij} pertence à K segue pela independência linear dos $u_j's$ em L sobre K que cada $\alpha_{ij} = 0$ com $1 \leq i \leq r$ e $1 \leq j \leq s$. Portanto, β é um conjunto linearmente independente de M sobre K.

Agora, falta mostrar que β é um conjunto gerador de M sobre K. Assim, seja $y \in M$ e $v_1, ..., v_r$ uma base de M sobre L e daí existem $\lambda_1, ..., \lambda_r \in L$ tais que,

$$y = \lambda_1 \cdot v_1 + ... + \lambda_r \cdot v_r. \tag{1.1}$$

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

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

Então, substituindo todos esses $\lambda_i's$ na equação (1.1) tem-se

$$\begin{aligned} y &= (\alpha_{11}u_1 + ... + \alpha_{1s}u_s) \cdot v_1 + ... + (\alpha_{r1}u_1 + ... + \alpha_{rs}u_s) \cdot v_s \\ &= \sum_{i,j} \alpha_{ij} v_i u_j, \ \alpha_{ij} \in K, \ 1 \leq i \leq r \ e \ 1 \leq j \leq s, \end{aligned}$$

como se queria demonstrar. □

Colorário 5. (a) $\overline{\mathbb{Q}}_{\mathbb{C}} = \{\alpha \in \mathbb{C} \mid \alpha \text{ é algébrico sobre } \mathbb{Q}\}$ é um subcorpo de $\mathbb{C}$, que é uma extensão algébrica infinita de $\mathbb{Q}$.

(b) $\overline{\mathbb{Q}}_{\mathbb{R}} = \{\alpha \in \mathbb{R} \mid \alpha \text{ é algébrico sobre } \mathbb{Q}\}$ é um subcorpo de $\mathbb{R}$, que é uma extensão algébrica infinita de $\mathbb{Q}$.

Demonstração. (a) Observe que $\overline{\mathbb{Q}}_{\mathbb{C}} \supset \mathbb{Q}$, pois dado $\overline{\alpha} \in \mathbb{Q}$ tem-se que todo racional é algébrico sobre $\mathbb{Q}$ através do polinômio $p(x) = x - \overline{\alpha}$. Agora, para mostrar que $\overline{\mathbb{Q}}_{\mathbb{C}}$ é um subcorpo de $\mathbb{C}$ é suficiente provar que

1) $\alpha, \beta \in \overline{\mathbb{Q}}_{\mathbb{C}} \Rightarrow \alpha - \beta \in \overline{\mathbb{Q}}_{\mathbb{C}}$
2) $\alpha, \beta \in \overline{\mathbb{Q}}_{\mathbb{C}} \Rightarrow \alpha \cdot \beta \in \overline{\mathbb{Q}}_{\mathbb{C}}$
3) $0 \neq \alpha \in \overline{\mathbb{Q}}_{\mathbb{C}} \Rightarrow \alpha^{-1} = \dfrac{1}{\alpha} \in \overline{\mathbb{Q}}_{\mathbb{C}}$

todas elas são mostradas ao mesmo tempo. Para isso, seja $K = \mathbb{Q}[\alpha]$ e $L = K[\beta]$. Como α é algébrico sobre $\mathbb{Q}$ segue que $[K : \mathbb{Q}]$ é finito. Como $L = K[\beta] \subset K = \mathbb{Q}[\alpha]$ segue que β é algébrico sobre $\mathbb{Q}$ e também sobre K, daí $[L : K]$ é finito. Pela proposição acima tem-se que

$$[L : \mathbb{Q}] = [L : K] \cdot [K : \mathbb{Q}] < \infty$$

e pela Proposição 1.61 tem-se que $L \supset \mathbb{Q}$ é uma extensão algébrica. Então o resultado segue imediatamente que $\alpha \pm \beta, \alpha \cdot \beta \in L$ e $\dfrac{1}{\alpha} \in L$ se $\alpha \neq 0$. Logo, tem-se que $\overline{\mathbb{Q}}_{\mathbb{C}} \supset \mathbb{Q}$ é uma extensão algébrica sobre $\mathbb{Q}$. Agora se $\alpha_i = \sqrt[2^i]{2}$ e $K_0 = \mathbb{Q}, K_1 = \mathbb{Q}[\alpha_1], ..., K_i = \mathbb{Q}[\alpha_i]$ tem-se que $M = \bigcup_{i=0}^{\infty} K_i$ é uma extensão algébrica infinita sobre $\mathbb{Q}$ e $M \subset \overline{\mathbb{Q}}_{\mathbb{R}} \subset \overline{\mathbb{Q}}_{\mathbb{C}}$.

(b) Observe que $\overline{Q}_{\mathbb{R}} = \overline{\mathbb{Q}}_{\mathbb{C}} \cap \mathbb{R}$ e $M = \bigcup_{i=0}^{\infty} K_i \subset \overline{\mathbb{Q}}_{\mathbb{R}}$ e aí com argumentos análogos ao item (a) tem-se que $\overline{\mathbb{Q}}_{\mathbb{R}}$ é um subcorpo de $\mathbb{R}$ e que é uma extensão algébrica infinita de $\mathbb{Q}$.

□

Colorário 6. Seja $K \supset \mathbb{Q}$ tal que $[K : \mathbb{Q}] = m$ e seja $p(x) \in \mathbb{Q}[x]$ um polinômio irredutível sobre $\mathbb{Q}$ de grau n. Se $M.D.C\{m, n\} = 1$ então $p(x)$ é um polinômio irredutível sobre K.

Demonstração. Seja $\alpha \in \mathbb{C}$ uma raiz de $p(x)$. Considere os corpos $\mathbb{Q}[\alpha] \subset K[\alpha]$ e suponha que $[K[\alpha] : K] = r$ e $[K[\alpha] : \mathbb{Q}[\alpha]] = s$. Pela Proposição 1.64

$$[K[\alpha] : \mathbb{Q}] = [K[\alpha] : \mathbb{Q}[\alpha]] \cdot [\mathbb{Q}[\alpha] : \mathbb{Q}] = s \cdot n$$

e

$$[K[\alpha] : \mathbb{Q}] = [K[\alpha] : K] \cdot [K : \mathbb{Q}] = r \cdot m.$$

então $n \cdot s = m \cdot r$ e como $M.D.C\{n, m\} = 1$ tem-se que r divide n. Mas, $r \leq n$ diz que $n = r$ e então $p(x)$ é irredutível sobre K. □

Colorário 7. Seja $L = Gal(x^p - 2, \mathbb{Q})$. Então $[L : \mathbb{Q}] = p \cdot (p - 1)$.

Demonstração. Lembre que $L = Gal(x^p - 2, \mathbb{Q}) = \mathbb{Q}[\alpha, u]$ onde $\alpha = \sqrt[p]{2} \in \mathbb{R}$ e $u = \left(\cos\frac{2\pi}{p} + i \cdot \sin\frac{2\pi}{p}\right) \in \mathbb{C}$ é uma raiz p-ésima da unidade tal que $1, u, u^2, ..., u^{p-1}$ são todas as p-ésimas raízes distintas da unidade em $\mathbb{C}$. Pela proposição 1.64 tem-se

$$[L : \mathbb{Q}] = [L : \mathbb{Q}[\alpha]] \cdot [\mathbb{Q}[\alpha] : \mathbb{Q}].$$

Pelo critério de Einsenstein tem-se que $[\mathbb{Q}[\alpha] : \mathbb{Q}] = p$. Agora, se $K = \mathbb{Q}[\alpha]$ tem-se que $L = K[u] \supset K \supset \mathbb{Q}$. Novamente pelo critério de Einsenstein tem-se que u é raiz do polinômio $f(x) = 1 + x + x^2 + ... + x^{p-2} + x^{p-1}$ que é irredutível de grau $p - 1$ sobre $\mathbb{Q}$. Como $[K : \mathbb{Q}] = p$ e $M.D.C(p, p-1) = 1$ tem-se que pelo corolário anterior que $f(x) = 1 + x + x^2 + ... + x^{p-2} + x^{p-1}$ é ainda irredutível sobre K tendo u como raiz. Portanto $[K[u] : K] = p - 1$ o que demonstra o corolário pois

$$L = K[u] \; e \; K = \mathbb{Q}[\alpha].$$

□

Teorema 1.65. Seja $L \supset K \supset \mathbb{Q}$ tal que $[L : K] < \infty$. Então existe $u \in L$ tal que $L = K[u]$.

Este último teorema a sua demonstração são encontrados em [Gonçalves 1979], pág. 102.

Aqui se encerra a construção teórica das extensões de corpos para então se discutir a construção de números e a sua possibilidade de construção sem necessariamente tentar usando as ferramentas.

CAPÍTULO 2

Números construtíveis

O objetivo deste capítulo é mostrar a possibilidade ou não de construções usando apenas régua não graduada e compasso. Quando se diz régua não graduada significa que o instrumento não possui marcações, é apenas uma ferramenta que interliga dois pontos através de uma reta.

Durante o desenvolvimento dos capítulos é possível observar uma relação íntima entre polinômios e suas raízes com os números construtíveis.

Para começar, considere $\mathcal{P}$ um subconjunto de $\mathbb{R}^2$ contendo pelo menos dois pontos distintos.

Definição 2.1. Diz-se que uma reta $r \subset \mathbb{R}^2$ é construtível em $\mathcal{P}$ se r contém dois pontos distintos de $\mathcal{P}$.

Definição 2.2. Diz-se que uma circunferência $c \subset \mathbb{R}^2$ é uma circunferência construtível em $\mathcal{P}$ se o seu centro pertence a $\mathcal{P}$ e um outro ponto de $\mathcal{P}$ pertence a c.

A partir das definições acima, são definidos o que são chamados de *operações elementares* em $\mathcal{P}$.

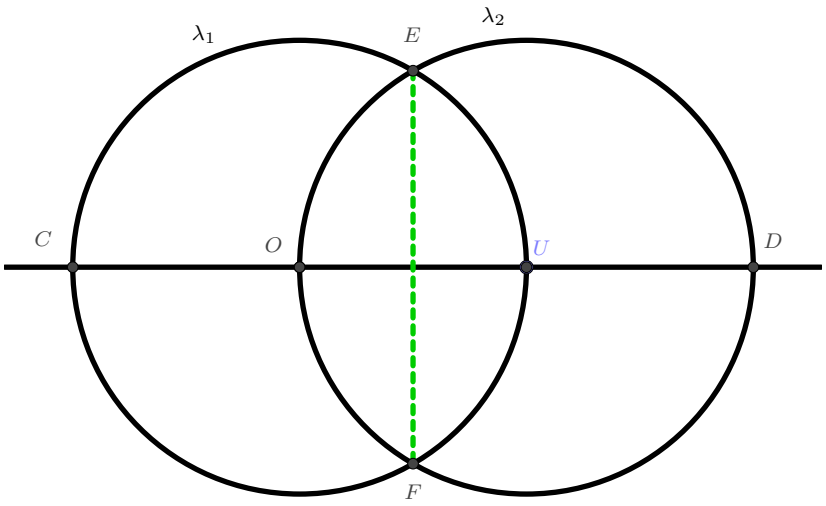
(i) Intersecção de duas retas em $\mathcal{P}$
(ii) Intersecção de uma reta em $\mathcal{P}$ e uma circunferência em $\mathcal{P}$.
(ii) Interseccção de duas circunferências em $\mathcal{P}$.

Definição 2.3. Diz-se que um ponto $A \in \mathbb{R}^2$ é construtível a partir de $\mathcal{P}$ se for possível determinar A por uma das operações elementares em $\mathcal{P}$. Denota-se $\langle \mathcal{P} \rangle$ o subconjunto dos pontos do plano que são construtíveis a partir de $\mathcal{P}$.

Exemplo 2.4. Seja o conjunto $\mathcal{P}_0$ formado pelos pontos $O = (0, 0)$ e $U = (1, 0)$. A seguir são encontrados todos os pontos construtíveis a partir de P_0 seguindo os seguintes passos:

1. Por O e U trace a reta construtível r;
2. Com a ponta seca do compasso centrada em O, trace uma circunferência que passe também pelo ponto U;

3. Com a ponta seca do compasso centrada em U, trace uma circunferência λ_1 que passe também pelo ponto O. Observe a figura a seguir.



Observe que a partir da intersecção da reta r e da circunferência λ_1 obtém-se o ponto $C = (-1, 0)$, pois o raio da circunferência é uma unidade de comprimento. Da mesma maneira, o ponto $D = (2, 0)$, que é a intersecção entre a reta r e a circunferência λ_2, foi construído. Agora, observe que os pontos O, U, E e F são os vértices de um losango de diagonais $\overline{OU}$ e $\overline{EF}$. As coordenadas dos pontos E e F podem ser encontradas observando que o triângulo OEU é equilátero, e como argumentado acima, $\overline{EF}$ é perpendicular a $\overline{OU}$, por serem as diagonais do losango. Daí, a abscissa é a metade do lado e a ordenada é a altura do triângulo equilátero, ou seja, $E = (\frac{1}{2}, \frac{\sqrt{3}}{2})$ e $F = (\frac{1}{2}, \frac{-\sqrt{3}}{2})$.

Concluí-se que $\mathcal{P}_1 = \langle \mathcal{P}_0 \rangle = \{O, U, C, D, E, F\}$.

Para generalizar, faz-se,
$P_0 = \{O, U\}$, $\mathcal{P}_1 = \langle \mathcal{P}_0 \rangle$, $\mathcal{P}_2 = \langle \mathcal{P}_1 \rangle$,..., $\mathcal{P}_{n+1} = \langle \mathcal{P}_n \rangle$, temos,

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

Definição 2.5. Define-se então $\mathcal{P}_\infty = \bigcup_{n=0}^{\infty} \mathcal{P}_n$.

Observe que $\mathcal{P}_\infty$ é um conjunto infinito, mesmo que $\mathcal{P}_n$ seja um subconjunto finito de $\mathbb{R}^2$ $\forall$ $n \in \mathbb{N}$ e que $\langle \mathcal{P}_\infty \rangle = \mathcal{P}_\infty$ e ainda que todo ponto formado por entradas com números inteiros é construtível. Isto é, $(a, b) \in P_\infty$ $\forall$ $a \in \mathbb{Z}$ e $b \in \mathbb{Z}$.

Definição 2.6. Os pontos do plano que pertencem a $\mathcal{P}_\infty$ são chamados de pontos construtíveis e as retas em $\mathcal{P}_\infty$, isto é, as retas que contém dois pontos distintos construtíveis são chamadas de retas construtíveis.

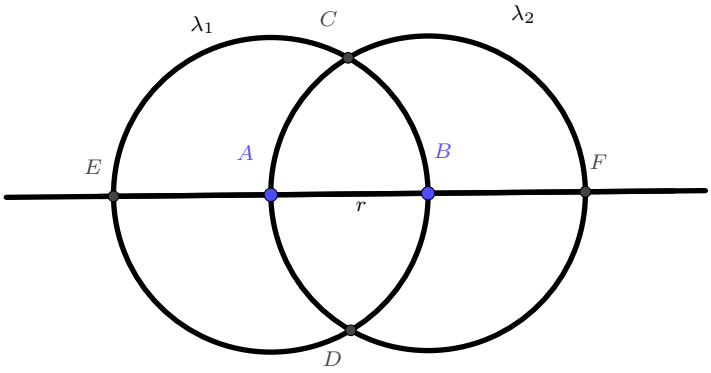
Definição 2.7. Um número real a é construtível se o ponto $(a, 0) \in \mathcal{P}_\infty$.

A seguir são apresentadas algumas proposições e alguns teoremas sobre a construtibilidade sem o uso das condições algébricas. A construção será feita apenas com a régua não graduada e o compasso.

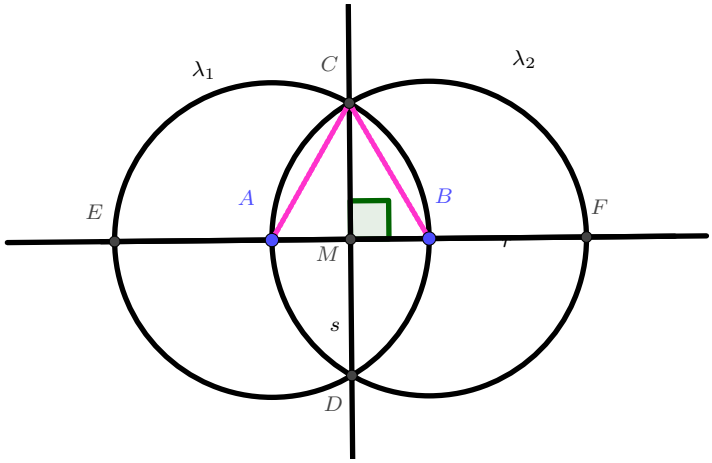
Proposição 2.8. Sejam A e B dois pontos distintos construtíveis, então o ponto médio M do segmento $\overline{AB}$ é construtível e as retas perpendiculares a $\overline{AB}$ passando pelos pontos A, B e M tambeém são construtíveis.

