UNIVERSIDADE FEDERAL DE SERGIPE
PRÓ-REITORIA DE PÓS-GRADUAÇÃO E PESQUISA
PROGRAMA DE MESTRADO PROFISSIONAL EM MATEMÁTICA

VONICLEITON RIBEIRO SILVA

CONSTRUÇÕES COM RÉGUA E COMPASSO

SÃO CRISTÓVAO-SE
2019

VONICLEITON RIBEIRO SILVA

CONSTRUÇÕES COM RÉGUA E COMPASSO

Dissertação apresentada ao
Programa de Pós-Graduação em
Matemática, da Universidade Federal
de Sergipe, como requisito parcial
para a obtenção do título
de Mestre em Matemática

Orientador: Evilson da Silva Vieira

SÃO CRISTÓVAO-SE
AGOSTO 2019

FICHA CATALOGRÁFICA ELABORADA PELA BIBLIOTECA CENTRAL
UNIVERSIDADE FEDERAL DE SERGIPE

Silva, Vonicleiton Ribeiro
S586c Construções com régua e compasso / Vonicleiton Ribeiro Silva ; orientador Evilson da Silva Vieira. - São Cristóvão, 2019.
100 f. : il.

Dissertação (mestrado em Matemática) – Universidade Federal de Sergipe, 2019.

1. Matemática. 2. Régua de cálculo. 3. Aritmética. 4. Números complexos. 4. Polinômios. 5. Polígonos. I. Vieira, Evilson da Silva orient. II. Título.

CDU 511

Dissertação submetida à aprovação pelo Programa de Pós-Graduação em Matemática da Universidade Federal de Sergipe, como parte dos requisitos para obtenção do grau de Mestre em Matemática.

Construções com régua e compasso

por

Vonicleiton Ribeiro Silva

Aprovada pela banca examinadora:

Prof. Evilson da Silva Vieira - UFS
Orientador

Prof. Aislan Leal Fontes - UFS
Primeiro Examinador

Profa. Maria de Andrade Costa e Silva - UFS
Segundo Examinador

São Cristóvão, 29 de Agosto de 2019

AGRADECIMENTOS

Agradeço,

Ao todo poderoso Deus pela vida e saúde necessários.

À minha mãe, Cleide, pelo amor e suporte de sempre.

Ao meu pai, Evandro, e à minha vozinha, Mariita, pelo que fizeram por mim enquanto estavam vivos.

À minha namorada, Geni, pelo companheirismo e resistência às ausências.

A todos os meus amigos que, nos poucos encontros que tivemos, apresentaram palavras de apoio.

Aos meus professores, de toda vida acadêmica, pelas muitas contribuições na minha formação.

Ao meu orientador, Evilson, pelos desafios motivadores e todo o aprendizado proporcionado.

À minha parceira de dissertação, Ana Nery, pela disponibilidade de sempre, me ajudando a superar muitos desafios dessa jornada.

A todos os meus colegas do mestrado pela oportunidade de compartilharmos experiências enriquecedoras, onde foram criados laços de eterna amizade.

Ao PROFMAT e à UFS pela oferta deste maravilhoso curso.

Muitíssimo obrigado a todos que contribuíram, direta ou indiretamente, para a realização deste sonho.

RESUMO

Desde os primórdios, os povos se interessavam por construções com régua e compasso. As inquietações sobre quais construções eram ou não possíveis com o uso destes instrumentos contribuíram, e contribuem até os dias atuais, para a evolução de diversas áreas de conhecimento dentro e fora da Matemática.

Explanamos, aqui, resultados da Teoria de Grupos, do estudo de Polinômios e de Extensões de Corpos, da Teoria de Galois e da forma como esta última relaciona conceitos envolvendo grupos e corpos.

Resultados esses, que nos darão respaldo para tratarmos das questões de construtibilidade, em especial, da problemática sobre quais polígonos regulares são construtíveis com régua e compasso e, de forma mais breve, dos três problemas gregos clássicos.

Palavras-chave: Régua e Compasso; Extensões de Corpos; Números Construtíveis.

Sumário

Introdução

Desde a antiguidade, os povos se interessavam por construções utilizando somente régua não graduada e compasso. Momento em que já estabeleciam uma relação entre a Álgebra, a Aritmética e a Geometria. As atividades de construção utilizando esses instrumentos possibilitaram e possibilitam até hoje um desenvolvimento da Matemática através dos resultados obtidos com o uso desses instrumentos, como por exemplo, avanços permitidos em virtude das reflexões feitas sobre as possibilidades e impossibilidades de determinadas construções.

Nesses alicerces, trataremos aqui de um dos problemas especiais que intrigavam os matemáticos desde a antiguidade, veja [6], qual seja, o da construção de polígonos regulares utilizando régua não graduada e compasso.

Foi feita uma vasta pesquisa bibliográfica que nos possibilitou um maior entendimento da imensa e valiosa teoria que trata dos resultados que apresentamos.

Nos esforçamos para apresentar um tratamento simplificado do tema que consiga, mesmo diante da abstração necessária a teoria, obter um texto numa linguagem compreensiva e agradável. E assim, podermos vislumbrarmos melhor a beleza de todo o caminho e do que seria o ápice do tema.

