INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA
DE SÃO PAULO

ALEXSANDER ANDREY GOMES TARCHA

UM ESTUDO DOS TRÊS PROBLEMAS CLÁSSICOS DA GEOMETRIA

SÃO PAULO
2019

ALEXSANDER ANDREY GOMES TARCHA

UM ESTUDO DOS TRÊS PROBLEMAS CLÁSSICOS DA GEOMETRIA

Trabalho de Conclusão de Curso apresentado ao Instituto Federal de Educação, Ciência e Tecnologia de São Paulo – IFSP, em cumprimento ao requisito parcial para obtenção do grau acadêmico de licenciado em Matemática.

Orientadora: Profa. Dra. Valéria Ostete Jannis Luchetta

SÃO PAULO
2019

Catalogação na fonte
Biblioteca Francisco Montojos - IFSP Campus São Paulo
Dados fornecidos pelo(a) autor(a)

T176e Tarcha, Alexsander Andrey Gomes
Um estudo dos três problemas clássicos da geometria / Alexsander Andrey Gomes Tarcha. São Paulo: [s.n.], 2019.
88 f.

Orientadora: Valéria Ostete Jannis Luchetta

Trabalho de Conclusão de Curso (Licenciatura em Matemática) - Instituto Federal de Educação, Ciência e Tecnologia de São Paulo, IFSP, 2019.

1. Três Problemas Clássicos da Geometria. 2. Números Construtíveis. 3. Álgebra. 4. Geometria. 5. Extensões de Corpos. I. Instituto Federal de Educação, Ciência e Tecnologia de São Paulo II. Título.

CDD 510

ALEXSANDER ANDREY GOMES TARCHA

UM ESTUDO DOS TRÊS PROBLEMAS CLÁSSICOS DA GEOMETRIA

Monografia apresentada ao Instituto Federal de Educação, Ciência e Tecnologia de São Paulo, em cumprimento ao requisito exigido para a obtenção do grau acadêmico de Licenciado em Matemática.

APROVADO EM 05/12/2019 **CONCEITO:** 8,5

Leandro Albino Mosca Rodrigues
Prof. Ms. Leandro Albino Mosca Rodrigues
Membro da Banca

Prof. Dr. Henrique Marins de Carvalho
Membro da Banca

Valéria O. Jannis Luchetta
Profa. Dra. Valeria Ostete Jannis Luchetta
Orientadora

Alexsander Andrey Gomes Tarcha
Aluno: Alexsander Andrey Gomes Tarcha

É preciso que, pelo contrário, desde os começos do processo, vá ficando cada vez mais claro que, embora diferentes entre si, quem forma se forma e re-forma ao formar e quem é formado forma-se e forma ao ser formado.

Paulo Freire

Agradecimentos

Quando eu não sei onde guardei um papel importante e a procura revela-se inútil, pergunto-me: se eu fosse eu e tivesse um papel importante para guardar, que lugar escolheria? Às vezes dá certo. Mas muitas vezes fico tão pressionada pela frase ”se eu fosse eu”, que a procura do papel se torna secundária, e começo a pensar, diria melhor, sentir.
E não me sinto bem. Experimente: se você fosse você, como seria e o que faria? Logo de início se sente um constrangimento: a mentira em que nos acomodamos acabou de ser locomovida do lugar onde se acomodara. No entanto já li biografias de pessoas que de repente passavam a ser elas mesmas e mudavam inteiramente de vida.
[...] “Se eu fosse eu”parece representar o nosso maior perigo de viver, parece a entrada nova no desconhecido.

Clárice Lispector

Acho que um trecho deste poema, foi a melhor forma de representar o que aconteceu nesses quatros anos de curso. Anos de um enriquecimento intelectual e cultural incríveis, anos de muitas mudanças, amadurecimento para mim à caminho de ser eu mesmo, ressaltando o poema. Neste momento, tenho uma lista de pessoas para agradecer, pessoas que proporcionaram tantas coisas boas para mim neste periódo.

Inicialmente quero agradecer meus pais Vera e Edison por todo o apoio na vida e nesses anos de estudo, também deixo para agradecer meus irmãos Anne, Patrick e Esther por terem me suportado todos esses anos de loucura por estudos e na vida também. A minha Vó Maria Hilda por toda apoio e preocupação. Agradeço toda minha familía em geral, por terem me proporcionado condições de continuar estudando.

Deixo este espaço aqui também para agradecer minha orientadora Valéria Luchetta, por todos os ensinamentos, desde as suas aula aos momentos de orientação. Graças a sua ajuda evoluí muito. Agradeço por ter me apresentado à área de Álgebra de uma maneira tão íncrivel, com alegria e entusiasmo, mostrando aos seus alunos como esta parte da Matemática é linda.

Neste momento de agradecimentos, não poderia deixar de agradecer os meus amigos do Instituto Federal. A melhor turma, como bríncavamos. Agradeço, inicial-

mente a Jéssica e ao Nicácio que juntamente comigo formavam o melhor trío do IF. Agradeço a vocês pela amizade e apoio durante esses anos. Também não poderia deixar de agradecer aos meus outros colegas da melhor turma. Agradeço ao Silas, Ramon, João, Michele, Sarah, Thaís, Naara e Augusto pela amizade e ajuda durante esses anos. Deixo este espaço aqui também para agradecer aos meus amigos Gabriel e Augusto Sibo. Obrigado vocês por toda ajuda e apoio e pelas saídas a Liberdade e ao Festival do Japão que foram sensacionais. Agora quero não poderia deixar de agradecer todos os meus Profs do Instituto Federal de forma geral, por todos os ensinamentos nesse período. Obrigado por tudo que vocês me ensinaram.

Quero agradecer também a minha psicóloga Byanka por todo amparo e cuidado durante esse período.

E por fim, gostaria de agradecer a todos que de alguma forma me auxiliaram durante a minha formação.

Resumo

Este trabalho trata-se de uma pesquisa sobre os três problemas clássicos da geometria (duplicação do cubo, trissecção do ângulo e quadratura do círculo) cujo objetivo é compreender as demonstrações das impossibilidades de construção, com régua não graduada e compasso referentes aos três problemas citados. Os problemas em questão surgiram na Grécia entre os séculos VI à V a.C. e obtiveram destaque devido a impossibilidade de serem resolvidos com o uso de régua não graduada e compasso. A busca por soluções durou mais de dois mil anos, até que em 1837, surgiram as primeiras provas de que seria impossível a resolução desses problemas com régua não graduada e compasso, por meio de conceitos algébricos desenvolvidos ao longo dos séculos. Para atingir o objetivo especificado, desenvolvemos os conceitos de anéis, corpos, polinômios e extensões de corpos, para assim apresentar a conceituação de números construtíveis e observar com mais cuidados os três problemas clássicos afim de apresentar as demonstrações das impossibilidades clássicas.

Palavras-chave: Três problemas clássicos da geometria. Números construtíveis. Álgebra. Geometria. Extensões de corpos.

Abstract

This work is a research about the three classical problems of geometry (cube doubling, angle trisection and the circle squaring) whose objective is to understand the demonstrations of the impossibilities of construction, with ungraded straightedge and compass referring to the three problems mentioned.The problems in question arose in Greece between the 6th and 5th centuries BC and were highlighted because they could not be solved using an ungraded straightedge and compass. The search for solutions lasted more than two thousand years, until in 1837 the first evidence emerged that it would be impossible to solve these problems with an ungraded traightedge and compass, through algebraic concepts developed over the centuries. To achieve the specified objective, we developed the concepts of rings, fields, polynomials, and extensions fields to present the conceptualization of constructible numbers for study the three classic problems in order to present the demonstrations of classical impossibilities.

Palavras-chaves: Three classical problems of geometry. Constructible numbers. Algebra. Geometry. Extensions Fields.

Lista de ilustrações

Lista de símbolos

$\mathbb{N}$	Conjuntos dos números Naturais
$\mathbb{Z}$	Conjuntos dos números Inteiros
$\mathbb{Q}$	Conjuntos dos números Racionais
$\mathbb{R}$	Conjuntos dos números Reais
$\mathbb{C}$	Conjuntos do números Complexos
α	Letra grega Alfa
β	Letra grega Beta
θ	Letra grega Theta
$\in$	Pertence
$\supset$	Contém
$\subset$	Contido
0	Elemento neutro aditivo dos conjunto numéricos $\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}$ e $\mathbb{C}$.
1	Unidade dos conjuntos númericos $\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}$ e $\mathbb{C}$.
$\overline{AB}$	Segmento cuja as extremidades são os pontos A e B.
AB	Medida do segmento $\overline{AB}$.
$\forall$	Para todo.

Sumário

1 Introdução

> A história da Matemática pode tirar do esconderijo onde se encontram os problemas que constituem o campo de experiência do matemático, ou seja, o lado concreto do seu fazer.
>
> Tatiana Roque e João Bosco Pitombeira

Historicamente, não há certeza quanto a origem dos instrumentos régua[1] e compasso. Segundo Silva (2013a) como a geometria já tinha se desenvolvido de alguma forma tanto na Mesopotâmia quanto no Egito, o local de origem também é incerto. Entretanto, a existência desses intrumentos foi de grande importância para o desenvolvimento da geometria, como por exemplo, nos processos de construção de figuras tais como ângulos, polígonos, circunferências e até mesmo a construção de números e soluções de problemas algébricos (SILVA, 2013a). Vale ressaltar que, no livro *Os Elementos*, Euclides não menciona o uso dos intrumentos régua e compasso para a construção, mas sim a linha reta e os círculos. Não há indícios que Euclides ultilizou esses instrumentos, visto que as construções eram feitas de modo abstrato com o uso de retas e círculos (SCHUBRING; ROQUE, 2014). Apesar disto, a resolução de problemas com o uso de régua não graduada e compasso para alguns matemáticos gregos era visto como algo estético e admirável.

> O que havia entre algumas correntes, ou grupos, era o desejo de usar apenas esses instrumentos, pois acreditavam existir uma certa beleza implícita em um problema, uma simplicidade, quando este pudesse ser construído apenas a partir da aplicação desta técnica. Se um problema pudesse ser resolvido apenas com régua e compasso, poderia ser considerado mais puro do ponto de vista matemático, do que um que necessitasse do uso de outras ferramentas[...]. (SILVA, 2013, p. 24).

Neste contexto, entre os séculos VI e V a.C., período de grandes realizações na Grécia, iniciou-se o estudo de três grandes problemas da geometria, sendo estes: a duplicação do cubo, a trissecção do ângulo e a quadratura do círculo (enunciaremos,

[1] A régua em que nos referimos não possuia medida.

posteriormente) que obtiveram destaque devido a impossibilidade[2], de serem resolvidos com o uso de régua não graduada e compasso (SOUZA, 2001). A busca por soluções dos três problemas, que durou por mais de dois mil anos, foi responsável por grandes avanços na Matemática. De acordo com Eves (2004), essas tentativas auxiliaram no desenvolvimento de, por exemplo, "partes da teoria das equações ligadas a domínios de racionalidade, números algébricos e a teoria dos grupos"(EVES, 2004, p. 134). Devido a essa importância os três problemas ficaram conhecidos como "os três problemas clássicos da geometria". Ainda pelo mesmo autor, somente no século XIX obteve-se conhecimento das provas de que seria impossível a construção por meio de régua não graduada e compasso os três problemas citados.

Conforme Souza (2001), as primeiras demonstrações completamente esclarecedoras das impossibilidades de construção dos problemas da duplição do cubo e da trissecção do ângulo foram apresentadas por Pierre Laurent Wantzel (1814-1848) em seu artigo *"Recherches sur les Moyens de Reconnaître si un Problème de Géométrie Peut se Résoudre avec la Règle et le Compass"*, publicado em 1837, por meio de conceitos algébricos desenvolvidos ao longo dos séculos. Já em relação ao problema da quadratura do círculo, segundo Vendemiatti (2009) o matemático alemão Ferdinand von Lindemann (1852-1939) demonstrou em 1882 que π é um número transcendente[3], assim, demonstrando, mesmo que indiretamente, que o problema da quadratura do círculo não era possível de ser resolvido com régua não graduada e compasso.

Segundo Boyer (2010), além da investigação dos três problemas clássicos, a segunda metade do século V.a.C. foi marcada pela maior investigação de problemas matemáticos fundamentais, tais como: a Quadratura de Lunas[4], os problemas das grandezas incomensuráveis[5], a razão áurea, entre outros. Devido a estes motivos, essa época ficou conhecida como a Idade Heroica da Matemática.

Em vista à relevância da Idade Heroica e dos três problemas clássicos da geometria, este trabalho tem como objetivo geral compreender as demonstrações das impossiblidades de construções, com régua não graduada e compasso, referente aos problemas da duplicação do cubo, trissecção do ângulo e a quadratura do círculo e cujos enunciados são respectivamente:

> i) o problema de construir o lado de um cubo cujo volume é o dobro de um cubo dado. ii) o problema de dividir um ângulo arbitrário dado em

[2] As construções com régua e compasso obedeciam três regras ou operações para construção (ver Capítulo 5) então a impossiblidade de resolução na qual está referida é, que a partir dessas regras é impossivel de se resolver os três problemas com o uso de régua não graduada e compasso.

[3] Ver Capítulo 4

[4] Enunciado da quadratura de lunas: segmentos de círculos semelhantes estão na mesma razão que os quadrados de suas bases, para mais informações consulte (BOYER, 2010, p. 45).

[5] Duas grandezas são incomensuráveis se a razão entre essas duas grandezas não pode ser expressa por um número racional.

> três partes iguais. iii) o problema de construir um quadrado com área igual à de um círculo dado (EVES, 2004, p.133-134).

Em função de atingir o objetivo geral especificado, temos como objetivos específicos, desenvolver os conhecimentos algébricos necessários para este fim tais como a teoria dos anéis e corpos, polinômios, extensões de corpos e construir o corpo dos números construtíveis.

Em relação a metodologia, consideramos nossa pesquisa, uma pesquisa bibliográfica de carater exploratório. Explorátoria, pois segundo Gil (2002) a pesquisa explorátoria "tem como objetivo proporcionar maior familiaridade com o problema com vistas a torna-lo mais explícito ou a construir hipóteses"(GIL, p. 41) e bibliográfica, pois é baseada em materiais já elaborados, como livros, dissertações e artigos científicos (GIL, 2002).

Vale ressaltar que, em nosso entendimento, esta pesquisa poderá auxiliar outros estudantes de Licenciatura em Matemática como referência para futuros estudos sobre o tema e outros assuntos correlatos. Nessa perspectiva, este estudo também é importante para professores de Matemática atuantes na Educação Básica, pois permite aos mesmos conhecerem os problemas e possivelmente desenvolverem o tema, com devidas adaptações, em suas aulas, visto que a Base Nacional Comum Curricular (2019) propõe que os conteúdos matemáticos sejam relacionados a diversos contextos inclusive da História da Matemática.

> Cumpre também considerar que, para a aprendizagem de certo conceito ou procedimento, é fundamental haver um contexto significativo para os alunos, não necessariamente do cotidiano, mas também de outras áreas do conhecimento e da própria história da Matemática (BNCC, 2019, p. 299).

Ademais, Lopes e Ferreira (2013) ressaltam que a matemática é uma ciência construída pela humanidade a partir de muitas tentativas e passível de erros. Sendo assim, conhecer e desenvolver estudos sobre os problemas citados, cuja procura por soluções durou mais de dois mil anos, ressalta a característica sócio-histórica de resoluções de problemas da matemática.

Portanto, conforme citado anteriormente, as demonstrações das impossibilidades foram realizadas por meio de conceitos algébricos. Dessa forma, para construção desse trabalho foram destinados capítulos para exposição de definições e proposições de álgebra abstrata e outros para construção do corpo dos números construtíveis, para assim obter as ferramentas necessárias para a prova das impossibilidades.

Para as definições e proposições de álgebra abstrata, os capítulos 2 ao 4 serão dedicados para construção do marco téorico algébrico, ou seja, para o desenvolvimento dos conceitos elementares de anéis, corpos, ideais, homomorfismo de anéis, polinômios em uma variável, polinômios irredutíveis e extensões de corpos,

que incluí as definições de números algébricos, números transcendentes e grau de extensão. No Capítulo 5, desenvolveremos construções básicas com régua e compasso (contrução de retas paralelas, construção do ângulo de 60º, entre outras) para assim, ter condições de definir o conceito de número construtível e, por fim, desenvolver a construção do corpo dos números construtíveis representado pelo conjunto: $C_{\mathbb{R}} = \{x \in \mathbb{R} \mid x \text{ é construtível}\}$.

No Capítulo 6, serão desenvolvidas as demonstrações das impossibilidades dos três problemas clássicos da geometria utilizando os conceitos desenvolvidos nos capítulos anteriores.

Em relação a escrita do trabalho, procuramos escrever de modo claro, para que estudantes de matemática, que por ventura não possuam um domínio tão vasto de álgebra abstrata consigam compreender o trabalho. No início de cada capítulo, acresentamos as bibliográfias utilizadas para construção do capítulo em questão, para que assim, seja facilitada a procura por bibliográfias de um determinado tema abordado no trabalho.

2 Tópicos de Anéis e Corpos

> A álgebra é generosa:
> frequentemente ela dá mais do
> que se lhe pediu.
>
> D'Alembert

Neste capítulo, vamos abordar a teoria dos anéis e corpos, que são essenciais para o desenvolvimento dos conceitos posteriores propostos neste trabalho. Serão apresentadas as definições iniciais das estruturas algébricas e as proposições mais importantes para a compreensão dos capítulos subsequentes, além das de ideais, homomorfismos e definições elementares de divisibilidade em $\mathbb{Z}$. Para composição deste capítulo foram utilizado os seguintes materiais: Domingues e Iezzi (2003); Gonçalves (1999); Milies e Coelho (2013), Jacobson (1985) e Monteiro (1978).

2.1 Anel

Definição 2.1. *Seja A um conjunto não vazio, no qual estão definidas duas operações: adição (+) e multiplicação (·) em A:*

$$+: \begin{array}{c} A \times A \to A \\ (a,b) \mapsto a+b \end{array} \quad \textit{e} \quad \cdot: \begin{array}{c} A \times A \to A \\ (a,b) \mapsto a \cdot b \end{array}$$

O conjunto A é chamado anel se são válidas as seguintes propriedades para quaisquer elementos a, b, c pertencentes A.

(i) $a + b = b + a$ *(**comutativa da adição**).*

(ii) $a + (b + c) = (a + b) + c$ *(**associativa da adição**).*

(iii) $\exists\ b \in A$ *tal que* $a + b = a$ *(**existência do elemento neutro aditivo**). Esse elemento $b \in A$ é chamado zero do anel A ou elemento nulo do anel A, simbolicamente representaremos: $b = 0_A$.*

(iv) $\forall\ a \in A$, $\exists\ b \in A$ *tal que* $a + b = 0_A$ *(**existência do elemento oposto**). Dado $a \in A$, representaremos o elemento oposto de a por $-a$.*

(v) $(a \cdot b) \cdot c = a \cdot (b \cdot c)$ *(**associativa da multiplicação**).*

(vi) $a \cdot (b + c) = a \cdot b + a \cdot c$ **e** $(b + c) \cdot a = b \cdot a + c \cdot a$ (***distributiva da operação de multiplicação em relação a operação de adição***).

Exemplo 2.1.1. *Os conjuntos númericos* $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ *e* $\mathbb{C}$, *com as operações usuais de adição e multiplicação são exemplos de anéis. Entretanto, o conjunto dos naturais (*$\mathbb{N}$*) não é um anel, pois não verifica a propriedade (iv), isto é, os elementos de* $\mathbb{N}$ *não possuem opostos.*

Exemplo 2.1.2. *Considere o conjunto das funções* $A = \{f \mid f : \mathbb{R} \to \mathbb{R}\}$ *onde estão definidas as seguintes operações:*

$$\begin{aligned} + : \quad & A \times A \to A \\ & (f, g) \mapsto f + g \end{aligned}$$

e

$$\begin{aligned} \cdot : \quad & A \times A \to A \\ & (f, g) \mapsto f \cdot g \end{aligned}$$

onde, $(f + g)(x) = f(x) + g(x)$, $(f \cdot g)(x) = f(x) \cdot g(x)\ \forall\ x \in \mathbb{R}$ *e a função* $h(x) = 0_A$ *é o elemento neutro aditivo de* A. *Nestas condições,* A *satisfaz a estrutura de anel.*

Proposição 2.1.1. *O elemento neutro aditivo de um anel* A *é único.*

Demonstração. Seja $0_A \in A$, tal que 0_A seja o elemento neutro aditivo de A. Suponha por absurdo que existe $b \in A$ tal que b também seja o elemento neutro aditivo de A, sendo assim temos:

$$0_A = 0_A + b = b + 0_A = b.$$

Portanto, o elemento neutro aditivo de A é único. □

Proposição 2.1.2. *Sejam* A *um anel e* $a \in A$. *O elemento oposto de* a *é único.*

Demonstração. Sejam $a, -a \in A$, tal que $-a$ seja o elemento oposto de a. Suponha por absurdo que existe $b \in A$ tal que, b também seja o elemento oposto de a, sendo assim temos:

$$\begin{gathered} a + (-a) = 0_A \text{ e } a + b = 0_A, \text{ logo} \\ a + (-a) = a + b \\ (a + (-a)) + (-a) = (a + b) + (-a) \\ 0_A + (-a) = (a + (-a)) + b \\ -a = 0_A + b \\ -a = b \end{gathered}$$

Portanto, o elemento oposto de a é único. □

Proposição 2.1.3. *Sejam A um anel e $a, b \in A$ então:*

(i) $a \cdot 0_A = 0_A \cdot a = 0_A$

Demonstração. Seja $a \in A$, temos: $a \cdot 0_A = a \cdot (0_A + 0_A) = a \cdot 0_A + a \cdot 0_A$, logo:

$$\begin{gathered} a \cdot 0_A = a \cdot 0_A + a \cdot 0_A \\ a \cdot 0_A + (-(a \cdot 0_A)) = (a \cdot 0_A + a \cdot 0_A) + (-(a \cdot 0_A)) \\ a \cdot 0_A + (-(a \cdot 0_A)) = a \cdot 0_A + (a \cdot 0_A + (-(a \cdot 0_A))) \\ 0_A = a \cdot 0_A + 0_A \\ 0_A = a \cdot 0_A \end{gathered}$$

O caso $0_A \cdot a$ é análogo ao anterior. Portanto, $a \cdot 0_A = 0_A \cdot a = 0_A$. □

(ii) $-(-a) = a$

Demonstração. Seja $a \in A$, tal que $a + (-a) = 0_A$. Assim, por definição, como o oposto de a é igual a $-a$, o oposto de $-a$ é a. Ademais, pela Proposição 2.1.2 o elemento oposto é único, sendo assim não existe outra possibilidade para o oposto de $-a$. Portanto, conclui-se que $-(-a) = a$. □

(iii) $-(a \cdot b) = (-a) \cdot b = a \cdot (-b)$

Demonstração. Vamos provar inicialmente que $-(a \cdot b) = (-a) \cdot b$. Dessa forma temos:

$$\begin{gathered} (-a) \cdot b + a \cdot b = \\ (-a + a) \cdot b = \\ 0_A \cdot b = 0_A \end{gathered}$$

Assim,concluímos que $(-a) \cdot b$ é o oposto de $a \cdot b$, ou seja, $-(a \cdot b) = (-a) \cdot b$.

Analogamente para o caso $-(a \cdot b) = a \cdot (-b)$ temos,

$$\begin{gathered} a \cdot (-b) + a \cdot b = \\ a \cdot (-b + b) = a \cdot 0_A = 0_A. \end{gathered}$$

Logo, $a \cdot (-b)$ é o oposto de $a \cdot b$, isto é, $a \cdot (-b) = -(a \cdot b)$. Por fim, conclui-se que $-(a \cdot b) = (-a) \cdot b = a \cdot (-b)$.

□

A partir deste momento, em um anel A também iremos denotar a operação $a + (-b)$ como $a + (-b) = a - b$. Destacamos também que $-(a_1 + a_2 + a_2 + ... + a_n) = -a_1 - a_2 - a_3 - ... - a_n$, $\forall\ a_i \in A$.

2.1.1 Anel comutativo

Quando a operação de multiplicação de um anel A é comutativa, ou seja, dados $a, b \in A$ quaisquer, temos:

$$a \cdot b = b \cdot a$$

O anel A é chamado anel comutativo.

Exemplo 2.1.3. *Os conjuntos númericos $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ e $\mathbb{C}$, com as operações usuais de adição e multiplicação são exemplos de anéis comutativos.*

Exemplo 2.1.4. *O conjunto $\mathbb{Z}[\sqrt{2}] = \left\{m + n \cdot \sqrt{2} \mid m, n \in \mathbb{Z}\right\}$, no qual estão definidas as seguintes operações de adição e multiplicação respectivamente:*

$$\begin{aligned} + : \quad & \mathbb{Z}[\sqrt{2}] \times \mathbb{Z}[\sqrt{2}] \to \mathbb{Z}[\sqrt{2}] \\ & (m + n\sqrt{2}, p + q\sqrt{2}) \mapsto (m + p) + (n + q) \cdot \sqrt{2} \end{aligned}$$

e

$$\begin{aligned} \cdot : \quad & \mathbb{Z}[\sqrt{2}] \times \mathbb{Z}[\sqrt{2}] \to \mathbb{Z}[\sqrt{2}] \\ & (m + n\sqrt{2}, p + q\sqrt{2}) \mapsto (m \cdot p + 2 \cdot n \cdot q) + (m \cdot q + n \cdot p)\sqrt{2} \end{aligned}$$

Satisfaz a estrutura de anel, ou seja, são válidas todas as propriedades da Definição 2.1. Além disso, $\mathbb{Z}[\sqrt{2}]$ é comutativo. Veja.