Demonstração. Observe os passos seguidos para efetuar a construção.

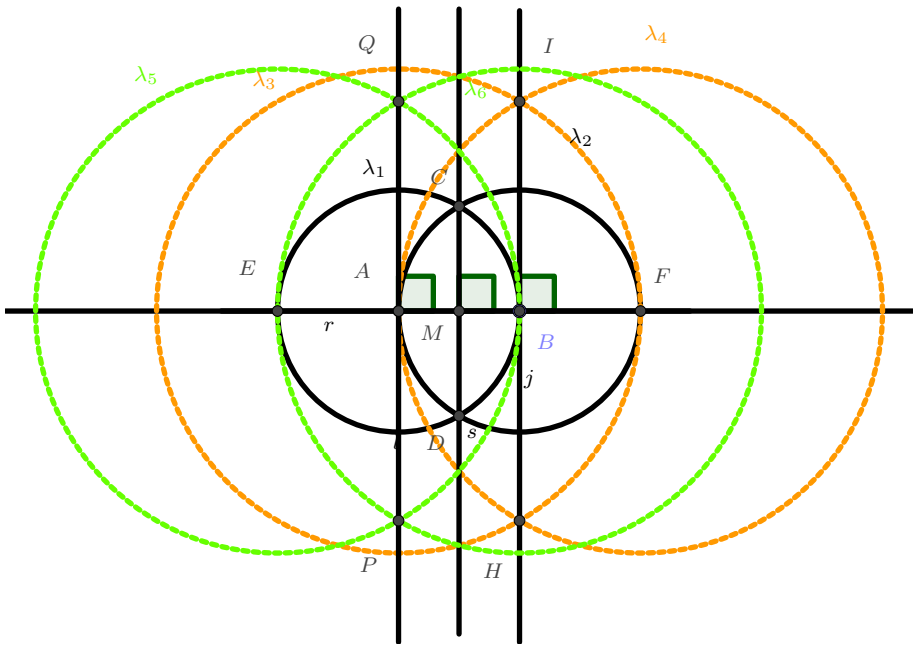
1 Por A e B construa a reta r que passa nesses dois pontos distintos.
2 Com o compasso, coloque a ponta seca no ponto A e construa a circunferência passando por B
3 Com o compasso, coloque a ponta seca no ponto B e construa a circunferência passando por A



Observe que usando as operações elementares de construção, pela intersecção das duas circunferências os pontos C e D são construídos, e pela intersecção das circunferências com a reta r os pontos E e F são construídos. Como C e D são pontos construtíveis, construa a reta s passando por eles e intersectando a reta r no ponto M, que também será um ponto construtível por ser a intersecção de duas retas construtíveis.



Como $ABCD$ é um losango cujas diagonais são $\overline{CD}$ e $\overline{AB}$ temos que elas são perpendiculares e pelo caso de congruência de triângulos LAL ($\overline{AB} \equiv \overline{CD}$; $A\hat{C}M \equiv B\hat{C}M$; $\overline{CM}$ um lado comum) tem-se que $\overline{AM} \equiv \overline{BM} \Rightarrow M$ é o ponto médio e por ser a intersecção de duas retas construtíveis também é construtível. Agora, como A é o ponto médio de $\overline{EB}$ e B é o ponto médio de $\overline{AF}$, seguindo os mesmos passos acima, construímos retas perpendiculares à r e passam pelos pontos A ou B.

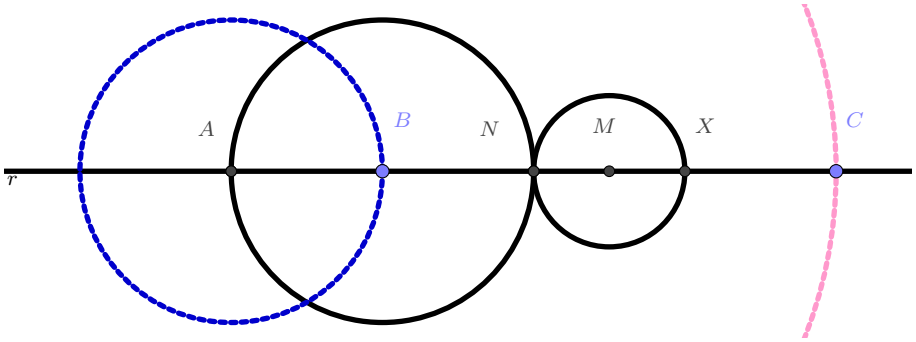


□

Proposição 2.9. Sejam A e r, respectivamente um ponto construtível e uma reta construtível tais que $A \in r$. Se B e C são construtíveis, então existe um ponto construtível X tal que $X \in r$ e os segmentos $\overline{AX}$ e BC possuem a mesma medida.

Demonstração. Usando circunferências centradas em B e centradas em A pode-se assumir que A, B e C pertencem à reta r. Pois, caso não pertençam basta construí-

los na reta r usando o compasso com a ponta seca em A e a outra no ponto ponto desejado.



Agora, entre os pontos B e C construa o ponto médio M, e com o compasso centrado no ponto B e raio $|\overline{AB}|$ trace uma circunferência cuja a intersecção com a reta r constrói o ponto N tal que $|\overline{AB}| = |\overline{BN}|$. Assim, tem-se que os pontos $A,\ B, C,\ M,\ N \in r$ são todos pontos construtíveis.

Seja $X \in r$ o ponto construtível tal que $|\overline{NM}| = |\overline{MX}|$. Como M é o ponto médio de $\overline{BC}$, tem-se que

$$\begin{aligned} |\overline{BM}| &= |\overline{MC}| \\ \Rightarrow |\overline{BN}| + |\overline{NM}| &= |\overline{MX}| + |\overline{XC}| \\ \Rightarrow |\overline{BN}| &= |\overline{XC}|. \end{aligned}$$

Logo, $|\overline{AB}| = |\overline{BN}| = |\overline{XC}|$.
Agora, observe que

$$|\overline{AX}| = |\overline{AB}| + |\overline{BX}|,$$

e como mostrado acima tem-se $|\overline{AB}| = |\overline{XC}|$, daí

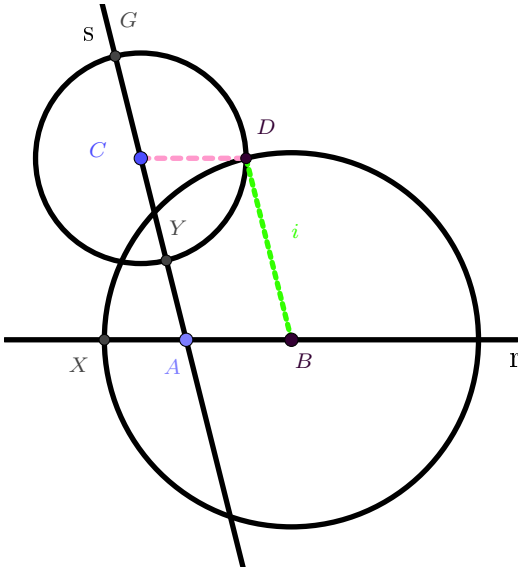
$$\begin{aligned} |\overline{AX}| &= |\overline{AB}| + |\overline{BX}| \\ &= |\overline{BX}| + |\overline{XC}| \\ &= |\overline{BC}| \end{aligned}$$

como se queria demonstrar. □

Proposição 2.10. Sejam $A,\ B$ e C três pontos construtíveis não alinhados. Então existe um ponto construtível D tal que $A,\ B,\ C$, e D formam um paralelogramo. Em particular, a reta passando por C e paralela ao segmento $\overline{AB}$ é construtível.

Demonstração. Sejam A, B e C três pontos construtíveis quaisquer, então construa as retas suportes r que contém A e B e a reta s que contém A e C. Pela proposição 3.7 existe $X \in r$ tal que $|\overline{AC}| = |\overline{BX}|$ e ainda existe $Y \in s$ tal que $|\overline{CY}| = |\overline{AB}|$.

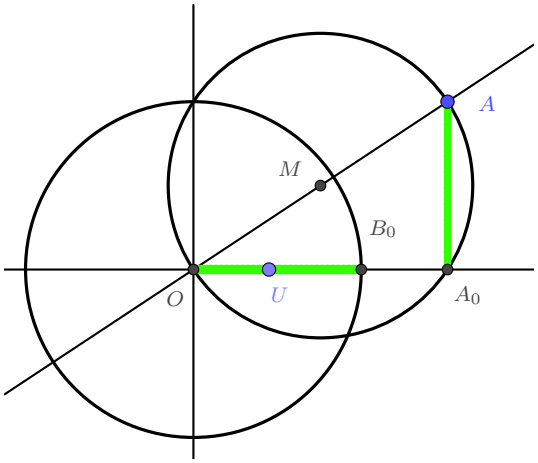
Agora, construindo a circunferência com centro no ponto B e passando por X e a circunferência com centro no ponto C e passando pelo ponto Y, temos que um dos pontos de intersecção entre as duas circunferências será o ponto D, que é construtível por ser a intersecção de duas circunferências construtíveis.



Por fim, como os pontos C e D são construtíveis, a reta que passa por eles também é construtível, e ainda como $\overline{CD}||\overline{AB}$ são congruentes, temos que A, B, C e D formam um paralelogramo. □

Proposição 2.11. Um ponto $A = (a, b) \in \mathbb{R}^2$ é construtível se, e somente se, as suas coordenadas $a, b \in \mathbb{R}$ são números construtíveis.

Demonstração. ($\Rightarrow$) Se $A = (a, b)$ é construtível, considere M o ponto médio de $\overline{OA}$ que também é construtível como visto anteriormente. Com a ponta seca do compasso centrada no ponto M e a outra ponta em A, trace uma circunferência que interceptará a reta suporte de $\overline{OU}$ no ponto $A_0 = (a, 0)$, que é um ponto construtível por se tratar da intersecção de uma reta e uma circunferências construtíveis, logo o número a é construtível. Em seguida, como o ponto $A = (a, 0)$ é construtível e pertencente à reta suporte de $\overline{OU}$, pela proposição 3.7 existe um ponto B_0 pertencente a reta suporte de $\overline{OU}$ tal que $|\overline{OB_0}| = |\overline{AA_0}|$ onde $B_0 = (b, 0)$ é um ponto construtível e então o número b é construtível, como queríamos mostrar. Observe a figura a seguir.



($\Leftarrow$) Reciprocamente, suponha a e b dois números reais construtíveis, isto é, $a, b \in P_\infty$. Observe que a reta determinada por O e U é construtível. Trace uma reta perpendicular a reta suporte de $\overline{OU}$ passando pelo ponto O, que como visto anteriormente é também construtível. Com a ponta seca do compasso centrada em O e a outra no ponta em $B_0 = (b, 0)$, construa a circunferência de centro O e raio $|\overline{OB_0}|$ que intercepta a reta perpendicular no ponto $(0, b)$, que é construtível por ser a intersecção de uma reta e uma circunferência construtíveis. Assim, tem-se três pontos construtíveis não colineares, deste modo o ponto $A = (a, b)$ também é construtível por se tratar do quarto vértice de um paralelogramo cujos os outros três vértices são construtíveis. □

Observe que como visto na proposição imediatamente acima pode-se perceber que os números construtíveis são exatamente as coordenadas dos pontos construtíveis.

Teorema 2.12. Seja o conjunto $\mathcal{C}_\mathbb{R} = \{\alpha \in \mathbb{R} \mid \alpha \text{ é construtível}\}$, então $\mathcal{C}_\mathbb{R}$ é um subcorpo de $\mathbb{R}$ contendo $\mathbb{Q}$.

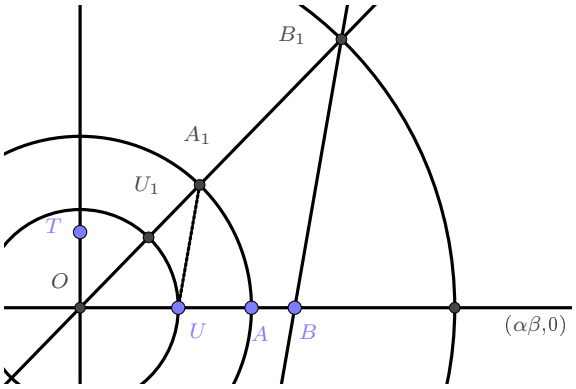
Demonstração. Como já foi possível observar o conjunto dos números inteiros é todo construtível partindo de $\overline{OU}$ com circunferência de raio 1, isto é, $\mathbb{Z} \subset \mathcal{C}_\mathbb{R}$. Para mostrar que $\mathcal{C}_\mathbb{R}$ é um subcorpo de $\mathbb{R}$ contendo $\mathbb{Q}$, basta que as afirmações a seguir sejam válidas.

(1) Dados $\alpha,\ \beta \in \mathcal{C}_\mathbb{R}$ então $\beta - \alpha \in \mathcal{C}_\mathbb{R}$.
(2) Dados $\alpha,\ \beta \in \mathcal{C}_\mathbb{R}$ então $\alpha \cdot \beta \in \mathcal{C}_\mathbb{R}$.
(3) Dados $0 \neq \alpha \in \mathcal{C}_\mathbb{R}$ então $\dfrac{1}{\alpha} \in \mathcal{C}_\mathbb{R}$.

Assim, sem perda de generalidade, considere $\beta > \alpha > 0$. Seja ainda, $A = (\alpha, 0)$ e $B = (\beta, 0)$ dois pontos construtíveis pertencentes a reta suporte de $\overline{OU}$, pela Proposição 3.7 existe um ponto construtível $X = (x, 0)$ à direita de O sobre

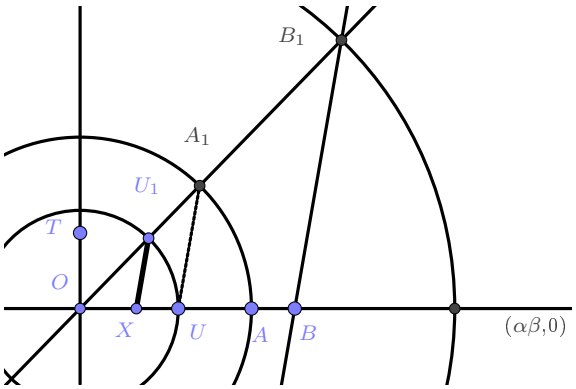
a reta suporte de $\overline{OU}$ tal que $\overline{OU}$ e $\overline{AB}$ possuam o mesmo comprimento. Daí, $(x-0, 0-0) = (\beta-\alpha, 0-0) = (\beta-\alpha, 0) \Rightarrow (x, 0) = (\beta-\alpha, 0) \Rightarrow x = \beta-\alpha$ é um número construtível, logo $\beta-\alpha \in \mathcal{C}_{\mathbb{R}}$ que é o que se queria mostra no item (1).
Para mostrar os itens (2) e (3), observe primeiro que existem retas construtíveis que contém o ponto O diferentes das retas suportes de $\overline{OU}$ e $\overline{OT}$ onde $T = (0, 1)$.
Seja r uma reta construtível que passa por O diferente das retas suportes de $\overline{OU}$ e $\overline{OT}$. Considere ainda $A = (\alpha, 0)$ e $B = (\beta, 0)$ pontos construtíveis sobre a reta suporte de $\overline{OU}$ de modo que $|\overline{OU_1}| = |\overline{OA}| = \alpha$, e como os triângulos OA_1U e OB_1B são semelhantes pelo caso ângulo-ângulo, já que as retas suportes de $\overline{UA_1}$ e $\overline{BB_1}$ são paralelas. Logo,

$$\frac{1}{|UA_1|} = \frac{\beta}{\overline{OB_1}} \Rightarrow \frac{1}{\alpha} = \frac{\beta}{|\overline{OB_1}|} \Rightarrow |\overline{OB_1}| = \alpha \cdot \beta.$$



Aí com a ponta seca do compasso centrada em O e a outra ponta em B_1 trace a circunferência até intercptar a reta suporte de $\overline{OU}$, construindo o ponto $(\alpha \cdot \beta, 0)$, que é construtível por ser resultado da intersecção de uma circunferência e uma reta construtível. Logo, $\alpha \cdot \beta$ é um número construtível.