O Capítulo 1 reservamos para a apresentação de alguns preliminares aritméticos, a definição e propriedades da importante Função Phi de Euler e resultados envolvendo relações de equivalência.

No Capítulo 2, introduzimos a Teoria de Grupos, onde apresentamos uma gama de resultados, os quais serviram como uma base que recorremos, com uma certa frequência, no transcorrer de todo o texto.

No Capítulo 3, fizemos um estudo do corpo $\mathbb{C}$ dos complexos, inclusive de alguns objetos geométricos no plano complexo. Isto, completa um conjunto de ferramentas teóricas que nos é necessário para o tratamento da construtibilidade. Tratamento esse, feito no Capítulo 7.

No Capítulo 4, introduzimos um estudo de polinômios sobre um corpo em uma indeterminada. Resultados sobre irredutibilidade de polinômios permitem fazer uma associação com conceitos envolvendo Extensões de Corpos.

No Capítulo 5, detalhamos Extensões de Corpos, procuramos evidenciar o uso do estudo de polinômios da validação dos resultados do capítulo e ficamos em condições de

introduzirmos, no Capítulo 6, resultados centrais da Teoria de Galois.

O Capítulo 6 reservamos para as questões de Normalidade e Separabilidade de Extensões, que culminam com os resultados essenciais da Teoria de Galois.

O Capítulo 7 é o centro do nosso trabalho. De posse de todo o aparato teórico dos capítulos anteriores, tivemos condições de descrever as possibilidades e limitações de construções com régua e compasso a luz dessas teorias.

Após descrevermos o funcionamento das construções com régua e compasso no Capítulo 7, reservamos o Capítulo 8 para apresentarmos uma caracterização dos polígonos regulares construtíveis feita por Gauss num belíssimo teorema, ápice de nosso trabalho.

No Capítulo 9, ainda pautados pelos resultados (validados) sobre construtibilidade, apresentamos demonstrações das famosas impossibilidades de duplicação do cubo, trissecção do ângulo e quadratura do círculo com o uso de régua e compasso.

Capítulo 1

Preliminares

Iremos apresentar neste capítulo uma série de definições e resultados que nos serve como pré-requisitos para auxiliar no entendimento de resultados mais intermediários e finais de nossa caminhada.

1.1 Alguns Resultados de Aritmética

Os resultados a seguir encontramos em [9], bem como suas demonstrações.

Teorema 1.1. *(Teorema Fundamental da Aritmética) Todo número $n \in \mathbb{N}, n > 1$ ou é primo ou se escreve de modo único (a menos da ordem dos fatores) como um produto de números primos.*

Proposição 1.2. *Sejam $a, b \in \mathbb{Z}$, $a \neq b$, temos que $\forall n \in \mathbb{N}$, $n \geqslant 2$,*

$$\frac{a^n - b^n}{a - b} = a^{n-1} + a^{n-2}b + \cdots + ab^{n-2} + b^{n-1}.$$

Proposição 1.3. *(Binômio de Newton) Sejam a e b números reais e $n \in \mathbb{N}$. Temos que*

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

onde $\binom{n}{i} = \dfrac{n!}{i!(n-i)!}$.

Lema 1.4. *Seja p um número primo. Então, $\binom{p}{i}$ é divisível por p, para $0 < i < p$.*

Demonstração.

Como $\binom{p}{i} = \dfrac{p!}{i!(p-i)!}$. De $p! = p(p-1)\cdots(p-i+1)(p-i)!$, temos

$$\binom{p}{i} = \frac{p!}{i!(p-i)!} = \frac{p(p-1)\cdots(p-i+1)}{i!}.$$

E assim,

$$i!\binom{p}{i} = p(p-1)\cdots(p-i+1).$$

A última igualdade mostra que $p \Big| \left(i! \cdot \binom{p}{i} \right)$. Mas, $\text{mdc}\,(p, i!) = 1$, pois, $p > i$ e é primo, assim $p \nmid i!$ e então, $p \Big| \binom{p}{i}$, como queríamos. □

Teorema 1.5. *(Pequeno Teorema de Fermat) Dado um número primo p tem-se que o número $a^p - a$ é divisível por p, $\forall a \in \mathbb{Z}$. Ou seja, $a^p \equiv a \pmod{p}$.*

Demonstração.

Se $p = 2$ o resultado é trivial, pois, $a^p - a = a(a-1)$ é par.

Seja p ímpar. Basta mostrarmos para $p \geqslant 0$, pois, resultados análogos obtém-se para p negativo.

Vamos usar indução sobre a: para $a = 0$ o resultado é válido, $p|0$.

Supondo válido para um $a \geqslant 0$, mostraremos ser válido para $a+1$: pela Proposição 1.3,

$$(a+1)^p - (a+1) = a^p - a + \binom{p}{1}a^{p-1} + \binom{p}{2}a^{p-2} + \cdots + \binom{p}{p-1}a^{p-1}.$$

Finalmente, por hipótese de indução e pelo Lema 1.4, p divide o segundo membro da igualdade acima. Logo, $a^p \equiv a \pmod{p}$. □

1.2 Função Phi de Euler

Apresentamos a seguir uma função que nos será muito útil em nossos propósitos. Algumas características e propriedades dessa função são essenciais em resultados centrais deste trabalho.