Dados $x, y \in \mathbb{Z}[\sqrt{2}]$ tais que $x = m + n \cdot \sqrt{2}$ e $y = p + q \cdot \sqrt{2}$ com $m, n, p, q \in \mathbb{Z}$, temos que:

$$x \cdot y = (m + n \cdot \sqrt{2}) \cdot (p + q \cdot \sqrt{2}) = (m \cdot p + 2 \cdot n \cdot q) + (m \cdot q + n \cdot p)\sqrt{2}.$$

Como os elementos m, n, p, q são elementos de $\mathbb{Z}$ que é um anel comutativo, então a propriedade comutativa é válida em $\mathbb{Z}$, logo temos:

$$x \cdot y = (m \cdot p + 2 \cdot n \cdot q) + (m \cdot q + n \cdot p)\sqrt{2} = (p \cdot m + 2 \cdot q \cdot n) + (q \cdot m + p \cdot n)\sqrt{2} = y \cdot x.$$

Portanto, $\mathbb{Z}[\sqrt{2}]$ é um anel comutativo.

2.1.2 Anel com unidade

O elemento neutro em relação a operação de multiplicação em um anel A é denomidado unidade. Simbolicamente denotamos 1_A. Quando um anel possui unidade,

tal anel é intitulado anel com unidade. Dessa forma, se A é um anel com unidade então $\exists\ 1_A \in A$ tal que:

$$a \cdot 1_A = a = 1_A \cdot a \ ,\forall\ a \in A.$$

Exemplo 2.1.5. *O conjunto* $\{0, 1, 2\}$ *com as operações de adição e multiplicação definidas pelas tábuas de operações respectivamente:*

+	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

·	0	1	2
0	0	0	0
1	0	1	2
2	0	2	1

É um anel com unidade finito cuja a unidade é o elemento 1.

Observe que, mesmo que um anel possua unidade isto não garante que este anel seja comutativo, como por exemplo:

Exemplo 2.1.6. *O conjunto das matrizes quadradas de ordem* n *com entradas em* $\mathbb{R}$ $(M_n(\mathbb{R}))$ *definido sobre as operações usuais é um exemplo de um anel com unidade, no qual não é comutativo. De fato, a unidade deste conjunto é a matriz identidade e o produto usual de matrizes não é comutativo. Veja,*

Seja a matriz $I \in M_2(\mathbb{R})$ *tal que*

$$\mathbf{I} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

Note que I *é a unidade de* $M_2(\mathbb{R})$*, pois dada uma matriz* $A \in M_2(\mathbb{R})$ *, temos que* $A \cdot I = I \cdot A = A$*. Entretanto, dadas as matrizes* B *e* C *pertencentes a* $M_2(\mathbb{R})$ *tais que:*

$$B = \begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix} \quad \textit{e} \quad C = \begin{pmatrix} 5 & 6 \\ 7 & 8 \end{pmatrix}$$

Temos que $B \cdot C = \begin{pmatrix} 19 & 22 \\ 43 & 50 \end{pmatrix} \neq C \cdot B = \begin{pmatrix} 23 & 34 \\ 31 & 46 \end{pmatrix}$ *. Portanto, o anel* $M_2(\mathbb{R})$ *não é comutativo.*

Proposição 2.1.4. *A unidade, se existir, em um anel* A*, é unica.*

Demonstração. Seja $1_A \in A$, tal que 1_A seja a unidade de A. Suponha, por absurdo, que $\exists\, b \in A$ onde b também seja a unidade de A, sendo assim temos:

$$b = 1_A \cdot b = b \cdot 1_A = 1_A.$$

Portanto, a unidade, se existir, em um anel é única. □

Proposição 2.1.5. *Sejam A um anel com unidade, a um elemento qualquer de A e 1_A a unidade de A então $(-1_A) \cdot a = -a$.*

Demonstração. Devemos provar que $(-1_A) \cdot a$ é o oposto de a. Assim:

$$(-1_A) \cdot a + a = ((-1_A) + 1_A)) \cdot a = 0_A \cdot a = 0_A.$$

Dessa forma, concluímos que $(-1_A) \cdot a = -a$.

□

2.1.3 Domínio de Integridade

Um anel A comutativo e com unidade é chamado domínio de integridade se a seguinte propriedade é válida: sejam $a, b \in A$, quaisquer:

$$a \cdot b = 0_A \Longrightarrow a = 0_A \text{ ou } b = 0_A.$$

Exemplo 2.1.7. *O conjunto númerico $\mathbb{Z}$ é um domínio de integridade.*

Proposição 2.1.6. *Sejam A um domínio de integridade e $a, b, c \in A$ tal que $a \neq 0_A$, assim se $a \cdot b = a \cdot c$, então $b = c$.*

Demonstração. Sejam $a, b, c \in A$ tal que $a \cdot b = a \cdot c$. Assim, temos:

$$a \cdot b = a \cdot c, \text{ logo}$$
$$a \cdot b - a \cdot c = a \cdot (b - c) = 0_A$$

Dessa forma, como A é um domínio de integridade temos que $a = 0_A$ ou $b - c = 0_A$. Como $a \neq 0_A$ segue que $b - c = 0_A$ o que resulta que $b = c$.

□

2.1.4 Subanel

Definição 2.2. *Sejam A um anel e B um subconjunto não vazio de A. Suponhamos que B seja fechado para as operações de adição e multiplicação de A, ou seja:*

(i) $x + y \in B, \forall\, x, y \in B$

(ii) $x \cdot y \in B, \forall\, x, y \in B$

Nessas condições, caso B seja um anel com as operações de A, o conjunto B é dito subanel de A.

Note que, se A é um anel e B é um subanel de A temos como resultado da Proposição 2.1.1 e a existência do elemento oposto em B, que o elemento neutro aditivo de B é o mesmo de A.

Exemplo 2.1.8. *Os anéis numéricos $\mathbb{Z}$ e $\mathbb{Q}$ são exemplos de subanéis de $\mathbb{R}$. De fato, temos que $\mathbb{Z} \subset \mathbb{R}$, $\mathbb{Q} \subset \mathbb{R}$ e $\mathbb{Z}, \mathbb{Q}$ e $\mathbb{R}$ são anéis. Note que, da mesma forma, $\mathbb{Z}$ também é subanel de $\mathbb{Q}$ e $\mathbb{R}$ é subanel de $\mathbb{C}$.*

Observe também que, como consequência da definição, todo anel é subanel de si próprio. De fato, seja A um anel, temos que $A \subset A$ e A é um anel, logo A é subanel de si próprio. De forma similiar o conjunto $\{0_A\}$ também é um subanel de A, já que $0_A + 0_A = 0_A$ e $0_A \cdot 0_A = 0_A$. A e $\{0_A\}$ são denominados subanéis triviais.

A proposição a seguir fornecerá condições para decidir se um subconjunto não vazio de um anel A é um subanel de A.

Teorema 2.1.1. *Sejam A um anel e B um subconjunto não vazio de A. B é um subanel de A se e somente se as seguintes condições são verificadas.*

(i) $0_A \in B$

(ii) $x - y \in B, \forall\, x, y \in B$

(iii) $x \cdot y \in B, \forall\, x, y \in B$

Demonstração. Se B é um subanel de A, segue que B é fechado para as operações de adição e multiplicação de A e B mantém a estrutura de anel. Sendo assim, as condições (i), (ii) e (iii) são satisfeitas, pois como B é um subanel de A temos que: $0_A \in B$; todo elemento de B possui oposto e B é fechado para a adição, ou seja, $x + (-y) \in B$, logo $x - y \in B$ e ainda como B é fechado para a multiplicação temos que $x \cdot y \in B$. A recíproca também é verdadeira, já que $0_A \in B$, o que garante

que o elemento neutro aditivo de A pertence a B, portanto B é não vazio; $x - y \in B$ o que certifica que todo elemento de B possui um oposto, veja: sejam $0_A, y \in B$, logo $0_A - y = -y \in B$. Por sua vez, pelas condições (ii) e (iii) segue que B é fechado para as operações de adição e multiplicação de A. Por fim, como todo elemento de B pertence a A e A é um anel, são válidas para os elementos de B as propriedades $(i), (ii), (v), (vi)$ da Definição 2.1. Portanto, B satisfaz a estrutura de anel, logo concluímos que B é um subanel de A.

□

Exemplo 2.1.9. *Seja A um anel. O conjunto $C(A) = \{a \in A \mid a \cdot x = x \cdot a, \forall\, x \in A\}$ formado por elementos comutativos de A, denominado centro do anel A, é um subanel de A. Certamente, pois pelo Teorema 2.1.1, temos,*

Sejam $a, b \in C(A)$ temos que,

(i) $0_A \in C(A)$*, pois* $0_A \cdot a = 0_A = a \cdot 0_A$

(ii) $a - b \in C(A)$
Queremos mostrar que: $(a-b)\cdot x = x\cdot(a-b)\ \forall\, x \in A$*. Note que, como* $a, b \in C(A)$*, temos que* $a \cdot x = x \cdot a$ *e* $b \cdot x = x \cdot b$*,* $\forall\, x \in A$*. Então, segue que:*

$$(a - b) \cdot x = a \cdot x - b \cdot x = x \cdot a - x \cdot b = x \cdot (a - b),$$ *logo* $a - b \in C(A)$*.*

(iii) $a \cdot b \in C(A)$
Devemos mostrar que $(a\cdot b)\cdot x = x\cdot(a\cdot b)\ \forall\, x \in A$*. Perceba que, como* $a, b \in C(A)$*, temos que* $a \cdot x = x \cdot a$ *e* $b \cdot x = x \cdot b$*,* $\forall\, x \in A$*, logo*

$$(a \cdot b) \cdot x = a \cdot (b \cdot x) = a \cdot (x \cdot b) = (a \cdot x) \cdot b = (x \cdot a) \cdot b = x \cdot (a \cdot b).$$

Sendo assim, $a \cdot b \in C(A)$*.*

Portanto, pelo Teorema 2.1.1, concluímos que $C(A)$ é um subanel de A.

2.2 Corpo

Nesta seção vamos apresentar a estrutura algébrica denominada corpo. Esta estrutura é importante devido ao grande número de propriedades, as quais seus elementos satisfazem. Em especial, podemos destacar a propriedade na qual difere um corpo de um domínio de integridade, que é a existência do elemento inverso.

Definição 2.2.1. *Um conjunto não vazio $\mathbb{K}$ é chamado corpo se $\mathbb{K}$ é um domínio de integridade, no qual todo elemento de $\mathbb{K}$, diferente do elemento nulo é inversível em relação a operação de multiplicação, ou seja:*

$$\forall\, x \in \mathbb{K}, x \neq 0_{\mathbb{K}}\ \exists\, x^{-1} \in \mathbb{K} \textit{ tal que } x \cdot x^{-1} = 1_{\mathbb{K}}.$$[1]

Exemplo 2.2.1. *Os conjuntos numéricos $\mathbb{Q}, \mathbb{R}$ e $\mathbb{C}$ são exemplos de corpos.*

Proposição 2.2.1. *Sejam $\mathbb{K}$ um corpo e $a \in \mathbb{K}$ tal que $a \neq 0_{\mathbb{K}}$. O elemento inverso de a é único.*

Demonstração. Seja $a \in \mathbb{K}$ tal que $a \neq 0_{\mathbb{K}}$. Suponha, por absurdo, que $\exists\, c, b \in \mathbb{K}$ tais que c e b sejam o inverso de a. Logo,

$$a \cdot b = 1_{\mathbb{K}} \text{ e } a \cdot c = 1_{\mathbb{K}} \text{ então temos:}$$
$$a \cdot b = a \cdot c$$
$$a \cdot b - a \cdot c = 0_{\mathbb{K}}$$
$$a \cdot (b - c) = 0_{\mathbb{K}}, \text{ logo } a = 0_{\mathbb{K}} \text{ ou } (b - c) = 0_{\mathbb{K}} \text{ e}$$

como $a \neq 0_{\mathbb{K}}$ segue que $b = c$. Portanto, o elemento inverso é único. □

Proposição 2.2.2. *Sejam $\mathbb{K}$ um corpo e $a, b \in \mathbb{K}$ tais que $a, b \neq 0_{\mathbb{K}}$, então $(a \cdot b)^{-1} = a^{-1} \cdot b^{-1}$.*

Demonstração. O que queremos mostrar é que o inverso de $a \cdot b$ é igual a $a^{-1} \cdot b^{-1}$, isto é, $(a \cdot b) \cdot (a^{-1} \cdot b^{-1}) = 1_{\mathbb{K}}$. Dessa forma: Sejam $a, b \in \mathbb{K}$ tais que $a, b \neq 0_{\mathbb{K}}$

$$(a \cdot b) \cdot (a^{-1} \cdot b^{-1}) = (a \cdot (b \cdot a^{-1}) \cdot b^{-1}) = (a \cdot (a^{-1} \cdot b) \cdot b^{-1}) = (a \cdot a^{-1}) \cdot (b \cdot b^{-1}) = 1_{\mathbb{K}} \cdot 1_{\mathbb{K}} = 1_{\mathbb{K}}.$$

□

2.2.1 Subcorpo

Definição 2.2.2. *Seja $\mathbb{K}$ um corpo e $\mathbb{L}$ um subconjunto não vazio de $\mathbb{K}$. $\mathbb{L}$ é dito subcorpo de $\mathbb{K}$ se $\mathbb{L}$ é fechado para as operações de $\mathbb{K}$ e $\mathbb{L}$ mantém a estrutura de corpo.*

Exemplo 2.2.2. *De forma similar aos subanéis, o corpo $\mathbb{Q}$, além de ser um subanel de $\mathbb{R}$, é um subcorpo de $\mathbb{R}$.*

Note que, se $\mathbb{K}$ é um corpo e $\mathbb{L}$ é um subcorpo de $\mathbb{K}$ então como consequência da definição, os resultados das Proposições 2.1.1 e 2.1.4 e a existência dos elementos inversos e opostos em $\mathbb{L}$, segue que a unidade e o elemento neutro aditivo de $\mathbb{L}$ coincidem com os de $\mathbb{K}$.

[1] Denotamos $x^{-1} = \dfrac{1}{x}$.

A proposição a seguir, fornecerá condições para decidirmos se um conjunto é um subcorpo.

Teorema 2.2.1. *Sejam $\mathbb{K}$ um corpo e L um subconjunto não vazio de $\mathbb{K}$. L é um subcorpo de $\mathbb{K}$ se e somente se as seguintes condições são verificadas.*

(i) $0_{\mathbb{K}}, 1_{\mathbb{K}} \in \mathbb{L}$.

(ii) $x - y \in \mathbb{L} \; \forall \; x, y \in \mathbb{L}$.

(iii) $x \cdot y^{-1} \in \mathbb{L} \; \forall \; x, y \in \mathbb{L}$ **e** $y \neq 0_{\mathbb{K}}$.

Demonstração. Se $\mathbb{L}$ é um subcorpo de $\mathbb{K}$, então $\mathbb{L}$ é fechado para as operações de adição e multiplicação em $\mathbb{K}$ e mantém a estrutura de corpo. Dessa forma, como $\mathbb{L}$ é um subcorpo de $\mathbb{K}$, temos que a condição (i) é verdadeira pelas Proposições 2.1.2 e 2.1.4. E ainda, por sua vez, como $\mathbb{L}$ é fechado para a operação de adição a condição (ii) é satisfeita e dado que $\mathbb{L}$ é fechado para a operação de multiplicação, o resultado da Proposição 2.2.1 então a condição (iii) é válida. A recíproca também é verdadeira, visto que as condições (i), (ii), (iii) garantem que $1_{\mathbb{K}}$ e $0_{\mathbb{K}}$ pertençam a $\mathbb{L}$, logo $\mathbb{L}$ é diferente do conjunto vazio, e $\mathbb{L}$ é fechado para as operações de adição e multiplicação, respectivamente. Assim, da condição (ii) temos que $0_{\mathbb{K}} - x = -x \in \mathbb{L}$, $\forall \; x \in \mathbb{L}$ e da condição (iii) segue $1_{\mathbb{K}} \cdot x^{-1} = x^{-1} \in \mathbb{L}$, $\forall \; \in x \in \mathbb{L}$, $x \neq 0_{\mathbb{K}}$. Por fim, como $\mathbb{L} \subset \mathbb{K}$ segue que as demais propriedades de um corpo são herdadas de $\mathbb{K}$. Portanto, $\mathbb{L}$ é um subcorpo de $\mathbb{K}$.

□

2.3 Ideais e homomorfismos

Nesta seção vamos apresentar, um tipo específico de subanel, o qual é denominado ideal sobre um anel. Também apresentaremos os conceitos de homomorfismo entre anéis e anéis quocientes. Esses conceitos serão de extrema importância para o desenvolvimento de um teorema no Capítulo 4.

2.3.1 A noção de ideal

Definição 2.3.1. *Sejam A um anel e I um subanel de A. Dizemos que I é um ideal de A se,*

$$a \cdot x \in I \text{ } \textbf{e} \text{ } x \cdot a \in I, \forall \; a \in A, \forall \; x \in I.$$

Exemplo 2.3.1. *Os conjuntos $\{0_A\}$ e o próprio A, são ideais de A, visto que $\{0_A\}$ e A são subanéis de A, o que garante que A e $\{0_A\}$ são fechados para a operação de*

multiplicação, logo temos que as condições de ideal são verdadeiras. A *e* $\{0_A\}$ *são ditos ideais triviais de* A*.*

Exemplo 2.3.2. *Considere o conjunto* $n\mathbb{Z} = \{n \cdot x \mid n, x \in \mathbb{Z}\}$*. Vamos mostrar que* $n\mathbb{Z}$ *é um subanel de* $\mathbb{Z}$*. Assim,*
Sejam $a, b \in n\mathbb{Z}$*, quaisquer tais que* $a = n \cdot x$ *e* $b = n \cdot y$*,* $n \in \mathbb{Z}$*, temos que:*

(i) $0 \in n\mathbb{Z}$*, pois* $\forall\ n \in \mathbb{Z}$*,* $0 = n \cdot 0 \in n\mathbb{Z}$*.*

(ii) $a - b = n \cdot x - n \cdot y = n \cdot (x - y) \in n\mathbb{Z}$*.*

(iii) $a \cdot b = (n \cdot x) \cdot (n \cdot y) = n \cdot (n \cdot x \cdot y) \in n\mathbb{Z}$*.*

Portanto, pelo Teorema 2.1.1 $n\mathbb{Z}$ *é um subanel de* $\mathbb{Z}$*.*

Agora, vamos mostrar $n\mathbb{Z}$ *é um ideal de* $\mathbb{Z}$*. Considere,* $z \in \mathbb{Z}$ *e* $a \in n\mathbb{Z}$*, tal que* $a = n \cdot x$ *para algum* $n \in \mathbb{Z}$ *segue que* $z \cdot a = z \cdot (n \cdot x) = n \cdot (x \cdot z) \in n\mathbb{Z}$*, de modo análogo temos que* $a \cdot z \in n\mathbb{Z}$*. Portanto, como* $n\mathbb{Z}$ *é um subanel de* $\mathbb{Z}$ *e* $z \cdot a \in n\mathbb{Z}$*, concluímos que* $n\mathbb{Z}$ *é um ideal de* $\mathbb{Z}$*.*

2.3.2 Ideais gerados por um número finito de elementos

Para quaisquer n elementos $a_1, a_2, ..., a_n (n \geq 1)$ de um anel comutativo A, indicaremos por $< a_1, a_2, ..., a_n >$ o seguinte subconjunto de A:

$$< a_1, a_2, ..., a_n >= \{x_1 \cdot a_1 + x_2 \cdot a_2 + ... + x_n \cdot a_n \mid x_1, x_2, ..., x_n \in A\}.$$

Vamos mostrar que $< a_1, a_2, ..., a_n >$ é um ideal de A. Sendo assim, devemos provar que:

(i) $< a_1, a_2, ..., a_n >$ é um subanel de A.

(ii) Dado $a \in A$ e $x \in< a_1, a_2, ..., a_n >$ temos que $a \cdot x \in< a_1, a_2, ..., a_n >$ e $x \cdot a \in< a_1, a_2, ..., a_n >$.

Demonstração. Considere o conjunto $S =< a_1, a_2, ..., a_n >$.

(i) Sejam $x, y \in S$, logo $x = x_1 \cdot a_1 + ... + x_n \cdot a_n$ e $y = y_1 \cdot a_1 + ... + y_n \cdot a_n$, com $x_i, y_i \in A$. Assim,

- $0_A \cdot a_1 + ... + 0_A \cdot a_n = 0_A \in S$.
- $x - y = (x_1 \cdot a_1 + ... + x_n \cdot a_n) - (y_1 \cdot a_1 + ... + y_n \cdot a_n) = (x_1 - y_1) \cdot a_1 + ... + (x_n - y_n) \cdot a_n \in S$, pois cada $x_i - y_i \in A$.

- $x \cdot y = (x_1 \cdot a_1 + ... + x_n \cdot a_n) \cdot (y_1 \cdot a_1 + ... + y_n \cdot a_n) = (x_1 \cdot a_1 \cdot y_1 \cdot a_1 + x_1 \cdot a_1 \cdot y_2 \cdot a_2 + ... + x_1 \cdot a_1 \cdot y_n \cdot a_n) + (x_2 \cdot a_2 \cdot y_1 \cdot a_1 + x_2 \cdot a_2 \cdot y_2 \cdot a_2 + ... + x_2 \cdot a_2 \cdot y_n \cdot a_n) + ... + (x_n \cdot a_n \cdot y_1 \cdot a_1 + x_n \cdot a_n \cdot y_2 \cdot a_2 + ... + x_n \cdot a_n \cdot y_n \cdot a_n) = a_1 \cdot (x_1 \cdot y_1 \cdot a_1 + x_1 \cdot y_2 \cdot a_2 + ... + x_1 \cdot y_n \cdot a_n) + a_2 \cdot (x_2 \cdot y_1 \cdot a_1 + x_2 \cdot y_2 \cdot a_2 + ... + x_2 \cdot y_n \cdot a_n) + ... + a_n \cdot (x_n \cdot y_1 \cdot a_1 + x_n \cdot y_2 \cdot a_2 + ... + x_n \cdot y_n \cdot a_n) \in S$, pois cada $x_i \cdot y_i \cdot a_i \in A$ e A é fechado para adição.

Portanto, pelo Teorema 2.1.1 S é um subanel de A.

(ii) Sejam $a \in A$ e $x \in < a_1, ..., a_n >$ tal que $x = x_1 \cdot a_1 + ... + x_n \cdot a_n$ com $x_i \in A$, temos:

$$a \cdot x = a \cdot (x_1 \cdot a_1 + ... + x_n) = a \cdot x_1 \cdot a_1 + ... + a \cdot x_n \cdot a_n.$$

Como cada $a \cdot x_i \cdot a_i$ são elementos de A, segue que $a \cdot x \in S$. O caso $x \cdot a$ é análogo, pois o anel A é comutativo.

Portanto, S é um ideal de A. □

Definição 2.3.2. *O conjunto $S =< a_1, a_2, ..., a_n >$ é denominado ideal gerado por $a_1, a_2, ...a_n$. Se $S =< a_1 >$, ou seja, gerado por único elemento, esse ideal é chamado ideal principal de A.*

Exemplo 2.3.3. *Seja A um anel comutativo com unidade. Os ideais trivais $\{0_A\}$ e A são principais. De fato, $\{0_A\} =< 0_A >= \{0_A \cdot a \mid a \in A\}$ (gerado por 0_A) e $A =< 1_A >= \{1_A \cdot a \mid a \in A\}$ (gerado por 1_A).*

Exemplo 2.3.4. *Seja o ideal $10\mathbb{Z} = \{10 \cdot n \mid n \in \mathbb{Z}\}$. Veja que $10\mathbb{Z}$ é um ideal gerado pelo elemento 10. Assim, $10\mathbb{Z}$ é um ideal principal, pois é gerado por um único elemento.*

Definição 2.3.3. *Seja A um anel e I um ideal de A. I é chamado ideal maximal em A se $I \neq A$ e se J é um ideal de A tal que $J \supset I$ então $J = A$ ou $J = I$.*

Exemplo 2.3.5. *No Exemplo 2.3.2 mostramos que o conjunto $J = n\mathbb{Z} = \{0, \pm n, \pm 2n...\}$ é um ideal de $\mathbb{Z}$. Se tomarmos o ideal $I = 2\mathbb{Z}$, temos que I é um ideal maximal de $\mathbb{Z}$. De fato, segue que $J = n\mathbb{Z} = \{0, \pm n, \pm 2n...\} \supset 2\mathbb{Z}$. Como $2\mathbb{Z} \neq J$ então $\exists\ a \in J$ tal que a seja ímpar, ou seja $a = 2t + 1$, para $t \in \mathbb{Z}$. Mas, como $2t \in J$, pois $J \supset I$ então $(2t + 1) - 2t = 1 \in J$, pois J é um ideal de $\mathbb{Z}$. Assim, $1 \cdot t \in J$, pois J é um ideal de $\mathbb{Z}$. Deste modo, concluímos que $J = 1 \cdot \mathbb{Z} = \mathbb{Z}$ e é gerado por 1. Portanto, I é um ideal maximal de $\mathbb{Z}$.*

2.3.3 Anel quociente

Nesta seção vamos definir o anel quociente. Optamos apresentar apenas os resultados mais importantes deste tópico e indicaremos as referências aos quais o leitor poderá encontrar essas demonstrações. No decorrer do trabalho haverão outras demonstrações que deixaremos apenas indicadas as referências.