Na figura acima, como $|\overline{OU}|$ é raio da circunferência de comprimento 1 e U_1 pertence a reta r, construa $X \in \overline{OU}$ tal que $\overline{XU_1}$ seja paralela a $\overline{UA_1}$. Observe,



segue da semelhança dos triângulos OAU_1 e OUA_1 que $\frac{|\overline{OU_1}|}{|\overline{OX}|} = \frac{|\overline{OA_1}|}{|\overline{OU}|}$ e como $|\overline{OU_1}| = |\overline{OU}| = 1$ e $|\overline{OA_1}| = \alpha$ tem-se $\frac{1}{|\overline{OX}|} = \frac{\alpha}{1}$, logo $|\overline{OX}| = \frac{1}{\alpha}$. Isto é, o número $\frac{1}{\alpha}$ é construtível. □

Para continuar com o desenvolvimento da teoria de construção e a apresentação do próximo teorema, observe as definições e construções que serão usadas.

Definição 2.13. Se $A = (u, v) \in \mathcal{P}_n$ diz-se que u e v são as coordenadas de $\mathcal{P}_n$, e denota-se por $\mathcal{A}_n$ o conjunto de todas as coordenadas de $\mathcal{P}_n$.

Exemplo 2.14. Observe que $\mathcal{P}_1 = \langle \mathcal{P}_0 \rangle$, onde

$$\mathcal{P}_1 = \left\{ (-1,0), (0,0), (1,0), (2,0), \left(\frac{1}{2}, \frac{\sqrt{3}}{2}\right), \left(\frac{1}{2}, -\frac{\sqrt{3}}{2}\right) \right\},$$

então as coordenadas de $\mathcal{P}_1$ é o conjunto $\mathcal{A}_1 = \left\{-1, -\frac{\sqrt{3}}{2}, 0, \frac{1}{2}, \frac{\sqrt{3}}{2}, 2\right\}$.

Observe que $\mathcal{A}_n \subset \mathcal{C}_\mathbb{R}$ $\forall n \in \mathbb{N}$, pois pela Proposição 3.9 todo ponto construtível do plano tem que suas entradas são números reais também construtíveis.

Agora, seja $K_0 = \mathbb{Q}, K_1 = \mathbb{Q}[\mathcal{A}_1], ..., K_n = \mathbb{Q}[\mathcal{A}_n], ...$ e como $\mathcal{A}_0 \subset \mathcal{A}_1 \subset ... \subset \mathcal{A}_n, ..., \mathcal{C}_\mathbb{R}$, temos:

$$\mathbb{Q} = K_0 \subset K_1 \subset K_2 \subset ... \subset K_n \subset K_{n+1} \subset ... \subset \mathcal{C}_\mathbb{R}.$$

Vale destacar ainda que se $\alpha \in \mathcal{C}_\mathbb{R}$ então $(\alpha, 0) \in \mathcal{P}_n$ para algum $n \in \mathbb{N}$, ou seja, $\alpha \in \mathcal{A}_n$ para algum $n \in \mathbb{N}$, e então $\alpha \in K_n$. Segue que, pode-se escrever o conjunto dos números construtíveis de um maneira cuja interpretação é conveniente para provar o próximo teorema, que é crucial para determinar se um número é ou não construtível. Veja como segue,

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

Teorema 2.15. $\mathcal{C}_\mathbb{R}$ é uma extensão algébrica dos racionais tal que para todo $\alpha \in \mathcal{C}_\mathbb{R}$ tem-se que o grau $[\mathbb{Q}[\alpha] : \mathbb{Q}]$ é uma potência de 2.

Demonstração. Basta que se prove $[\mathbb{Q}[\alpha] : \mathbb{Q}] = 2^r$ para algum r natural.

Com efeito, se $\alpha \in \mathcal{C}_\mathbb{R} = \bigcup_{n=0}^{\infty} K_n$, vai existir $n \in \mathbb{N}$ tal que $\alpha \in K_n = \mathbb{Q}[\mathcal{A}_n]$. Veja ainda que como $K_n \supset \mathbb{Q}[\alpha] \supset \mathbb{Q}$ pela Proposição 1.64 tem-se que

$$[K_n : \mathbb{Q}] = [K_n : \mathbb{Q}[\alpha]] \cdot [\mathbb{Q}[\alpha] : \mathbb{Q}],$$

assim, pode-se dizer que $[\mathbb{Q}[\alpha] : \mathbb{Q}]$ divide $[K_n : \mathbb{Q}]$, logo é suficiente mostrar que $[K_n : \mathbb{Q}] = 2^s$ para algum s natural, pois tanto $[K_n : \mathbb{Q}[\alpha]]$ quanto $[\mathbb{Q}[\alpha] : \mathbb{Q}]$ seriam potências de dois para que o resultado também fosse potência de 2. Suponha por indução que $[K_i : \mathbb{Q}]$ é uma potência de 2 para todo i tal que $0 \leq i < n$, e mostre que $[K_n : \mathbb{Q}]$ é uma potência de 2.

Como $K_{n-1} \subset K_n$ e pela proposição 1.64 tem-se que

$$[K_n : \mathbb{Q}] = [K_n : K_{n-1}] \cdot [K_{n-1} : \mathbb{Q}],$$

e então basta mostrar que $[K_n : K_{n-1}]$ é uma potência de 2 já que por hipótese foi assumida que $[K_i : \mathbb{Q}]$ é potência de 2 para todo $1 \leq i \leq n-1$.

Seja $L = K_n$ e $L_0 = K_{n-1}$. Sabe-se que $L = L_0[\mathcal{A}_n]$. Se $\mathcal{A}_n = \{\alpha_1, \alpha_2, ..., \alpha_k\}$ tem-se que $L = L_0[\alpha_1, \alpha_2, ..., \alpha_k]$. Usando a notação

$$L_0 \subset L_1 = L_0[\alpha_1] \subset L_2 = L_1[\alpha_2] \subset ... \subset L_i = L_{i-1}[\alpha_i] \subset ... \subset L_k = L$$

é suficiente mostrar que $[L_i : L_{i-1}] = 1$ ou 2, com $1 \leq i \leq k$, $L_i = L_{i-1}[\alpha_i]$ e $\alpha_i \in \mathcal{A}_n$. Assim existe $\beta_i \in \mathcal{A}_n$ tal que $A_i = (\alpha_i, \beta_i)$ ou $B_i = (\beta_i, \alpha_i) \in \mathcal{P}_n$. Sem perda de generalidade, suponha que $A_i = (\alpha_i, \beta_i) \in \mathcal{P}_n$. Como $\mathcal{P}_n = \langle \mathcal{P}_{n-1} \rangle$ é o conjunto dos pontos construtíveis gerados por $\mathcal{P}_{n-1}$ tem-se que $A_i = (\alpha_i, \beta_i)$ é obtido por uma das três operações elementares de construção definidas no início do capítulo. Assim o polinômio possui seus coeficientes em $\mathcal{A}_{n-1}$ e sua raiz está em $\mathcal{A}_{n-1}$ ou em $\mathcal{A}_n$, o que implica que ele terá grau um ou grau dois. Portanto, tem-se que α_i satisfaz uma equação de grau menor ou igual a 2 com coeficientes sobre o corpo $K_{n-1} = \mathbb{Q}[\mathcal{A}_{n-1}]$.

Logo, como $K_{n-1} = L_0 \subset L_{i-1}$ $1 \leq i \leq k$ segue que α_i é raiz de um polinômio de grau 1 ou 2 sobre o corpo L_{i-1} e isto diz que $[L_i : L_{i-1}] = 1$ ou 2 como se queria demonstrar. □

Proposição 2.16. Se n é um número ímpar maior ou igual à 3 e p um número primo maior ou igual à 2 então $\sqrt[n]{p}$ não é construtível.

Demonstração. Se $\alpha = \sqrt[n]{p}$ com n ímpar maior igual à 3 com p um número primo maior ou igual a 2, então o polinômio que tem α como raiz e é irredutível sobre $\mathbb{Q}$ é representado por $p(x) = irr(\alpha, \mathbb{Q}) = x^n - p$ e portanto $[\mathbb{Q}[\alpha] : \mathbb{Q}] = n$ que é ímpar, como não é uma potência de 2 pelo teorema anterior não é construtível. □

Para a resolução do próximo exemplo, é necessário lembrar de algumas identidades trigonométricas. Lembre-se que sendo θ um ângulo qualquer, lembre da relação fundamental $\sin^2\theta + \cos^2\theta = 1$ e da soma de arcos $\sin(\theta_1 \pm \theta_2) = \sin\theta_1 \cdot \cos\theta_2 \pm \sin\theta_2 \cdot \cos\theta_1$ e $\cos(\theta_1 \pm \theta_2) = \cos\theta_1 \cdot \cos\theta_2 \mp \sin\theta_1 \cdot \sin\theta_2$.

Observação 2. Observe que $\cos 3\theta = 4\cos^3\theta - 3\cos\theta$

$$\begin{aligned}\cos 3\theta = \cos(2\theta+\theta) &= \cos 2\theta\cdot\cos\theta - \sin 2\theta\cdot\sin\theta\\ &= (\cos^2\theta - \sin^2\theta)\cdot\cos\theta - 2\cdot\sin\theta\cdot\cos\theta\cdot\sin\theta\\ &= \cos^3\theta - \sin^2\cdot\cos\theta - 2\sin^2\theta\cdot\cos\theta\\ &= \cos^3\theta - \cos\theta + \cos^3\theta - 2\cos\theta + 2\cos^3\theta\\ &= 4\cos^3\theta - 3\cos\theta.\end{aligned}$$

Como se queria demonstrar.

Exemplo 2.17. O número $u = \cos\dfrac{2\pi}{18}$ não é construtível.

Com efeito, veja que $\cos 3u = \cos\dfrac{6\pi}{18} = \cos\dfrac{\pi}{3} = \dfrac{1}{2}$, daí usando a observação acima

$$\begin{aligned}\cos 3u &= 4\cos^3 u - 3\cos u\\ \frac{1}{2} &= 4\cos^3 u - 3\cos u\\ &\Rightarrow\ 8\cos^3 u - 6\cos u - 1 = 0.\end{aligned}$$

Isto é, $u = \cos\dfrac{2\pi}{18}$ é raiz do polinômio $p(x) = 8x^3 - 6x - 1$. O polinômio é irredutível sobre o conjunto dos números racionais, pois ao procurar raízes racionais usando o teorema das raízes racionais com os divisores do coeficientes do monômio de maior grau e os divisores do termo independente, nenhuma das combinações é raiz racional. Então $[\mathbb{Q}[u] : \mathbb{Q}] = 3$ e como não é potência de 2, o número não é construtível.

O exemplo acima, é um dos problemas clássicos das construções geométricas, o famoso problema da trissecção de um ângulo. Que foi mostrado não ser possível com o uso apenas da régua e do compasso.

A seguir são enunciados outros dois exemplos a fim de concluir a ilustração dos três problemas clássicos de construções geométricas.

Exemplo 2.18 (Duplicação do volume do cubo)**.** Considere um primeiro cubo cujas suas arestas são todas iguais a α e um segundo cubo cujas suas arestas são todas iguais à 1. Assim, não é possível construir um cubo cujo volume do primeiro seja igual ao dobro do volume do segundo. A saber, $\alpha^3 = 2\cdot 1$. Observe que $x^3 - 2 = irr(\alpha, \mathbb{Q})$ e daí $[\mathbb{Q}[\alpha], \mathbb{Q}] = 3$, que não é uma potência de 2 e pelo teorema 2.15 como não é uma potência de 2, tem-se que α não é um número construtível como se queria demonstrar.

Exemplo 2.19 (Quadratura do círculo)**.** Seja um quadrado de lado α e um círculo de raio 1. Não é possível construir um quadrado tal que a sua área seja igual a

área do círculo. Com efeito, veja que que se $\alpha^2 = \pi$ tem-se que $\pi \notin \mathbb{Q}$, e daí ele transcedente sobre $\mathbb{Q}$ e então $\pi \notin \mathcal{C}_{\mathbb{R}}$. Então $\alpha \notin \mathcal{C}_{\mathbb{R}}$ não é um número construtível.

CAPÍTULO 3

Aplicação ao novo ensino médio: Sugestão de trilha

A proposta deste capítulo é construir um material que pode ser aplicado a alunos do ensino médio em formato de trilhas de ensino ou também como uma variação na aplicação da teoria de polinômios. Ele também ser usado como uma espécie de apostila para aplicação de uma específica de aprofundamento em matemática ou minicurso para alunos de graduação ou do ensino médio. A seguir é apresentada uma breve introdução dos pontos principais da BNCC e posteriormente uma apresentação de um material com linguagem adequada ao ensino médio.

3.1 Breve discussão sobre a BNCC

Já faz um certo tempo que o mundo vem mudando sua velocidade de transformação dos métodos de informação, do modo de vida e seus pensamentos políticos e econômicos. Diante dessas mudanças diversos pesquisadores e gestores do âmbito público e privado que pensam na educação vem discutindo uma atualização do modo de ensinar da escola de maneira que a torne uma instituição mais atrativa e o conhecimento ali gerado seja mais significativo para o aluno.

A partir dessa perspectiva, e depois de um longo debate, o plano nacional de educação (PNE) aprovado no ano de 2014, apontou uma necessidade de uma renovação do ensino médio, de tal forma que o ensino oferecido fosse mais amplo, com uma maior interdisciplinaridade, maior flexibilidade de conteúdos e protagonismo do estudante na construção de seu conhecimento. Desse modo, em 2017 a Lei nº 13.415 estabelece uma mudança na estrutura do ensino médio onde ela define uma nova organização curricular. Nessa organização, a divisão é feita pela formação geral básica, que é baseada em um documento chamado base nacional comum curricular (BNCC) e uma formação flexível e de escolha do estudante. [FTD 2022]

A BNCC é a referência nacional para os estados e municípios confeccionarem seus currículos básicos e suas propostas pedagógicas. Pode-se dizer também que é a

fonte usada para definir os critérios necessários para o desenvolvimento da educação de maneira unificada como uma política pública. Com esse parâmetro curricular a intenção é que os alunos das esferas municipais, estaduais e federais tenham o mesmo currículo básico e independente da região tenham as mesmas habilidades e competências desenvolvidas no mesmo período. Levando em conta também os aspectos sociais e culturais aos quais está sujeito, e para atender essa demanda as trilhas de conhecimento foram criadas. A sua implementação teve início no ano de 2022 para as primeiras séries, no ano de 2023 para as primeiras e segundas séries e para o ano de 2024 já será para todo o ensino médio.

Portanto a BNCC propõe o que é básico e o que é diverso. E o entendimento é que as competências e as diretrizes comuns e os currículos variados. Essa ideia estabelece uma direção que deve guiar os currículos e define quais conteúdos devem ser aplicados para atingir as competências e elas devem ser garantidas a todos os estudantes brasileiros. Assim, o que é proposto é o que são aprendizagens essenciais e não conteúdos mínimos.

Ao adotar essa maneira de pensar a educação, a BNCC define as competências gerais que estruturam as três fases do ensino básico, que estão relacionadas e vão se desenvolvendo ao longo das etapas. O documento também define as competências específicas que estão ligadas a cada área de ensino e aponta quais habilidades e competências que são desenvolvidas através das áreas de conhecimento. Para o ensino médio, são quatro áreas. Linguagens e suas tecnologias, matemática e suas tecnologias, ciência da natureza e suas tecnologias e ciências humanas e suas tecnologias. O documento define também que português e matemática são as únicas áreas que devem ser desenvolvidas em todas as três séries do ensino médio.

A definição de competência usada no documento [BRASIL] é em suma a mobilização de conhecimentos (conceitos e procedimentos), habilidades (práticas, cognitivas e socioemocionais), atitudes e valores para preparar o aluno para o cotidiano, tornando-o um cidadão responsável e apto a iniciar o seu processo de inserção no mundo do trabalho. E nesse mesmo documento é possível observar todas as competências básicas que são propostas para serem desenvolvidas nas três etapas da educação básica.