Definição 1.6. Seja φ a seguinte função:

$$\begin{array}{rccc} \varphi: & \mathbb{N} & \longrightarrow & \mathbb{N} \\ & n & \longmapsto & \varphi(n), \end{array}$$

onde $\varphi(n) = \#(\{0 < m < n : \text{mdc}\,(m, n) = 1, m \in \mathbb{Z}\})$, onde $\#(A)$ denota a cardinalidade do conjunto A. Esta função é a que chamamos de Função Phi de Euler.

Proposição 1.7. *Sejam p primo e $n \in \mathbb{N}$. Então, $\varphi(p^n) = (p-1)p^{n-1}$.*

Demonstração. De 1 até p^n temos p^n números naturais. Pela Definição 1.6, se excluirmos do conjunto desses números os números que não são primos com p^n obtemos exatamente o conjunto que queremos determinar a cardinalidade. Como p é primo, os números que queremos excluir são precisamente os múltiplos de p, $\{p, 2p, \ldots, p^{n-1}p\}$, ou seja, são precisamente p^{n-1} números. Logo,

$$\varphi(p^n) = p^n - p^{n-1} = (p-1)p^{n-1}$$

□

Definição 1.8. Chamamos de "Sistema Completo de Resíduos Módulo n" a todo conjunto de números inteiros cujos restos na divisão por n são os números $0, 1, 2, \ldots, n-1$, sem repetições e numa ordem qualquer.

Lema 1.9. *Sejam $a, k, n \in \mathbb{Z}$, com $n > 1$ e $\text{mdc}\,(k, n) = 1$. Se $a_1, \ldots, a_n$ é um sistema completo de resíduos módulo n, então*

$$a + ka_1, \ldots, a + ka_n$$

também é um sistema completo de resíduos módulo n.

Demonstração. Encontramos em [9]. □

Proposição 1.10. *Sejam p e q primos entre si. Então, $\varphi(pq) = \varphi(p)\varphi(q)$.*

Demonstração.

Se $p = 1$ ou $q = 1$ o resultado é válido trivialmente. Sejam $p > 1$ e $q > 1$. Considere a seguinte tabela com os números de 1 a pq.

$$\begin{array}{ccccccc} 1 & 2 & \ldots & j & \ldots & q \\ q+1 & q+2 & \ldots & q+j & \ldots & 2q \\ \vdots & \vdots & & \vdots & & \vdots \\ (p-1)q+1 & (p-1)q+2 & \ldots & (p-1)q+j & \ldots & pq \end{array}$$

Para determinar quantos dos números na tabela acima são primos com pq, ou seja, $\varphi(pq)$, notemos que $\text{mdc}\,(k, pq) = 1$ se, e somente se, $\text{mdc}\,(k, p) = 1 = \text{mdc}\,(k, q)$. Desta forma, basta determinarmos na tabela quantos dos números são primos com p e q simultaneamente.

Se o primeiro número de uma coluna não for primo com q então os demais números da coluna também não são (pois, os demais números da coluna são resultados da soma de um múltiplo de q com o primeiro número da coluna). Portanto, os números que queremos fazer a contagem estão necessariamente nas outras colunas, que são em número $\varphi(q)$, onde estão os primos com q.

Agora, analisando essas $\varphi(q)$ colunas, quais dos números dessas colunas são primos com p?

Como $\text{mdc}\,(p, q) = 1$, pelo Lema 1.9, a sequência

$$j, q + j, \ldots, (p-1)q + j$$

forma um sistema completo de resíduos módulo p e, assim, $\varphi(p)$ desses números são primos com p.

Portanto, podemos concluir que $\varphi(p) \cdot \varphi(q)$ dos números da tabela são, simultaneamente primos com p e q, logo $\varphi(pq) = \varphi(p) \cdot \varphi(q)$. □

1.3 Relação de Equivalência e Conjunto Quociente

É importante que o leitor esteja familiarizado com o conceito de relação de equivalência. De qualquer forma, pelo seu auxílio na compreensão dos importantes resultados sobre "Classes Laterais" que veremos mais a frente, faremos aqui uma breve explanação do mesmo.

Seja um conjunto C, e uma relação R entre pares de elementos de C. Dados dois elementos $a, b \in C$ fazemos aRb para dizer que a se relaciona com b por R. Esta relação é dita "de Equivalência" se ela satisfazer as seguintes propriedades:

Para todos $a, b, c \in C$, valem

1. Reflexividade, aRa para todo $a \in C$;
2. Simetria, se aRb, então bRa;
3. Transitividade, se aRb e bRc, então aRc.

Diante de uma relação de equivalência surge a "classe de equivalência de um elemento". Seja um conjunto C e um elemento $a \in C$, definimos como classe de equivalência $\overline{a}$ do elemento a em relação a R, o conjunto $\overline{a} = \{x \in C; xRa\}$.