Seja A um anel e I um ideal de A. Definimos o conjunto quociente de A pelo ideal I o conjunto $A/I = \{\overline{x} \mid \overline{x} = x + y, x \in A, y \in I\}$. Definimos as seguintes operações de adição e multiplicaçãem A/I, respectivamente:

$$+: \begin{array}{c} A/I \times A/I \to A/I \\ (\overline{x}, \overline{y}) \mapsto \overline{x+y} \end{array} \quad \text{e} \quad \cdot: \begin{array}{c} A/I \times A/I \to A/I \\ (\overline{x}, \overline{y}) \mapsto \overline{x \cdot y} \end{array}$$

Com as operações assim definidas o conjunto A/I satisfaz as propriedades de anel.

Demonstração. Consultar Gonçalves (1999, p. 51).

□

Teorema 2.3.1. *Seja A um anel comutativo com unidade e seja I um ideal de A. Então, I é um ideal maximal de A se e somente se A/I é um corpo.*

Demonstração. Consultar Gonçalves (1999, p. 52). □

2.3.4 Homomorfismo de Anéis

Definição 2.3.4. *Sejam A e B anéis. Uma função $f : A \to B$ diz-se um homomorfismo de A em B se satisfaz as seguintes condições:*

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

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

Nestas condições, se f for bijetiva então diz-se que f é um isomorfismo de anéis.

Exemplo 2.3.6. *Considere o anel $A = \mathbb{Z}[\sqrt{2}] = \left\{m + n \cdot \sqrt{2} \mid m, n \in \mathbb{Z}\right\}$ no qual estão definidas as mesmas operações do Exemplo 2.1.4 e seja $f : A \to A$ definida por $f(m + n \cdot \sqrt{2}) = m - n \cdot \sqrt{2}$. A aplicação é um homomorfismo de anéis, pois:*

Sejam, $x, y \in A$ tais que $x = m + n \cdot \sqrt{2}$ e $y = p + q \cdot \sqrt{2}$ com $m, n, p, q \in \mathbb{Z}$, temos

(i) $f(x+y) = f((m+p)+(n+q)\cdot\sqrt{2}) = (m+p)-((n+q)\cdot\sqrt{2}) = (m+p)-n\cdot\sqrt{2}-q\cdot\sqrt{2} = m-n\cdot\sqrt{2}+p-q\cdot\sqrt{2} = f(m+n\cdot\sqrt{2})+f(p+q\cdot\sqrt{2}) = f(x)+f(y)$.

(ii) $f(x\cdot y) = f((m+n\cdot\sqrt{2})\cdot(p+q\cdot\sqrt{2})) = f((m\cdot p+2\cdot n\cdot q)+(m\cdot q+n\cdot p)\sqrt{2}) = (m\cdot p+2\cdot n\cdot q)-(m\cdot q+n\cdot p)\cdot\sqrt{2} = m\cdot p+2\cdot n\cdot q-m\cdot q\cdot\sqrt{2}-n\cdot p\cdot\sqrt{2} = p\cdot(m-n\cdot\sqrt{2})-(m-n\cdot\sqrt{2})\cdot q\cdot\sqrt{2} = (m-n\cdot\sqrt{2})\cdot(p-q\cdot\sqrt{2}) = f((m+n\cdot\sqrt{2})\cdot f(p+q\cdot\sqrt{2}) = f(x)\cdot f(y)$. *Deste modo, concluímos que f é um homomorfismo.*

Perceba que, além desta função ser um homomorfismo, é também um isomorfismo. De fato, se $f(x) = f(y)$, segue que $f(m+n\sqrt{2}) = f(p+q\sqrt{2})$, então $m-n\sqrt{2} = p-q\sqrt{2}$, logo $m-p = (n-q)\sqrt{2}$ e como $m,n,p,q \in \mathbb{Z}$ segue que $m-p = 0$ e $n-q = 0$ o que implica que, $m = p$ e $n = q$. Portanto, $x = y$ o que resulta que f é injetiva. Agora, basta mostrar que f é sobrejetiva. Tomando $z \in A$ (contradomínio) tal que $z = m-n\cdot\sqrt{2}$, com $m,n \in \mathbb{Z}$ temos que $\exists\, x \in A$ (domínio) tal que $x = m+n\cdot\sqrt{2}$, no qual $f(x) = z$. De fato, pois temos que $f(x) = f(m+n\cdot\sqrt{2}) = m-n\cdot\sqrt{2}$ e, por sua vez, $m-n\cdot\sqrt{2} = z$, assim $f(x) = z$. Isto prova que f é sobrejetiva. Sendo assim, concluímos que f é um homomorfismo de anéis bijetivo, ou seja, um isomorfismo.

Note que dois anéis isomorfos diferem apenas pelos nomes de seus elementos e operações. Essencialmente são o mesmo anel e cada um deles pode ser considerado uma "cópia"um do outro. O próximo exemplo, tornará um pouco mais claro essa ideia.

Exemplo 2.3.7. *Considere a função $f : \mathbb{R} \to \mathbb{C}$, tal que $f(a) = (a,0)$. A aplicação é um homomorfismo injetor de anéis, pois:*

Sejam $a,b \in \mathbb{R}$, temos:

(i) $f(a+b) = (a+b,0) = (a,0)+(b,0) = f(a)+f(b)$.

(ii) $f(a\cdot b) = (a\cdot b,0)$. Por sua vez, $f(a)\cdot f(b) = (a,0)\cdot(b,0) = (a\cdot b,0)$[2]. Portanto, $f(a\cdot b) = f(a)\cdot f(b)$.

E ainda, f é injetiva, pois se $f(a) = f(b)$ então $(a,0) = (b,0)$ o que resulta que $a = b$. Note que, como a função f, é um homomorfismo injetor de anéis, é possível obter um isomorfismo $g : \mathbb{R} \to Imf$[3], tal que $g(x) = f(x)$. Dessa forma, essa função representa uma cópia de $\mathbb{R}$ em $\mathbb{C}$. Sendo assim, quando enunciamos que "$\mathbb{R} \subset \mathbb{C}$", o que de fato acontece é um isomorfismo representado pela função g.

[2] Lembre-se que o produto usual em $\mathbb{C}$ é dado por: sejam $(a,b),(x,y) \in \mathbb{C}$ temos que $(a,b)\cdot(x,y) = (a\cdot x-b\cdot y, a\cdot y+x\cdot b)$.

[3] O conjunto Imf é denominado imagem da função f.

Definição 2.3.5. *Sejam A e B anéis e $f : A \to B$ um homomorfismo. Chama-se núcleo de f, e denotamos por $N(f)$ (ou $Ker(f)$) o seguinte subconjunto de A:*

$$N(f) = \{x \in A \mid f(x) = 0_B\}.$$

Note que $N(f) \neq \emptyset$, pois em um homomorfismo de anéis temos que, $f(0_A) = 0_B$. De fato,

$$f(0_A) = f(0_A + 0_A) = f(0_A) + f(0_A) \text{ , logo}$$
$$f(0_A) = f(0_A) + f(0_A)$$
$$f(0_A) - f(0_A) = f(0_A)$$
$$0_B = f(0_A) .$$

Dessa forma, o elemento nulo do anel sempre pertencerá ao núcleo do homomorfismo.

Lema 2.3.1. *Sejam A, B anéis e $f : A \to B$ um homomorfismo, então:*

(i) $Imf = \{f(a) \mid a \in A\}$ é um subanel de A.

(ii) $N(f)$ é um ideal de A e f é injetiva se e somente se, $N(f) = 0_A$.

(iii) Os anéis $A/N(f)$ e Imf são isomorfos.

Demonstração. Consultar Gonçalves (1999, p. 57). □

2.4 Divisibilidade em $\mathbb{Z}$

Definição 2.4.1. *Sejam $a, b \in \mathbb{Z}$. Diz-se que a divide b se existe $c \in \mathbb{Z}$ tal que $a \cdot c = b$. Simbolicamente representa-se $a \mid b$. Se a não divide b, simbolicamente representamos: $a \nmid b$*

Exemplo 2.4.1. *$2|6$, pois $6 = 2 \cdot 3$. Por outro lado, $4 \nmid 3$, pois não existe $c \in \mathbb{Z}$, tal que $3 = 4 \cdot c$.*

Definição 2.4.2. *Diz-se que um número inteiro p é primo se, e somente se, p satisfaz as seguintes condições:*

(i) $p \neq 0$ e $p \neq \pm 1$;

(ii) os únicos divisores de p são -1, 1, p e $-p$.

Lema 2.4.1. *Sejam $p, a, b \in \mathbb{Z}$ onde p é primo. Se $p|(a \cdot b)$ então $p|a$ ou $p|b$.*

Demonstração. Consultar Milies e Coelho (2013, p. 78). □

3 Noções Básicas de Polinômios à luz da Teoria dos Anéis

Neste capítulo vamos apresentar o anel dos polinômios definido sobre um corpo $\mathbb{K}$ denominado $\mathbb{K}[x]$. Além das definições básicas de polinômios também apresentaremos o algorítmo da divisão em $\mathbb{K}[x]$, os polinômios irredutíveis e o critério de Eisenstein para verificação da irredutibilidade. Esses conceitos serão de extrema importância, para a construção da teoria de extensão de corpos e para as provas das impossilidades clássicas. Para composição deste capítulo foram utilizados os livros e a dissertação de Gonçalves (1999), Domingues e Iezzi (2003) e Santos (2017), respectivamente.

Definição 3.1. *Seja $\mathbb{K}$ um corpo qualquer. Considere a expressão formal:*

$$p(x) = a_0 + a_1x + a_2x^2 + ... + a_nx^n + ...$$

onde cada $a_i \in \mathbb{K}$ para todo $i \in \mathbb{N}$ e $\exists\ n \in \mathbb{N}$ tal que $a_j = 0_{\mathbb{K}}\ \forall j \geq n$. Essa expressão é denominada polinômio sobre $\mathbb{K}$ em uma indeterminada x e os elementos a_i são chamados coeficientes do polinômio $p(x)$.

Exemplo 3.1. *Seja $p(x) = 2x^2 + 4x + 1$ um polinômio sobre o corpo $\mathbb{R}$, onde os coeficientes de $p(x)$ são $a_2 = 2$, $a_1 = 4$ e $a_0 = 1$.*

Exemplo 3.2. *Considere $q(x) = \frac{1}{2}x + 1$, onde $a_1 = \frac{1}{2}$ e $a_0 = 1$.*

Definição 3.2. *Dado um polinômio $p(x) = a_0+a_1x+a_2x^2+...+a_nx^n+...$ sobre um corpo $\mathbb{K}$ tal que $a_n \neq 0_{\mathbb{K}}$ e $a_j = 0_{\mathbb{K}}\ \forall j > n$. Denominamos $n \in \mathbb{N}$ como grau do polinômio $p(x)$. Em simbologia $\partial(p(x)) = n$. Nesse caso indicamos $p(x) = a_0 + a_1x + a_2x^2 + ... + a_nx^n$.*

Considerando os polinômios dos Exemplos 3.1 e 3.2 temos que $\partial(p(x)) = 2$ e $\partial(q(x)) = 1$.

Definição 3.3. *(Identidade de polinômios). Sejam $p(x) = a_0 + a_1x + a_2x^2 + ... + a_nx^n$ e $q(x) = b_0 + b_1x + b_2x^2 + ... + b_mx^m$ polinômios sobre um corpo $\mathbb{K}$, $p(x)$ e $q(x)$ são chamados idênticos se e somente se $a_i = b_i\ \forall\ i \in \mathbb{N}$.*

3.1 Polinômio Constante e Polinômio Identicamente Nulo

Definição 3.1.1. *O polinômio $p(x) = a_0$, onde $a_0 \neq 0_{\mathbb{K}}$ sobre $\mathbb{K}$ é denomidado polinômio constante. No caso de $p(x)$ constante, temos $\partial(p(x)) = 0$.*

Exemplo 3.1.1. *O polinômio $p(x) = 2$ é constante.*

Definição 3.1.2. *Seja* $p(x) = 0_{\mathbb{K}} + 0_{\mathbb{K}}x + 0_{\mathbb{K}}x^2 + ... + 0_{\mathbb{K}}x^n$*, onde* $0_{\mathbb{K}}$ *é o elemento neutro em relação a adição do corpo* $\mathbb{K}$*. Nesse caso* $p(x)$ *é denominado polinômio identicamente nulo. Podemos denotar o polinômio identicamente nulo simplesmente como* $p(x) = 0_{\mathbb{K}}$*. Da forma como foi definido, o grau do polinômio nulo não está definido.*

Definição 3.1.3. *O polinômio no qual o coeficiente do maior grau é igual a unidade é denotado por polinômio mônico.*

3.2 Anéis de Polinômios

Nesta seção vamos conferir que o conjunto dos polinômios sobre um corpo $\mathbb{K}$, satisfazem a estrutura de um domínio de integridade para as duas operações que definiremos a seguir. Devido a tecnicalidade da demonstração, a prova de que $\mathbb{K}[x]$ é um domínio de integridade está posta no Apendíce A.

Definição 3.2.1. *Sejam* $p(x) = a_0 + a_1x + a_2x^2 + ... + a_nx^n$ *e* $q(x) = b_0 + b_1x + b_2x^2 + ... + b_mx^m$ *dois elementos do conjunto* $\mathbb{K}[x]$*, onde* $m \leq n$*. Definimos duas operações:*

- ***Adição***

$$p(x)+q(x) = (a_0+b_0)+(a_1+b_1)x+(a_2+b_2)x^2+...+(a_m+b_m)x^m+a_{m+1}x^{m+1}+...+a_nx^n$$
e
$$\partial(p(x) + q(x)) = n.$$

- ***Multiplicação***

$$p(x) \cdot q(x) = c_0 + c_1x + ... + c_{n+m}x^{n+m}, \quad \textit{onde } c_i = \sum_{j=0}^{i=n+m} a_j \cdot b_{i-j}$$
e
$$\partial(p(x) \cdot q(x)) = n + m.$$

Também podemos denotar o produto dos polinômios p *e* q *da seguinte forma:* $p(x) \cdot q(x) = (p \cdot q)(x)$ *e a soma da forma* $p(x) + q(x) = (p + q)(x)$*.*

Exemplo 3.2.1. *Sejam* $p(x) = 2x^2 + 5x + 3$ *e* $q(x) = 10x^3 + x^2 + 6x + 11$*. Veja que* $a_0 = 3$*,* $a_1 = 5$*,* $a_2 = 2$ *e* $b_0 = 11$*,* $b_1 = 6$*,* $b_2 = 1$*,* $b_3 = 10$*. Logo,*
Adição

$$p(x) + q(x) = (3 + 11) + (5 + 6)x + (2 + 1)x^2 + 10x^3 = 14 + 11x + 3x^2 + 10x^3.$$

Multiplicação

$c_0 = a_0 \cdot b_0 = 3 \cdot 11 = 33.$

$c_1 = a_1 \cdot b_0 + a_0 \cdot b_1 = 5 \cdot 11 + 3 \cdot 6 = 73.$

$c_2 = a_2 \cdot b_0 + a_1 \cdot b_1 + a_0 \cdot b_2 = 2 \cdot 11 + 5 \cdot 6 + 3 \cdot 1 = 55.$

$c_3 = a_3 \cdot b_0 + a_2 \cdot b_1 + a_1 \cdot b_2 + a_0 \cdot b_3 = 0 \cdot 11 + 2 \cdot 6 + 5 \cdot 1 + 3 \cdot 10 = 47.$

$c_4 = a_4 \cdot b_0 + a_3 \cdot b_1 + a_2 \cdot b_2 + a_1 \cdot b_3 + a_0 \cdot b_4 = 0 \cdot 11 + 0 \cdot 6 + 2 \cdot 1 + 5 \cdot 10 + 3 \cdot 0 = 52.$

$c_5 = a_5 \cdot b_0 + a_4 \cdot b_1 + a_3 \cdot b_2 + a_2 \cdot b_3 + a_1 \cdot b_4 + a_0 \cdot b_5 = 0 \cdot 11 + 0 \cdot 6 + 0 \cdot 1 + 2 \cdot 10 + 5 \cdot 0 + 3 \cdot 0 = 20.$

Portanto,

$$p(x) \cdot q(x) = c_0 + c_1 x + c_2 x^2 + c_3 x^3 + c_4 x^4 + c_5 x^5 = 33 + 73x + 55x^2 + 47x^3 + 52x^4 + 20x^5.$$

Note que pelo Exemplo 3.2.1, é facil ver que o coeficiente de maior grau do produto de polinômios é dado por $2 \cdot 10$, os quais os fatores são os coeficientes de maior grau dos polinômios em questão. Dessa forma, de modo geral para os polinômios $p(x) = a_0 + a_1 x + a_2 x^2 + ... + a_n x^n$ e $q(x) = b_0 + b_1 x + b_2 x^2 + ... + b_m x^m$, onde $m \leq n$ com coeficientes em $\mathbb{K}$, o valor do coeficiente de maior grau, c_{m+n} é o produto de $a_n \cdot b_m$.

Assim, observe que o conjunto $\mathbb{K}[x]$ não é um corpo, pois os polinômios, com exceção do polinômio constante, não possuem inverso. De fato, suponha que $p(x) \cdot q(x) = 1_{\mathbb{K}}$, tal que $p(x), q(x) \in \mathbb{K}[x]$, $p(x) = a_0 + a_1 x + a_2 x^2 + ... + a_n x^n$ e $q(x) = b_0 + b_1 x + b_2 x^2 + ... + b_m x^m$ onde $m \leq n$. Pela Definição 3.2.1 obtemos que $p(x) \cdot q(x) = c_0 + c_1 x + ... + c_{n+m} x^{n+m}$, onde $c_i = \sum_{j=0}^{i=n+m} a_j \cdot b_{i-j}$. Dessa forma, segue o $a_0 \cdot b_0 = 1$ e $c_i = 0$ $\forall i \neq 0$. Assim, os únicos polinômios nessas condições são os polinômios constantes inversíveis em $\mathbb{K}$. Sendo assim, os elementos inversíveis de $\mathbb{K}[x]$ são os inversíveis em $\mathbb{K}$. Como $\mathbb{K}$ é um corpo, procede que todos os seus elementos não nulos são inversíveis. Portanto, em $\mathbb{K}[x]$, todos os polinômios constantes são inversíveis.

Note também que o anel dos polinômios poderia ser construido sobre um domínio de integridade, visto que para as demonstrações das propriedades não foi necessário a inversiblidade dos elementos.

3.2.1 Divisibilidade em $\mathbb{K}[x]$

Teorema 3.2.1. *Dados os polinômios p, g e $\in \mathbb{K}[x]$, com $g \neq 0$, então existem únicos polinômios q e r pertencentes a $\mathbb{K}[x]$ tais que $p(x) = g(x) \cdot q(x) + r(x)$ onde $r(x) = 0_{\mathbb{K}}$ ou $\partial(r(x)) < \partial(g(x))$.*

Demonstração. Consultar Domingues e Iezzi (2003, p. 291). □

Exemplo 3.2.2. *Dados os polinômios* $p, q \in \mathbb{R}[x]$ *tais que* $p(x) = x^2 + 2x + 1$ *e* $q(x) = x - 1$. *Note que o polinômio* $p(x) = x^2 + 2x + 1 = (x-1) \cdot (x+3) + 4$, *onde* $g(x) = x + 3$ *e* $r(x) = 4$.

3.2.2 Ideais em $\mathbb{K}[x]$

Nesta seção vamos mostrar que todo ideal em $\mathbb{K}[x]$ é um ideal principal. Da Definição 2.3.2 podemos concluir que a forma geral de um ideal principal em $\mathbb{K}[x]$ é o conjunto dos múltiplos de um elemento $p \in \mathbb{K}[x]$

$$< p >= \{f(x) \cdot p(x) \mid f(x) \in K[x]\}.$$

Denominaremos $< p >= \mathbb{K}[x] \cdot p(x)$.

Teorema 3.2.2. *Todo ideal de* $\mathbb{K}[x]$ *é principal.*

Demonstração. Seja J um ideal de $\mathbb{K}[x]$. Vamos mostrar que J é principal, ou seja,

$$J = \mathbb{K}[x] \cdot p(x) = \{f(x) \cdot p(x) \mid f(x) \in \mathbb{K}[x]\}.$$

Provaremos por casos:

(i) $J = \{0_{\mathbb{K}}\}$.
Neste caso, é imediato pelo Exemplo 2.3.3 que J é um ideal principal.

(ii) Se $q \in J$ é um polinômio constante e $J \neq \{0_{\mathbb{K}}\}$.
Seja $q(x) = a \neq 0_{\mathbb{K}}$. Sendo assim, existe $a^{-1} \in \mathbb{K}[x]$ tal que $a^{-1} \cdot a = 1_{\mathbb{K}}$ e como J é um ideal de $\mathbb{K}[x]$ segue que $a^{-1} \cdot a = 1_{\mathbb{K}} \in J$. Portanto, se $1_{\mathbb{K}} \in J$, temos que $\forall f \in \mathbb{K}[x]$ vem que $f(x) \cdot 1_{\mathbb{K}} = f(x) \in J$, pois J é um ideal de $\mathbb{K}[x]$, logo $J = \mathbb{K}[x]$ e é gerado por $1_{\mathbb{K}}$.

(iii) Se $p \in J$, tal que $\partial(p(x)) > 0$, e p é um polinômio de menor grau possível em J.
Como $p \in J$ e J é um ideal de $\mathbb{K}[x]$, segue que $\forall f \in \mathbb{K}[x]$, temos que $f(x) \cdot p(x) \in J$, logo $\mathbb{K}[x] \cdot p(x) \subset J$. Agora, basta mostrar que $J \subset K[x] \cdot p(x)$. Seja $g \in J$, assim pelo Algoritmo da Divisão temos que existem $q, r \in \mathbb{K}[x]$, tais que:

$$g(x) = p(x) \cdot q(x) + r(x), \text{ onde } r(x) = 0_{\mathbb{K}} \text{ ou } \partial(r(x)) < \partial(p(x)).$$

Portanto, como $r(x) = g(x) - p(x) \cdot q(x)$ e $g, p \in J$, logo $r \in J$. Note que o grau de p é o menor entre os elementos de J, segue assim que $r(x) = 0_{\mathbb{K}}$ o que resulta que $g(x) = p(x) \cdot q(x) \in \mathbb{K}[x] \cdot p(x)$, isto é, $J \subset \mathbb{K}[x] \cdot p(x)$. Concluímos assim, que $J = \mathbb{K}[x] \cdot p(x)$ o que implica que J é um ideal principal.

□

3.2.3 Polinômios Irredutíveis

Definição 3.2.2. *Seja $p \in \mathbb{K}[x]$ tal que $\partial(p(x)) \geq 1$ e $\mathbb{K}$ é um corpo*[1]*. Dizemos que p é um polinômio irredutível sobre $\mathbb{K}$ se toda vez que $p(x) = g(x) \cdot h(x)$, onde $g(x), h(x) \in \mathbb{K}[x]$ resulta que $g(x)$ ou $h(x)$ são constantes*[2]*. Se $p(x)$ não for irredutível sobre $\mathbb{K}$ então dizemos que p é redutível sobre $\mathbb{K}$.*

Exemplo 3.2.3. *Considere o polinômio $f \in \mathbb{R}[x]$ tal que $f(x) = 2x + 1$. Observe que $f(x)$ é irredutível sobre $\mathbb{R}$, pois $f(x) = 2x + 1 = 2 \cdot \left(x + \frac{1}{2}\right)$.*

Exemplo 3.2.4. *Por sua vez, o polinômio $g(x) = x^2 + 1$ é redutível sobre $\mathbb{C}$, dado que $g(x) = x^2 + 1 = (x + i) \cdot (x - i)$. Entretanto $g(x)$ é irredutível sobre $\mathbb{R}$, pois:*

Se $g(x)$ fosse redutível sobre $\mathbb{R}$ teríamos:

$$g(x) = (x - a) \cdot (x - b) \text{ onde } a, b \in \mathbb{R}$$

$$x^2 + 1 = (x - a) \cdot (x - b)$$

$$x^2 + 1 = x^2 - xb - ax + ab$$

$$x^2 + 1 = x^2 - (a + b)x + ab$$

Por identidade de polinômios concluímos que $b^2 = -1$ que é um absurdo, pois $b \in \mathbb{R}$.