Como o foco do material de aplicação desenvolvido aqui nesse trabalho é o ensino médio, uma das maiores mudanças que a BNCC fez na estrutura do ensino médio é a carga horária. Antes a escola era obrigada e oferecer 2400 horas totais (800 para cada série), essa carga foi ampliada para 3000 horas totais, distribuídas pelos três anos do ensino médio. Desse total de horas, 60% deve ser destinado a formação básica e os outros 40% devem ser necessariamente destinadas a um currículo flexível e fundamentado nos itinerários formativos, permitindo o aluno a trilhar um caminho

a sua escolha e exercer o seu protagonismo. Em outras palavras, a BNCC deixa claro a definição das competências gerais e dos conhecimentos essenciais que devem ser oferecidos aos estudantes na parte comum do currículo e deixa a cargo do aluno desde as séries iniciais do ensino médio escolher sua área de interesse pessoal e profissional.

A parte flexível do currículo desenvolve as trilhas de aprendizagem, que são matérias criadas de acordo com a necessidade da região e realidade que aluno está inserido. Assim, o as trilhas de conhecimentos são oferecidas no início do ano, e cada aluno pode escolher as suas, de acordo com sua afinidade e vontade. No Estado de Goiás por exemplo, são 13 trilhas. Contudo, a escolha dos itinerários é feita de acordo com a capacidade da escola de oferecê-la, levando em consideração o quantitativo de alunos necessários e a sua estrutura para atender a essa demanda. Então, se a escola tem condições de oferecer três trilhas, as três mais votadas são escolhidas. O Estado de Goiás permite que o estudante faça a trilha que ele deseja em outra unidade escolar diferente da que é matriculado. Mas nesse momento de implantação isso não é comum. Vale comentar aqui que com a falta de organização dos currículos variados, os conteúdos de matemática foram reduzidos drasticamente e isso ao longo do tempo vai enfraquecer o letramento de matemática dos alunos em geral. Claro que essa análise se dá pelo senso comum do que é visto atualmente em todas as esferas de ensino, a matemática não é a área de conhecimento mais popular e nem a mais escolhida.

Visando construir um material que tenha utilidade a essa proposta de ensino e seja um norte para a trilha de aprofundamento, e seja possível de ser usada para alunos da terceira série do ensino médio em uma trilha de aprendizagem, que também pode ser tratada como um itinerário formativo no aprofundamento dos conceitos de matemática. A proposta de aplicação no ensino médio também pode ser utilizada como um minicurso que associa a teoria de polinômios a de construção de números usando apenas régua e compasso, para alunos do ensino médio ou graduandos de licenciatura em matemática.

A área de matemática e suas tecnologias no ensino médio tem o objetivo de ampliar todo o conjunto de conhecimentos e habilidades acumulados no ensino fundamental de modo a ampliar os conhecimentos matemáticos e melhorar a tomada de decisão na resolução de um exercício e também desenvolver uma maior capacidade e criatividade de resolver problemas mais teóricos e que exigem um nível maior de abstração.

Assim, as aprendizagens previstas para o ensino médio são fundamentais para o aperfeiçoamento do letramento bem como a ampliação das habilidades propostas por meio dos conhecimentos adquiridos no ensino fundamental e proporcionar condições melhores para compreender a realidade e propor ideias inovadoras.

Partindo desse ideal, em conjunção com as competências gerais da educação básica propostas na BNCC e com as áreas de matemática do ensino fundamental, no ensino médio, a área de matemática e suas tecnologias deve garantir aos estudantes o desenvolvimento de competências específicas, as quais são apontadas a seguir e foram retiradas de [BRASIL].

1. Utilizar estratégias, conceitos e procedimentos matemáticos para interpretas situações em diversos contextos, sejam atividades cotidianas, sejam fatos das ciências da natureza e humanas, das questões socioeconômicas ou tecnológicas, divulgados por diferentes meios, de modo a contribuir para uma formação geral.
2. Propor ou participar de ações para investigar desafios do mundo contemporâneo e tomar decisões éticas e socialmente responsáveis, com base na análise de problemas sociais, como do trabalho, entre outros, mobilizando e articulando conceitos, procedimentos e linguagens próprios da matemática.
3. Utilizar estratégias, conceitos, definições e procedimentos matemáticos para interpretar, construir modelos e resolver problemas em diversos contextos, analisando a plausibilidade dos resultados e a adequação das soluções propostas, de modo a construir argumentação consistente.
4. Compreender e utilizar, com flexibilidade e precisão, diferentes registros de representação matemáticos (algébricos, geométricos, estatístico, computacional etc.), na busca de solução e comunicação de resultados de problemas.
5. Investigar e estabelecer conjecturas a respeito de diferentes conceitos e propriedades matemáticas, empregando estratégias e recursos, como observação de padrões, experimentações e diferentes tecnologias, identificando a necessidade, ou não, de uma demonstração cada vez mais formal na validação das referidas conjecturas.

Em cada competência listada acima, dentro da área de matemática e suas tecnologias os conteúdos desenvolvem habilidades que proporcionam o alcance das competências. Tais habilidades previstas para a área de matemática e suas tecnologias são reconhecidas por códigos. Por exemplo, o código **EM13MAT102** deve ser lido da seguinte maneira.

EM: O primeiro par de letras indica a etapa de Ensino Médio.
13: O primeiro par de números (13) indica que as habilidades descritas podem ser desenvolvidas em qualquer série do Ensino Médio, conforme definição dos currículos.
MAT: A segunda sequência de letras indica a área (três letras) ou o componente curricular (duas letras): LGG = Linguagens e suas Tecnologias, LP =

Língua Portuguesa, MAT = Matemática e suas Tecnologias, CNT = Ciências da Natureza e suas Tecnologias, CHS = Ciências Humanas e Sociais Aplicadas. **102**: Os números finais indicam a competência específica à qual se relaciona a habilidade (1º número) e a sua numeração no conjunto de habilidades relativas a cada competência (dois últimos números).

Todas as habilidades podem ser encontradas no documento online da BNCC.

Cada escola precisa oferecer, no mínimo duas trilhas de conhecimento que podem ser integradas com outras áreas de ensino ou de aprofundamento. Os alunos podem escolher a partir da 2ª série qual trilha cursar. Essas trilhas tem o objetivo de incentivar a criatividade, a investigação científica, o empreendedorismo e a intervenção sociocultural.

Pensando em um contexto para o Estado de Goiás a trilha a qual essa dissertação propõe uma contribuição é: *Imersão na matemática escolar: conhecimentos essenciais para o desenvolvimento da sociedade.* Que é um itinerário formativo que se enquadra como uma trilha de aprofundamento e tem como principal intenção aprofundar os conhecimentos acerca da matemática escolar desenvolvidos nas etapas do ensino fundamental e médio a fim de ampliar os conhecimentos científicos, procedimentos e atitude vida da apropriação desses. [GO]

No material desenvolvido na próxima seção as principais habilidades da BNCC desenvolvidas são:

- **(EM13MAT105)** Utilizar as noções de transformações isométricas (translação, reflexão, rotação e composições destas) e transformações homotéticas para construir figuras e analisar elementos da natureza e diferentes produções humanas (fractais, construções civis, obras de arte, entre outras).
- **(EM13MAT301)** Resolver e elaborar problemas do cotidiano, da Matemática e de outras áreas do conhecimento, que envolvem equações lineares simultâneas, usando técnicas algébricas e gráficas, com ou sem apoio de tecnologias digitais.
- **(EM13MAT401)** Converter representações algébricas de funções polinomiais de 1º grau em representações geométricas no plano cartesiano, distinguindo os casos nos quais o comportamento é proporcional, recorrendo ou não a softwares ou aplicativos de álgebra e geometria dinâmica.
- **(EM13MAT402)** Converter representações algébricas de funções polinomiais de 2º grau em representações geométricas no plano cartesiano, distinguindo os casos nos quais uma variável for diretamente proporcional ao quadrado da outra, recorrendo ou não a softwares ou aplicativos de álgebra e geometria dinâmica, entre outros materiais.

- **(EM13MAT510)** Investigar conjuntos de dados relativos ao comportamento de duas variáveis numéricas, usando ou não tecnologias da informação, e, quando apropriado, levar em conta a variação e utilizar uma reta para descrever a relação observada.

3.2 Sugestão de trilha para o novo Ensino médio

Antes da aplicação da BNCC na construção dos currículos, a teoria de polinômios era apresentada com um viés algébrico. Visando ampliar essa abordagem, o material deste capítulo propõe a construção de números reais usando apenas régua não graduada e compasso. É possível determinar a possibilidade de construção através das raízes dos polinômios. Inicialmente, é apresentada a teoria de construção, depois a de polinômios e por fim, uma ligação entre esses dois conteúdos. O material apresentado é dividido em 8 partes, e ao final de cada parte é proposto alguns exercícios para fixação da teoria. É importante observar também que esse é apenas um roteiro e outras fontes podem ser bastante úteis.

3.2.1 Parte 1 - Construção de números

Desde a Grécia antiga diversos problemas de construção usando régua e compasso são estudados, e em alguns problemas não conseguiram encontrar soluções e isso gerou diversos estudos ao longo da história. Inicialmente, são apresentadas algumas definições e teoremas sobre construção.

Definição 3.1. Diz-se que uma reta $r \in \mathbb{R}^2$ é construtível em $\mathcal{P}$ se r contém dois pontos distintos de $\mathcal{P}$.

Definição 3.2. Diz-se que uma circunferência $c \in \mathbb{R}^2$ é uma circunferência construtível em $\mathcal{P}$ se o seu centro pertence a $\mathcal{P}$ e um outro ponto de $\mathcal{P}$ pertence a c.

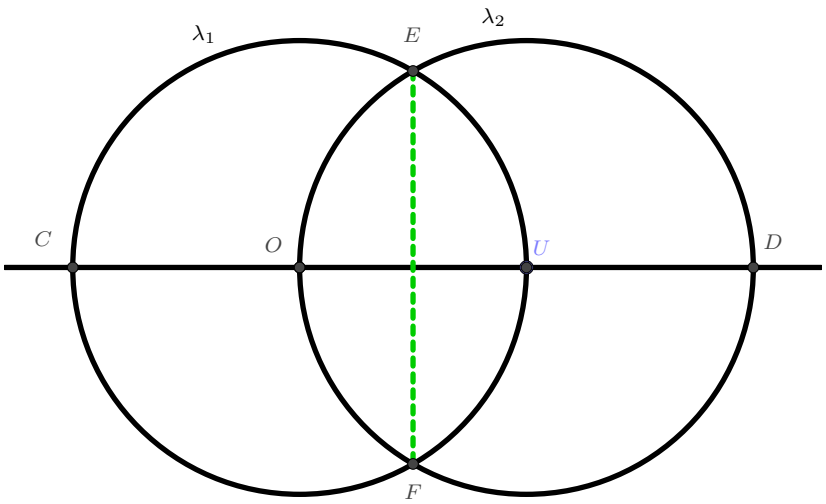
A seguir são definidos o que são chamados de *operações elementares* em $\mathcal{P}$.

(i) Intersecção de duas retas em $\mathcal{P}$;
(ii) Intersecção de uma reta em $\mathcal{P}$ e uma circunferência em $\mathcal{P}$;
(ii) Interseccção de duas circunferências em $\mathcal{P}$.

Definição 3.3. Diz-se que um ponto $A \in \mathbb{R}^2$ é construtível a partir de $\mathcal{P}$ se for possível determinar A por uma das operações elementares em $\mathcal{P}$. Denota-se $\langle \mathcal{P} \rangle$ o subconjunto dos pontos do plano que são construtíveis a partir de $\mathcal{P}$.

Exemplo 3.4. Seja o conjunto $\mathcal{P}_0$ formado pelos pontos $O = (0,0)$ e $U = (1,0)$. A seguir serão encontrados todos os pontos construtíveis a partir de P_0 seguindo os seguintes passos:

1. Por O e U trace a reta construtível r.
2. Com a ponta seca do compasso centrada em O, trace uma circunferência que passe também pelo ponto U.
3. Com a ponta seca do compasso centrada em U trace uma circunferência que passe também pelo ponto O.



Observe que a partir da intersecção da reta r e da circunferência λ_1 obtém-se o ponto $C = (-1,0)$, pois o raio da circunferência é uma unidade de comprimento. Da mesma maneira, o ponto $D = (2,0)$ que é a intersecção entre a reta r e a circunferência λ_2 foi construído. Agora, observe que os pontos O, U, E e F são os vértices de um losango de diagonais $\overline{OU}$ e $\overline{EF}$. As coordenadas dos pontos E e F podem ser encontras observando que o triângulo OEU é equilátero e como argumentado acima, $\overline{EF}$ é perpendicular a $\overline{OU}$, por serem as diagonais do losango. Daí, a abscissa é a metade do lado e a ordenada é a altura do triângulo equilátero, ou seja, $E = (\frac{1}{2}, \frac{\sqrt{3}}{2})$ e $F = (\frac{1}{2}, \frac{-\sqrt{3}}{2})$.

Concluí-se que $\mathcal{P}_1 = \langle \mathcal{P}_0 \rangle = \{O, U, C, D, E, F\}$.

Para generalizar, faça $P_0 = \{O, U\}$, $\mathcal{P}_1 = \langle \mathcal{P}_0 \rangle$, $\mathcal{P}_2 = \langle \mathcal{P}_1 \rangle$,..., $\mathcal{P}_{n+1} = \langle \mathcal{P}_n \rangle$, temos,

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

Definição 3.5. Definimos $\mathcal{P}_\infty = \bigcup_{n=0}^{\infty} \mathcal{P}_n$.

Observe que $\mathcal{P}_\infty$ é um conjunto infinito, mesmo que $\mathcal{P}_n$ seja um subconjunto finito de $\mathbb{R}^2 \; \forall \; n \in \mathbb{N}$ e que $\langle \mathcal{P}_\infty \rangle = \mathcal{P}_\infty$ e ainda que todo ponto formado por entradas com números inteiros é construtível. Isto é, $(a, b) \in P_\infty \; \forall \; a \in \mathbb{Z}$ e $b \in \mathbb{Z}$.

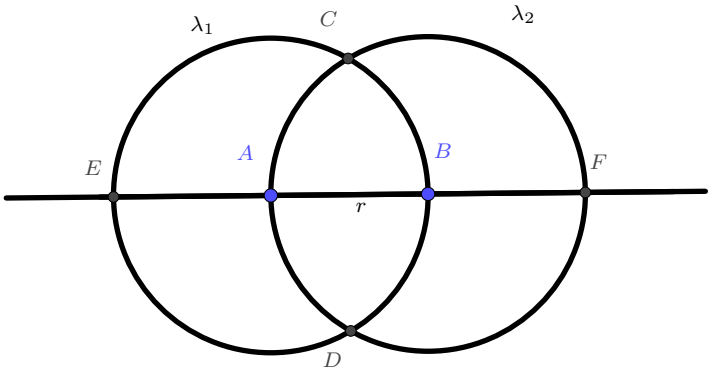
3.2.2 Parte 2 - Propriedades de construção

A seguir são apresentadas algumas proposições e alguns teoremas sobre a construtíbilidade sem o uso das condições algébricas, a construção será feita apenas com a régua e o compasso.

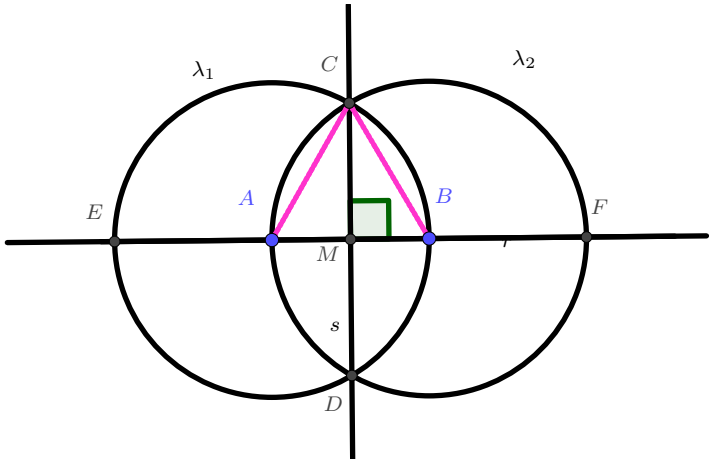
Proposição 3.6. Sejam A e B dois pontos distintos construtíveis, então o ponto médio M do segmento $\overline{AB}$ é construtível e as retas perpendiculares a $\overline{AB}$ passando pelos pontos A, B e M tambeém são construtíveis.

Demonstração. Siga os passos para efetuar a construção.