Uma imediata e valiosa consequência de uma relação de equivalência é que ela "particiona" um conjunto, vejamos isso na proposição seguinte, cuja demonstração pode ser vista em [8]:

Proposição 1.11. *Sejam uma relação R em um conjunto C e $a, b \in C$. Então:*

1. $\overline{a} = \overline{b}$ *se, e somente se,* aRb;
2. *Se* $\overline{a} \neq \overline{b}$, *então* $\overline{a} \cap \overline{b} = \varnothing$;
3. $\bigcup_{a \in C} \overline{a} = C$.

Demonstração. Disponível em [8]. □

Chegamos à congruência $\mod n$:

Exemplo 1.12. No conjunto $\mathbb{Z}$ dos números inteiros definimos uma relação R da seguinte forma:

Dado um $n \in \mathbb{Z}$. Seja $a, b \in \mathbb{Z}$ dizemos que aRb se, e somente se, $a - b$ for um múltiplo de n. Verifica-se facilmente que esta relação R, que denotamos por $\equiv \pmod n$, é uma relação de equivalência em $\mathbb{Z}$.

Desta forma, pela Proposição 1.11, esta relação particiona o conjunto $\mathbb{Z}$.

Em [8], podemos ver uma prova de que $\equiv \pmod n$ nos fornece n classes distintas dadas por $\left\{\overline{0}, \overline{1}, \ldots, \overline{n-1}\right\}$.

Após introduzirmos a definição de relação de equivalência apresentamos uma noção diretamente associada, que é a de "Conjunto Quociente".

Definição 1.13. Dada uma relação de equivalência R num conjunto C, definimos como conjunto quociente de C por R, C/R, ao conjunto de todas as classes de equivalência relacionadas à R.

Exemplo 1.14. Na congruência mod 5, pelo Exemplo 1.12, determinamos o seguinte conjunto quociente: $\frac{\mathbb{Z}}{\equiv \text{ mod } 5} = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{4}\}$. De maneira mais elegante, escrevemos este conjunto como $\mathbb{Z}_5$.

Capítulo 2

Grupos

Nesse capítulo, damos uma introdução a Teoria de Grupos. A gama de resultados que apresentamos aqui, são frequentemente revisitados e utilizados no desenvolver dos capítulos seguintes.

Valiosas contribuições para a Teoria de Grupos foram dadas por Évariste Galois, foi ele, inclusive, quem primeiro utilizou a palavra "grupo" em seu sentido técnico, veja [6]. Mais a frente, quando apresentarmos o Teorema da Correspondência de Galois, veremos como esse teorema é eficaz na demonstração do surpreendente Teorema de Gauss sobre a caracterização de polígonos regulares construtíveis, que acaba por ser o resultado principal de nosso trabalho.

2.1 Grupos

Definição 2.1. Grupo é um par formado por um conjunto G e uma operação $*$ que associa dois elementos desse grupo (por exemplo a e b) a um terceiro $a*b$ nesse mesmo conjunto, onde essa operação satisfaz determinadas condições. Quais sejam essas condições:

i - Associatividade, ou seja: sejam a, b, c elementos de G, então $(a*b)*c = a*(b*c)$;

ii - Existência de um elemento neutro e tal que: $a*e = e*a = a$ para todo $a \in G$;

iii - Existência de inversos a' para todo $a \in G$, tais que: $a*a' = a'*a = e$.

Notação 2.2. Por vezes utilizaremos G para denotar o grupo $(G, *)$, o que não prejudicará o entendimento em virtude do contexto, da mesma forma, por vezes, utilizaremos ab para representar $a*b$, e a^{-1} para representar o inverso a'.

Obs: Se além dessas condições o grupo satisfazer a seguinte dizemos que o grupo é abeliano:

$\star$ Comutatividade, ou seja: para todos $a, b \in G$, temos $a*b = b*a$.

A denominação "abeliano" é em homenagem a Niels Henrik Abel, outro grande matemático que deu valiosas contribuições a Teoria de Grupos.

Apresentamos algumas propriedades decorrentes da definição de grupos:

Proposição 2.3. *O elemento neutro e cada inverso são únicos.*

Demonstração.

i - Unicidade do elemento neutro:

Sejam e_1 e e_2 dois elementos neutros de um grupo G, precisamos mostrar que, necessariamente, $e_1 = e_2$. De fato, $e_1 = e_1 * e_2$ por e_2 ser elemento neutro do grupo, e $e_1 * e_2 = e_2$ por e_1 ser também elemento neutro do grupo, sendo assim, então

$$e_1 = e_1 * e_2 = e_2.$$

ii - Unicidade de cada inverso:

Sejam a'_1 e a'_2 dois inversos de um elemento a, precisamos mostrar que, necessariamente, $a'_1 = a'_2$. De fato,

$$a'_1 = a'_1 * e = a_1 * (a * a'_2) = (a_1 * a) * a'_2 = e * a'_2 = a'_2.$$

□

Exemplo 2.4.