Portanto, $g(x)$ é irredutível sobre $\mathbb{R}$.

Proposição 3.2.1. *Todo polinômio de grau 1 é irredutível sobre um corpo $\mathbb{K}$.*

Demonstração. Seja $p \in K[x]$ um polinômio de grau 1. Sendo assim, considere $p(x) = a_0 + a_1x$, $a_1 \neq 0$. Por sua vez, $p(x) = a_1 \cdot \left(\frac{a_0}{a_1} + x\right)$, o que prova a tese. □

Por meio dos exemplos anteriores vimos que nem sempre é simples descobrir se um polinômio é irredutível sobre um corpo. Em razão disto, a seguir apresentaremos um critério para decidir se um polinômio com coeficientes inteiros é irredutível sobre corpo $\mathbb{Q}$.

Lema 3.2.1. *(Lema de Gauss) Seja $p \in \mathbb{Z}[x]$ tal que $p(x)$ seja irredutível sobre $\mathbb{Z}$ então $p(x)$ é irredutível sobre $\mathbb{Q}$.*

[1] Note que, $\mathbb{K}$ também poderia ser um domínio de integridade.
[2] Uma forma equivalente, é dizer que um dos polinômios é inversível.

Demonstração. Consultar Gonçalves (1999, p. 82). □

Teorema 3.2.3. *(Critério de Eisenstein) Seja* $f(x) = a_0 + a_1x + a_2x^2 + ... + a_nx^n$ *um polinômio em* $\mathbb{Z}[x]$*.*

Suponhamos que exista um primo p *tal que:*

(i) $p \nmid a_n$

(ii) $p|a_0, a_1, a_2, ..., a_{n-1}$

(iii) $p^2 \nmid a_0$

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

Demonstração. Para mostrar que $f(x)$ é irredutível sobre $\mathbb{Q}$ pelo Lema 3.2.1 é suficiente provar que $f(x)$ é irredutível sobre $\mathbb{Z}$.

Sendo assim, suponhamos por absurdo que $f(x)$ seja redutível sobre $\mathbb{Z}$. Dessa forma, seja $f(x) = g(x) \cdot h(x)$ onde $g, h \in \mathbb{Z}[x]$ e $1 \leq \partial(g(x)) < \partial(f(x)) = n$ e $1 \leq \partial(h(x)) < \partial(f(x))$. Considere $g(x) = b_0+b_1x+b_2x^2+...+b_rx^r$ e $h(x) = c_0+c_1x+, ..., +c_sx^s$ logo $n = r + s$.

Como $f(x) = g(x) \cdot h(x)$ da Definição 3.2.1 resulta que o coeficente a_0 de $f(x)$ é igual a $a_0 = b_0 \cdot c_0$. Por hipótese , $p|a_0$, logo $p|(b_0 \cdot c_0)$ então pelo Lema 2.4.1 temos que $p|b_0$ ou $p|c_0$. Entretanto, como $p^2 \nmid a_0$ segue que p divide apenas um dos inteiros, pois se $p|b_0$ e $p|c_0$ obteríamos:

$$b_0 = p \cdot k \text{ e } c_0 = p \cdot q$$

onde $k, q \in \mathbb{Z}$ resulta que $b_0 \cdot c_0 = p^2 \cdot (kq)$, o que contradiz a hipótese de que $p^2 \nmid a_0$. Portanto, sem perda de generalidade, considere que $p|b_0$ e $p \nmid c_0$.

Novamente pela Definição 3.2.1 obtemos:

$$a_1 = b_0 \cdot c_1 + b_1 \cdot c_0.$$

Como $p|b_0$, $p|a_1$ segue que $b_0 = k \cdot p$ e $a_1 = d \cdot p$, $d, k \in \mathbb{Z}$, deste modo temos:

$$p \cdot d = p \cdot (k \cdot c_1) + b_1 \cdot c_0.$$

Portanto, $b_1 \cdot c_0 = p \cdot (c - k \cdot c_1)$ o que implica que $p|(b_1 \cdot c_0)$, logo como $p \nmid c_0$ pelo Lema 2.4.1 concluímos que $p|b_1$.

Ainda pela Definição 3.2.1 temos que:

$$a_2 = b_0 \cdot c_2 + b_1 \cdot c_1 + b_2 \cdot c_0$$

Por sua vez, como $p|b_0$, $p|a_2$, $p|b_1$ e $p \nmid c_0$, segue pelo Lema 2.4.1 que $p|b_2$. Portanto, suponhamos que p divida todos os coeficientes de $g(x)$ de índice $3 \leq i \leq r-1$. Logo, como $p|a_{r-1}$, $p|(b_0, b_1, ..., b_{r-1})$, $p \nmid c_0$ com raciocínio semelhante aos casos de b_1 e b_2 concluímos pelo Lema 2.4.1 que $p|b_r$.

Da Definição 3.2.1 vem que $a_n = b_r \cdot c_s$, e como $p|b_r$ resulta que $p|a_n$ que é um absurdo, pois $p \nmid a_n$ por hipótese. Logo, $f(x)$ é irredutível sobre $\mathbb{Z}$.

Assim, pelo Lema 3.2.1, concluímos que $f(x)$ é irredutível sobre $\mathbb{Q}$. □

Exemplo 3.2.5. *Considere o polinômio $f \in \mathbb{Z}[x]$ tal que $p(x) = x^2 + 2x + 2$.*

Tomando $p = 2$, obtemos que $2 \nmid 1$, $2|2$ e $2^2 \nmid 2$. Portanto, segue do Teorema 3.2.3 que $f(x)$ é irredutível sobre $\mathbb{Q}$.

Exemplo 3.2.6. *Por outro lado, nem sempre é possível aplicar o critério de Eisenstein diretamente. Existem polinômios que são irredutíveis sobre $\mathbb{Q}$, mas ao primeiro momento não satisfazem o critério. Como por exemplo o polinômio $q \in \mathbb{Z}[x]$ tal que $q(x) = 3x^2 + 2x + 1$. Veja.*

Tomando $p = 2$, obtemos que $2 \nmid 3$. Entretanto, $2 \nmid 1$ o que não satisfaz a condição (ii) do Teorema. Agora, tomando $p = 3$, temos $3|3$ o que contradiz a condição (i) do critério. Portanto, observando os casos possíveis vemos que q não satisfaz o critério de Eisenstein de forma direta. A proposição a seguir nos auxiliará neste problema.

Proposição 3.2.2. *Seja $p(x) = a_0 + a_1x + ... + a_nx^n$ um polinômio em $\mathbb{K}[x]$ tal que $\mathbb{K}$ seja um corpo. Assim, p é irredutível sobre $\mathbb{K}$ se e somente, se $p(x + a) = a_0 + a_1(x + a) + ... + a_n(x + a)^n$ é irredutível sobre $\mathbb{K}$, para algum $a \in \mathbb{K}$.*

Demonstração. Para demonstrar, vamos considerar a aplicação $f : \mathbb{K}[x] \to \mathbb{K}[x]$, tal que $f(p(x)) = p(x + a)$. Provaremos que f é um isomorfismo. Para isso temos que mostrar que f é bijetiva e f é um homomorfismo de anéis. Sejam $p, q \in \mathbb{K}[x]$, primeiramente mostraremos que f é um homomorfismo de anéis. Assim, $\forall\ x \in \mathbb{K}$ temos:

- $f(p(x)+q(x)) = f((p+q)(x)) = (p+q)(x+a) = p(x+a)+q(x+a) = f(p(x))+f(q(x))$.
- $f(p(x) \cdot q(x)) = f((p \cdot q)(x)) = (p \cdot q)(x + a) = p(x + a) \cdot q(x + a) = f(p(x)) \cdot f(q(x))$.

Portanto, f é um homomorfismo. Agora basta mostrar que f é bijetiva. Do Lema 2.3.1 temos que se f é um homomorfismo segue que f é injetiva se somente se $N(f) = 0_{\mathbb{K}}$. Dessa forma, considere $p \in N(f)$ tal que $p(x) = a_0 + a_1x + ... + a_nx^n$, assim temos que $f(p(x)) = p(x + a) = a_0 + a_1(x + a) + ... + a_n(x + n)^n$, logo se $p \in N(f)$ resulta que $f(p(x)) = p(x+a) = 0_{\mathbb{K}}$. Deste modo, temos $p(x+a) = a_0+a_1(x+a)+...+a_n(x+a)x^n =$

$0_{\mathbb{K}} + 0_{\mathbb{K}}(x+a) + ... + 0_{\mathbb{K}}(x+a)^n$ o que implica, que $a_0 = a_1 = ...a_n = 0_{\mathbb{K}}$. Portanto, f é injetiva. Agora mostraremos que f é sobrejetiva. Veja que $\forall\ p \in \mathbb{K}[x]$ (contradomínio), $\exists\ p(x-a) \in \mathbb{K}[x]$ (domínio) tal que $f(p(x-a)) = p(x)$. De fato, temos que $p(x-a) = a_0 + a_1(x-a) + ... + a_n(x-a)x^n$, logo $f(p(x-a)) = a_0 + a_1(x-a+a) + ... + a_n(x-a+a)^n = a_0 + a_1x + ... + a_nx^n = p(x)$. Isto prova que f é sobrejetiva. Por conseguinte, temos que f é um isomorfismo. Perceba que, se f é um isomorfismo, operar com $p(x+a)$ é essencialmente operar com $p(x)$. Assim, $p(x)$ é irredutível sobre $\mathbb{K}$ se e somente se $p(x+a)$ é irredutível sobre $\mathbb{K}$.

□

Exemplo 3.2.7. *De volta ao Exemplo 3.2.6 com o polinômio* $p(x) = 3x^2 + 2x + 1$*. Aplicando a transformação vista na Proposição anterior para* $a = 1$*, teremos o polinômio* $p(x+1) = 3x^2 + 8x + 6$*. Assim, considerando o primo* $p = 2$*, temos que* $p(x+1)$ *é irredutível em* $\mathbb{Q}$ *pelo critério de Eisenstein. Portanto, pela Proposição 3.2.2 temos que* $p(x)$ *é irredutível sobre* $\mathbb{Q}$*.*

4 Noções Básicas de Extensões de Corpos

Neste capítulo, vamos abordar os conceitos básicos de extensão de corpos tais como, números algébricos, números transcedentes, extensão algébrica e grau de uma extensão. Os conceitos aqui abordados vão ser de grande relevância para as demonstrações das impossilidades clássicas, em especial o Teorema 4.4.2 que é essencial para as provas. Para composição deste capítulo utilizamos o livro e as dissertações de Gonçalves (1999), Santos (2017), Silva (2013b) e Biazzi (2014) respectivamente.

Definição 4.1. *Sejam $\mathbb{E}$ um corpo e $\mathbb{K}$ um subcorpo de $\mathbb{E}$. Nessas condições, denominamos o corpo $\mathbb{E}$ como uma extensão do corpo $\mathbb{K}$.*

Exemplo 4.1. *$\mathbb{R}$ é uma extensão de $\mathbb{Q}$, pois $\mathbb{Q} \subset \mathbb{R}$ e $\mathbb{Q}$ é um subcorpo de $\mathbb{R}$.*

Neste capítulo em diante vamos denominar o corpo $\mathbb{E}$ como uma extensão do corpo $\mathbb{K}$.

4.1 Números algébricos e transcedentes

Definição 4.2. *Dizemos que um elemento $\alpha \in \mathbb{E}$ é algébrico sobre $\mathbb{K}$ se existir um polinômio não nulo $p \in \mathbb{K}[x]$ tal que $p(\alpha) = 0_{\mathbb{K}}$, isto é, se α satisfaz a equação polinomial:*

$$a_0 + a_1\alpha + ... + a_n\alpha^n = 0_{\mathbb{K}}$$

com coeficientes em $\mathbb{K}$ e nem todos nulos. Se $\mathbb{K}$ é um subcorpo de $\mathbb{E}$ e todo elemento de $\mathbb{E}$ é algébrico sobre $\mathbb{K}$, dizemos que $\mathbb{E}$ é uma extensão algébrica sobre $\mathbb{K}$.

Caso α não seja algébrico sobre $\mathbb{K}$, α é chamado transcedente sobre $\mathbb{K}$.

Exemplo 4.1.1. *$\sqrt[3]{2}$ é um elemento algébrico sobre $\mathbb{Q}$, pois $\sqrt[3]{2} \in \mathbb{R}$ e $\exists\, p \in \mathbb{Q}[x] - \{0\}$ dado por $p(x) = x^3 - 2$ tal que $p(\sqrt[3]{2}) = 0$.*

Exemplo 4.1.2. *Por outro lado, os números e e π são elementos trascendentes sobre $\mathbb{Q}$, pois $\nexists\, p \in \mathbb{Q}[x] - \{0\}$ tal que $p(e) = 0$ ou $p(\pi) = 0$.*

Para a consulta das demonstrações da transcendencia de π e de e indicamos Jones Sidney A. Morris (1991, p. 115).

Observa-se do Exemplo 4.1.1 que o número $\sqrt[3]{2}$ é algébrico sobre $\mathbb{Q}$. Entretanto, podemos ir além e concluir que todos os números da forma $\sqrt[n]{2}$ para $2 \leq n$ são algébricos sobre $\mathbb{Q}$, considerando o polinômio $p(x) = x^n - 2$.

Proposição 4.1.1. *Se $\alpha \in \mathbb{K}$ então α é algébrico sobre $\mathbb{K}$.*

Demonstração. Consideremos $p \in \mathbb{K}[x] - \{0\}$ e $\alpha \in \mathbb{K}$ tal que $p(x) = x - \alpha$. Logo $p(\alpha) = \alpha - \alpha = 0_{\mathbb{K}}$. □

Exemplo 4.1.3. *Da Proposição 4.1.1 segue que todo corpo $\mathbb{K}$ é algébrico sobre si mesmo. Por exemplo, todo elemento de $\mathbb{R}$ é algébrico sobre $\mathbb{R}$.*

4.2 Polinômio Minimal

Definição 4.2.1. *Seja α algébrico sobre $\mathbb{K}$. O polinômio mônico de menor grau em $\mathbb{K}[x]$ tal que $p(\alpha) = 0$ é intitulado polinômio minimal de α em $\mathbb{K}$.*

Exemplo 4.2.1. *O polinômio $p(x) = x - 2 \in \mathbb{Q}[x]$ é o polinômio minimal de 2 em $\mathbb{Q}$.*

Proposição 4.2.1. *Todo polinômio minimal em $\mathbb{K}[x]$ é irredutível sobre $\mathbb{K}$.*

Demonstração. Seja $p \in \mathbb{K}[x]$ um polinômio minimal de α em $\mathbb{K}$. Suponhamos, por absurdo, que p é redútível sobre $\mathbb{K}$, logo $\exists\ g, h \in \mathbb{K}[x]$ tal que $p(x) = g(x) \cdot h(x)$ e $\partial p(x) > \partial g(x) > 0$ e $\partial p(x) > \partial h(x) > 0$. Como p é um polinômio minimal de α em $\mathbb{K}$ temos que $p(\alpha) = 0_{\mathbb{K}}$, isto é, $0_{\mathbb{K}} = h(\alpha) \cdot g(\alpha)$. Dessa forma, $g(\alpha) = 0_{\mathbb{K}}$ ou $h(\alpha) = 0_{\mathbb{K}}$, contrariando o fato de que p tem grau mínimo entre os polinômios que anulam α. Portanto, $p(x)$ é irredutível sobre $\mathbb{K}$. □

Devido à irredutibilidade do polinômio minimal, a partir desta seção, o polinômio minimal de α em $\mathbb{K}$ será representado por $p(x) = irr(\alpha, \mathbb{K})$. Do Exemplo 4.2.1, temos que o polinômio minimal de 2 em $\mathbb{Q}$ pode ser escrito na forma: $p(x) = irr(2, \mathbb{Q})$.

4.3 O corpo $\mathbb{K}[\alpha]$

Considere $\alpha \in \mathbb{E}$, definimos $\mathbb{K}[\alpha] = \{f(\alpha) \mid f \in \mathbb{K}[x]\}$. Caso α seja algébrico sobre $\mathbb{K}$ o teorema a seguir permitirá provar que o conjunto $\mathbb{K}[\alpha]$ é um subcorpo de $\mathbb{E}$, onde $\mathbb{E}$ é uma extensão de $\mathbb{K}$.

Lema 4.3.1. *Sejam $\mathbb{E}$ uma extensão, α algébrico sobre $\mathbb{K}$ e $\partial(irr(\alpha, \mathbb{K})) = n$. Dessa forma, todo $f(\alpha) \in \mathbb{K}[\alpha]$ pode ser escrito de modo único na forma $f(\alpha) = a_0 + a_1\alpha + ... + a_{n-1}\alpha^{n-1}$.*

Demonstração. Sejam $p, f \in \mathbb{K}[x]$ e $\alpha \in \mathbb{E}$ algébrico sobre $\mathbb{K}$ tais que $f(\alpha) \in \mathbb{K}[\alpha]$, $p(x) = irr(\alpha, \mathbb{K})$ e $\partial(irr(\alpha, \mathbb{K})) = n$. Vamos provar inicialmente que $f(\alpha) = a_0 + a_1\alpha + ... + a_{n-1}\alpha^{n-1}$.

Pelo algoritmo da divisão temos que $\exists\ q, r \in \mathbb{K}[x]$ tais que:

$f(x) = p(x) \cdot q(x) + r(x)$, onde $r(x) = 0$ ou $\partial(r(x)) < \partial(p(x))$. Assim,

$$f(\alpha) = p(\alpha) \cdot q(\alpha) + r(\alpha).$$

Como $p(x) = irr(\alpha, \mathbb{K})$ segue que $p(\alpha) = 0_{\mathbb{K}}$, logo $f(\alpha) = r(\alpha)$. Dessa forma, considerando $r(x) = a_0 + a_1x + ... + a_{n-1}x^{n-1}$, temos que $r(\alpha) = a_0 + a_1\alpha + ... + a_{n-1}\alpha^{n-1}$, o que resulta que $f(\alpha) = a_0 + a_1\alpha + ... + a_{n-1}\alpha^{n-1}$. Agora, vamos mostrar a unicidade. Suponha que $f(\alpha) = a_0 + a_1\alpha + ... + a_{n-1}\alpha^{n-1} = b_0 + b_1\alpha + ... + b_{n-1}\alpha^{n-1}$, $a_i, b_i \in \mathbb{K}$, $\forall\, i \in \{0, ..., n-1\}$. Dessa forma, temos:

$$a_0 + a_1\alpha + ... + a_{n-1}\alpha^{n-1} = b_0 + b_1\alpha + ... + b_{n-1}\alpha^{n-1}, \text{ o que resulta que}$$
$$(a_0 - b_0) + (a_1 - b_1)\alpha + ... + (a_{n-1} - b_{n-1})\alpha^{n-1} = 0_{\mathbb{K}}.$$

Assim, considere $q \in \mathbb{K}[x]$ tal que $q(x) = (a_0 - b_0) + (a_1 - b_1)x + ... + (a_{n-1} - b_{n-1})x^{n-1}$. Como $q(\alpha) = 0_{\mathbb{K}}$ e $\partial(q(x)) < n = \partial(irr(\alpha, \mathbb{K}))$, contrariando a minimalidade do grau do polinômio p, assim segue que $q(x) = 0_{\mathbb{K}}$, logo $a_i = b_i\ \forall i$. Portanto, $f(\alpha) \in \mathbb{K}[\alpha]$ pode ser escrito de modo único na forma $f(\alpha) = a_0 + a_1\alpha + ... + a_{n-1}\alpha^{n-1}$.

□

Teorema 4.3.1. *Sejam $\theta \in \mathbb{E}$, $\mathbb{E}$ é uma extensão do corpo $\mathbb{K}$ e se $f : \mathbb{K}[x] \to \mathbb{E}$ definida por $f(p(x)) = p(\theta)$ é um homomorfismos de anéis, então:*

(i) $Imf = \mathbb{K}[\theta]$.

(ii) Se θ é algébrico sobre $\mathbb{K}$ e $p(x) = irr(\theta, \mathbb{K})$ então $N(f)$ é um ideal maximal de $\mathbb{K}[x]$.

(iii) $\mathbb{K}[x]/N(f)$ é isomorfo a $\mathbb{K}[\theta]$.

Demonstração. (i) Seja o conjunto $Imf = \{f(p(x)) \mid p \in \mathbb{K}[x]\}$. Como $f(p(x)) = p(\theta) \in Imf$ e $p(\theta) \in \mathbb{K}[\theta]$, logo $Imf \subset \mathbb{K}[\theta]$. Se $p(\theta) \in \mathbb{K}[\theta]$ então $\exists\ p \in \mathbb{K}[x]$ tal que $f(p(x)) = p(\theta)$, assim $p(\theta) \in Imf$. Portanto, concluímos que $Imf = \mathbb{K}[\theta]$.

(ii) Como θ é algébrico sobre $\mathbb{K}$ segue que $p(\theta) = 0_{\mathbb{E}}$ e $p(x) = irr(\theta, \mathbb{K})$. Deste modo, como $f(p(x)) = p(\theta)$, temos que $p \in N(f)$. Assim, como $N(f)$ é um ideal de $\mathbb{K}[x]$ (Pelo Lema 2.3.1), podemos escrever $N(f)$ da seguinte forma:

$$N(f) = \{q(x) \cdot p(x) \mid q(x) \in K[x],\ p(x) = irr(\theta, \mathbb{K})\}.$$

Dado que $N(f)$ é um ideal de $K[x]$, então basta mostrar que $N(f)$ é um ideal maximal de $\mathbb{K}[x]$, ou seja, devemos provar que se $J \supset N(f)$ é um ideal de $\mathbb{K}[x]$ então $J = \mathbb{K}[x]$ ou $J = N(f)$.

Seja J um ideal de $\mathbb{K}[x]$ tal que $J \supset N(f)$. Do Teorema 3.2.2, temos que todo ideal de $\mathbb{K}[x]$ é principal, logo $J = \mathbb{K}[x] \cdot h(x)$. Sendo assim, como $N(f) \subset J$ e $irr(\theta, \mathbb{K}) = p(x) \in N(f)$, segue que p é da forma $p(x) = g(x) \cdot h(x)$, $g \in \mathbb{K}[x]$. Pelo Teorema 4.2.1 temos que $p(x)$ é irredutível sobre $\mathbb{K}$, logo como $p(x) = g(x) \cdot h(x)$, segue que $g(x) = a, a \in (\mathbb{K} - \{0_{\mathbb{K}}\})$ ou $h(x) = b, b \in (\mathbb{K} - \{0_{\mathbb{K}}\})$. Tomemos $g(x) = a$, sendo assim temos que $h(x) = a^{-1} \cdot p(x)$, o que resulta que $h \in N(f) = \mathbb{K}[x] \cdot p(x)$ e como $h \in J$, vem que $J \subset N(f)$. Portanto, como $N(f) \subset J$ e $J \subset N(f)$, segue que $J = N(f)$. Por fim, concluímos que $N(f)$ é um ideal maximal.

(iii) Do Lema 2.3.1, obtemos que $\mathbb{K}[x]/N(f)$ é isomorfo a Imf. E ainda, por sua vez, de (i), segue $Imf = K[\theta]$. Portanto, $\mathbb{K}[x]/N(f)$ é isomorfo a $K[\theta]$.

□

Agora, com os resultados obtidos no Teorema acima e pelo Teorema 2.3.1, podemos concluir que $K[\theta]$ é um corpo. De fato, como $N(f)$ é um ideal maximal de $\mathbb{K}[x]$, segue do Teorema 2.3.1 que $\mathbb{K}[x]/N(f)$ é um corpo e ainda $\mathbb{K}[x]/N(f)$ é isomorfo a $\mathbb{K}[\theta]$, logo $\mathbb{K}[\theta]$ é um corpo. Por sua vez, como $\mathbb{K}[\theta] \subset \mathbb{E}$ e $\mathbb{K}[\theta]$ é um corpo fechado para as operações de $\mathbb{E}$, assim, segue $\mathbb{K}[\theta]$ é um subcorpo de $\mathbb{E}$. Da mesma forma $\mathbb{K}$ também é um subcorpo de $\mathbb{K}[\theta]$, pois $\mathbb{K} \subset \mathbb{K}[\theta]$ e $\mathbb{K}$ é um corpo fechado para as operações de $\mathbb{K}[\theta]$. Portanto, da Definição 4.1 concluímos que $\mathbb{E}$ é uma extensão de $\mathbb{K}[\theta]$ e $\mathbb{K}[\theta]$ é uma extensão de $\mathbb{K}$.

O corpo $\mathbb{K}[\theta]$, também pode ser utilizado para obter mais extensões como segue os exemplos abaixo.