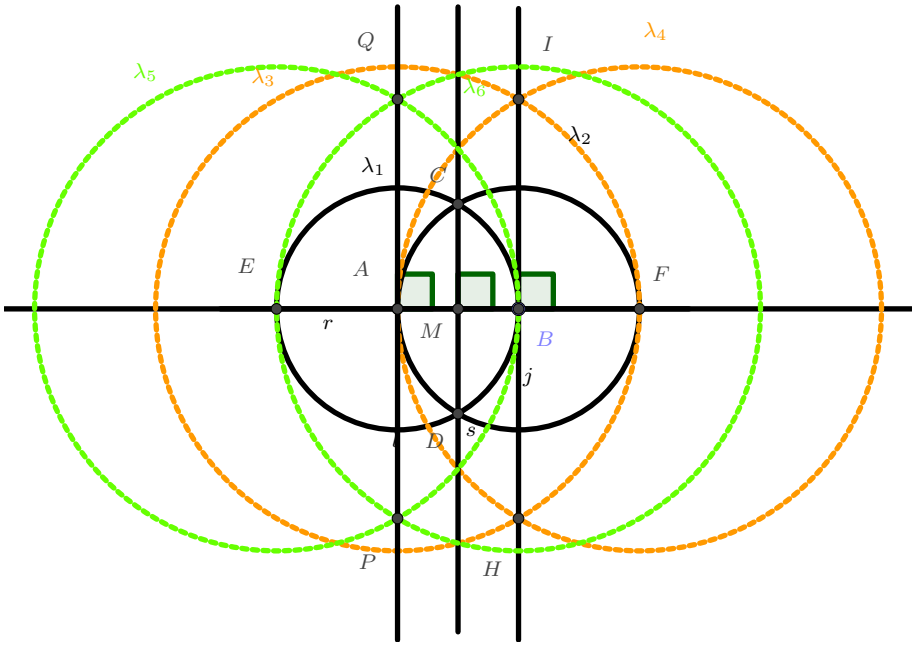
1 Por A e B construa a reta r que passa nesses dois pontos distintos.
2 Com o compasso, coloque a ponta seca no ponto A e construa a circunferência passando por B
3 Com o compasso, coloque a ponta seca no ponto B e construa a circunferência passando por A



Observe que usando as operações elementares de construção, pela intersecção das duas circunferências os pontos C e D são construtíveis, e pela intersecção das circunferências com a reta r os pontos E e F são construtíveis. Como C e D são pontos construtíveis, construa a reta s passando por eles e intersectando a reta r no ponto M, que também é um ponto construtível, pois é a intersecção de duas retas construtíveis.



Como $ABCD$ é um losango cujas diagonais são $\overline{CD}$ e $\overline{AB}$ tem-se que elas são perpendiculares e pelo caso de congruência de triângulos LAL ($\overline{AB} \equiv \overline{CD}$; $A\hat{C}M \equiv B\hat{C}M$; $\overline{CM}$ um lado comum) tem-se que $\overline{AM} \equiv \overline{BM}$, então M é o ponto médio, e por ser a intersecção de duas retas construtíveis também é construtível. Agora, como A é o ponto médio de $\overline{EB}$ e B é o ponto médio de $\overline{AF}$, seguindo os mesmos passos acima, são construídas as retas perpendiculares à r e que passa pelos pontos A e outra que passa pelo ponto B.

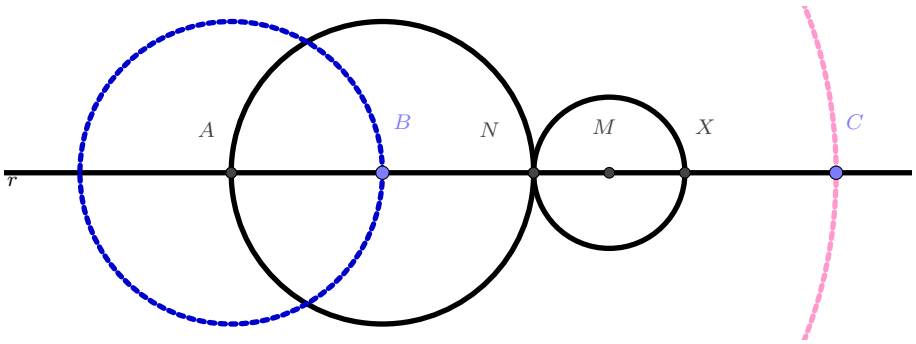


□

Proposição 3.7. Sejam A e r, respectivamente um ponto construtível e uma reta construtível tais que $A \in r$. Se B e C são construtíveis, então existe um ponto construtível X tal que $X \in r$ e os segmentos $\overline{AX}$ e BC possuem a mesma medida.

Demonstração. Usando circunferências centradas em B e centradas em A pode-se assumir que A, B e C pertencem à reta r. Pois, caso não pertençam basta construí-

los na reta r usando o compasso com a ponta seca em A e a outra no ponto ponto desejado.



Agora, entre os pontos B e C construa o ponto médio M, e com o compasso centrado no ponto B e raio $|\overline{AB}|$ trace uma circunferência cuja a intersecção com a reta r constrói o ponto N tal que $|\overline{AB}| = |\overline{BN}|$. Assim, tem-se que os pontos $A,\ B,\ C,\ M,\ N \in r$ são todos pontos construtíveis.

Seja $X \in r$ o ponto construtível tal que $|\overline{NM}| = |\overline{MX}|$. Como M é o ponto médio de $\overline{BC}$, tem-se que

$$\begin{aligned} |\overline{BM}| &= |\overline{MC}| \\ \Rightarrow |\overline{BN}| + |\overline{NM}| &= |\overline{MX}| + |\overline{XC}| \\ \Rightarrow |\overline{BN}| &= |\overline{XC}|. \end{aligned}$$

Logo, $|\overline{AB}| = |\overline{BN}| = |\overline{XC}|$.
Agora, observe que

$$|\overline{AX}| = |\overline{AB}| + |\overline{BX}|,$$

e como mostrado acima tem-se $|\overline{AB}| = |\overline{XC}|$, daí

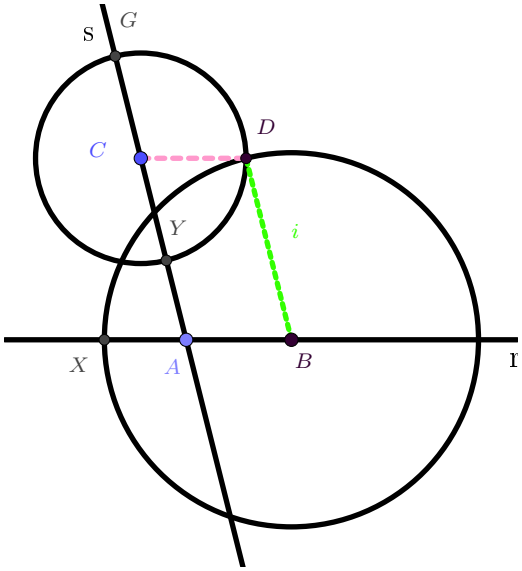
$$\begin{aligned} |\overline{AX}| &= |\overline{AB}| + |\overline{BX}| \\ &= |\overline{BX}| + |\overline{XC}| \\ &= |\overline{BC}| \end{aligned}$$

como se queria demonstrar. □

Proposição 3.8. Sejam $A,\ B$ e C três pontos construtíveis não alinhados. Então existe um ponto construtível D tal que $A,\ B,\ C$, e D formam um paralelogramo. Em particular, a reta passando por C e paralela ao segmento $\overline{AB}$ é construtível.

Demonstração. Sejam A, B e C três pontos construtíveis quaisquer, então construa as retas suportes r que contém A e B e a reta s que contém A e C. Pela proposição 3.7 existe $X \in r$ tal que $|\overline{AC}| = |\overline{BX}|$ e ainda existe $Y \in s$ tal que $|\overline{CY}| = |\overline{AB}|$.

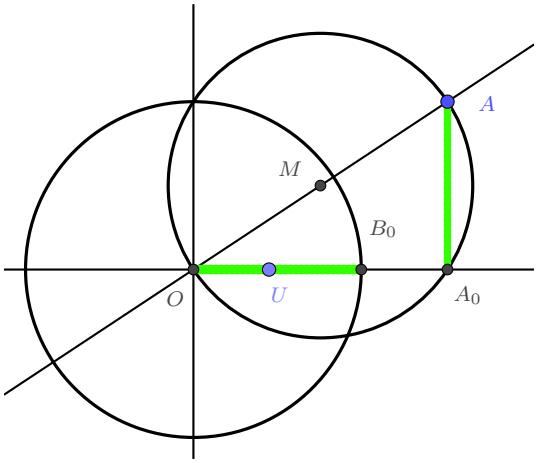
Agora, construindo a circunferência com centro no ponto B e passando por X e a circunferência com centro no ponto C e passando pelo ponto Y, temos que um dos pontos de intersecção entre as duas circunferências será o ponto D, que é construtível, por ser a intersecção de duas circunferências construtíveis.



Por fim, como os pontos C e D são construtíveis, a reta que passa por eles também é construtível, e ainda como $\overline{CD}||\overline{AB}$ são congruentes, temos que A, B, C e D formam um paralelogramo. □

Proposição 3.9. Um ponto $A = (a, b) \in \mathbb{R}^2$ é construtível se, e somente se, as suas coordenadas $a, b \in \mathbb{R}$ são números construtíveis.

Demonstração. ($\Rightarrow$) Se $A = (a, b)$ é construtível, considere M o ponto médio de $\overline{OA}$ que também é construtível como visto anteriormente. Com a ponta seca do compasso centrada no ponto M e a outra ponta em A, trace uma circunferência que interceptará a reta suporte de $\overline{OU}$ no ponto $A_0 = (a, 0)$, que é um ponto construtível por se tratar da intersecção de uma reta construtível e uma circunferência construtível, logo o número a é construtível. Em seguida, como o ponto $A = (a, 0)$ é construtível e pertencente à reta suporte de $\overline{OU}$, pela proposição 3.7 existe um ponto B_0 pertencente a reta suporte de $\overline{OU}$ tal que $|\overline{OB_0}| = |\overline{AA_0}|$ onde $B_0 = (b, 0)$ é um ponto construtível e então o número b é construtível, como se queria mostrar. Observe a figura abaixo.



($\Leftarrow$) Reciprocamente, suponha a e b dois números reais construtíveis, isto é, $a, b \in P_\infty$. Observe que a reta determinada por O e U é construtível. Trace uma reta perpendicular a reta suporte de $\overline{OU}$ passando pelo ponto O, que como visto anteriormente é também construtível. Com a ponta seca do compasso centrada em O e a outra no ponta em $B_0 = (b, 0)$, construa a circunferência de centro O e raio $|\overline{OB_0}|$ que intercepta a reta perpendicular no ponto $(0, b)$, que é construtível por ser a intersecção de uma reta e uma circunferência construtíveis. Assim, tem-se três pontos construtíveis não colineares, deste modo o ponto $A = (a, b)$ também é construtível por se tratar do quarto vértice de um paralelogramo cujos os outros três vértices são construtíveis. □

Observe que como visto na proposição acima pode-se perceber que os números construtíveis são encontrados através das entradas das coordenadas dos pontos construtíveis

3.2.3 Parte 3 - Introdução a polinômios

Na antiguidade existiam vários problemas práticos do cotidiano cuja sua solução se passava pela solução de equações polinomiais.

Antes de definir um polinômio, lembre-se que um monômio é uma expressão formada por uma parte literal (letra) e um coeficiente (número). Pode ser que o expoente da parte literal seja zero e isso implicará em ter só o coeficiente, e mesmo assim ele é considerado um monômio de grau zero.

Agora, de modo informal pode-se dizer que um polinômio em uma indeterminada x é uma adição de vários monômios. Observe a seguir uma definição formal.

Definição 3.10. Um polinômio na indeterminada x é uma expressão do tipo

$$p(x) = a_0 + a_1x + ... + a_{n-1}x^{n-1} + a_nx^n$$

onde $a_0, a_2, ..., a_n$ são números reais.

A partir da definição acima pode-se definir ainda o grau de um polinômio, que é o maior número natural que é expoente da indeterminada x caso seu coeficiente seja diferente de zero. Isto é, se $a_n \neq 0$, diz-se que n é o grau do polinômio e $a_0, a_1, ..., a_n$ são seus coeficientes.

Exemplo 3.11. Observe,

- $p(x) = 2x + 1$ é um polinômio de grau 1.
- $p(x) = 5x^2 - 7x = 1$ é um polinômio de grau 2.
- $p(x) = \dfrac{\sqrt{2}}{4}x^3$ é um monômio de grau 3.

Exemplo 3.12. Encontre o valor de k para que o polinômio $p(x) = (k^2 - 4) \cdot x^2 + (k + 2) \cdot x + 7$ tenha grau 1.

Para que $p(x)$ tenha grau 1, é necessário que os coeficientes de todos os monômio de grau maior ou igual à 2 sejam iguais à zero e o coeficiente do monômio de grau 1 seja diferente de zero. Daí

$$\begin{aligned} k^2 - 4 = 0 \quad & e \quad k + 2 \neq 0 \\ k = \pm 2 \quad & e \quad k \neq -2 \end{aligned}$$

logo, $k = 2$ é o valor procurado.

Definição 3.13 (Valor numérico). O valor numérico é encontrado quando a indeterminada do polinômio é substituída por um número qualquer. Isto é, após substituído o número na indeterminada do polinômio o resultado encontrado é o que se chama valor numérico.

Quando o objeto de estudo for funções polinomiais, esse valor numérico também pode ser chamado de imagem.

Exemplo 3.14. Considere o polinômio $p(x) = 3x^2 + 2x + 1$, encontre o valor numérico de 1 e i.

Primeiro substitua 1 na indeterminada x,

$$p(1) = 3 \cdot 1^2 + 2 \cdot 1 + 1 = 6.$$

Agora, substitua a indeterminada por i,

$$p(i) = 3 \cdot i^2 + 2 \cdot i + 1 = -2 + 2 \cdot i.$$

Definição 3.15 (**Igualdade de polinômio**). Dois ou mais polinômios são iguais se possuem os coeficientes das variáveis de mesmo grau iguais. Em outras palavras, se $p(x) = a_0 + a_1x + ... + a_nx^n$ e $q(x) = b_0 + b_1x + ... + b_nx^n$ são polinômios de grau n, então $p(x) = q(x)$ se $a_i = b_i$ pra todo $i = 1, ...n$.

Exemplo 3.16. calcule para quais números complexos a e b os polinômios $p_1(x) = (a^2 - 31) \cdot x^3 + 2x + 2$ e $p_2(x) = 5x^3 + (a - b) \cdot x + 2$ são iguais na indeterminada x.

Basta que os coeficientes das incógnitas de mesmo grau sejam iguais. Daí,

$$\begin{cases} a^2 - 31 = 5 \\ a - b = 2 \end{cases}$$

resolvendo a primeira equação tem-se

$$\begin{aligned} a^2 - 31 &= 5 \\ a^2 &= 36 \\ a &= \pm 6. \end{aligned}$$

Agora, isolando b na segunda equação tem-se

$$\begin{aligned} a - b &= 2 \\ -b &= 2 - a \\ b &= a - 2. \end{aligned}$$

Assim, para $a = -6$ tem-se que $b = -8$ e para $a = 6$ que $b = 4$.

Definição 3.17 (**Polinômios identicamente nulos**). Diz-se que um polinômio é identicamente nulo quando todos os coeficientes do polinômio são iguais à zero.

Exemplo 3.18. Determine m, n e q para que o polinômio $p(x) = (m + n - 2) \cdot x^2 + (n + p) \cdot x + (p - 2)$ seja identicamente nulo.

Basta igualar todos os coeficientes a zero,

$$\begin{cases} m + n - 2 = 0 \\ n + q = 0 \\ q - 2 = 0 \end{cases}$$

daí, $q = 2$ e substituindo na segunda equação encontra-se que $n = -2$. Agora, substituindo o valor de n na primeira equação tem-se que $m = 4$.

Lista de Exercícios Propostos

1. Determine o grau de cada polinômio abaixo.
   a) $p(x) = 2x^2 - 3x + 4$
   b) $q(x) = 5x \cdot (x^3 - 1) + 7$
   c) $t(x) = 2x - 3x^5$
2. Determine o valor de m para que o polinômio $p(x) = (m^2 - 1)x^2 + 3x - 1$ seja do $2^{\underline{o}}$ grau.
3. Dado o polinômio $p(x) = 5x^3 - 3x^2 + 2x + 4$, encontre os valores numéricos para $x = 2$ e $x = 4$.
4. Determine o valor de k para que os polinômios $p(x) = (k^2 - 3)x^3 + 2x - 1$ e $q(x) = x^3 + 2x - 1$ sejam iguais.
4. Determine o valor de k e m para que o polinômio $p(x) = (k^3 - 1) \cdot x^3 - (m+1)x$ seja identicamente nulo.