1 - $(\mathbb{Z}, +)$ (grupo aditivo dos inteiros - com a adição usual dos inteiros);

2 - $(\mathbb{Z}_n, \oplus)$ (grupo aditivo dos inteiros $\mod n$ - com a adição $\mod n$ dos inteiros);

3 - $(\mathbb{Q}\backslash\{0\}, \cdot)$ (grupo multiplicativo dos racionais não nulos - com a multiplicação usual dos racionais);

4 - $(\mathbb{Z}_n^*, *)$ (grupo multiplicativo das unidades de inteiros $\mod n$ - com a multiplicação $\mod n$ dos inteiros);

5 - $(\mathbb{C}^1, \cdot)$ (grupo multiplicativo dos complexos $z = a + bi$ tais que $a^2 + b^2 = 1$, onde $\mathbb{C}^1$ é o círculo unitário);

6 - $(U_n, \cdot)$ (grupo multiplicativo das raízes n-ésimas da unidade - com a multiplicação usual dos complexos)(onde $U_n = \{x \in \mathbb{C}; x^n - 1 = 0\}$);

7 - $(D_n, *)$ (grupo diedral ou grupo das simetrias de um n-ágono regular - com a operação composição de simetrias).

Chamamos de "ordem de G", $|G|$, de um grupo G, o número de elementos do conjunto G desse grupo, quando o conjunto G tem infinitos elementos dizemos que $|G| = \infty$.

2.2 Subgrupos

Dado um subconjunto H de um grupo G, estabelecemos a seguinte definição:

Definição 2.5. Subgrupo de um grupo G é, basicamente, um grupo $(H, *)$ onde H é um subconjunto não vazio de G e $*$ é a restrição da operação $*$ de G aos elementos de H.

Notação 2.6. Usaremos $H < G$ para representar que H é subgrupo de G.

Proposição 2.7. *Sejam G um grupo, $H \neq \varnothing$ um subconjunto de G, H com a restrição da operação de G a H é um subgrupo de G se, e somente se, $a * b' \in H$ sempre que $a, b \in H$.*

Demonstração.

$\Rightarrow$) Seja $H < G$, notemos inicialmente alguns resultados:

i - Os elementos neutros de G e H são os mesmos, ou seja, $e_g = e_h$;

ii - Sendo $b \in H$, temos $b'_g = b'_h$, os elementos inversos de um elemento $b \in H$ são os mesmos tanto em H quanto em G.

Com isso, tomando $a, b \in H$, temos que $b' \in H$, pois H é grupo. E pelo mesmo motivo, $a * b' \in H$.

$\Leftarrow$) Se $a * b' \in H$ sempre que $a, b \in H$, precisamos mostrar que $H < G$, para isso basta verificarmos os seguintes itens:

i - Como $H \neq \emptyset$ tomemos $a \in H$ e, da hipótese, $a * a' = e \in H$;

ii - De item anterior, $e \in H$. Assim, sempre que $b \in H$, temos $b' \in H$, pois, da hipótese, $e * b' = b' \in H$;

iii - H é fechado para sua operação. Pois, da hipótese e do item anterior, se $a, b \in H$ então $b' \in H$ e, assim, com a e $b' \in H$ teremos $a * (b')' \in H$, logo $a * b \in H$;

iv - Acontece a associatividade, pois se $a, b, c \in H$, então $a, b, c \in G$ e em G acontece a associatividade.

□

Exemplo 2.8.

1 - Se $(G, *)$ é um grupo, $(\{e\}, *)$ e o próprio G são subgrupos do grupo G, ditos subgrupos triviais;

2 - (Retirado de [7]) Seja $U_n = \left\{1, e^{\frac{2\pi i}{n}}, e^{\frac{4\pi i}{n}}, \ldots, e^{\frac{2(n-1)\pi i}{n}}\right\}$(o grupo multiplicativo das raízes n-ésimas da unidade). Temos a seguinte cadeia de subgrupos de $\mathbb{C} - \{0\}$:

$$U_n < \bigcup_{j\in\mathbb{N}} U_j = \{\text{raizes da unidade}\} < \mathbb{C}^1 < \mathbb{C} - \{0\}$$

onde $\mathbb{C}^1$ é o grupo dos números complexos de norma 1, citado no item 5 do Exemplo 2.4.

3 - $D_n < S_n$, onde D_n é o grupo Diedral ou grupo das simetrias do polígono regular de n lados e S_n é o grupo das permutações de n elementos, (note que neste exemplo estamos relacionando grupos de elementos diferentes, isso será elucidado quando introduzirmos o conceito de isomorfismo. E então, o que diremos é que: o grupo das permutações isomorfo a D_n, é subgrupo de S_n).

Conseguiremos determinar características importantes de subgrupos e grupos que, devido a Teoria de Galois, podemos relacionar com resultados de corpos, conceito que vamos introduzir e detalhar em capítulos posteriores. Essas relações, conjuntamente com outras que envolvem, por exemplo, o conceito de polinômio, explana e valida os resultados que precisamos sobre as construções com régua e compasso.

2.2.1 Subgrupo Gerado por um Elemento

Definição 2.9. Seja G um grupo e $a \in G$. Definimos potência inteira de a da seguinte forma:

i) $a^0 = e$;

ii) $a^n = a^{n-1} * a$, se $n \geqslant 1$;

iii) $a^n = (a^{-n})^{-1}$, se $n < 0$.