Exemplo 4.3.1. *O conjunto* $\mathbb{R}\ [i] = \{a + bi \mid a, b \in \mathbb{R}\}$ *é uma extensão de* $\mathbb{R}$. *De fato, seja* $i \in \mathbb{C}$, *definimos:* $\mathbb{R}[i] = \{p(i) \mid p \in \mathbb{R}[x]\}$. *Como* $p \in \mathbb{R}[x]$ *segue, do algoritmo da divisão, que:*

$$p(x) = g(x) \cdot q(x) + r(x), \text{ onde } \partial(r(x)) < \partial(g(x)).$$

Dessa forma, considere $g(x) = x^2 + 1$ *e* $r(x) = bx + a$, *logo* $p(x) = (x^2 + 1) \cdot q(x) + bx + a$. *Portanto,* $p(i) = a + bi$, *o que resulta no conjunto* $\mathbb{R}\ [i] = \{a + bi \mid a, b \in \mathbb{R}\}$. *Note que, o conjunto* $\mathbb{R}[i] = \mathbb{C}$.

Exemplo 4.3.2. *De forma similar ao exemplo anterior podemos obter o conjunto* $\mathbb{Q}[\sqrt{2}] = \left\{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\right\}$ *como uma extensão de* $\mathbb{Q}$. *Veja.*
Considere o conjunto $\mathbb{Q}[\sqrt{2}] = \left\{p(\sqrt{2}) \mid p \in \mathbb{Q}[x]\right\}$. *Analogamente ao exemplo anterior, tomando* $g(x) = (x^2 - 2)$ *e* $r(x) = bx + a$, *temos pelo Algoritmo da Divisão que* $p(\sqrt{2}) = a + b\sqrt{2}$, *logo* $\mathbb{Q}[\sqrt{2}] = \left\{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\right\}$.

4.4 Grau de uma Extensão

Nesta seção, vamos utilizar conceitos básicos de Álgebra Linear, tais como espaço vertorial, subespaço, dependência linear, base e dimensão. Devido ao escopo do trabalho, as noções de Álgebra Linear estão postas de maneira superficial, iremos enunciar somente alguns resultados que serão necessários para continuidade do trabalho. Para mais informações sobre os conceitos de Álgebra Linear, indicamos Callioli, Domingues e Costa (1990) e Santos (2010).

Definição 4.4.1. *Sejam $\mathbb{K}$ um corpo e V um conjunto não vazio no qual estão definidas as operações de adição e de multiplicação por escalar:*

$$+: \begin{array}{c} V \times V \to V \\ (u,v) \mapsto u+v \end{array} \quad \textit{e} \quad \cdot: \begin{array}{c} \mathbb{K} \times V \to V \\ (\alpha,u) \mapsto \alpha \cdot u \end{array}$$

O conjunto V, munido dessas duas operações, é um espaço vetorial sobre $\mathbb{K}$ se forem satisfeitas as seguintes propriedades, para todo $u, v, w \in V$ e $\alpha, \beta \in \mathbb{K}$:

(i) $u + v = v + u$ ***(comutativa da adição)***

(ii) $(u + v) + w = u + (v + w)$ ***(associativa da adição)**.*

(iii) $\exists\ 0_V \in V$ *tal que* $u + 0_V = u$ ***(existência do elemento neutro aditivo)**.*

(iv) $\forall\ u \in V$, $\exists (-u) \in V$ *tal que* $u + (-u) = 0_V$ ***(existência do elemento oposto)**.*

(v) $\alpha \cdot (\beta \cdot u) = (\alpha \cdot \beta) \cdot u$ ***(associativa da multiplicação)**.*

(vi) $(\alpha + \beta) \cdot u = \alpha \cdot u + \beta \cdot u$ ***(distributiva I)**.*

(vii) $\alpha \cdot (u + v) = \alpha \cdot u + \alpha \cdot v$ ***(distributiva II)**.*

(viii) $\exists\ 1_{\mathbb{K}}$ *tal que* $1_{\mathbb{K}} \cdot v = v \cdot 1_{\mathbb{K}} = v$ ***(existência do elemento neutro multiplicativo)**.*

Definição 4.4.2. *Seja V um espaço vetorial sobre $\mathbb{K}$. Um subespaço vetorial de V é um subconjunto $W \subset V$ tal que:*

(i) $0_V \in W$.

(ii) $u + v \in W$, $\forall\ u, v \in W$.

(iii) $\alpha \cdot u \in W$, $\forall\ \alpha \in \mathbb{K}$ *e* $\forall\ u \in W$.

Proposição 4.4.1. *Todo subespaço vetorial é um espaço vetorial.*

Demonstração. Consultar Callioli, Domingues e Costa (1990, p. 54). □

Definição 4.4.3. *Seja V um espaço vetorial sobre $\mathbb{K}$. Dizemos que um conjunto $L = \{u_1, u_2, ..., u_n\} \subset V$ é linearmente independentente (L.I.) se, e somente se, uma igualdade do tipo*

$$\alpha_1 \cdot u_1 + ... + \alpha_n \cdot u_n = 0_V$$

com os $\alpha_i \in \mathbb{K}$, só for possível para $\alpha_1 = ... = \alpha_n = 0_{\mathbb{K}}$. Caso o conjunto L não seja (L.I.) dizemos que L é linearmente dependente (L.D.).

Definição 4.4.4. *Seja V um espaço vetorial sobre $\mathbb{K}$. Uma base de V é um subconjunto finito $B \subset V$, tal que $B = \{u_1, u_2, ..., u_n\}$ para o qual as seguintes condições se verificam:*

(i) B é L.I.

(ii) $\{\alpha_1 \cdot u_1 + \alpha_2 \cdot u_2 + ... + \alpha_n \cdot u_n \mid \alpha_1, ..., \alpha_n \in \mathbb{K}\} = V$.

Definição 4.4.5. *Seja V um espaço vetorial finitamente gerado. Denomina-se dimensão de V (notação: $dimV$) o número de elementos de uma base qualquer de V. Diz-se também, neste caso, que V é um espaço de dimensão finita.*

Proposição 4.4.2. *Todo espaço vetorial V possui uma base.*

Demonstração. Consultar Callioli, Domingues e Costa (1990, p. 77). □

Teorema 4.4.1. *(Teorema da Invariância) Seja V um espaço vetorial de dimensão n, então toda base de V possui n elementos.*

Demonstração. Consultar Callioli, Domingues e Costa (1990, p. 99). □

Proposição 4.4.3. *Seja V um espaço vetorial e $B \subset V$ tal que $B = \{a_1, ..., a_n\}$. Os elementos de V podem ser escritos como combinação linear dos elementos de B de modo único se e somente se B é uma base de V.*

Demonstração. Consultar Santos (2010, p. 70). □

Proposição 4.4.4. *Seja V um espaço vetorial e W um subespaço vetorial de V então $dim(W) \leq dim(V)$.*

Demonstração. Consultar Callioli, Domingues e Costa (1990, p. 79). □

De volta ao estudo de extensões, vamos definir o conceito de grau de uma extensão. Uma extensão $\mathbb{E}$, pode ser vista como um espaço vetorial sobre $\mathbb{K}$, com as seguintes operações:

$$+: \begin{array}{c} \mathbb{E}\times\mathbb{E}\to\mathbb{E} \\ (x,y)\mapsto x+y \end{array} \quad \text{e} \quad \cdot: \begin{array}{c} \mathbb{K}\times\mathbb{E}\to\mathbb{E} \\ (\alpha,x)\mapsto \alpha\cdot x \end{array}$$

Nesta perspectiva, temos como resultado que $\mathbb{K}[\alpha] \subset \mathbb{E}$ é um subespaço vetorial de $\mathbb{E}$, visto que dados $p, q \in \mathbb{K}[\alpha]$ e $\beta \in \mathbb{K}$, temos que $0_{\mathbb{E}} \in \mathbb{K}[\alpha]$, $p(\alpha) - q(\alpha) \in \mathbb{K}[\alpha]$ e $\beta \cdot p(\alpha) \in \mathbb{K}[\alpha]$.

Definição 4.4.6. *A dimensão do espaço vetorial formado pela extensão é denominada grau da extensão. Simbolicamente o grau de uma extensão é representado por:* $[\mathbb{E} : \mathbb{K}]$.

Exemplo 4.4.1. $\mathbb{C} \supset \mathbb{R}$ *é uma extensão de* $\mathbb{R}$*, cuja dimensão é* 2*. Veja: sabendo que, se* $z \in \mathbb{C}$*, segue que* $z = a + bi$*,* $a, b \in \mathbb{R}$*. Com isso podemos considerar o conjunto* $B = \{1, i\}$ *linearmente independente como base de* $\mathbb{C}$*. Logo, concluímos que* $[\mathbb{C} : \mathbb{R}] = 2$.

Exemplo 4.4.2. *Da mesma forma, podemos obter a o grau da extensão de* $\mathbb{Q}$*, o corpo* $\mathbb{Q}[\sqrt{2}]$*. Seja* $z \in \mathbb{Q}[\sqrt{2}]$ *tal que* $z = a + b \cdot \sqrt{2}$*,* $a, b \in \mathbb{Q}$*. Sendo assim, considere o conjunto* $B = \left\{1, \sqrt{2}\right\}$ *linearmente independente como base de* $\mathbb{Q}[\sqrt{2}]$*. Logo* $[\mathbb{Q}[\sqrt{2}] : \mathbb{Q}] = 2$.

Definição 4.4.7. *Se o grau de uma extensão* $\mathbb{E}$ *é finito, então esta é intitulada uma extensão finita. Caso contrário, a extensão é dita infinita.*

Exemplo 4.4.3. *Os dois exemplos anteriores são exemplos de extensões finitas.*

Voltando ao propósito do nosso trabalho, o resultado a seguir é a primeira proposição essencial para a prova das impossibilidades dos três problemas clássicos, em especial, o item (i).

Teorema 4.4.2. *Sejam* $\mathbb{K}$ *um corpo e* $\mathbb{E}$ *uma extensão de* $\mathbb{K}$*, então*

(i) Se α *é um elemento algébrico sobre* K *e* $\partial(irr(\alpha, K)) = n$*, então* $1, \alpha, ..., \alpha^{n-1}$ *é uma base do espaço vetorial* $\mathbb{K}[\alpha]$ *sobre* $\mathbb{K}$ *e* $[\mathbb{K}[\alpha] : \mathbb{K}] = n$.

(ii) Se $\mathbb{E}$ *é uma extensão finita então* $\mathbb{E}$ *é algébrica.*

(i) *Demonstração.* Do Lema 4.3.1 temos que todo $p \in K[\alpha]$ pode ser escrito de modo único da seguinte forma: $p(\alpha) = a_0 + a_1\alpha + ... + a_{n-1}\alpha^{n-1}$. Note que $p(\alpha)$ está escrito de maneira única como combinição linear dos elementos do conjunto $\left\{1, \alpha, ..., \alpha^{n-1}\right\}$, sendo assim pela Proposição 4.4.3 o conjunto $\left\{1, \alpha, ..., \alpha^{n-1}\right\}$ forma uma base de $\mathbb{K}[\alpha]$, segue assim que $[\mathbb{K}[\alpha] : \mathbb{K}] = n$. □

(ii) *Demonstração.* Como $\mathbb{E}$ é finita, $\exists\ n \in \mathbb{N}$ tal que $[\mathbb{E} : \mathbb{K}] = n$. Por sua vez, seja $\alpha \in \mathbb{E}$, assim $\mathbb{K}[\alpha]$ é um subespaço vetorial sobre $\mathbb{E}$ então pela Proposição 4.4.4 temos que $dim(\mathbb{K}[\alpha]) < dim(\mathbb{E})$ e $\mathbb{K} \subset \mathbb{K}[\alpha]$ o que implica que $[\mathbb{K}[\alpha] : \mathbb{K}] = m < n$. Dessa forma, como a dimensão de $\mathbb{K}[\alpha]$ é m, então pela Proposição 4.4.2 temos que $\exists\ V \subset \mathbb{K}[\alpha]$, tal que $V = \left\{1, \alpha, ..., \alpha^{m-1}\right\}$, de tal forma que V seja base de $\mathbb{K}[\alpha]$ e assim, por consequência, V é L.I.. Segue então que o conjunto $W \subset \mathbb{K}[\alpha]$, onde $W = \left\{1, \alpha, ..., \alpha^{m-1}, \alpha^m\right\}$ é (L.D.), pois W possui $m+1$ elementos e a dimensão de $\mathbb{K}[\alpha] = m$. Portanto, segue do Teorema da Invariância que o número máximo de elementos dos conjuntos linearmente independentes de $\mathbb{K}[\alpha]$ é m. Assim, temos que $a_0 + a_1\alpha + a_2\alpha^2 + ... + a_m\alpha^m = p(\alpha) = 0_{\mathbb{K}}$ com $a_i \in \mathbb{K}$ nem todos nulos, o que resulta que α é algébrico $\mathbb{K}$. □

Veja que com os resultados obtidos no teorema anterior, é possível verificar se as extensões são finitas ou infinitas.

Exemplo 4.4.4. *Considere $\mathbb{R}$ uma extensão de $\mathbb{Q}$. Seja a contrapositiva do item (i) dada por "Se $\mathbb{E}$ não é algébrica então $\mathbb{E}$ é infinita". Dessa forma, como $\pi \in \mathbb{R}$ é transcedente sobre $\mathbb{Q}$, temos pelo Teorema 4.4.2 que $\mathbb{R}$ sobre $\mathbb{Q}$ é um extensão infinita.*

Os resultado a seguir será importante para a demonstração do Teorema 5.3.4 que é o segundo teorema essencial para as provas das impossibilidades clássicas.

Proposição 4.4.5. *Sejam $\mathbb{L} \supset \mathbb{E} \supset \mathbb{K}$ corpos tais que $[\mathbb{L} : \mathbb{E}]$ e $[\mathbb{E} : \mathbb{K}]$ são finitos então $[\mathbb{L} : \mathbb{K}]$ é finito e:*

$$[\mathbb{L} : \mathbb{K}] = [\mathbb{L} : \mathbb{E}] \cdot [\mathbb{E} : \mathbb{K}].$$

Demonstração. Suponhamos que $\{\alpha_1, \alpha_2, ..., \alpha_m\}$ e $\{\beta_1, \beta_2, ..., \beta_n\}$ sejam bases de $\mathbb{L}$ sobre $\mathbb{E}$ e de $\mathbb{E}$ sobre $\mathbb{K}$, respectivamente. Dessa forma, $[\mathbb{L} : \mathbb{E}] = m$ e $[\mathbb{E} : \mathbb{K}] = n$. Assim, queremos provar que $[\mathbb{L} : \mathbb{K}] = m \cdot n$, ou seja, provaremos que o conjunto $\{\alpha_i \cdot \beta_j\}$ é L.I. e gera o corpo $\mathbb{L}$ para $1 \leq i \leq m$ e $1 \leq j \leq n$. Para isso, considere a equação:

$$\sum_{i,j}(\lambda_{i,j} \cdot \alpha_i \cdot \beta_j) = 0_{\mathbb{L}}, \text{ onde } \lambda_{i,j} \in \mathbb{K} \text{ e } 1 \leq i \leq m \text{ e } 1 \leq j \leq n.$$

Dessa forma, desenvolvendo a somatória temos:

$$(\lambda_{1,1}\alpha_1\beta_1 + \lambda_{1,2}\alpha_1\beta_2 + ... + \lambda_{1,n}\alpha_1\beta_n) + ... + (\lambda_{m,1}\alpha_m\beta_1 + ... + \lambda_{m,n}\alpha_m\beta_n) = 0_{\mathbb{L}}$$

Assim, podemos reescrever a equação do seguinte modo:

$$\alpha_1(\lambda_{1,1}\beta_1 + ... + \lambda_{1,n}\beta_n) + \alpha_2(\lambda_{2,1}\beta_1 + ... + \lambda_{2,n}\beta_n) + ... + \alpha_m(\lambda_{m,1}\beta_1 + ... + \lambda_{m,n}\beta_n) = 0_{\mathbb{L}}$$

Como $\{\alpha_1, ..., \alpha_m\}$ é um base do espaço vetorial de $\mathbb{L}$ sobre $\mathbb{E}$ segue que o conjunto $\{\alpha_1, ..., \alpha_m\}$ é L.I.. Portanto,

$$\lambda_{1,1}\beta_1 + ... + \lambda_{1,n}\beta_n = 0_{\mathbb{E}}$$
$$.$$
$$.$$
$$.$$
$$\lambda_{m,1}\beta_1 + ... + \lambda_{m,n}\beta_n = 0_{\mathbb{E}}$$

Assim, como o conjunto $\{\beta_1, \beta_2, ..., \beta_n\}$ é base do espaço vetorial de $\mathbb{E}$ sobre $\mathbb{K}$ resulta que cada $\lambda_{i,j} = 0_{\mathbb{K}}$. Portanto, o conjunto $\{\alpha_i \cdot \beta_j\}$ é L.I.. Agora, basta mostrar que $\{\alpha_i \cdot \beta_j\}$ gera $\mathbb{L}$. Inicialmente temos que $\{\alpha_1, ..., \alpha_m\}$ é uma base do espaço vetorial do espaço vetorial $\mathbb{L}$ sobre $\mathbb{E}$, logo $\forall\ \alpha \in \mathbb{L}$ temos:

$$\alpha = \lambda_1\alpha_1 + ... + \lambda_m\alpha_m = \sum_{i=1}^{m} \lambda_i\alpha_i \text{ onde } \lambda_i \in \mathbb{E}, \forall\ i.$$

E ainda, como cada $\lambda \in \mathbb{E}$ e $\{\beta_1, \beta_2, ..., \beta_n\}$ é uma base do espaço vetorial $\mathbb{E}$ sobre $\mathbb{K}$. Podemos escrever cada λ_i como combinação linear dos elementos da base. Assim, $\exists a_{i,j} \in \mathbb{K}$ tais que:

$$\lambda_1 = \sum_{j=1}^{n} a_{1,j}\beta_j,\ \lambda_2 = \sum_{j=1}^{n} a_{2,j}\beta_j,\ ...,\ \lambda_m = \sum_{j=1}^{n} a_{m,j}\beta_j$$

Agora, substituindo cada λ_i na primeira equação temos que:

$$\alpha = \sum_{i}^{m} a_{i,j}\beta_j\alpha_i, \text{ onde cada } a_{i,j} \in \mathbb{K}.$$

Portanto, o conjunto $\{\alpha_i \cdot \beta_j\}$ L. I e gera o corpo $\mathbb{L}$. Desta forma, $\{\alpha_i \cdot \beta_j\}$ é uma base do espaço vetorial $\mathbb{L}$ sobre $\mathbb{K}$ de dimensão $n \cdot m$. Por fim, $[\mathbb{L} : \mathbb{K}] = m \cdot n = [\mathbb{L} : \mathbb{E}] \cdot [\mathbb{E} : \mathbb{K}]$ □

5 Números Construtíveis: Construções com régua e compasso e Extensões de Corpos

Neste capítulo, vamos utilizar todo conhecimento algébrico visto até esta etapa do trabalho e relacionaremos essas definições à geometria euclidiana. Para corporificar esta relação é preciso estudar as construções com régua não graduada e compasso e os números contrutíveis para assim podermos avaliar os enunciados dos problemas clássicos com mais cuidado e demonstrar as impossiblidades. Para composição deste capítulo foram utilizados os seguintes materiais: Biazzi (2014), Jones Sidney A. Morris (1991) Santos (2017) e Guerra (2012).

As construções com régua e compasso obedeciam rigorosas regras, definidas pelos antigos geômetras gregos, que deveriam ser seguidas em todas as construções. Em cada construção era considerado um conjunto de pontos iniciais que definimos da seguinte forma:

$$P = \{P_0, P_1, ..., P_m\}.$$

Nas construções tinha-se que circunferências e retas também poderiam ser dadas e a inclusão de novos pontos (adicionados ao conjunto inicial P) e outros objetos geométricos não poderiam ser adicionados de forma aleatória na construção. Existia um conjunto de operações com régua (não graduada) e compasso permitidas para este fim, as chamadas operações elementares com régua e compasso, as quais definiremos a seguir.

Definição 5.1. *Regras de Construções*

(i) Dados dois pontos, podemos traçar uma reta que passa pelos dois pontos e prolongá-la até o infinito nas duas direções.

(ii) Dados dois pontos, podemos traçar o segmento de reta que une os dois pontos.

(iii) Dado um ponto e um segmento de reta, podemos traçar a circunferência com centro nesse ponto e raio igual ao comprimento do segmento de reta.

As construções eram as mais diversas, desde a construção de reta paralelas à construção de segmentos proporcionais. Na próxima seção, vamos apresentar algumas construções elementares com régua e compasso.

5.1 Construções elementares

Nesta seção vamos exibir algumas contruções elementares com régua e compasso e enunciar o Teorema de Tales.

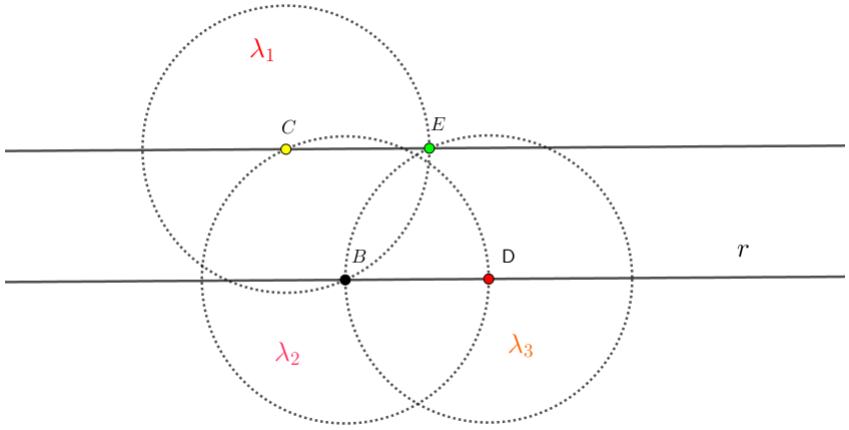
5.1.1 Construção de retas paralelas

Dada uma reta r e um ponto C fora de r, construir uma reta[1] paralela a r que passa por C.

Etapas de Construção.

Seja r uma reta e C um ponto fora de C. Considere um ponto B na reta r e trace uma circunferência λ_1 de centro em C e raio CB. Com o mesmo raio CB trace uma circunferência λ_2 com centro em B. Seja D um ponto de interseção de λ_2 com a reta r. Em seguida, trace uma circuferência λ_3 de centro em D e raio BD, obtendo o ponto E como a interseção da circunferências λ_1 e λ_3. Por fim, trace a reta que passa pelos pontos C e E que é paralela a r.

Figura 1 – Construção de retas paralelas.



Fonte: Autor.

Justificativa

Para justificar a construção note que as circunferências $\lambda_1, \lambda_2, \lambda_3$ possuem o mesmo raio, assim os segmentos $\overline{CE}$, $\overline{BD}$, $\overline{BC}$ e $\overline{ED}$ possuem a mesma medida, logo o quadrilátero $CBDE$ é um losango, o que implica que $\overline{CE}$ é paralelo à $\overline{BD}$.

[1] Duas retas são paralelas se a interseção entre elas é vazia ou são a mesma reta.

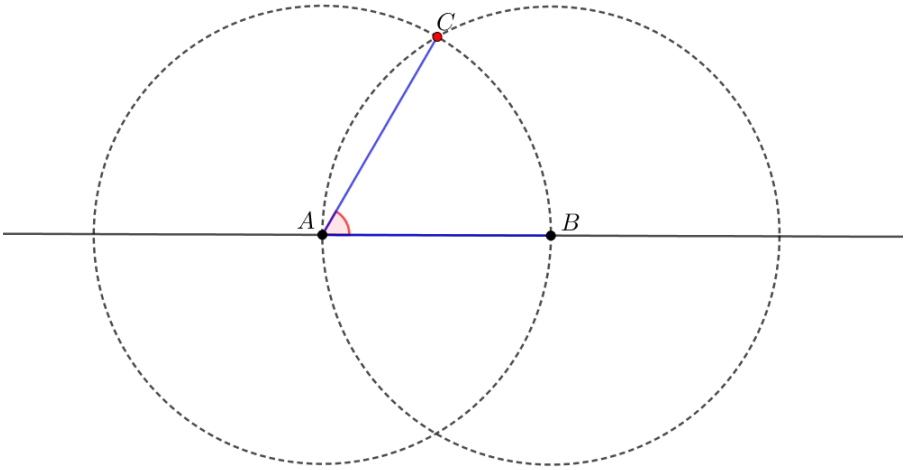
5.1.2 Construção do ângulo de 60 graus

Dada uma reta r e um segmento $\overline{AB}$ sobre r, construir um ângulo de 60 graus.

Etapas de Construção.

Trace a circunfêrencia de centro em A raio AB, em seguida com o mesmo raio trace a circunferência de centro em B. Seja C um ponto de interseção entre as duas circunferências. Sendo assim, trace o segmento $\overline{AC}$, portanto, o ângulo $\angle BAC$ tem medida 60 graus.

Figura 2 – Construção do ângulo de 60 graus.



Fonte: Autor.