3.2.4 Parte 4 - Operações com polinômios

Na parte anterior foram abordadas as definições de polinômio, grau de um polinômio, igualdade de polinômios e polinômios identicamente nulos. Em continuidade com o estudo dos polinômios, aqui o objetivo é aprender as 4 operações básicas com polinômios. Além disso, será iniciada uma discussão sobre as raízes de um polinômio.

Adição de polinômios: Na adição de polinômios basta adicionar os termos semelhantes, isto é, adicionar os coeficientes das indeterminadas de mesmo grau.

Exemplo 3.19. Sejam os polinômios $p(x) = 3x^2 + 2x - 4$ e $q(x) = x^5 + 2$, então o polinômio $p(x) + q(x)$ é encontrado adicionando os seus coeficientes dos monômios de mesmo grau. Assim.

$$\begin{aligned} p(x) + q(x) &= (3x^2 + 2x - 4) + (x^5 + 2) \\ &= x^5 + 3x^2 + 2x - 2. \end{aligned}$$

Subtração de polinômios: Na subtração de polinômios basta subtrair os termos semelhantes, ou seja, subtrair os coeficientes das variáveis de mesmo grau.

Exemplo 3.20. Sejam $p(x) = 3x^2 + 2x - 4$ e $q(x) = 2x + 2$ dois polinômios, então o polinômio $p(x) - q(x)$ é dado por

$$\begin{aligned} p(x) - q(x) &= (3x^2 + 2x - 4) - (2x + 2) \\ &= 3x^2 + (2 - 2)x + (-4 - 2) \\ &= 3x^2 - 6. \end{aligned}$$

A seguir é definido o produto de polinômios, mas antes disso, observe como é feito o produto de dois monômios. Considere $n, m \in \mathbb{N}$, então o produto dos monômios $t_1(x) = a_n x^n$ e $t_2(x) = b_m x^m$ é dado por

$$t_1(x) \cdot t_2(x) = a_n b_m x^{n+m}.$$

Daí, para fazer o produto do polinômio de grau n, dado por $p(x) = a_0 + a_1 x + ... + a_n x_n$ pelo polinômio $q(x) = b_0 + b_1 x + ... + b_m x^m$ onde $n \leq m$. Siga os passos:

- Complete a escrita de $p(x)$ e $q(x)$ até o termo $n + m$ colocando $a_k = 0$ para $k > n$ e $b_k = 0$ para $k > m$.
- Define-se

  $$t(x) = p(x) \cdot q(x) = c_0 + c_1 x + ... + c_{n+m} x^{n+m}$$

  onde, $c_i = a_0 b_i + a_1 b_{i-1} + ... + a_{i-1} b_0 + a_i b_0$ para $0 \leq i \leq n + m$.

Multiplicação de polinômios: Em palavras, o que está escrito acima, na prática, é que basta multiplicar cada monômio do primeiro polinômio por todos os monômios do outro polinômio e depois agrupar os termos de mesmo grau.

Exemplo 3.21. Sejam os polinômios $p(x) = 3x^2 + 2x - 4$ e $q(x) = 2x + 2$ então o seu produto é dado por

$$\begin{aligned} p(x) \cdot q(x) &= (3x^2 + 2x - 4) \cdot (2x + 2) \\ &= 6x^3 + 4x^2 - 8x + 6x^2 + 4x - 8 \\ &= 6x^3 + 10x^2 - 4x - 8. \end{aligned}$$

Agora para a divisão de polinômios é preciso construir algumas ideias e enunciar um teorema, mas aqui será apresentado apenas o método das chaves. Esse método funciona bem parecido com o algoritmo da divisão para números inteiros.

diz-se que um polinômio $a(x)$ divide o polinômio $b(x)$ se existir $q(x)$ tal que $b(x) = q(x) \cdot a(x)$.

Exemplo 3.22. Observe o polinômio $a(x) = x^4 + x^3 + x^2 + x + 1$, ele divide o polinômio $x^5 - 1$, pois

$$(x - 1) \cdot (x^4 + x^3 + x^2 + x + 1) = x^5 - 1$$

Teorema 3.23. Sejam $a(x)$ e $b(x)$ dois polinômios com coeficientes reais e $b(x) \neq 0$. Então existem polinômios com os coeficientes $q(x)$ e $r(x)$, com $r(x) = 0$ ou grau de

$r(x)$ menor que o grau de $b(x)$ tais que

$$a(x) = b(x) \cdot q(x) + r(x).$$

Além disso, $q(x)$ e $r(x)$ são determinados de modo único.

A demonstração do teorema é omitida e pode ser encontrada em [Naves] O método da chave será explicado através de um exemplo.

Exemplo 3.24. Considere os polinômios $p(x) = 6x^3 - 2x^2 + x + 3$ e $t(x) = x^2 - x + 1$, ao efetuar a divisão de $p(x)$ por $t(x)$ usando o método das chaves. Coloca-se os polinômios em uma espécie de chave como a usada no algoritmo da divisão de números inteiros. Então o processo se inicia com alguns questionamentos,

- Qual monômio que multiplicado por x^2 o seu resultado é $6x^3$? a resposta é $6x$. Que é colocada abaixo do polinômio $t(x)$ nas chaves e esse $6x$ é multiplicado por todos os termos do polinômio $t(x)$. O resultado dessa multiplicação é subtraído de $p(x)$ obtendo como resultado o polinômio $4x^2 - 5x + 3$.
- No segundo passo, pense em um monômio que multiplicado por $t(x)$ o resultado obtido aparecerá $4x^2$. Esse monômio é $+4$, que é posicionado ao lado de $6x$ abaixo do polinômio $t(x)$ nas chaves, obtendo a soma $6x + 4$. Faz-se o mesmo processo de multiplicação de 4 por todos os termos de $t(x)$, e o resultado dessa multiplicação é subtraído de $4x^2 - 5x + 3$ obtendo $-x - 1$.
- Como o grau de $-x - 1$ é menor que o grau de $t(x)$ o processo se encerra aí. Concluindo que o quociente é $q(x) = 6x + 4$ e o resto é $r(x) = -x - 1$.

Observe todo esse processo que foi descrito logo acima algebricamente:

$$\begin{array}{rl|l} 6x^3 - 2x^2 & + x + 3 & x^2 - x + 1 \\ \cline{3-3} -6x^3 + 6x^2 - 6x & & 6x + 4 \\ \cline{1-2} 4x^2 - 5x + 3 & & \\ -4x^2 + 4x - 4 & & \\ \cline{1-2} -x - 1 & & \end{array}$$

Esse método de divisão é o mais comum, existem outros métodos que não comentados aqui. Porém nas próximas partes é apresentado o método de divisão de Briot-Ruffini, que trabalha com a divisão de por polinômios da forma $ax + b$.

Lista de Exercícios Propostos

1. Considere os polinômios $p_1(x) = x^3 - 2x + 4x - 1$ e $q(x) = 2x^2 + x - 1$. Determine:

a) $p(x) + q(x)$
b) $p(x) - q(x)$
c) $p(x) \cdot q(x)$
d) $\dfrac{p(x)}{q(x)}$

2. Sejam $p(x) = 2x^3 - 3x + k$ e $d(x) = x - 1$. Determine o valor de k para que o resto da divisão de $p(x)$ por $d(x)$ seja igual à zero.

3.2.5 Parte 5 - Equações polinomiais ou zeros

Inicia-se essa parte definindo o conceito de raiz ou zero de um polinômio e são desenvolvidos alguns exemplos para ilustras a definição.

Raízes ou zeros do polinômio: É o conjunto dos números complexos que faz o valor do polinômio ser igual à zero quando a indeterminada é substituída por esses números. Isto é, $k \in \mathbb{C}$ é raiz, então $p(k) = 0$.

Observe que quando $p(x) = 0$, se tem uma equação polinomial. Equações polinomiais foram objeto de estudos de grandes matemáticos, como cardano e Tartaglia em batalhas matemáticas do século XVII onde se tem registro do surgimento da solução por operações simples de adição, multiplicação, subtração, divisão potencias e raízes das equações de grau 3 [Krerley e Adán 2012]. Essa soloção é atribuída à Tartaglia, mais tarde na história vale destacar outros dois grandes matemáticos que são Abel e Galois, que na sua busca da resolução das equações de grau 5 encontraram que é impossível um método geral para sua resolução usando apenas as operações acima citadas.

Exemplo 3.25. Sabendo que -1 é raiz de $p(x) = 5x^3 + 2x^2 - mx + 1$. Calcule o valor de m.

Resolução (1). Como -1 é raiz de $p(x)$ então $p(-1) = 0$. Daí,

$$\begin{aligned} p(-1) &= 5 \cdot (-1)^3 + 2 \cdot (-1)^2 - m \cdot (-1) + 1 \\ &= -5 + 2 + m + 1 \\ &= m - 2, \end{aligned}$$

logo $m - 2 = 0$. Então o valor de m é 2.

Encontrar a solução de uma equação polinomial pode ser extremamente difícil e muitas vezes até impossível. Porém, para algumas equações existem alguns métodos que facilitam essa busca.

Antes de começar, analise a equação $x^2 + 1 = 0$. Se a procura se dá apenas para números reais então diz-se que essa equação não possui solução real. Agora se

a procura se dá por raízes complexas, então essa equação terá duas raízes que são $\pm i$. Observe abaixo o teorema de D´Alembert que inicia uma maneira de escrever um polinômio em sua forma fatorada.

Teorema 3.26. Seja uma constante qualquer a. Um polinômio $p(x)$ é divisível por $x-a$ se, e somente se, a é raiz de $p(x)$

Exemplo 3.27. Determine se o polinômio $p(x) = x^5 - 3x^3 + 3x^2 - 4x - 12$ é divisível por $x+2$. Basta aplicar o teorema acima enunciado, tem-se que:

$$p(-2) = (-2)^5 - 3\cdot(-2)^3 + 3\cdot(-2)^2 - 4\cdot(-2) - 12 = -32 + 24 + 12 + 8 - 12 = 0.$$

Logo $x+2$ divide $p(x)$.

Considere agora, um polinômio qualquer $p(x)$ de grau n com $r_1, r_2, ..., r_n$ suas raízes não necessariamente distintas onde

$$p(x) = a_0 + a_1x + a_2x^2 + ... + a_{n-1}x^{n-1} + a_nx^n$$

com $a_n \neq 0$ então ele pode ser escrito em sua **forma fatorada em fatores lineares** por

$$p(x) = a_n \cdot (x - r_1) \cdot (x - r_2) \cdot ... \cdot (x - r_n).$$

Exemplo 3.28. Para polinômios do 2º grau do tipo $p(x) = ax^2 + bx + c$, onde x_1 e x_2 são suas raízes e $a \neq 0$, observe que

$$\begin{aligned} p(x) &= a \cdot \left(x^2 - \left(\frac{-b}{a}\right) \cdot x + \frac{c}{a}\right) \\ &= a \cdot (x^2 - (x_1 + x_2) \cdot x + x_1 \cdot x_2) \\ &= a \cdot (x^2 - x_1 \cdot x - x_2 \cdot x + x_1 \cdot x_2) \\ &= a \cdot (x \cdot (x - x_1) - x_1 \cdot (x - x_2)) \\ &= a \cdot (x - x_1) \cdot (x - x_2) \end{aligned}$$

é uma forma fatorada do polinômio.

Exemplo 3.29. Agora um exemplo numérico de um polinômio de grau 2. Seja $p(x) = x^2 - 3x - 4$, daí observe que $a = 1$, $b = -3$ e $c = -4$. Usando o método de soma e produto para encontrar suas raízes, tem-se que a soma $S = \dfrac{-(-3)}{1} = 3$ e o produto $P = \dfrac{-4}{1} = -4$ tal que os números procurados são 4 e -1. Logo a forma fatorada desse polinômio é

$$p(x) = (x + 1) \cdot (x - 4).$$

Exemplo 3.30. Para encerrar, observe o polinômio $p(x) = x^2 + 1$. Esse polinômio não pode ser fatorado se suas raízes estiverem definidas apenas no conjunto dos números reais, pois $x^2+1 = 0$ não admite solução real. Agora, se ele admitir soluções no conjunto dos números complexos, tem-se que suas raízes são $+i$ e $-i$. Logo, sua forma fatorada é $p(x) = (x - i) \cdot (x + i)$.

Lista de Exercícios Propostos

1. Dado o polinômio $p(x) = x^3 - x^2 + x - 1$, dos números citados em cada item abaixo diga quais são raízes e quais não são. Justifique.
   a) $x = 1$
   b) $x = -1$
   c) $x = 4$
   d) $x = i$
   e) $x = -i$
2. No exercício anterior, considere o polinômio $p(x)$ e escreva-o na sua forma fatorada com raízes complexas.

3.2.6 Parte 7 - Fatoração de polinômios

Considere um polinômio $p(x)$ de grau n. Ao fazer $p(x) = 0$ o polinômio se transforma em uma equação de grau n. O problema é então encontrar as raízes dessa equação e para isso será apresentado um método que pode ajudar na procura de raízes reais.

A equação $a_n x^n + a_{n-1}x^{n-1} + ... + a_x + a_0 = 0$ onde $a_n \neq 0$ é chamada de equação de grau n e $a_0, a_1, ..., a_n$ são seus coeficientes. O objetivo é descrever maneiras de resolver esta equação. De modo direto, pode-se dizer que resolver essa equação é o mesmo que encontrar todas as n raízes de um polinômio de grau n.

O conjunto solução de uma equação de grau n é o conjunto formado por todas as raízes de uma equação algébrica. Caso não mencionado o conjunto universo que contém todas essas soluções, o conjunto considerado será o dos números complexos.

Exemplo 3.31. O conjunto solução da equação $x^2 + 3x - 4 = 0$, usando o processo de soma e produto, tem que a soma é -3 e o produto é -4. Pensando nas soluções se tem que $x' = -4$ e $x'' = 1$. Portanto, o conjunto solução é $\{-4, 1\}$.

Abaixo, seguem dois teoremas que garantem a existência de raízes para as equações sob determinadas condições.

Teorema 3.32. Toda equação polinomial de grau n, com $n \geq 1$, admite pelo menos uma raiz complexa.

Teorema 3.33. Todo polinômio de grau n, $n \geq 1$, pode ser fatorado em n fatores do primeiro grau.

Observe que os teoremas garantem a existência raízes complexas, e a partir dessas raízes existe uma maneira de escrever o polinômio em sua forma fatorada. Porém, se a procura for por raízes reais, vão existir polinômios que não possuem raízes no conjunto. Assim, eles não poderão ser fatorados. Os polinômios que não podem ser fatorados são chamados de **polinômios irredutíveis** para o conjunto dos números reais. De maneira análoga, se a procura for por raízes racionais e esse polinômio for irredutível, ele é dito irredutível por raízes racionais.

Pode acontecer ainda do polinômio ter raízes iguais e quando isso acontece, diz-se que a raiz possui multiplicidade. Por exemplo, se a raiz r_1 aparece só uma vez na fatoração do polinômio em multiplicação de fatores lineares, ela é dita simples. Se a raiz aparecer duas vezes diz-se que a raiz tem multiplicidade 2. E se aparece n vezes diz-se que ela tem multiplicidade n.

Considere a equação $x^2 - 4x + 4 = 0$, observe que 2 é raiz, usando redução por produtos notáveis é possível observar que sua fatoração é da forma $x^2 - 4x + 4 = (x-2)^2 = 0$. Nesse caso, diz-se que a raiz 2 tem multiplicidade dois.

Assim, seja a equação polinomial de grau n, na indeterminada x e raízes $r_1, r_2, ..., r_n$. A fatoração dessa equação resulta na seguinte expressão através do teorema da fatoração

$$a_n \cdot (x - r_1) \cdot (x - r_2) \cdot ... \cdot (x - r_n) = 0.$$

Exemplo 3.34. Na equação $(x-3)^2 \cdot (x+1) \cdot (x+5)^3 = 0$, tem-se que 3 tem multiplicidade 2, -1 é raiz simples e -5 tem multiplicidade 3.

Agora, é apresentado um dispositivo prático que permite dividir polinômios quaisquer por um polinômio mônico do primeiro grau do tipo $x \pm a$. Esse dispositivo é chamado de método de **Briott-Ruffini**. Esse método vai auxiliar na fatoração de polinômios do terceiro grau. Vale comentar que aqui não é feita a demonstração do método, porém caso haja interesse em [Naves] é encontrado.