A partir desta definição, apresentamos o conceito de subgrupo "gerado" a partir de um elemento:

Definição 2.10. Seja a um elemento de um grupo G, definimos como "subgrupo gerado por a", ao conjunto:

$$\langle a\rangle = \{a^n; n \in \mathbb{Z}\}$$

Na próxima proposição demonstramos que o conjunto dado por essa definição é realmente um subgrupo.

Proposição 2.11. *Dado um grupo G, o conjunto $\langle a\rangle$ com a operação de G é um subgrupo de G.*

Demonstração. Pela Proposição 2.7, é suficiente verificarmos os seguintes dois itens.

i - $\langle a\rangle \neq \varnothing$. De fato, $e \in \langle a\rangle$, pois, $e = a^0$ e como $0 \in \mathbb{Z}$, $a^0 \in \langle a\rangle$;

ii - $xy^{-1} \in \langle a\rangle$ sempre que $x, y \in \langle a\rangle$. Ora, se $x, y \in \langle a\rangle$, temos que $x = a^r$ e $y = a^s$, para alguns $r, s \in \mathbb{Z}$. Assim, $xy^{-1} = a^r a^{-s} = a^{r-s}$, logo $xy^{-1} = a^m \in \langle a\rangle$ para $m = r - s \in \mathbb{Z}$.

□

Chamamos de "ordem de a", $|a|$, de um elemento $a \in G$, ao número de elementos do conjunto $\langle a\rangle$, quando este conjunto é infinito denotamos $|a| = \infty$.

2.3 Classes Laterais

O que foi apresentado na Seção 1.3, nos deixa em condições de estabelecermos o conceito de "Classes Laterais" (nesta seção) e resultados correlatos, como o de Grupo Quociente (na seção seguinte).

Seja G um grupo, H um subgrupo de G e $x \in G$, chamamos de "classe lateral a esquerda de H em G, por x" o conjunto:

$$xH = \{x * h; h \in H\}$$

De maneira análoga, definimos a "classe lateral a direita de H em G, por x"

$$Hx = \{h * x; h \in H\}$$

Dado um subgrupo H de um grupo G, pela forma como foi definido as classe laterais, obtemos o seguinte resultado com relação ao número de elementos/representantes das classes laterais.

Proposição 2.12. *Todas as classes laterais de H em G tem a mesma cardinalidade, igual a cardinalidade de H.*

Demonstração. Resultados semelhantes aos obtidos aqui, podem ser obtidos para classes laterais a direita Hx.

Se verificarmos que a seguinte função é bijetiva, terminamos a demonstração.

Seja a função:

$$\begin{array}{rccc} f: & H & \longrightarrow & xH \\ & h & \longmapsto & xh \end{array}$$

i - Sejam $xh_1, xh_2 \in xH$ tais que

$$xh_1 = xh_2$$

por x pertencer ao grupo G ele tem inverso x' e, assim

$$\begin{array}{rcl} x'xh_1 & = & x'xh_2 \Leftrightarrow \\ h_1 & = & h_2 \end{array}$$

Provando a injetividade;

ii - Agora, tomemos um $y \in xH$, então $\exists h_i \in H$ tal que $y = xh_i$ e, assim

$$f(h_i) = y$$

Provando a sobrejetividade.

De (i) e (ii), temos a bijetividade. □

Apresentamos a seguir a definição de "índice", a qual está diretamente relacionada à noção de Grupo Quociente, esta última será detalhada na Seção 2.4.

Definição 2.13. Sendo G um grupo e H um subgrupo de G. Como consequência da Proposição 2.12, o número de elementos do conjunto das classes laterais a esquerda de H em G é igual ao número de elementos do conjunto das classes laterais a direita de H em G. Esse número chamamos de "índice de H em G" e denotamos por $(G : H)$.

Apresentamos, a seguir, o importante Teorema de Lagrange que relaciona as ordens de grupos e subgrupos.

Teorema 2.14. *(Lagrange) Sejam G um grupo finito e H um subgrupo de G. Então,*

$$|G| = (G : H)|H|.$$

Demonstração. Seja G um grupo finito de ordem n e $H < G$. Pela Proposição 1.11, uma relação de equivalência em G o particiona. Sendo assim, temos

$$|G| = |x_1H| + |x_2H| + \cdots |x_mH|,$$

onde, $x_1H, x_2H, \ldots, x_mH$ são as m classes laterais (distintas, pela Proposição 1.11) de H em G.

Pela Proposição 2.12, $|x_iH| = |H|$ para todo $1 \leqslant i \leqslant m$. Assim,

$$|G| = m \cdot |H|.$$

Pela definição de índice, segue o resultado:

$$|G| = (G : H)|H|.$$

□

2.4 Subgrupos Normais e Grupos Quocientes

Definição 2.15. (Subgrupo Normal) Seja G um grupo e H um subgrupo de G, diremos que H é um subgrupo normal de G, denotamos por $H \lhd G$, se $xH = Hx$ para todo $x \in G$, ou seja, se as classes laterais a esquerda de H em G são iguais as classes laterais a direita de H em G. Quando isso acontece temos $xHx^{-1} = x^{-1}Hx = H, \forall x \in G$.