Justificativa

Da forma em que foram construídas, as duas circunferências possuem o mesmo raio AB. Em consequência disto, o triângulo ABC é equilátero, logo todos os seus ângulos possuem medida 60 graus.

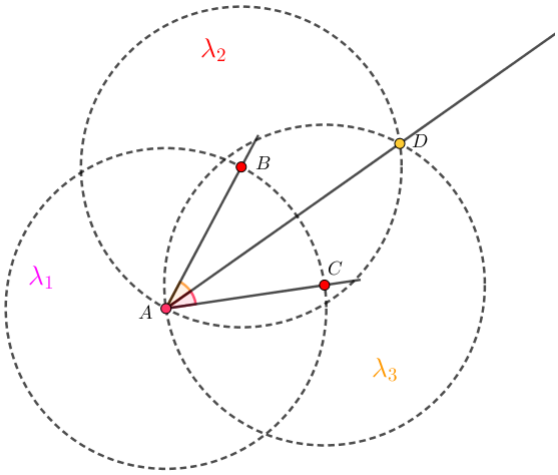
5.1.3 Construção da Bissecção de um ângulo

Dado um ângulo com vértice em um ponto A, construir a reta que divide este ângulo em duas partes iguais.

Etapas de Construção

Com centro em A, trace uma circunfêrencia λ_1 de raio arbitrário. Sejam B e C os pontos de interseção de λ_1 com os lados do ângulo. Agora, com mesmo raio e com centro em B trace a circunfêrencia λ_2. Em seguida, da mesma forma com centro em C trace a circunferência λ_3. Seja D o ponto de interseção de λ_2 e λ_3, diferente de A. Por fim, trace a semireta $\overrightarrow{AD}$ que divide o ângulo em duas partes iguais.

Figura 3 – Bissecção de um ângulo arbitrário.



Fonte: Autor.

Justificativa

Da forma em que foram construídas, as circunfêrencias $\lambda_1, \lambda_2, \lambda_3$ possuem o mesmo raio, logo os segmentos $\overline{AB}$, $\overline{AC}$, $\overline{CD}$ e $\overline{DB}$ possuem a mesma medida. Dessa forma, o quadrilátero $ABDC$ é um losango, assim como em losango as diagonais são bissetrizes, temos que AD é bissetriz do ângulo $\angle BAC$.

Note que é possível bissectar um ângulo arbritário. Apesar disto, veremos no próximo capítulo que não é possível trissectar um ângulo qualquer.

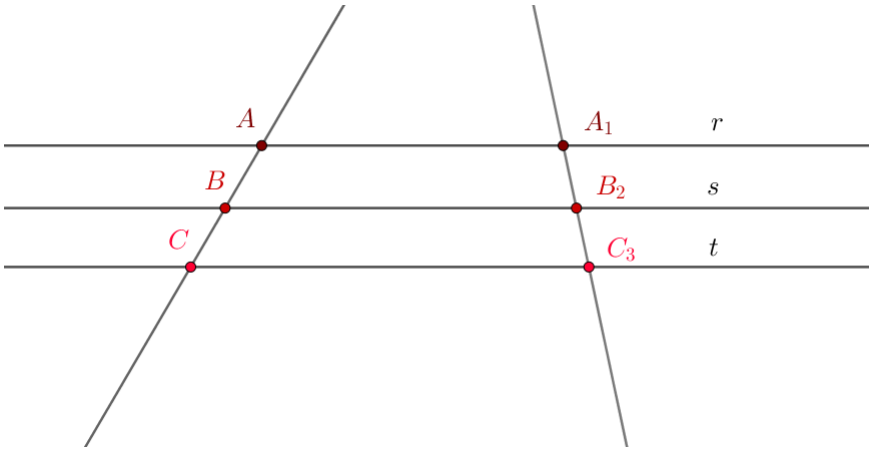
A seguir vamos enunciar o Teorema de Tales, um resultado de grande importância para Geometria Euclidiana. Este Teorema será necessário para proseguir com as próximas construções. Entretanto, não vamos mostrar este resultado. Para mais informações sobre o Teorema de Tales consulte Dulce e Pombeo (1993).

5.1.4 Teorema de Tales

Teorema 5.1.1. *(Teorema de Tales). Sejam r, s, t retas paralelas. Dados os pontos $A, A_1 \in r$, $B, B_2 \in s$ e $C, C_3 \in t$ de modo que A, B, C e A_1, B_2, C_3 sejam dois ternos de pontos colineares. Então,*

$$\frac{AB}{A_1B_2} = \frac{BC}{B_2C_3} = \frac{AC}{A_1C_3}.$$

Figura 4 – Teorema de Tales.



Fonte: Autor.

5.1.5 Adição, produto e quociente

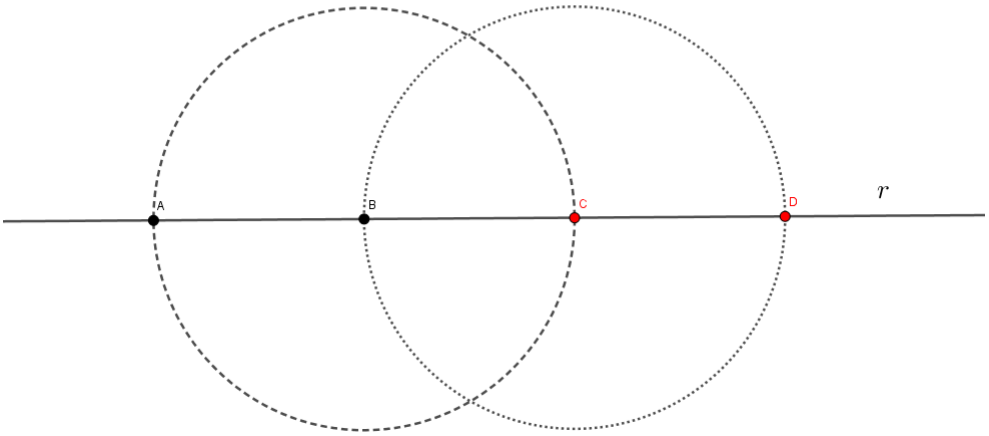
Dado um segmento $\overline{AB}$ de medida $AB = 1$ construir o segmento de medida 3.

Etapas de construção

Dada uma reta r e um segmento $AB = 1$ sobre r, pelas operações elementares, podemos traçar uma circuferência de centro em B e raio AB, assim encontrando o ponto $C \neq A$ como um ponto interseção da reta r e a circunferência, logo formando o segmento $\overline{AC}$ de comprimento 2. Para encontrar um segmento de comprimento 3, basta repetir o procedimento, traçando uma circunferência com centro em C e raio AB, e encontrar o ponto $D \neq B$ como um ponto de interseção da reta r com a circunferência formando o segmento $\overline{AD}$ de comprimento 3.

A Figura 5 ilustra este procedimento:

Figura 5 – Adição de segmentos a partir de um segmento de medida 1.



Fonte: Autor.

Observando o resultado anterior podemos generalizar o procedimento e construir segmentos cuja as medidas são valores absoluto de números reais. Por exemplo, poderíamos construir um segmento de medida α, sendo α um número real positivo. Os resultados a seguir exploram este fato.

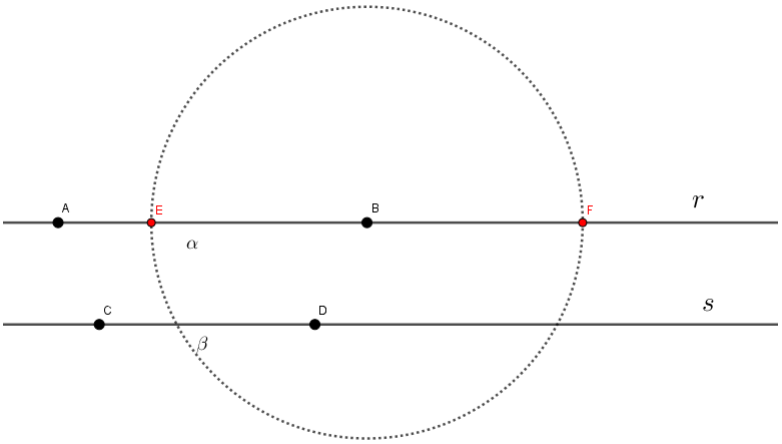
5.1.5.1 Construindo uma soma

Sejam r e s retas tais que os pontos A, B pertençam a r e os pontos C, D a s de tal forma que as medidas dos segmentos $\overline{AB}$ e $\overline{CD}$, obtidas da mesma forma que o processo anterior, são $AB = \alpha$ e $CD = \beta$ onde α e β são números reais e $\alpha > \beta > 0$, construir os segmentos de medida $\alpha + \beta$ e $\alpha - \beta$.

Etapas de Construção.

Dadas as retas r e s. Considere sobre r o segmento $\overline{AB}$ sobre s o $\overline{CD}$ tais que $AB = \alpha$ e $CD = \beta$. Sendo assim, pelas operações elementares de construção com régua e compasso, podemos construir uma circunferência de centro em B e raio CD, obtendo assim os pontos E e F, como a interseção da reta r com a circunferência de centro em B e raio CD. Portanto, $AF = \alpha + \beta$ e $AE = \alpha - \beta$.

Figura 6 – Adição de segmentos de forma geral.



Fonte: Autor.

De forma similiar ao procedimento da construção 5.1.5.1 podemos construir os segmentos cujas medidas são valores absolutos de produtos e quocientes de números reais.

5.1.5.2 Construindo um produto e um quociente.

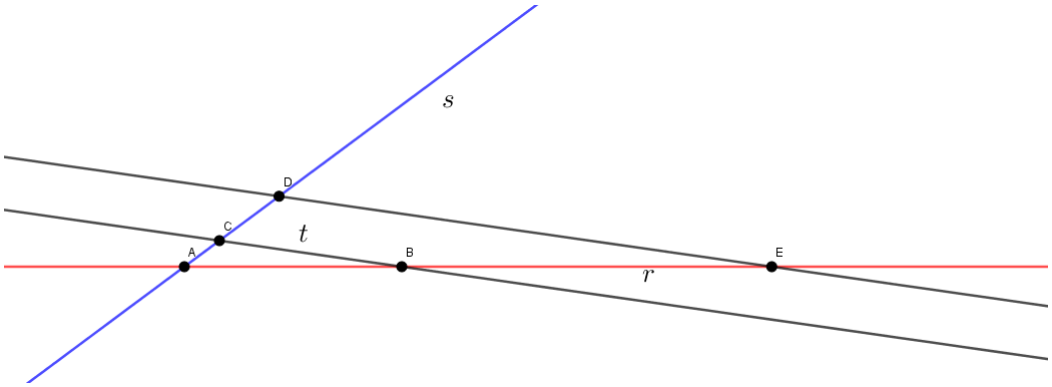
Sejam α e β, números reais tais que $\alpha, \beta > 0$ e α e β são medidas de segmentos, construir os segmentos de medidas $\alpha \cdot \beta$ e $\dfrac{\alpha}{\beta}$.

Etapas de Construção.

Construíndo $\alpha \cdot \beta$.
Sejam uma reta r, e o segmento $\overline{AB}$ sobre r, tal que $AB = \alpha$. Trace uma reta s, concorrente[2] a r em A. Em s, considere os segmentos $AC = 1$ e $AD = \beta$. Sendo assim, trace uma reta t que passa pelos pontos C e B e em seguida construa uma reta paralela a t que passe por D. Seja E o ponto de interseção entre a reta paralela a t e a reta t. A imagem a seguir ilustra o procedimento.

[2] Duas retas são ditas concorrentes se essas duas retas se intersectam em um único ponto.

Figura 7 – Produto de segmentos.



Fonte: Autor.

Dessa forma, como r e s são transversais as retas t e a reta paralela a t, pelo Teorema de Tales temos:

$$\frac{AD}{AC} = \frac{AE}{AB}.$$

Como $AC = 1$, $AD = \beta$ e $AB = \alpha$, vem que,

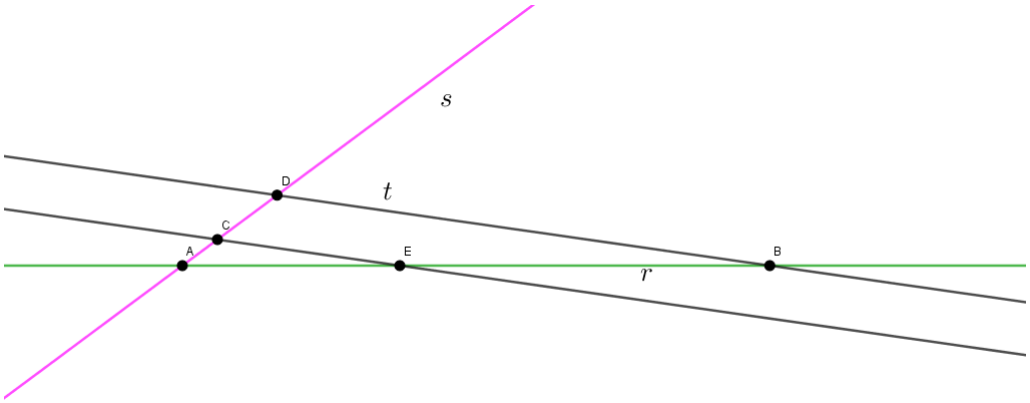
$$\frac{\beta}{1} = \frac{AE}{\alpha}.$$

Portanto, $AE = \alpha \cdot \beta$.

Construindo $\frac{\alpha}{\beta}$.

Analogamente ao caso anterior trace a reta s concorrente a r em A. Assim, em s considere os segmentos $AC = 1$, $AD = \beta$ e em r o segmento $AB = \alpha$. Nessas condições trace a reta t que passe por D e B e construa a reta paralela a t que passe por C. Seja E o ponto de interseção entre a reta paralela a t e a reta r. A imagem a seguir ilustra o procedimento.

Figura 8 – Quociente de segmentos.



Fonte: Autor.

Portanto, pelo Teorema de Tales:

$$\frac{AE}{AB} = \frac{AC}{AD}$$

Como $AC = 1$, $AD = \beta$ e $AB = \alpha$, vem que

$$\frac{AE}{\alpha} = \frac{1}{\beta}.$$

Por fim, $AE = \dfrac{\alpha}{\beta}$.

5.1.5.3 Construindo raízes quadradas

Dados segmentos de comprimento 1 e α, tais que $\alpha > 0$, construir um segmento de comprimento $\sqrt{\alpha}$.

Etapas de Construção

Consideremos sobre uma reta r o segmento unitário AB e o segmento BC de comprimento $BC = \alpha$. Seja M o ponto médio do segmento AC e construa uma semi-circunferência com centro em M e diâmetro AC. Em seguida, trace a perpendicular s a r em B. Assim, seja D o ponto de interseção da reta s com a semicircunferência. Assim, considere o triângulo $\triangle ADC$. Como AC é o diamêtro da circunfêrencia, segue que o ângulo $\angle CDA$ é reto. Logo, os triângulos $\triangle ADB$ e $\triangle CDB$ são semelhantes. Portanto, temos a seguinte relação:

$$\frac{BC}{BD} = \frac{BD}{AB}$$

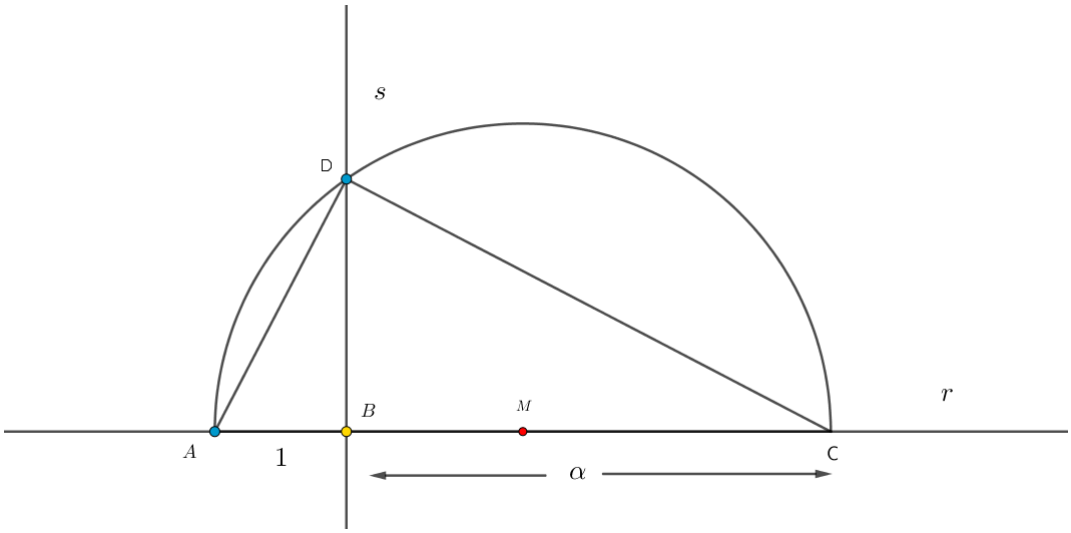
isto é,

$$\frac{\alpha}{BD} = \frac{BD}{1}$$

portanto,

$$\sqrt{\alpha} = BD.$$

Figura 9 – Construção da raiz quadrada.



Fonte: Autor.

5.2 Números construtíveis

Das construções anteriores, por meio de um segmento de comprimento 1, foi possível construir, em número finito de passos, segmentos cujas medidas são valores absolutos de números reais. Portanto, estamos em condições para definir a noção de número construtível.

Definição 5.2.1. *Seja α um número real com valor absoluto $|\alpha|$. Então α é dito construtível se podemos construir, num número finito de operações ((i) (ii), (iii) da Definição 5.1), pontos A e B cuja distância[3] entre eles é $|\alpha|$ unidades, a partir de um conjunto inicial de pontos $\{P_0, P_1\}$ cuja distância entre P_0 e P_1 é 1 unidade.*

Exemplo 5.2.1. *Como consequência da definição, temos que os números inteiros são construtíveis, visto que repetindo o processo de construção de um segmento de medida 3, podemos construir um segmento de medida $|\alpha|$ para $\alpha \in \mathbb{Z}$.*

Assim, nos resultados a seguir veremos que a soma de dois números construtíveis é um número construtível e da mesma forma o produto e o quociente de dois números construtíveis é um número construtível.

[3] Definimos distância como a medida do segmento $\overline{AB}$.

Proposição 5.2.1. *Sejam α e β números construtíveis então α + β, α - β, $\alpha \cdot \beta$, $\frac{\alpha}{\beta}$ e $\sqrt{\alpha}$ são construtíveis.*

Demonstração. A demonstração de que $\alpha + \beta$, $\alpha - \beta$ $\alpha \cdot \beta$, $\frac{\alpha}{\beta}$ e $\sqrt{\alpha}$ são construtíveis segue imediatamente das construções desenvolvidas nas subseções 5.1.5.1, 5.1.5.2 e 5.1.5.3. □

Assim, podemos concluir que o conjunto dos números racionais é construtível, pois $\frac{\alpha}{\beta}$ é construtível, para o caso particular de $\alpha, \beta \in \mathbb{Z}$. A noção de número construtível representa um elo entre a Geometria e a Álgebra Abstrata. No próxima seção veremos que o conjunto dos números construtíveis é um corpo.

5.3 Corpo dos Números construtíveis

Nesta seção vamos mostrar que o conjunto dos números construtíveis formam um subcorpo de $\mathbb{R}$, para que desta forma seja possível utilizar os resultados obtidos, no decorrer do trabalho, para analisarmos os problemas clássicos.

Seja o conjunto $C_{\mathbb{R}}$ um subconjunto de $\mathbb{R}$ tal que todo elemento pertencente a $C_{\mathbb{R}}$ seja construtível. Vamos mostrar que $C_{\mathbb{R}}$ é um subcorpo de $\mathbb{R}$, ou seja, provar que $C_{\mathbb{R}}$ é um corpo.

Teorema 5.3.1. *O conjunto dos números construtíveis $C_{\mathbb{R}}$ é um corpo.*

Demonstração. Da Proposição 5.2.1 temos que se $\alpha, \beta \in C_{\mathbb{R}}$, obtemos que $\alpha - \beta \in C_{\mathbb{R}}$ e $\frac{\alpha}{\beta} \in C_{\mathbb{R}} (\beta \neq 0)$. Assim, como $\alpha \in C_{\mathbb{R}}$ também temos que $\alpha - \alpha = 0 \in C_{\mathbb{R}}$ e $\frac{\alpha}{\alpha} = 1 \in C_{\mathbb{R}} (\alpha \neq 0)$. Portanto, da Proposição 2.2.1 temos que $C_{\mathbb{R}}$ é um subcorpo de $\mathbb{R}$. Sendo assim, concluímos que $C_{\mathbb{R}}$ é um corpo. □

Ademais, se $C_{\mathbb{R}}$ é um subcorpo de $\mathbb{R}$, segue que $\mathbb{R}$ é uma extensão de $C_{\mathbb{R}}$. E ainda, por sua vez, $\mathbb{Q} \subset C_{\mathbb{R}}$ e $\mathbb{Q}$ é um subcorpo de $C_{\mathbb{R}}$, o que resulta que $C_{\mathbb{R}}$ é um extensão de $\mathbb{Q}$.

Neste momento, temos condições de enunciar o segundo teorema essencial para a prova das impossibilidades clássicas. Entretanto, antes de enuncia-lo vamos enunciar dois teoremas para prosseguir com a demonstração deste resultado.

Teorema 5.3.2. *(Raízes quadradas sucessivas geram números construtíveis). Um número real α é um número construtível se existem números reais positivos $\lambda_1, \lambda_2, ..., \lambda_n$ tais que:*

$$\lambda_1 \in \mathbb{K}_1, \textit{ onde } \mathbb{K}_1 = \mathbb{Q}$$
$$\lambda_2 \in \mathbb{K}_2, \textit{ onde } \mathbb{K}_2 = \mathbb{K}_1[\sqrt{\lambda_1}]$$
$$\lambda_3 \in \mathbb{K}_3, \textit{ onde } \mathbb{K}_3 = \mathbb{K}_2[\sqrt{\lambda_2}]$$
$$.$$
$$.$$
$$.$$
$$\lambda_n \in \mathbb{K}_n, \textit{ onde } \mathbb{K}_n = \mathbb{K}_{n-1}[\sqrt{\lambda_{n-1}}]$$

e finalmente,

$$\alpha \in \mathbb{K}_{n+1}, \textit{ onde } \mathbb{K}_{n+1} = \mathbb{K}_n[\sqrt{\lambda_n}].$$

Não demonstraremos o resultado acima, porém o exemplo a seguir irá ilucidar a ideia do teorema.

Exemplo 5.3.1. *Seja* $\alpha = 5\sqrt{2} + \dfrac{\sqrt{8-3\sqrt{2}}}{1-\sqrt{2}}$. *Vamos mostrar que* α *é construtível utilizando o teorema acima. Tomando* $\lambda_1 = 2 \in \mathbb{K}_1$, *onde* $\mathbb{K}_1 = \mathbb{Q}$ *e* $\lambda_2 = 8 - 3\sqrt{2} = 8 - 3\sqrt{\lambda_1} \in \mathbb{K}_2$, *onde* $\mathbb{K}_2 = \mathbb{K}_1[\sqrt{\lambda_1}]$. *Portanto,* $\alpha = 5\sqrt{\lambda_1} + \dfrac{\sqrt{\lambda_2}}{1-\sqrt{\lambda_1}} \in \mathbb{K}_3$, *onde* $\mathbb{K}_3 = \mathbb{K}_2[\sqrt{\lambda_2}]$. *Assim, produzimos números reais positivos* λ_1, λ_2 *que satisfazem as hipóteses do Teorema 5.3.2. Logo, concluímos que* α *é construtível.*

Teorema 5.3.3. *(Todos os números construtíveis vem de raízes quadradas). Se* α *é um número construtível então existem números reais positivos* $\lambda_1, \lambda_2, ..., \lambda_n$ *tais que:*

$$\lambda_1 \in \mathbb{K}_1, \textit{ onde } \mathbb{K}_1 = \mathbb{Q}$$
$$\lambda_2 \in \mathbb{K}_2, \textit{ onde } \mathbb{K}_2 = \mathbb{K}_1[\sqrt{\lambda_1}]$$
$$\lambda_3 \in \mathbb{K}_3, \textit{ onde } \mathbb{K}_3 = \mathbb{K}_2[\sqrt{\lambda_2}]$$
$$.$$
$$.$$
$$.$$
$$\lambda_n \in \mathbb{K}_n, \textit{ onde } \mathbb{K}_n = \mathbb{K}_{n-1}[\sqrt{\lambda_{n-1}}]$$

e finalmente,

$$\alpha \in \mathbb{K}_{n+1}, \textit{ onde } \mathbb{K}_{n+1} = \mathbb{K}_n[\sqrt{\lambda_n}].$$

Demonstração. Consultar Jones Sidney A. Morris (1991, p. 100). □

Teorema 5.3.4. *Se* α *é um número construtível então* α *é algébrico sobre* $\mathbb{Q}$ *e* $\partial(irr(\alpha, \mathbb{Q}))$ *é uma potência de* 2, $2^s (s \geq 0)$.