Método de Briott-Ruffini:

1- Escreva os coeficientes do polinômio qualquer na horizontal, da esquerda para direita, do coeficiente monômio de maior grau para o de maior grau. (se o monômio de determinado grau não aparecer coloque zero no coeficiente.)

2- Na esquerda dos coeficientes do polinômio qualquer escreva o termo independente do polinômio de primeiro grau e o separe dos demais por uma linha vertical.

3- Agora, na linha de baixo repita o coeficiente que acompanha o monômio de maior grau. E o multiplique pelo termo independente do polinômio de grau um. O resultado, adicione com o coeficiente do monômio de grau inferior ao que repetiu-se. Aí sim, esse resultado coloque imediatamente abaixo desse coeficiente.

4- Repita os passos 3 e 4 até chegar no último coeficiente. Se o último resultado for zero a divisão é exata, e os números que ficaram na linha de baixo são os coeficientes de um polinômio de grau uma unidade menor que aquele polinômio qualquer.

5- Por fim, reescreva o polinômio qualquer como o produto do polinômio de grau um pelo novo polinômio cujos coeficientes foram encontrados pelos passos anteriores.

Exemplo 3.35. Para exemplificar o método de Briott-Ruffinni divida os polinômios $p(x) = x^4 + x^3 - 2$ por $t(x) = x - 2$. Colocando os coeficientes como indicado no passo 1.

2	1	1	0	0	-2

Descendo o coeficiente que acompanha o monômio de quarto grau, que é o maior grau dos monômios que formam o polinômio $p(x)$.

2	1	1	0	0	-2
	1				

Agora multiplica-se 1 por 2 e o resultado adiciona-se com o próximo coeficiente que nesse caso também é 1.

2	1	1	0	0	-2
	1	3			

Seguindo os mesmos passos para os próximos números, tem-se que $3 \cdot 2 + 0 = 6$, coloca-se 6 em baixo do 0. Depois, $6 \cdot 2 + 3 = 15$, coloca-se 15 em baixo do 3. Por fim, $15 \cdot 2 + (-2) = 28$, coloca-se 28 em baixo do -2.

2	1	1	0	0	-2
	1	3	6	18	34

Portanto o processo está encerrado. O polinômio $p(x)$ após ser dividido por $t(x)$ pelo método de Briott-Ruffini, obteve o quociente $q(x) = 1 \cdot x^3 + 3 \cdot x^2 + 6 \cdot x + 18$ e o resto $r(x) = 34$.

A seguir são apresentadas as relações de Girrard para uma equação de 3º grau. Mas antes de demonstrar essas relações, vale destacar que, são válidas para equações de grau n com $(n > 1)$ e demonstradas por um processo chamado de indução.

Dada a equação $ax^3 + bx^2 + cx + d = 0$ com $a \neq 0$, ela pode ser reescrita da seguinte forma:

$$x^3 + \frac{b}{a} \cdot x^2 + \frac{c}{a} \cdot x + \frac{d}{a} = 0.$$

Sejam r_1, r_2 e r_3 suas raízes, pelo teorema da decomposição tem-se

$$x^3 + \frac{b}{a} \cdot x^2 + \frac{c}{a} \cdot x + \frac{d}{a} = (x - r_1) \cdot (x - r_2) \cdot (x - r_3)$$

multiplicando os elementos do 2º membro,

$$x^3 + \frac{b}{a} \cdot x^2 + \frac{c}{a} \cdot x + \frac{d}{a} = x^3 - (r_1 + r_2 + r_3) \cdot x^2 + (r_1 \cdot r_2 + r_1 \cdot r_3 + r_2 \cdot r_3) \cdot x - r_1 \cdot r_2 \cdot r_3 = 0.$$

Utilizando a igualdade de polinômios obtém-se:

$$\begin{cases} r_1 + r_2 + r_3 = -\dfrac{b}{a} \\ r_1 \cdot r_2 + r_1 \cdot r_3 + r_2 \cdot r_3 = \dfrac{c}{a} \\ r_1 \cdot r_2 \cdot r_3 = -\dfrac{d}{a} \end{cases}.$$

Perceba que as relações de Girrard são importantes quando se conhece alguma informação dobre suas raízes.

Exemplo 3.36. Se a soma de duas das raízes da equação $x^3 - 7x + 6 = 0$ é 3, resolva a equação.

Utilizando as relações de Girrard, suponha que $r_1 + r_2 = 3$, assim reescrevendo a equação $x^3 + 0 \cdot x^2 - 7 \cdot +6 = 0$ tem-se

$$\begin{cases} r_1 + r_2 + r_3 = -\dfrac{0}{1} = 0 \\ r_1 \cdot r_2 + r_1 \cdot r_3 + r_2 \cdot r_3 = \dfrac{-7}{1} = -7 \\ r_1 \cdot r_2 \cdot r_3 = -\dfrac{6}{1} = -6 \end{cases} .$$

Na primeira equação já é possível encontrar r_3, pois $3 + r_3 = 0$ e daí $r_3 = -3$. Agora que já é conhecida uma das raízes, com o método de Briott-Ruffini fatore o polinômio de tal maneira que

-3	1	0	-7	6
	1	-3	2	0

.

a equação pode ser escrita como

$$x^3 - 7x + 6 = 0 = (x + 3) \cdot (x^2 - 3x + 2) = 0.$$

Resolvendo a equação do segundo grau $x^2 - 3x + 2 = 0$ tem-se que a soma das raízes é 3 e o produto é 2, logo suas razões são $r_1 = 2$ e $r_2 = 1$, o que conclui o problema.

Para encerrar essa seção, o teorema das raízes racionais é enunciado. Ele um teorema que não garante a existência de raízes racionais, contudo, se elas existirem, ele mostra como encontrá-las.

Teorema 3.37. Em um equação com coeficientes inteiros, se o número racional $\alpha = \dfrac{p}{q}$ (com $p \neq 0$, e p e q inteiros e primos entre si) é raiz da equação, então tem-se que q é divisor do coediciente de maior grau da equação e p é divisor do termo independente na equação.

Demonstração. [Naves] □

Vale observar que o teorema acima possibilita a formação de um conjunto de possíveis raízes racionais. Se nenhum dos elementos desse conjunto for raiz então a equação não possui raiz racional.

Exemplo 3.38. Considere a equação $x^5 - 2x^4 - x + 2 = 0$, encontre todas as raízes racionais dela e escreva sua fatoração com raízes racionais. Considere os divisores do coeficiente do monômio de maior grau $D(1) = \{\pm 1\}$ e os divisores do termo independente $D(2) = \{\pm 1, \pm 2\}$. Assim, o conjunto das possíveis raízes racionais

dado pela divisão dos elementos de $D(2)$ pelos elementos de $D(1)$ é $C = \{\pm 1, \pm 2\}$. Testando todas as possíveis raízes tem-se que

$$2^5 - 2 \cdot 2^4 - 2 + 2 = 32 - 32 - 2 + 2 = 0,$$

$$(-2)^5 - 2 \cdot (-2)^4 - (-2) + 2 = -32 - 32 + 2 + 2 = -60 \neq 0,$$

$$(-1)^5 - 2 \cdot (-1)^4 - (-1) + 2 = -1 - 2 + 1 + 2 = 0,$$

e

$$1^5 - 2 \cdot 1^4 - 1 + = 1 - 2 - 1 + 2 = 0.$$

Logo, as raízes racionais encontradas são $-1, 1$ e 2. Utilizando o método de Briott-Ruffini para escrever o polinômio em sua forma fatorada. Primeiro considere o -1 como raiz para reduzir o polinômio de grau 5 para um produto de dois polinômios. Um linear e o outro de grau 4.

1	1	-2	0	0	-1	2
	1	-1	-1	-1	-2	0

tem-se que o início da fatoração é

$$x^5 - 2x^4 - x - 2 = (x - 1) \cdot (x^4 - x^3 - x^2 - x - 2) = 0.$$

Agora, considerando 2 como raiz e utilizando o método de Briott-Ruffini para fatorar agora o equação de $4^{\underline{o}}$ grau $x^4 - x^3 - x^2 - x - 2 = 0$, tem-se:

2	1	-1	-1	-1	-2
	1	1	1	1	0

Onde a fatoração do polinômio agora é

$$x^5 - 2x^4 - x - 2 = (x - 1) \cdot (x - 2) \cdot (x^3 + x^2 + x + 1) = 0.$$

Por fim, utilizando que -1 é raiz da equação e fatorando a equação de $3^{\underline{o}}$ grau $x^3 + x^2 + x + 1 = 0$, tem-se:

-1	1	1	1	1
	1	0	1	0

Concluindo assim a fatoração, que fica:

$$x^5 - 2x^4 - x + 2 = (x-1)\cdot(x-2)\cdot(x+1)\cdot(x^2+1).$$

Observe que o x^2+1 é irredutível para raízes racionais, logo o exercício está concluído.

Lista de Exercícios Propostos

1. Fatore os polinômios a seguir no conjunto dos reais.
   a) $p(x) = x^4 + 4x^3 + 5x^2 + 8x + 6$
   b) $p(x) = x^3 + 3x^2 + 38x - 120$
   c) $p(x) = x^3 + x - 2$.

3.2.7 Parte 8 - Construção dos números racionais e alguns irracionais

Para início de conversa, defina o conjunto $\mathcal{C}_{\mathbb{R}} = \{\alpha \in \mathbb{R} \mid \text{é construtível}\}$ formado por todos os números reais que podem ser obtidos por construção usando apenas régua não graduada e compasso.

Como já foi discutido anteriormente, já é de conhecimento comum que o conjunto dos números inteiros é todo construtível, a partir de $O = (0,0)$ e $U = (1,0)$. Pois, basta fazer a intersecção das circunferências de raio 1 com a reta construtível que passa por O e U.

O objetivo é mostrar que o conjunto $\mathcal{C}_{\mathbb{R}}$ é um subconjunto dos números reais que contém o conjunto dos números racionais e possui algumas propriedades que o tornam um subcorpo dos reais, isto é, possui todas as propriedades nas operações de adição e multiplicação dos reais, porém com os elementos que pertencem à $\mathcal{C}_{\mathbb{R}}$. Não se pode deixar de frisar o caráter forte dessa afirmação, que é: Todos os números racionais são construtíveis e além disso existem alguns números reais que não são racionais e também são construtíveis.

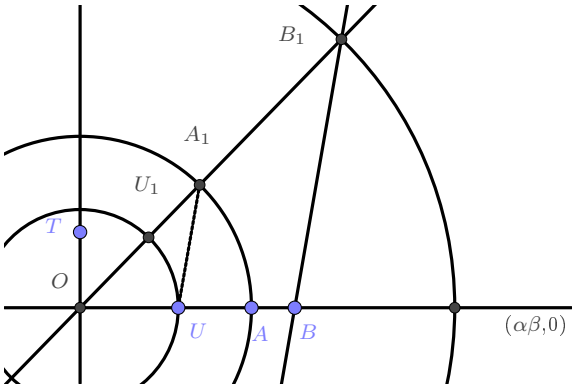
Para mostrar oque todos os números racionais são construtíveis, basta que as afirmações a seguir sejam válidas.

(1) Dados $\alpha,\ \beta \in \mathcal{C}_{\mathbb{R}}$ então $\beta - \alpha \in \mathcal{C}_{\mathbb{R}}$.
(2) Dados $\alpha,\ \beta \in \mathcal{C}_{\mathbb{R}}$ então $\alpha \cdot \beta \in \mathcal{C}_{\mathbb{R}}$.
(3) Dados $0 \neq \alpha \in \mathcal{C}_{\mathbb{R}}$ então $\dfrac{1}{\alpha} \in \mathcal{C}_{\mathbb{R}}$.

Assim, sem perda de generalidade, considere $\beta > \alpha > 0$. Seja ainda, $A = (\alpha, 0)$ e $B = (\beta, 0)$ dois pontos construtíveis pertencentes a reta suporte de $\overline{OU}$, pela Proposição 3.7 existe um ponto construível $X = (x, 0)$ à direita de O sobre a

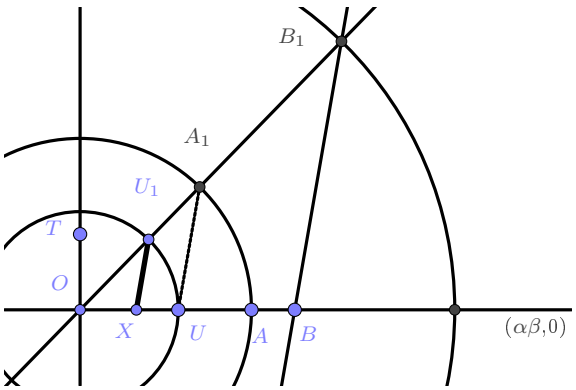
reta suporte de $\overline{OU}$ tal que $\overline{OU}$ e $\overline{AB}$ possuam o mesmo comprimento. Daí, $(x-0, 0-0) = (\beta-\alpha, 0-0) = (\beta-\alpha, 0) \Rightarrow (x, 0) = (\beta-\alpha, 0) \Rightarrow x = \beta-\alpha$ é um número construtível, logo $\beta-\alpha \in \mathcal{C}_{\mathbb{R}}$ que é o que se queria mostra no item (1).
Para mostrar os itens (2) e (3), observe primeiro que existem retar construtíveis que contém o ponto O diferentes das retas suportes de $\overline{OU}$ e $\overline{OT}$ onde $T = (0, 1)$.
Seja r uma reta construtível que passa por O diferente das retas suportes de $\overline{OU}$ e $\overline{OT}$. Considere ainda $A = (\alpha, 0)$ e $B = (\beta, 0)$ pontos construtíveis sobre a reta suporte de $\overline{OU}$ de modo que $|\overline{OU_1}| = |\overline{OA}| = \alpha$, e como os triângulos OA_1U e OB_1B são semelhantes pelo caso ângulo-ângulo, já que as retas suportes de $\overline{UA_1}$ e $\overline{BB_1}$ são paralelas. Logo,

$$\frac{1}{|UA_1|} = \frac{\beta}{\overline{OB_1}} \Rightarrow \frac{1}{\alpha} = \frac{\beta}{|\overline{OB_1}|} \Rightarrow |\overline{OB_1}| = \alpha \cdot \beta.$$



Aí com a ponta seca do compasso centrada em O e a outra ponta em B_1 trace a circunferência até interceptar a reta suporte de $\overline{OU}$, construindo o ponto $(\alpha \cdot \beta, 0)$, que é construtível por ser resultado da intersecção de uma cricunferência e uma reta construtível. Logo, $\alpha \cdot \beta$ é um número construtível.

Na figura acima, como $|\overline{OU}|$ é raio da circunferência de comprimento 1 e U_1 pertence a reta r, construa $X \in \overline{OU}$ tal que $\overline{XU_1}$ seja paralela a $\overline{UA_1}$. Observe,



segue da semelhança dos triângulos OAU_1 e OUA_1 que $\frac{|\overline{OU_1}|}{|\overline{OX}|} = \frac{|\overline{OA_1}|}{|\overline{OU}|}$ e como

$|\overline{OU_1}| = |\overline{OU}| = 1$ e $|\overline{OA_1}| = \alpha$ tem-se $\frac{1}{|\overline{OX}|} = \frac{\alpha}{1}$, logo $|\overline{OX}| = \frac{1}{\alpha}$. Isto é, o número $\frac{1}{\alpha}$ é construtível.

Para essa demonstração, ao considerar números construtíveis $\alpha, \beta \in \mathcal{C}_{\mathbb{R}}$, com as ferramentas que se possui nessa aula, a escolha está restrita aos números inteiros. Portanto, ao mostrar que o inverso de um número inteiro diferente de zero é construtível e a multiplicação de dois números inteiros é construtível, conclui-se que o conjunto dos números racionais é todo construtível.

Exemplo 3.39. Na demonstração anterior mostrou-se que todos os números racionais são construtíveis. porém, foi comentado que existem números que não são racionais que também são construtíveis. Observe que o número $\frac{\sqrt{2}}{3}$ é um exemplo de número irracional construtível, como já mostrado no exemplo 3.4 da aula 1.

Definição 3.40. Se $A = (u, v) \in \mathcal{P}_n$ diz-se que u e v são as coordenadas de $\mathcal{P}_n$, e denota-se por $\mathcal{A}_n$ o conjunto de todas as coordenadas de $\mathcal{P}_n$.