A noção de "Subgrupo Normal" é fundamental em nossos propósitos, tem resultados centrais do trabalho que só são válidos devido a peculiaridades exclusivas de subgrupos normais. A seguir apresentamos alguns exemplos de subgrupos normais.

Exemplo 2.16. Seja G um grupo.

i - Seja H um subgrupo de G. Se $(G : H) = 2$, então $H \lhd G$.

De fato, como $(G : H) = 2$, temos duas classes laterais. Assim, se $x \in H$, então $xH = H = Hx$. Se $x \notin H$, temos a classe $xH \notin H$ e ficamos com as classes laterais a esquerda H e xH. De maneira análoga, temos como classes laterais a direita H e Hx. Como vimos as classes laterais particionam o grupo, portanto, $xH \notin H$ e $Hx \notin H$ implica $xH = Hx$. Pela Definição 2.15, $H \lhd G$.

ii - O conjunto $Z(G) = \{a \in G; ax = xa, \forall x \in G\}$, que chamamos de centro de G, é um subgrupo normal de G.

De fato, para todo $a \in Z(G)$ e todo $x \in G$, pela definição de $Z(G)$, $ax = xa$. Assim, $xZ(G) = Z(G)x$ e, pela Definição 2.15, $Z(G) \lhd G$.

iii - Se $H < Z(G)$, então $H \lhd G$.

De fato, como $H < Z(G)$, temos $ax = xa$, para todo $x \in H$ e, o resultado segue análogo ao item anterior.

O próximo resultado evidencia a relação entre os conceitos de "Classes Laterais" e "Subgrupos Normais".

Proposição 2.17. *Se G é abeliano, então todo subgrupo de G é normal.*

Demonstração. Seja G um grupo abeliano e H um subgrupo de G. Pela Definição de subgrupo normal 2.15, H é um subgrupo normal de G se, $xH = Hx$ para todo $x \in G$.

Dito isso, tomemos $x \in G$ e seja $h_1, h_2, \ldots, h_n$ os elementos de H, temos

$$xH = \{xh_1, xh_2, \ldots, xh_n\}.$$

Por G ser abeliano, $ab = ba$ para todos $a, b \in G$. Assim, como os elementos de H naturalmente pertencem a G, temos $xh_i = h_i x$ para todo $1 \leqslant i \leqslant n$, o que nos leva a

$$xH = \{xh_1, xh_2, \ldots, xh_n\} = \{h_1 x, h_2 x, \ldots, h_n x\} = Hx,$$

demonstrando que $H \lhd G$. □

A seguinte definição, vista em [4], complementa o que já vimos sobre classes laterais e permite definir "Grupo Quociente".

Definição 2.18. (Operação Multiplicação de Subconjuntos) Seja G um grupo, A e B subconjuntos de G. Definimos o produto AB por:

$$AB = \varnothing,$$

se $A = \varnothing$ ou $B = \varnothing$ e

$$AB = \{xy | x \in A \text{ e } y \in B\},$$

se $A \neq \varnothing$ e $B \neq \varnothing$.

Na próxima definição, notemos que só faz sentido definir "Grupo Quociente" quando consideramos um subgrupo normal. No transcorrer do texto, frequentemente, percebemos a relevância do conceito de subgrupo normal.

Definição 2.19. (Grupo Quociente) Seja G um grupo e H um subgrupo normal de G, "Grupo Quociente de G por H", denotamos por $(G/H, *)$ ou simplesmente G/H, é o par formado pelo conjunto das classes laterais a esquerda de H em G, G/H, com a operação $*$ multiplicação de subconjuntos restrita à G/H.

2.5 P-Grupos Finitos

Nesta seção relatamos características de uma classe de grupo da qual temos uma especial necessidade.

Definição 2.20. Sejam p um número primo e G um grupo finito tal que $|G|$ é igual uma potência de p. G é dito um p-grupo.

Proposição 2.21. *Seja G um p-grupo finito de ordem p^n, onde p é primo e $n \geqslant 1$. Então, existe um subgrupo H de G tal que $|H| = p$.*

Demonstração.

Seja G um p-grupo finito tal que $|G| = p^n$. Como $n \geqslant 1$ a ordem de G é um múltiplo de p, assim, $e \neq \exists \alpha \in G$. Pelo Teorema 2.14 (Teorema de Lagrange), o subgrupo $\langle \alpha \rangle$ tem ordem p^k, com $1 \leqslant k \leqslant n$. Se $k = 1$, terminamos a prova.