Demonstração. Sejam α um número construtível e $\lambda_1, \lambda_2, ..., \lambda_n$ definidos pelo Teorema 5.3.3. Dessa forma, tomando $\lambda_i \in \mathbb{K}_i$ onde $1 \leq i \leq n$, segue que $\sqrt{\lambda_i}$ é raiz do polinômio $(x^2-\lambda_i) \in \mathbb{K}_i[x]$, ou seja, $\sqrt{\lambda_i}$ é algébrico sobre $\mathbb{K}_i$ e $(x^2-\lambda_i) = irr(\sqrt{\lambda_i}, \mathbb{K}_i)$. Entretanto, se $\sqrt{\lambda_i} \in \mathbb{K}_i$ temos que $x - \sqrt{\lambda_i} = irr(\sqrt{\lambda_i}, \mathbb{K}_i)$. Sendo assim, concluímos que:

$$\partial(irr(\sqrt{\lambda_i}, \mathbb{K}_i)) = 1 \text{ ou } 2.$$

Por sua vez, do Teorema 5.3.3 temos que $\mathbb{K}_{i+1} = \mathbb{K}_i[\sqrt{\lambda_i}]$. Dessa forma, como $\mathbb{K}_i[\sqrt{\lambda_i}]$ é uma extensão de $\mathbb{K}_i$ e $\partial(irr(\sqrt{(}\lambda_i), \mathbb{K}_i)) = 1$ ou 2 então pelo Teorema 4.4.2 item (i) segue que:

$$[\mathbb{K}_{i+1} : \mathbb{K}_i] = 1 \text{ ou } 2, \text{ onde } (1 \leq i \leq n).$$

Note que da forma em que os conjuntos $\mathbb{K}_1, ..., \mathbb{K}_{n+1}$ foram definidos temos a seguinte torre de corpos:

$$\mathbb{Q} = \mathbb{K}_1 \subseteq \mathbb{K}_2 \subseteq ... \subseteq \mathbb{K}_{n+1}.$$

Assim, aplicando repetidamente o Teorema 4.4.5 temos que:

$$[\mathbb{K}_{n+1} : \mathbb{Q}] = [\mathbb{K}_2 : \mathbb{K}_1] \cdot [\mathbb{K}_3 : \mathbb{K}_2] \cdot ... \cdot [\mathbb{K}_{n+1} : \mathbb{K}_n] = 2^s \text{ para algum inteiro } s \geq 0.$$

Portanto, como a extensão $\mathbb{K}_{n+1}$ é finita segue do Teorema 4.4.2 item (ii) que $\mathbb{K}_{n+1}$ é algébrica, logo $\alpha \in C_{\mathbb{R}}$ é algébrico sobre $\mathbb{Q}$. E ainda, como $\alpha \in \mathbb{K}_{n+1}$ podemos considerar a torre:

$$\mathbb{Q} \subseteq \mathbb{Q}[\alpha] \subseteq \mathbb{K}_{n+1}.$$

Dessa forma, temos que $\partial(irr(\alpha, \mathbb{Q}))$ é um fator de $[\mathbb{K}_{n+1} : \mathbb{Q}]$. Portanto, $\partial(irr(\alpha, \mathbb{Q})) = 2^t$, para algum inteiro $t \geq 0$.

6 Prova das Impossiblidades Geométricas

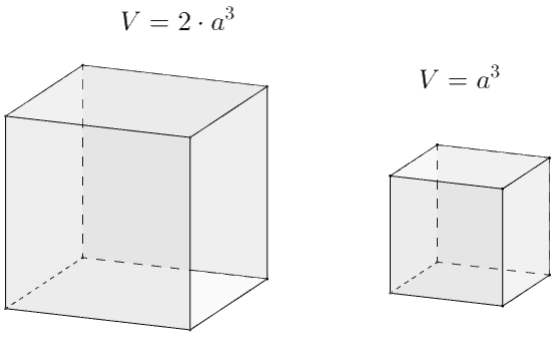
> Diz-se que uma delegação fora enviada ao oráluco de Apolo em Delos para perguntar como a peste poderia ser combatida e que o oráculo respondeu que o altar de Apolo, cúbico, deveria ser duplicado. Os atenienses, ao que se diz, obedientemente dobraram as dimensões do altar, mas isto não adiantou para afastar a peste. É claro, o altar tivera seu volume multiplicado por oito e não por dois.
>
> Lenda sobre a origem do problema da duplicação do cubo retirado de (BOYER, 2010, p.44)

Neste capítulo, vamos apresentar as provas das impossíbilidades clássicas. É importante ressaltar, que para realização do objetivo destas demonstrações nos valemos de todo conteúdo desenvolvido até o momento no trabalho. Com o desenvolvimento destas provas, podemos perceber quantos resultados foram necessários para que as demonstrações pudessem ser desenvolvidas de um modo simples, o que torna os três problemas clássicos de grande revelância para o desenvolvimento da Matemática. Para composição deste capítulo foram utilizados os materiais de Biazzi (2014) e Santos (2017).

6.1 Duplicação do Cubo

Teorema 6.1.1. *É impossível construir com régua não graduada e compasso um cubo, cujo volume é o dobro de um cubo dado.*

Figura 10 – Duplicação do cubo.



Fonte: Autor.

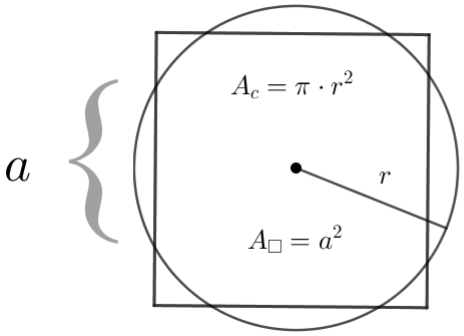
Construir um cubo, cujo o volume seja o mesmo de um cubo dado, se resume a construir arestas $a \in C_{\mathbb{R}}$ e $b \in C_{\mathbb{R}}$ tal que $a^3 = 2 \cdot b^3$. A seguir mostraremos que a construção deste problema é impossível com régua e compasso.

Demonstração. Suponha, por absurdo, que a tese seja falsa. Sendo assim, $\exists\, a, b \in C_{\mathbb{R}}$ arestas de cubos, tais que $a^3 = 2 \cdot b^3$. Tomando $b^3 = 1$, temos $a^3 = 2$, logo $a^3 - 2 = 0$. Relacionando essa igualdade com o polinômio $p(x) = x^3 - 2$, temos pelo Teorema 3.2.3 que $p(x)$ é irredutível sobre $\mathbb{Q}$ para o primo $p = 2$. Por sua vez, $p(x)$ é mônico e $p(\sqrt[3]{2}) = 0$, logo $p(x) = irr(\sqrt[3]{2}, \mathbb{Q})$. Portanto, pelo Teorema 4.4.2 item (i), temos que $[\mathbb{Q}[\sqrt[3]{2}] : \mathbb{Q}] = 3$, que é uma contradição, pois como $\sqrt[3]{2} \in C_{\mathbb{R}}$ é algébrico sobre $\mathbb{Q}$, resulta pelo Teorema 5.3.4 que $[\mathbb{Q}[\sqrt[3]{2}] : \mathbb{Q}]$ é uma potência de 2. Logo, segue a tese. □

6.2 Quadratura do Círculo

Teorema 6.2.1. *É impossível construir com régua não graduada e compasso um quadrado, cuja área é a mesma de um círculo dado.*

Figura 11 – Quadratura do círculo.



Fonte: Autor.

Construir um quadrado cujo a área é a mesma de um círculo dado, significa construir $a \in C_{\mathbb{R}}$ lado de um quadrado tal que $a^2 = \pi \cdot r^2$ e r raio de um círculo. A seguir vamos mostrar que este problema é impossível com régua e compasso.

Demonstração. Suponha, por absurdo, que a tese seja falsa. Sendo assim, $\exists\, r, a \in C_{\mathbb{R}}$ tal que $\pi \cdot r^2 = a^2$. Tomando $r = 1$, temos: $\pi = a^2 = a \cdot a$. Da Proposição 5.2.1 temos que $a \cdot a$ é construtível, pois $a \in C_{\mathbb{R}}$, e ainda pelo Teorema 5.3.4 temos que se $a^2 \in C_{\mathbb{R}}$ então a^2 é algébrico sobre $\mathbb{Q}$ e como $a^2 = \pi$, então π é algébrico sobre $\mathbb{Q}$, o que é um absurdo, pois π é transcedente sobre $\mathbb{Q}$. Portanto, a tese é verdadeira. □

Para dar prosseguimento à próxima demonstração, vamos retomar alguns conceitos básicos de trigonometria.

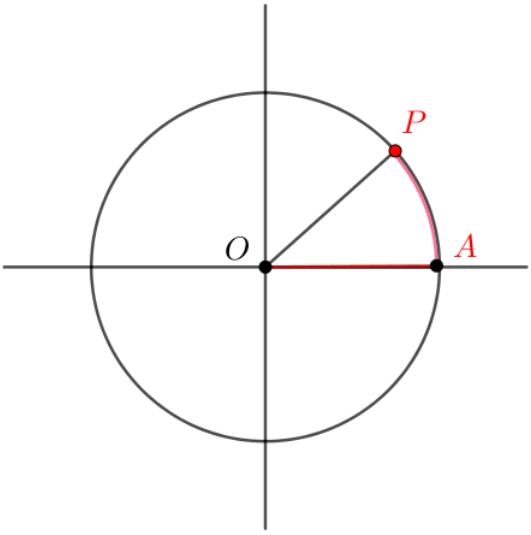
6.3 Noções de trigonometria

Definição 6.3.1. *Consideremos sobre o plano cartesiano a circunferência λ de centro em $O = (0, 0)$ e raio 1. Assim, vamos definir uma função f, que associa a cada número real x a um ponto P de λ . E ainda, considere o ponto $A = (1, 0)$. Dessa forma, se:*

- *Se $x = 0$ então P coincide com A.*
- *Se $x > 0$ então realizamos a partir de A um percurso de comprimento x no sentido anti-horário, e marcamos P como o ponto final deste percurso.*
- *Se $x < 0$ então realizamos um percurso, a partir de A, no sentido horário de comprimento $|x|$. O ponto final do percurso é P.*

A circunferência λ acima definida é denominada ciclo ou circunferência trigonométrica.

Figura 12 – Circunferência trigonométrica.



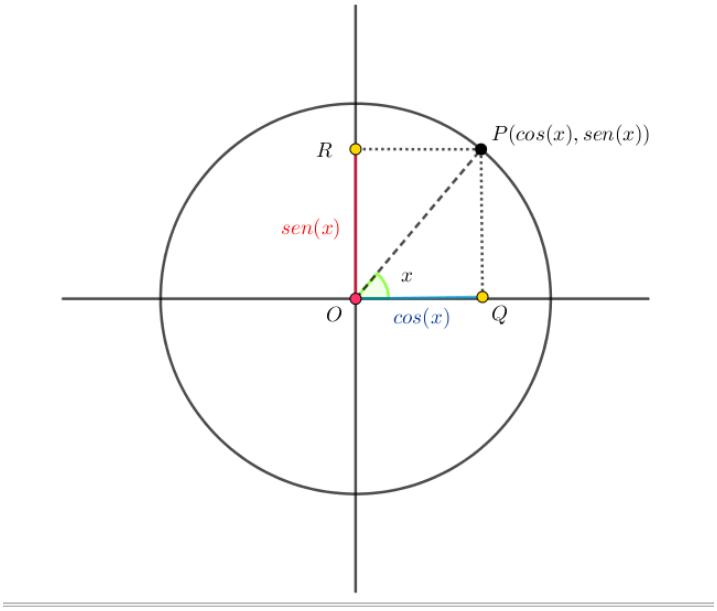
Fonte: Autor.

Definido a circunferência trigonométrica, temos condições de definir as funções seno e cosseno.

Definição 6.3.2. *Dado um número real x, seja P sua imagem na circunferência trigonométrica. Denominamos cosseno de x (representamos $\cos(x)$) a medida do segmento $\overline{OQ}$ (ver figura) abscissa do ponto P no plano cartesiano e denominamos seno (representamos $\operatorname{sen}(x)$) a medida do segmento $\overline{OR}$ ordenada do ponto P. Assim, definimos a função cosseno $f : \mathbb{R} \to \mathbb{R}$ que associa cada número real x ao número*

real $OP = \cos(x)$*, isto é,* $f(x) = \cos(x)$ *e a função seno* $g : \mathbb{R} \to \mathbb{R}$ *que associa cada número real* x *ao número real* $OR = \operatorname{sen}(x)$*, ou seja,* $g(x) = \operatorname{sen}(x)$*.*

Figura 13 – Funções seno e cosseno.



Fonte: Autor.

Note que este valor x representa o ângulo $\angle QOP$ no triângulo $\triangle OPQ$, pois o triângulo em questão é um triângulo retângulo.

Proposição 6.3.1. *Seja* $\alpha, \theta \in \mathbb{R}$ *, temos que as seguintes identidades são verdadeiras:*

(i) $\cos^2(\theta) + \operatorname{sen}^2(\theta) = 1$*.*

(ii) $\cos(\alpha + \theta) = \cos(\alpha) \cdot \cos(\theta) - \operatorname{sen}(\alpha) \cdot \operatorname{sen}(\theta)$*.*

(iii) $\operatorname{sen}(\alpha + \theta) = \operatorname{sen}(\alpha) \cdot \cos(\theta) + \operatorname{sen}(\theta) \cdot \cos(\alpha)$*.*

(iv) $\cos(2\theta) = \cos^2(\theta) - \operatorname{sen}^2(\theta)$*.*

(v) $\operatorname{sen}(2\theta) = 2 \cdot \cos(\theta) \operatorname{sen}(\theta)$*.*

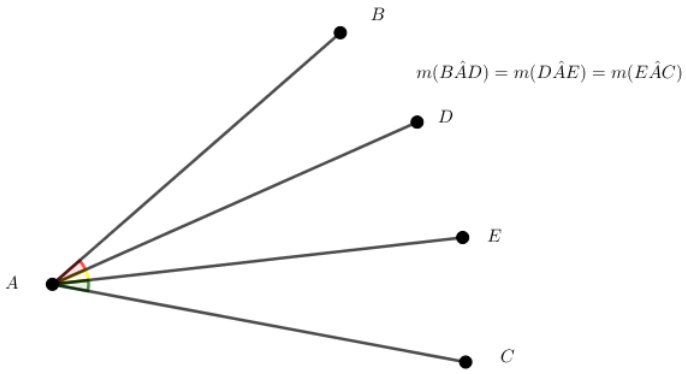
Demonstração. Consultar Iezzi (1977). □

Para mais informações sobre trigonometria consulte Iezzi (1977).

6.4 Trissecção do Ângulo

Teorema 6.4.1. *É impossível dividir, com régua não graduada e compasso, em três partes iguais a medida de um ângulo arbritrário.*

Figura 14 – Trissecção do ângulo.



Fonte: Autor.

Nas construções elementares foi visto que é possível construir um ângulo de 60°. Logo, como o problema da trisseção do ângulo se refere a trissectar um ângulo arbitrário, vamos supor que seja possível trissectar o ângulo de 60°. Assim, a medida dos ângulos obtidos é 20°, portanto, em suma, o problema se resume em construir os segmentos que dividem o ângulo dado em três partes iguais, ou seja, construir os arcos de circunferência cujos ângulos são 20^o, 40^o e 60^o. Logo, retomando a Definição 6.3.2 da seção anterior temos que na circunferência trigonométrica, os valores dos segmentos que são abscissas do ponto P, relacionados aos ângulos 20^o, 40^o e 60^o, são $\cos(20^o)$, $\cos(40^o)$ e $\cos(60^o)$ e as ordenadas são $\operatorname{sen}(20^o)$, $\operatorname{sen}(40^o)$ e $\operatorname{sen}(60^o)$. Assim, para obtermos a angulação desejada devemos construir os segmentos de medidas $\cos(20^o)$ e $\operatorname{sen}(20^o)$. Dessa forma, o problema consiste em provar que $\cos(20^o)$ e $\operatorname{sen}(20^o)$ são construtíveis. Veremos a seguir que isto não é possível, pois $\cos(20^o)$ não é construtível.

Demonstração. Vamos mostrar que $\cos(20^o)$ não é construtível. Considere $\theta = 20^o$. Da Proposição 6.3.1 temos que:

$$\cos(3\theta) = \cos(2\theta + \theta) = \cos(2\theta) \cdot \cos(\theta) - \operatorname{sen}(2\theta) \cdot \operatorname{sen}(\theta) \Leftrightarrow$$
$$\cos(3\theta) = (\cos^2(\theta) - \operatorname{sen}^2(\theta)) \cdot \cos(\theta) - (2 \cdot \operatorname{sen}(\theta) \cdot \cos(\theta)) \cdot \operatorname{sen}(\theta) \Leftrightarrow$$
$$\cos(3\theta) = \cos^3(\theta) - \operatorname{sen}^2(\theta) \cdot \cos(\theta) - 2 \cdot \operatorname{sen}^2(\theta) \cdot \cos(\theta) \Leftrightarrow$$
$$\cos(3\theta) = \cos^3(\theta) - 3 \cdot \operatorname{sen}^2(\theta) \cdot \cos(\theta) = \cos^3(\theta) - 3 \cdot (1 - \cos^2(\theta)) \cdot \cos(\theta)) \Leftrightarrow$$
$$\cos(3\theta) = 4 \cdot \cos^3(\theta) - 3 \cdot \cos(\theta).$$

Por sua vez, como $\theta = 20^o$, segue que $\cos(3\theta) = \cos(60^o) = \frac{1}{2}$. Assim, $\frac{1}{2} = 4 \cdot \cos^3(\theta) - 3 \cdot \cos(\theta)$. Portanto, temos a equação:

$$8 \cdot \cos^3(\theta) - 6 \cdot \cos(\theta) - 1 = 0.$$

Tomando $x = 2 \cdot \cos\theta$, temos o seguinte polinômio p:

$$p(x) = x^3 - 3x - 1.$$

Vamos mostrar que p é irredutível sobre $\mathbb{Q}$. Note que não é possível aplicar o critério de Eisenstein diretamente. Sendo assim, vamos aplicar uma tranformação semelhante a do Exemplo 3.2.7. Assim, temos o polinômio $p(x+1) = x^3 + 3x^2 - 3$. Portanto, para o primo $p = 3$ temos pelo critério de Eisenstein que $p(x+1)$ é irredutível sobre $\mathbb{Q}$. Assim, pela Proposição 3.2.2 temos que $p(x)$ é irredutível sobre $\mathbb{Q}$. Logo, como $p(x)$ é irredutível, mônico e de menor grau em que $p(2 \cdot \cos(20^o)) = 0$, segue que $p(x) = irr(2 \cdot \cos(20^o), \mathbb{Q})$ e $\partial(irr(2 \cdot \cos(20^o), \mathbb{Q})) = 3$. Portanto, pelo Teorema 4.4.2 temos que $[\mathbb{Q}[2 \cdot \cos(20^o)] : \mathbb{Q}] = 3$, o que contradiz o Teorema 5.3.4. Em vista disso, $2 \cdot \cos(20^o)$ não é construtível, o que resulta pela Proposição 5.2.1 que $\cos(20^o)$ não é construtível. Portanto, não é possível trissectar um ângulo de 60º. Assim, segue a tese. □

Por fim, concluímos que não é possível trissectar um ângulo arbitrário. Com isso, concluímos o nosso principal objetivo.

7 Conclusão

> Não há ensino sem pesquisa e pesquisa sem ensino. Esses quefazeres se encontram um no corpo do outro. Enquanto ensino continuo buscando, reprocurando. Ensino porque busco, porque indaguei, porque indago e me indago. Pesquiso para constatar, constatando, intervenho, intervindo educo e me educo. Pesquiso para conhecer o que ainda não conheço e comunicar ou anunciar a novidade.
>
> Paulo Freire

Concluímos que, com o trabalho desenvolvido, foi possível perceber o quanto de conhecimento matemático, foi mobilizado ao longo da história na tentativa de resolver estes problemas que ao primeiro momento pareciam ser simples. Com o desenvolvimento deste trabalho também percebemos o quanto a Álgebra e a Geometria estão intimamente ligadas, pois questões da geometria, como os três problemas clássicos, somente foram resolvidas com o auxílio de ferramentas algébricas.

E ainda, como ressaltamos durante o trabalho, esses problemas destacam a característica colaborativa da Matemática, ou seja, que a Matemática é uma ciência construída socialmente por de diversos pensadores durante a história. Em nossa perspectiva essa visão da Matemática deve ser discutida desde a Educação Básica, para que os alunos tenham a oportunidade de conhecer este lado da Matemática.

Por fim, destacamos que este trabalho pode ser utilizado para futuros estudos na área de Álgebra ou Geometria, ou até mesmo para apresentar aos alunos de Matemática ou professores de Matemática já atuantes, a rica teoria que envolve os três problemas clássicos da geometria.

Ademais, como indicação de futuras pesquisas destacamos o desenvolvimento de atividades para educação básica envolvendo os três problemas clássicos, visto que segundo a Base Nacional Comum Curricular (2019) uma das competências específicas da disciplina de Matemática no Ensino Fundamental, constituí em reconhecer a matemática como uma ciência humana fruto das necessidades e transformações históricas.

> Reconhecer que a Matemática é uma ciência humana, fruto das necessidades e preocupações de diferentes culturas, em diferentes momentos históricos, e é uma ciência viva, que contribui para solucionar problemas ciêntificos e tecnológicos e para alicerçar descobertas e construções, inclusive com impactos no mundo do trabalho. (p. 267)

Nesta perspectiva faz-se necessário desenvolver diferentes propostas que revelem para os estudantes essa característica da matemática. Sendo assim, em nossa visão elaborar propostas de atividades que envolvam os três problemas clássicos, devido a sua importância histórica, são um dos caminhos para atingir tal objetivo.

Referências

BIAZZI, R. N. *Polinômios Irredutíveis: Critérios e Aplicações*. 2014. 74 f. Dissertação (Mestrado em Matemática) — Universidade Estatual Paulista “Julio Mesquita Filho”, São Paulo, 2014.

BOYER, C. B. *História da Matemática*. 3. ed. São Paulo: Blucher, 2010.

BRASIL. *Base Nacional Comum Curricular: Ensino Infantil, Ensino Fundamental e Ensino Médio*. Brasília, DF, 2019.

CALLIOLI, C. A.; DOMINGUES, H. H.; COSTA, R. C. F. *Álgebra Linear e Aplicações*. 6. ed. São Paulo: Atual, 1990.

DOMINGUES, H. H.; IEZZI, G. *Álgebra Moderna*. 4. ed. São Paulo: Saraiva, 2003.

DULCE, O.; POMBEO, J. N. *Fundamentos de Matemática Elementar*. 7. ed. São Paulo: Atual, 1993. v. 9.

EVES, H. *Introdução à História da Matemática*. 3. ed. São Paulo: Unicamp, 2004.

GIL, A. C. *Como elaborar projetos de pesquisa*. 4. ed. São Paulo: Atlas, 2002.

GONÇALVES, A. *Introdução à Álgebra*. 4. ed. Rio de Janeiro: IMPA, 1999.

GUERRA, V. C. *Impossibilidades em Construções Geométricas: Aspectos Históricos e Matemáticos.* 76 f. Monografia (Graduação em Matemática) — Universidade Federal de São Carlos, São Carlos, 2012.

IEZZI, G. *Fundamentos de Matemática Elementar*. 2. ed. São Paulo: Atual, 1977. v. 3.

JACOBSON, N. *Basic Algebra 1*. 2. ed. USA: W H Freeman Co (Sd), 1985.

JONES SIDNEY A. MORRIS, K. R. P. A. *Abstract Algebra and Famous Impossibilities*. New York: Springer-Verlag, 1991. (Universitext).

LOPES, L. S.; FERREIRA, A. L. A. Um olhar sobre a história nas aulas de matemática. *Abakós*, v. 2, n. 1, p. 75–88, 2013.

MILIES, C. P.; COELHO, S. P. *Números Uma Introdução à Matemática*. 3. ed. São Paulo: Edusp, 2013.

MONTEIRO, L. H. J. *Elementos de álgebra*. 2. ed. Rio de Janeiro: Livro Técnico e Científico, 1978.

SANTOS, J. L. *Extensões de Corpos e os três problemas clássicos de construção matemática*. 2017. 67 f. Dissertação (Mestrado em Matemática) — Universidade Federal do Piauí, Piauí, 2017.

SANTOS, R. de J. *Álgebra Linear e Aplicações*. 2010. Disponível em: ⟨https://www.ime.unicamp.br/~deleo/MA327/ld2.pdf⟩.

SCHUBRING, G.; ROQUE, T. O papel da régua e do compasso nos elementos de euclides: uma prática interpretada como regra. *História Unisinos*, v. 18, n. 1, p. 91–103, 2014.

SILVA, A. G. da. *Construções geométricas com régua e compasso*. 2013. 131 f. Dissertação (Mestrado em Matemática) — Universidade Federal de Alagoas, Maceió, 2013.

SILVA, E. O. *Extensões Algébricas dos Racionais*. 39 f. Monografia (Graduação em Matemática) — Universidade Estadual da Paraíba, Paraíba, 2013.