Exemplo 3.41. Observe que $\mathcal{P}_1 = \langle \mathcal{P}_0 \rangle$, onde

$$\mathcal{P}_1 = \left\{ (-1,0), (0,0), (1,0), (2,0), \left(\frac{1}{2}, \frac{\sqrt{3}}{2}\right), \left(\frac{1}{2}, -\frac{\sqrt{3}}{2}\right) \right\},$$

então as coordenadas de $\mathcal{P}_1$ é o conjunto $\mathcal{A}_1 = \left\{-1, -\frac{\sqrt{3}}{2}, 0, \frac{1}{2}, \frac{\sqrt{3}}{2}, 2\right\}$.

O conjunto $\mathcal{A}_1$ possui dois exemplos de números reais construtíveis que não são racionais. Diz-se que esses números pertencem ao que pode-se chamar de extensão dos racionais, cuja a definição é apresentada mais a frente nessa aula.

Observe que $\mathcal{A}_n \subset \mathcal{C}_{\mathbb{R}}$ $\forall n \in \mathbb{N}$, pois pela proposição 3.9 todo ponto construtível do plano tem que suas entradas são números reais também construtíveis.

Agora, seja $K_0 = \mathbb{Q}, K_1 = \mathbb{Q}[\mathcal{A}_1], ..., K_n = \mathbb{Q}[\mathcal{A}_n], ...$ e como $\mathcal{A}_0 \subset \mathcal{A}_1 \subset ... \subset \mathcal{A}_n, ..., \mathcal{C}_{\mathbb{R}}$, temos:

$$\mathbb{Q} = K_0 \subset K_1 \subset K_2 \subset ... \subset K_n \subset K_{n+1} \subset ... \subset \mathcal{C}_{\mathbb{R}}.$$

Onde os corpos $K[A_i]$ são extensões dos racionais, como por exemplo, $\mathbb{Q}[\mathcal{A}_1] = \mathcal{Q}[\sqrt{3}] = \{a + b\sqrt{3} \mid a, b \in \mathbb{Q}\}$.

Vale destacar ainda que se $\alpha \in \mathcal{C}_{\mathbb{R}}$ então $(\alpha, 0) \in \mathcal{P}_n$ para algum $n \in \mathbb{N}$, ou seja, $\alpha \in \mathcal{A}_n$ para algum $n \in \mathbb{N}$. e então $\alpha \in K_n$. Um outra maneira de definir p conjunto dos números reais que são construtíveis usando o que acima foi exposto é

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

A seguir é enunciada uma proposição que destaca alguns números irracionais que não são construtívies, o que reforça o fato de que nem todo número é real é possível de ser construtível usando apenas régua sem marcações e compasso.

Proposição 3.42. Se n é um número ímpar maior ou igual à 3 e p um número primo maior ou igual à 2 então $\sqrt[n]{p}$ não é construtível.

A raiz cúbica de 2 é um número não construtível desde que usado apenas régua não graduada e compasso. A seguir será feita um paralelo dos polinômios e a construção dos números.

Um número é chamado de algébrico sobre o conjunto dos números racionais se ele for raiz de um polinômio com coeficientes racionais. Por exemplo, $\sqrt[3]{2}$ é algébrico pois é raiz do polinômios $p(x) = x^3 - 2$. Agora, π não é algébrico, ele é chamado de número transcedente sobre os racionais pois não é raiz de nenhum polinômio com coeficientes racionais e então não é construtível.

Observe que tanto o conjunto dos números racionais $\mathbb{Q}$ quanto o conjunto dos números reais $\mathbb{R}$ possuem estrutura de corpo. Além desse fato, é importante observar que existem outros conjuntos com estrutura de corpo que contém os números racionais e estão contidos nos números reais. Esses conjuntos são chamados de extensões dos racionais. Um exemplo é o conjunto $\mathbb{Q}[\sqrt{2}] = \{a+b\cdot\sqrt{2} \mid a, b \in \mathbb{Q}\}$. Com efeito, qualquer elemento dos racionais está contido em $\mathbb{Q}[\sqrt{2}]$, basta tomar $b = 0$. E como a soma de um número racional com um irracional é irracional, e portanto real, a afirmação está justificada.

Considere uma extensão qualquer K dos racionais, se para todo $\alpha \in K$ for raiz de um polinômio com coeficientes em $\mathbb{Q}$, diz-se que K é uma extensão algébrica. Aqui, pode-se começar a encontrar uma relação entre a construção dos números e as raízes de polinômios, pois o conjunto $\mathbb{C}_{\mathbb{R}}$ é uma extensão algébrica dos racionais. Isto é, todos os números construtíveis devem ser raízes de um polinômios com coeficientes racionais.

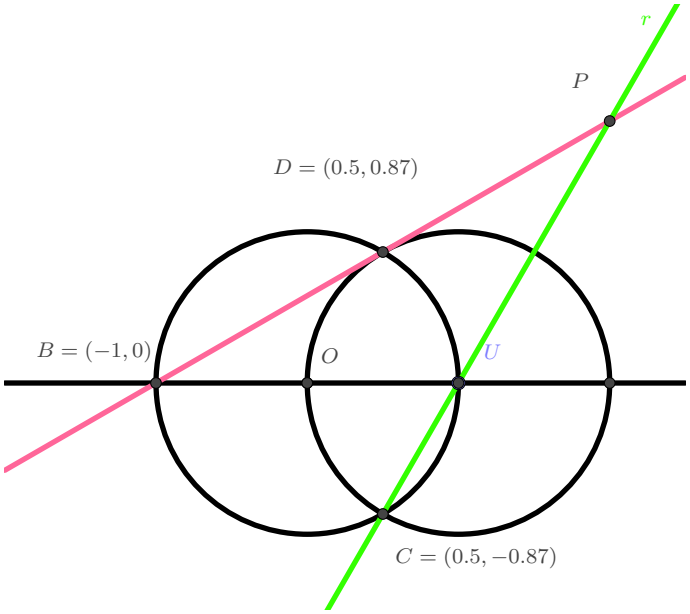
Para garantir a construção de um ponto que pertence ao conjunto $\mathcal{P}_{n+1} = \langle \mathcal{P}_n \rangle$, e consequentemente das coordenadas desse ponto que pertencem ao conjunto $\mathcal{A}_n$, observe que se $A = (\alpha_i, \beta_i)$ construtível é obtido por uma das três operações elementares de construção, as coordenadas desse ponto obrigatoriamente tem que ser raiz de um polinômio de grau um ou grau dois com coeficientes em A_i ou A_{i+1}. Observe os exemplos a seguir.

Exemplo 3.43. Na construção do conjunto $\mathcal{A}_1$ que é formado pelas coordenadas dos pontos construtíveis a gerados por $\mathcal{P}_0$ encontrou-se dois números irracionais

construtíveis que são $\frac{\sqrt{3}}{2}$ e $-\frac{\sqrt{3}}{2}$. Agora, a partir do conjunto $\mathcal{P}_1 = \langle \mathcal{P}_0 \rangle$, onde

$$\mathcal{P}_1 = \left\{ (-1,0), (0,0), (1,0), (2,0), \left(\frac{1}{2}, \frac{\sqrt{3}}{2}\right), \left(\frac{1}{2}, -\frac{\sqrt{3}}{2}\right) \right\},$$

considere os retas construtíveis r e s, onde a primeira passa pelos pontos $(1,0)$ e $\left(\frac{1}{2}, \frac{-\sqrt{3}}{2}\right)$ e a segunda pelos pontos $(-1,0)$ e $\left(\frac{1}{2}, \frac{\sqrt{3}}{2}\right)$. Como são retas construtíveis, sua intersecção constrói o ponto P. Observe a figura abaixo.



Observe que a equação reduzida da reta r é $y = \sqrt{3}x - \sqrt{3}$ e a equação da reta s é $y = \frac{\sqrt{3}}{3} \cdot x + \frac{\sqrt{3}}{3}$. Resolvendo o sistema formado por essas duas equações obtém-se as coordenadas do ponto $P = (2, \sqrt{3})$, que pertence ao conjunto $\mathcal{P}_2$. E assim o número irracional $\sqrt{3}$ que pertencerá ao conjunto das coordenadas de $\mathcal{P}_2$ denominado por $\mathcal{A}_2$ é raiz de um polinômio com coeficientes em $\mathbb{Q}[\mathcal{A}_1]$. A saber o polinômio é dado por $p(x) = \frac{x}{2} - \frac{\sqrt{3}}{2}$. Perceba que os coeficientes desse polinômio são $\frac{1}{2}$ e $\frac{-\sqrt{3}}{2}$ pertencem ao conjunto $\mathcal{A}_1$.

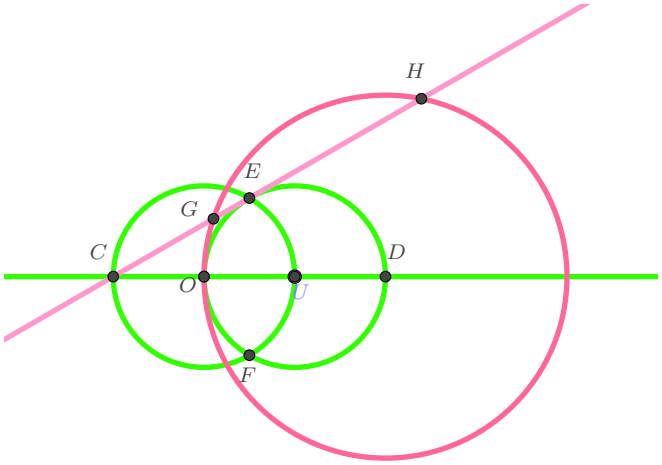
A construção de $\sqrt{3}$ é bastante trivial, desse modo é interessante construir outro número irracional cujo os passos não sejam tão simples.

Exemplo 3.44. Seja o polinômio $p(x) = 4x^2 - 10x + 1$, observe que os coeficientes pertencem à $K_1 = \mathbb{Q}[\mathcal{A}_1]$ onde $\mathcal{A}_1 = \left\{ -1, -\frac{\sqrt{3}}{2}, 0, \frac{1}{2}, 1, \frac{\sqrt{3}}{2}, 2 \right\}$ é o conjunto das coordenadas de $\mathcal{P}_1$. Perceba ainda que $\mathcal{A}_1 = \mathbb{Q}[\sqrt{3}] = \{a + b\sqrt{3},\ a, b \in \mathbb{Q}\}$. Usando a fórmula resolutiva de uma equação do segundo grau, são encontradas $\frac{5}{4} \pm \frac{\sqrt{21}}{2}$.

Esses dois números irracionais são construtíveis, e mais, esses números pertencem ao conjunto $\mathcal{A}_2$. Os números são construtívies pois a extensão $\mathbb{Q}[\sqrt{3}]$ é construída logo após os racionais, e o seu índice que é um número natural calculado pela quantidade de vetores que formam a sua base é dois. Em outras palavras, pode-se afirmar que o número é construtível sempre que tiver uma extensão seguida da outra, com coeficientes pertencentes a uma delas e o número for raíz desse polinômio.

Como foi mostrado a construção com passos algébricos, agora pode-se partir para a construção usando apenas a régua e o compasso. Partindo do conjunto dos pontos construtíveis $\mathcal{P}_1$ construi-se a reta que passa por $E = (-1, 0)$ e $C = \left(\frac{1}{2}, \frac{\sqrt{3}}{2}\right)$ e a circunferência que passa pelos pontos $F = (2, 0)$ e $O = (0, 0)$ cujo o centro é F e o raio é 2. Considere então, as equações da reta e da circunferência respectivamente

$$\begin{cases} y = \dfrac{\sqrt{3}}{2} \cdot (x + 1) \\ (x - 2)^2 + y^2 = 4 \end{cases}$$



cuja intersecção é formada pelos pontos construtíveis $P_1 = \left(\frac{5}{4} - \frac{\sqrt{21}}{2}; \frac{3\sqrt{3}}{4} - \frac{\sqrt{7}}{3}\right)$ e $P_2 = \left(\frac{5}{4} - \frac{\sqrt{21}}{2}; \frac{3\sqrt{3}}{4} + \frac{\sqrt{7}}{3}\right)$. Esses números são irracionais e pertencem ao conjunto das coordenadas de $\mathcal{P}_2$. Assim, é possível construir uma infinidade de números irracionais e verificar se sua construção é possível apenas pelos polinômios de grau um ou dois, que tenham seus coeficientes na extensão dos racionais.

Nos últimos dois exemplos, é possível observar a relação entre polinômios e a construção de números, sejam eles racionais ou irracionais. Pois, basta que esse número faça parte da coordenada de um ponto construtível, que foi obtido por uma das três operações elementares de construção e tambeém que seja raiz de um polinômio de grau um ou dois com coeficientes nas extensões $\mathbb{Q}[\mathcal{A}_n]$ ou $\mathbb{Q}[\mathcal{A}_{n+1}]$.

Considerações Finais

As construções de números usando apenas o compasso e a régua sem medidas podem ser feitas usando apenas passos geométricos, porém, em alguns problemas a dedução desses passos ou mesmo a descoberta de quais passos seguir pode não ser uma tarefa fácil. Em alguns casos, a construção é até impossíveis. Deste modo, ao apresentar um teorema que descreve condições para dizer se um número pode ou não ser construído usando as operações elementares de construção é uma ferramenta muito útil, e pode integralizar o estudo da álgebra com a geometria.

Além disso, olhando para o ensino de matemática na educação básica, o ensino da geometria construtiva não é um hábito comum entre os professores, dada a carga horária curta, a dificuldade em utilizar os materiais mínimos ou qualquer outro problema estrutural da educação. Assim, ao propor um material que pode ser seguido e apresenta uma espécie de roteiro ajuda na mudança desse hábito. No ensino médio por exemplo, pouco se vê sobre construções, e a proposição de uma espécie de integração entre a teoria de polinômios e a teoria de construção usando apenas régua não graduada e compasso, algumas portas para uma nova visão de ensino e aprendizagem desses conteúdos se apresenta. Na maioria dos livros antes da mudança do currículo com o início da implantação da nova BNCC, a teoria de polinômios e as construções geométricas eram abordadas totalmente independentes uma da outra.

A necessidade dessa integração de conceitos para uma formação mais ampla e de acordo com a nova proposta do novo ensino médio, deu início a proposição de uma sequência de passos e conceitos que interligam conceitos e teoremas de construção de números usando apenas régua não graduada e compasso com a teoria de polinômios.

O material aqui desenvolvido se enquadra como uma das trilhas de conhecimento propostas pela documento da BNCC como um itinerário de aprofundamento dentro de área de matemática e suas tecnologias. Ele pode ser usado tanto para uma trilha de aprofundamento quanto como base para um minicurso ou específica de matemática. E assim, destacar que a construção de números pode ser interpretada e usada como uma aplicação algébrica para a teoria de polinômios garantindo uma

abordagem interdisciplinar dentro dos próprios campos de estudos da matemática.

Dado o caráter teórico do material, é de suma importância que os alunos se dediquem, a escolha dessa trilha implica em estudar conteúdos que geralmente ele não costumam dominar com facilidade. Porém, com a introdução de um caráter mais geométrico associado aos polinômios, caso o professor decida usar softwares como o geogebra (inclusive todas as figuras aqui no material foram construídas usando o geogebra) isso pode ser um atrativo a mais para a aula e o conteúdo em si. Destaco aqui que o roteiro para ser usado está pronto, e a sua utilização com êxito dependerá bastante do público ao qual será aplicado.

Referências Bibliográficas

[BRASIL]BRASIL. *Ministério da Educação. Base Nacional Comum Curricular.* Disponível em: <http://basenacionalcomum.mec.gov.br/abase/>.

[FTD 2022]FTD, S. d. e. *ensino médio: matemática e suas tecnologias: 2 série*. [S.l.]: FTD, 2022.

[GO]GO, S. *Novo Ensino Médio: como vai funcionar em Goiás a partir de 2022*. Disponível em: <https://site.educacao.go.gov.br/novo-ensino-medio>.

[Gonçalves 1979]GONÇALVES, A. *Introdução à álgebra*. [S.l.]: Instituto de Matemática Pura e Aplicada, 1979.

[Krerley e Adán 2012]KRERLEY, I. M. O.; ADÁN, J. C. F. *Iniciação à matemática: um curso com problemas e soluções*. [S.l.]: SBM, 2012.

[livre]LIVRE, S. *Aplicativo Geogebra online*.

[Naves]NAVES, W. S. *Matemática no texto*: Geometria analítica, números complexos, polinômios e equações polinomiais. [S.l.: s.n.].

[Nobre 1995]NOBRE, S. Coleção tópicos de história da matemática para uso na sala de aula. tradução de hygino h. domingues, editora atual, são paulo, 1993. *Bolema-Boletim de Educação Matemática*, v. 10, n. 11, p. 90–91, 1995.