SOUZA, J. M. R. *Trissecção do Ângulo e Duplicação do Cubo: As soluções na Antiga Grécia*. 2001. 114 f. Dissertação (Mestrado em Matemática) — Faculdade de Ciências da Universidade do Porto, Portugal, 2001.

VENDEMIATTI, A. D. *A quadratura do círculo e a gênese do número π*. 2009. 145 f. Dissertação (Mestrado em Ensino de Matemática) — Pontifícia Universidade Católica de São Paulo, São Paulo, 2009.

A Demonstração que $\mathbb{K}[x]$ é um domínio de integridade

Vamos mostrar que $\mathbb{K}[x]$ é um domínio de integridade. Sejam $p(x) = a_0 + a_1x + a_2x^2 + ... + a_nx^n, q(x) = b_0 + b_1x + b_2x^2 + ... + b_mx^m, f(x) = f_0 + f_1x + ... + f_sx^s \in \mathbb{K}[x]$, onde $s \leq m \leq n$ logo, temos:

(i) $p(x) + q(x) = q(x) + p(x)$ (**comutativa da adição**).

Demonstração. $p(x) + q(x) = (a_0 + a_1x + a_2x^2 + ... + a_nx^n) + (b_0 + b_1x + b_2x^2 + ... + b_mx^m) = (a_0 + b_0) + (b_1 + a_1)x + (a_2 + b_2)x^2 + ... + (a_m + b_m)x^m + a_{m+1}x^{m+1} + ... + a_nx^n$.

Como cada $a_i, b_j \in K$ para $\forall\ i \leq n$, $\forall\ j \leq m$ e $\mathbb{K}$ é um corpo, então a propriedade comutativa é válida para os elementos de $\mathbb{K}$, logo:
$(a_0 + b_0) + (b_1 + a_1)x + (a_2 + b_2)x^2 + ... + (a_m + b_m)x^m + a_{m+1}x^{m+1} + ... + a_nx^n = (b_0 + a_0) + (b_1 + a_1)x + (b_2 + a_2)x^2 + ... + (b_m + a_m)x^m + a_{m+1}x^{m+1} + ... + a_nx^n = (b_0 + b_1x + b_2x^2 + ... + b_mx^m) + (a_0 + a_1x + a_2x^2 + ... + a_nx^n) = q(x) + p(x)$.

□

(ii) $p(x) + (q(x) + f(x)) = (p(x) + q(x)) + f(x)$ (**associativa da adição**).

Demonstração. $p(x) + (q(x) + f(x)) = (a_0 + a_1x + a_2x^2 + ... + a_nx^n) + ((b_0 + f_0) + (b_1 + f_1)x + (b_2 + f_2)x^2 + ... + (b_s + f_s)x^s + b_{s+1}x^{s+1} + ... + b_mx^m) = (a_0 + (b_0 + f_0)) + (a_1 + (b_1 + f_1))x + (a_2 + (b_2 + f_2))x^2 + ... + (a_s + (b_s + f_s))x^s + (a_{s+1} + b_{s+1})x^{s+1} + ... + (a_m + b_m)x^m + a_{m+1}x^{m+1} + ... + a_nx^n$.

Como cada coeficiente de p, g e f são elementos de $\mathbb{K}$, e $\mathbb{K}$ é corpo, então a propriedade associativa é válida, logo:

$(a_0 + (b_0 + f_0)) + (a_1 + (b_1 + f_1))x + (a_2 + (b_2 + f_2))x^2 + ... + (a_s + (b_s + f_s))x^s + (a_{s+1} + b_{s+1})x^{s+1} + ... + (a_m + b_m)x^m + a_{m+1}x^{m+1} + ... + a_nx^n = ((a_0 + b_0) + f_0) + ((a_2 + b_2) + f_2)x + ... + ((a_s + b_s) + f_s)x^s + (a_{s+1} + b_{s+1})x^{s+1} + ... + (a_m + b_m)x^m + a_{m+1}x^{m+1} + ... + a_nx^n = ((a_0 + b_0) + (a_1 + b_1)x + ... + (a_m + b_m)x^m + a_{m+1}x^{m+1} + ... + a_nx^n) + (f_0 + f_1x + ... + f_sx^s) = ((a_0 + a_1x + ... + a_nx^n) + (b_0 + b_1x + ... + b_mx^m)) + (f_0 + f_1x + ... + f_sx^s) = (p(x) + q(x)) + f(x)$.

□

(iii) $\exists!\ g \in \mathbb{K}[x]$ tal que $p(x) + g(x) = p(x)$ (**existência do elemento neutro aditivo**). De fato,

Demonstração. Seja $g(x) = g_0 + g_1x + ... + g_rx^r$ onde $r \leq n$. Suponhamos que a igualdade a seguir é válida, assim,

$$p(x) + g(x) = p(x)$$
$$(a_0 + a_1x + a_2x^2 + ... + a_nx^n) + (g_0 + g_1x + ... + g_rx^r) = a_0 + a_1x + a_2x^2 + ... + a_nx^n$$
$$(a_0+g_0)+(a_1+g_1)x+...+(a_r+g_r)x^r+a_{r+1}x^{r+1}+...+a_nx^n = a_0+a_1x+a_2x^2+...+a_nx^n.$$

Por identidade de polinômios, resulta:

$$a_0 + g_0 = a_0$$
$$a_1 + g_1 = a_1$$
$$.$$
$$.$$
$$.$$
$$a_r + g_r = a_r$$

Como cada coeficiente de p e g são elementos de $\mathbb{K}$, e $\mathbb{K}$ é um corpo, logo existe o elemento neutro para a operação de adição usual. Sendo assim:

$$g_0 = g_1 = ... = g_r = 0_{\mathbb{K}}.$$

Portanto g é o polinômio nulo.

□

(iv) $\forall p \in \mathbb{K}[x]$, $\exists! g(x) \in \mathbb{K}[x]$ tal que $p(x) + g(x) = 0_K$, onde $0_{\mathbb{K}}$ é o polinômio nulo (**existência do elemento oposto**).

Demonstração. Seja $g(x) = g_0 + g_1x + ... + g_rx^r$ onde $r \leq n$. Suponhamos que a igualdade a seguir é válida, deste modo, temos:

$$p(x) + g(x) = 0_{\mathbb{K}}$$
$$(a_0 + a_1x + a_2x^2 + ... + a_nx^n) + (g_0 + g_1x + ... + g_rx^r) = 0_{\mathbb{K}} + 0_{\mathbb{K}}x + 0_{\mathbb{K}}x^2 + ... + 0_{\mathbb{K}}x^n$$
$$(a_0 + g_0) + (a_1 + g_1)x + ... + (a_r + g_r)x^r + a_{r+1}x^{r+1} + ... + a_nx^n =$$
$$0_{\mathbb{K}} + 0_{\mathbb{K}}x + 0_{\mathbb{K}}x^2 + ... + 0_{\mathbb{K}}x^n.$$

Por identidade de polinômios, resulta:

$$a_0 + g_0 = 0_{\mathbb{K}}$$
$$a_1 + g_1 = 0_{\mathbb{K}}$$
$$...$$
$$a_r + g_r = 0_{\mathbb{K}}$$
$$a_{r+1} = ... = a_n = 0_{\mathbb{K}}$$

Como cada coefiente de p e g são elementos de $\mathbb{K}$, e $\mathbb{K}$ é um corpo, logo existe o elemento oposto. Sendo assim:

$$g_0 = -a_0,\ g_1 = -a_1, ...g_r = -a_r.$$

Portanto, g é tal que seus coefientes são os opostos dos elementos de p.

□

(v) $p(x) \cdot q(x) = q(x) \cdot p(x)$ (**comutativa da multiplicação**).

Demonstração. $p(x) \cdot q(x) = (a_0 + a_1x + ... + a_nx^n) \cdot (b_0 + b_1x + ... + b_mx^m) = a_0 \cdot b_0 + (a_0 \cdot b_1 + a_1 \cdot b_0)x + (a_0 \cdot b_2 + a_1 \cdot b_1 + a_2 \cdot b_0)x^2 + ... + a_n \cdot b_m x^{n+m}$

Como $\mathbb{K}$ é um corpo, segue que a propriedade comutativa é satisfeita tanto para adição, quanto para a multiplicação, logo obtemos:

$a_0 \cdot b_0 = b_0 \cdot a_0$,
$a_0 \cdot b_1 + a_1 \cdot b_0 = b_1 \cdot a_0 + b_0 \cdot a_1 = b_0 \cdot a_1 + b_1 \cdot a_0$,
$a_0 \cdot b_2 + a_1 \cdot b_1 + a_2 \cdot b_0 = b_2 \cdot a_0 + b_1 \cdot a_1 + b_0 \cdot a_2 = b_0 \cdot a_2 + b_1 \cdot a_1 + b_2 \cdot a_0$
...
$a_n \cdot b_m = b_m \cdot a_n$.

Portanto, dessa forma, $p(x) \cdot q(x) = q(x) \cdot p(x)$.

□

(vi) $p(x) \cdot (q(x) \cdot f(x)) = (p(x) \cdot q(x)) \cdot f(x)$ (**associativa da multiplicação**).

Demonstração. $p(x) \cdot (q(x) \cdot f(x)) = (a_0 + a_1x + a_2x^2 + ... + a_nx^n) \cdot [(b_0 + b_1x + b_2x^2 + ... + b_mx^m) \cdot (f_0 + f_1x + f_2x^2 + ... + f_sx^s)] = (a_0 + a_1x + a_2x^2 + ... + a_nx^n) \cdot [(b_0 \cdot f_0) + (b_1 \cdot f_0 + b_0 \cdot f_1)x + (b_2 \cdot f_0 + b_1 \cdot f_1 + b_0 \cdot f_2)x^2 + ... + (b_m \cdot f_s)x^{m+s}] = a_0 \cdot (b_0 \cdot f_0) + [a_1 \cdot (b_0 \cdot f_0) + (a_0 \cdot (b_1 \cdot f_0 + b_0 \cdot f_1))]x + [a_2 \cdot (b_0 \cdot f_0) + a_1 \cdot (b_1 \cdot f_0 + b_0 \cdot f_1) + a_0 \cdot (b_2 \cdot f_0 + b_1 \cdot f_1 + b_0 \cdot f_2)]x^2 + ... + a_n \cdot (b_m \cdot f_s)x^{m+s+n}$.
Agora, desenvolvendo o segundo membro temos:
$(p(x) \cdot q(x)) \cdot f(x) = [(a_0 + a_1x + a_2x^2 + ... + a_nx^n) \cdot (b_0 + b_1x + ... + b_mx^m)] \cdot (f_0 + f_1x + f_2x^2 + ... + f_sx^s) = [(a_0 \cdot b_0) + (a_1 \cdot b_0 + a_0 \cdot b_1)x + (a_2 \cdot b_0 + a_1 \cdot b_1 + a_0 \cdot b_2)x^2 + ... + (a_n \cdot$

$b_m)x^{n+m}]\cdot(f_0+f_1x+f_2x^2+...+f_sx^s) = (a_0\cdot b_0)\cdot f_0+[(a_1\cdot b_0+a_0\cdot b_1)\cdot f_0+(a_0\cdot b_0)\cdot f_1]x+[(a_2\cdot b_0+a_1\cdot b_1+a_0\cdot b_2)\cdot f_0+(a_1\cdot b_0+a_0\cdot b_1)\cdot f_1+(a_0\cdot b_0)\cdot f_2]x^2+...+((a_n\cdot b_m)\cdot f_s)x^{m+s+n}$.
Como $\mathbb{K}$ é um corpo, então são válidas as propriedades associativa e distributiva para os elementos de $\mathbb{K}$. Logo,

$a_0 \cdot (f_0 \cdot b_0) = (a_0 \cdot b_0) \cdot f_0$

$a_1 \cdot (b_0 \cdot f_0) + (a_0 \cdot (b_1 \cdot f_0 + b_0 \cdot f_1)) = (a_1 \cdot b_0) \cdot f_0 + (a_0 \cdot b_1) \cdot f_0 + (a_0 \cdot b_0) \cdot f_1 = (a_1 \cdot b_0 + a_0 \cdot b_1) \cdot f_0 + (a_0 \cdot b_0) \cdot f_1$

$a_2 \cdot (b_0 \cdot f_0) + a_1 \cdot (b_1 \cdot f_0 + b_0 \cdot f_1) + a_0 \cdot (b_2 \cdot f_0 + b_1 \cdot f_1 + b_0 \cdot f_2) = (a_2 \cdot b_0) \cdot f_0 + (a_1 \cdot b_1) \cdot f_0 + (a_1 \cdot b_0) \cdot f_1 + (a_0 \cdot b_2) \cdot f_0 + (a_0 \cdot b_1) \cdot f_1 + (a_0 \cdot b_0) \cdot f_2 = (a_2 \cdot b_0 + a_1 \cdot b_1 + a_0 \cdot b_2) \cdot f_0 + (a_1 \cdot b_0 + a_0 \cdot b_1) \cdot f_1 + (a_0 \cdot b_0) \cdot f_2$
...
$a_n \cdot (b_m \cdot f_s) = (a_n \cdot b_m) \cdot f_s$.

Dessa forma, como os coeficientes dos produtos acima são iguais, segue que: $a_0\cdot(b_0\cdot f_0)+[a_1\cdot(b_0\cdot f_0)+(a_0\cdot(b_1\cdot f_0+b_0\cdot f_1))]x+[a_2\cdot(b_0\cdot f_0)+a_1\cdot(b_1\cdot f_0+b_0\cdot f_1)+a_0\cdot(b_2\cdot f_0+b_1\cdot f_1+b_0\cdot f_2)]x^2+...+a_n\cdot(b_m\cdot f_s)x^{m+s+n} = (a_0\cdot b_0)\cdot f_0+[(a_1\cdot b_0+a_0\cdot b_1)\cdot f_0+(a_0\cdot b_0)\cdot f_1]x+[(a_2\cdot b_0+a_1\cdot b_1+a_0\cdot b_2)\cdot f_0+(a_1\cdot b_0+a_0\cdot b_1)\cdot f_1+(a_0\cdot b_0)\cdot f_2]x^2+...+((a_n\cdot b_m)\cdot f_s)x^{m+s+n}$, o que implica que $p(x) \cdot (q(x) \cdot f(x)) = (p(x) \cdot q(x)) \cdot f(x)$.

□

(vii) $p(x) \cdot (q(x) + f(x)) = p(x) \cdot q(x) + p(x) \cdot f(x)$ (**distributiva**).

Demonstração. $p(x) \cdot q(x) = a_0 \cdot b_0 + (a_1 \cdot b_0 + a_0 \cdot b_1)x + (a_2 \cdot b_0 + a_1 \cdot b_1 + a_0 \cdot b_2)x^2 + ... + (a_m \cdot b_0 + ... + a_0 \cdot b_m)x^m + ... + (a_n \cdot b_m)x^{n+m}$

$p(x) \cdot f(x) = a_0 \cdot f_0 + (a_1 \cdot f_0 + a_0 \cdot f_1)x + (a_2 \cdot f_0 + a_1 \cdot f_1 + a_0 \cdot f_2)x^2 + ... + (a_s \cdot f_0 + ... + a_0 \cdot f_s)x^s + ... + (a_n \cdot f_s)x^{n+s}$

Fazendo $p(x) \cdot q(x)$ + $p(x) \cdot f(x)$ obtemos: $p(x) \cdot q(x) + p(x) \cdot f(x) = (a_0 \cdot b_0 + a_0 \cdot f_0) + ((a_1 \cdot b_0 + a_0 \cdot b_1) + (a_1 \cdot f_0 + a_0 \cdot f_1))x + ((a_2 \cdot b_0 + a_1 \cdot b_1 + a_0 \cdot b_2) + (a_2 \cdot f_0 + a_1 \cdot f_1 + a_0 \cdot f_2))x^2 + ... + ((a_s \cdot b_0 + ... + a_0 \cdot b_s) + (a_s \cdot f_0 + ... + a_0 \cdot f_s))x^s + ... + ((a_{n+s} \cdot b_0 + ... + a_{n+s-m} \cdot b_m + ... + a_0 \cdot b_{n+s}) + a_n \cdot f_s)x^{n+s} + ... + (a_n \cdot b_m)x^{n+m}$.

Por outro lado, temos que $p(x) \cdot (q(x) + f(x)) = p(x) \cdot ((b_0 + f_0) + (b_1 + f_1)x + (b_2 + f_2)x^2 + ... + (b_s + f_s)x^s + b_{s+1}x^{s+1} + ... + b_mx^m) = a_0 \cdot (b_0 + f_0) + (a_1 \cdot (b_0 + f_0) + a_0 \cdot (b_1 + f_1))x + (a_2 \cdot (b_0 + f_0) + a_1 \cdot (b_1 + f_1) + a_0 \cdot (b_2 + f_2))x^2 + ... + (a_s \cdot (b_0 + f_0) +$

$... + a_0 \cdot (b_s + f_s))x^s + ... + (a_{n+s} \cdot (f_0 + b_0) + ... + a_n \cdot (f_s + b_s) + ... + a_{n+s-m} \cdot b_m + ... + a_0 \cdot b_{n+s})x^{n+s} + ... + (a_n \cdot b_m)x^{n+m}$.

Portanto, como os coeficientes de p, q e f são elementos de $\mathbb{K}$, que é um corpo, segue que a distributiva e a associativa são válidas para os elementos de $\mathbb{K}$. Sendo assim, se utlizarmos a distributiva em quaisquer dos casos, obtemos a tese. Veja,

$a_0 \cdot (b_0 + f_0) = a_0 \cdot b_0 + a_0 \cdot f_0$
$a_1 \cdot (b_0 + f_0) + a_0 \cdot (b_1 + f_1) = a_1 \cdot b_0 + a_1 \cdot f_0 + a_0 \cdot b_1 + a_0 \cdot f_1 = (a_1 \cdot b_0 + a_0 \cdot b_1) + (a_1 \cdot f_0 + a_0 \cdot f_1)$
$a_2 \cdot (b_0 + f_0) + a_1 \cdot (b_1 + f_1) + a_0 \cdot (b_2 + f_2) = a_2 \cdot b_0 + a_2 \cdot f_0 + a_1 \cdot b_1 + a_1 \cdot f_1 + a_0 \cdot b_2 + a_0 \cdot f_2 =$
$(a_2 \cdot b_0 + a_1 \cdot b_1 + a_0 \cdot b_2) + (a_2 \cdot f_0 + a_1 \cdot f_1 + a_0 \cdot f_2)$.

...

$a_s \cdot (b_0 + f_0) + ... + a_0 \cdot (b_s + f_s) = a_s \cdot b_0 + a_s \cdot f_0 + ... + a_0 \cdot b_s + a_0 \cdot f_s =$
$(a_s \cdot b_0 + a_{s-1} \cdot b_1 + ... + a_0 \cdot b_s) + (a_s \cdot f_0 + a_{s-1} \cdot f_1 + ... + a_0 \cdot f_s)$.

...

$a_{n+s} \cdot (f_0 + b_0) + ... + a_n \cdot (f_s + b_s) + ... + a_{n+s-m} \cdot b_m + ... + a_0 \cdot b_{n+s}$. Note que $a_j = 0_{\mathbb{K}}$ para $j \in \mathbb{N}$ tal que $j > n$ e $b_i = 0_{\mathbb{K}}$, $i \in \mathbb{N}$ e $i > m$. Sendo assim
$a_{n+s} \cdot (f_0 + b_0) + ... + a_n \cdot (f_s + b_s) + ... + a_{n+s-m} \cdot b_m + ... + a_0 \cdot b_{n+s} = a_n \cdot (f_s + b_s) +$
$... + a_{n+s-m} \cdot b_m = a_n \cdot f_s + a_n \cdot b_s + ... + a_{n+s-m} \cdot b_m = (a_n \cdot b_s + ... + a_{n+s-m} \cdot b_m) + (a_n \cdot f_s)$.

Portanto, como os coefientes do primeiro membro são iguais aos coeficientes do segundo membro segue que, $p(x) \cdot (q(x) + f(x)) = p(x) \cdot q(x) + p(x) \cdot f(x)$. Perceba que não há necessidade de mostrar o caso $(q(x) + f(x)) \cdot p(x) = q(x) \cdot p(x) + f(x) \cdot p(x)$, visto que em (v), demonstramos a propriedade comutativa.

□

(viii) $\exists!\ q \in \mathbb{K}[x]$ tal que $p(x) \cdot q(x) = p(x)$ e q diferente do polinômio nulo. (**existência da unidade**)

Demonstração. Se $p(x) \cdot q(x) = p(x)$, então $(a_0 + a_1 x + ... + a_n x^n) \cdot (b_0 + b_1 x + ... + b_m x^m) = a_0 \cdot b_0 + (a_0 \cdot b_1 + a_1 \cdot b_0)x + (a_0 \cdot b_2 + a_1 \cdot b_1 + a_2 \cdot b_0)x^2 + ... + (a_n \cdot b_m)x^{n+m} = a_0 + a_1 x + ... + a_n x^n$. Sendo assim, por identidade dos polinômios obtemos que $a_0 \cdot b_0 = a_0$. Dessa forma, como os coeficientes dos polinômios p, q estão em $\mathbb{K}$,

segue que $b_0 = 1_{\mathbb{K}}$. Agora, considerando $b_0 = 1_{\mathbb{K}}$, por identidade de polinômios obtemos que $a_0 \cdot b_1 + a_1 \cdot b_0 = a_0 \cdot b_1 + a_1 \cdot 1_{\mathbb{K}} = a_1$, o que implica que $a_0 \cdot b_1 = 0_{\mathbb{K}}$, então como p é qualquer temos que $b_1 = 0_{\mathbb{K}}$. De forma similiar, considerando a equação $a_0 \cdot b_2 + a_1 \cdot b_1 + a_2 \cdot b_0 = a_2$, $b_0 = 1_K$ e $b_1 = 0_{\mathbb{K}}$, temos que $a_0 \cdot b_2 = 0_{\mathbb{K}}$ o que resulta que $b_2 = 0_{\mathbb{K}}$. Portanto, de forma recursiva, $b_1 = b_2 = ...b_m = 0_{\mathbb{K}}$, o que acarreta que $q(x) = 1_{\mathbb{K}}$. Por fim, concluímos que a unidade de $\mathbb{K}[x]$ é a unidade $\mathbb{K}$.

□

(ix) $p(x) \cdot q(x) = 0_{\mathbb{K}} \Rightarrow p(x) = 0_{\mathbb{K}}$ ou $q(x) = 0_{\mathbb{K}}$ (**Não possuí divisores de zero**)

Demonstração. Suponhamos que $p(x) \cdot g(x) = 0_{\mathbb{K}}$, isto é, $(a_0 + a_1x + ... + a_nx^n) \cdot (b_0 + b_1x + ... + b_mx^m) = a_0 \cdot b_0 + (a_0 \cdot b_1 + a_1 \cdot b_0)x + (a_0 \cdot b_2 + a_1 \cdot b_1 + a_2 \cdot b_0)x^2 + ... + (a_n \cdot b_m)x^{n+m} = 0_{\mathbb{K}} + 0_{\mathbb{K}}x + ...0_{\mathbb{K}}x^{n+m}$

Sendo assim, por identidade de polinômios, temos:

$$a_0 \cdot b_0 = 0_{\mathbb{K}} \tag{A.1}$$

$$a_0 \cdot b_1 + a_1 \cdot b_0 = 0_{\mathbb{K}} \tag{A.2}$$

$$a_0 \cdot b_2 + a_1 \cdot b_1 + a_2 \cdot b_0 = 0_{\mathbb{K}} \tag{A.3}$$

Como $\mathbb{K}$ é um corpo, da igualdade A.1 obtemos que $a_0 = 0_{\mathbb{K}}$ ou $b_0 = 0_{\mathbb{K}}$. Sem perda de generalidade, vamos considerar o caso em que $a_0 = 0_{\mathbb{K}}$ e $b_0 \neq 0_{\mathbb{K}}$.

Sendo assim, se $a_0 = 0_{\mathbb{K}}$, da equação A.2 obtemos que $a_1 \cdot b_0 = 0_{\mathbb{K}}$ o que resulta que $a_1 = 0_{\mathbb{K}}$, pois $b_0 \neq 0_{\mathbb{K}}$.

Agora, considerando $a_0 = 0_{\mathbb{K}}$ e $a_1 = 0_{\mathbb{K}}$ e $b_0 \neq 0_{\mathbb{K}}$ da igualdade A.3 obtemos que $a_2 = 0_{\mathbb{K}}$. Portanto, de forma recursiva, temos que $a_0 = a_1 = ... = a_n = 0_{\mathbb{K}}$, o que resulta que $p(x) = 0_{\mathbb{K}}$. De forma análoga se considerarmos $b_0 = 0_{\mathbb{K}}$ e $a_0 \neq 0_{\mathbb{K}}$, obtemos o caso em que $q(x) = 0_{\mathbb{K}}$. Assim, concluímos que a lei do cancelamento é válida em $\mathbb{K}[x]$.

Portanto, $\mathbb{K}[x]$ é um domínio de integridade. □