Seja $k \neq 1$. Note que $|\alpha| = p^k$. Tomemos $\beta = \alpha^{p^{k-1}}$ e seja $H = \langle \beta \rangle$ afirmamos que,

$$H = \langle \beta \rangle = \left\{\beta, \beta^2, \ldots, \beta^p\right\}.$$

De fato, como $|\alpha| = p^k$ e, pela forma como definimos β, os elementos $\beta, \beta^2, \ldots, \beta^p$ são todos distintos e,

$$\beta^p = (\alpha^{p^{k-1}})^p = \alpha^{p^k} = e.$$

Portanto, $|H| = |\langle \beta \rangle| = p$. □

Proposição 2.22. *Seja G um p-grupo finito de ordem p^n com p primo e $n \geqslant 1$. Então, $|Z(G)| \geqslant p$.*

Demonstração. Disponível em [7]. □

2.6 Homomorfismos e Isomorfismos de Grupos

Apresentamos, nesta seção, um encadeamento de informações que nos dará familiaridade com os conceitos de "homomorfismo", "isomorfismo" e "automorfismo" de maneira que, quando estivermos em capítulos posteriores, teremos condições de falar destes termos com naturalidade.

Definição 2.23. Seja $(G, *)$ e $(J, \cdot)$ dois grupos e $f : G \longrightarrow J$ uma função, dizemos que f é um homomorfismo de grupos se $f(a * b) = f(a) \cdot f(b)$ para todos $a, b \in G$.

Observação: nas condições da Definição 2.23, quando f é bijetiva dizemos que f é um isomorfismo.

Notação 2.24. Se existe um isomorfismo $f : G \longrightarrow J$, dizemos que G e J são isomorfos, $G \simeq J$.

Notemos que, em outras palavras, a Definição 2.23 diz que uma função que aplica elementos de um grupo em outro é um homomorfismo se ela "preservar" as operações.

No caso do isomorfismo, temos que além da função preservar as operações, os elementos dos grupos são associados bijetivamente. Isso nos trás como consequência que qualquer dos grupos isomorfos pode ser analisado através do outro, ou seja, as conclusões tiradas na análise dum grupo tem suas correspondentes no outro. Essa consequência, a depender das características dos grupos, suas operações e seus elementos, pode facilitar análises sobre esses grupos.

Exemplo 2.25. Seja $f : (\mathbb{Z}, +) \longrightarrow (\mathbb{Z}, +), f(x) = ax$ para um $a \in \mathbb{Z}, f$ é um homomorfismo.

De fato, sejam $\alpha, \beta \in \mathbb{Z}$, temos que $f(\alpha + \beta) = a(\alpha + \beta) = a\alpha + a\beta = f(\alpha) + f(\beta)$.

Proposição 2.26. *Seja G e J grupos, e_G e e_J os elementos neutros de G e J, respectivamente, e $f : G \longrightarrow J$ um homomorfismo. Então:*

i - $f(e_G) = e_J$;

ii - $f(x^{-1}) = [f(x)]^{-1}$.

Demonstração.

As operações nos dois grupos serão denotadas indistintamente por "$\cdot$".

i - $f(e_G) = e_J$. De fato, utilizando a definição de homomorfismo,

$$f(e_G) = f(e_G \cdot e_G) = f(e_G) \cdot f(e_G). \tag{2.1}$$

Por outro lado, pelo fato de $f(e_G)$ e e_J serem elementos de J com e_J o elemento neutro, temos

$$f(e_G) = e_J \cdot f(e_G). \tag{2.2}$$

De 2.1 e 2.2,

$$e_J \cdot f(e_G) = f(e_G) \cdot f(e_G).$$

E, por fim,

$$\begin{aligned} e_J \cdot f(e_G) \cdot [f(e_G)]^{-1} &= f(e_G) \cdot f(e_G) \cdot [f(e_G)]^{-1} \Leftrightarrow \\ e_G &= f(e_G). \end{aligned}$$

ii - $f(x^{-1}) = [f(x)]^{-1}$. De fato, da definição de homomorfismo, das propriedades do elemento neutro e do item anterior,

$$f(x) \cdot f(x^{-1}) = f(x \cdot x^{-1}) = f(e_G) = e_J = f(x) \cdot [f(x)]^{-1},$$

que resulta em,

$$\begin{aligned} f(x) \cdot f(x^{-1}) &= f(x) \cdot (f(x))^{-1} \Leftrightarrow \\ (f(x))^{-1} \cdot f(x) \cdot f(x^{-1}) &= (f(x))^{-1} \cdot f(x) \cdot (f(x))^{-1} \Leftrightarrow \\ f(x^{-1}) &= (f(x))^{-1}. \end{aligned}$$

□

Proposição 2.27. *Sejam G, J e L grupos, $f : G \longrightarrow J$ e $g : J \longrightarrow L$ homomorfismos/homomorfismos injetores/homomorfismos sobrejetores. Então, $f \circ g : G \longrightarrow L$ é um homomorfismo/homomorfismo injetor/homomorfismo sobrejetor.*

Demonstração.

Denotaremos as operações nos dois grupos indistintamente por $\cdot$.

Primeiramente para o caso dos homomorfismos:

Se $a, b \in G$, então, pela definição de homomorfismo, conjuntamente com as propriedades da composição de funções, temos que,

$$(g \circ f)(a \cdot b) = g(f(a \cdot b)) = g(f(a) \cdot f(b)) = g(f(a)) \cdot g(f(b)) = (g \circ f)(a) \cdot (g \circ f)(b).$$

Assim,

$$(g \circ f)(a \cdot b) = (g \circ f)(a) \cdot (g \circ f)(b).$$

Provando que $f \circ g$ é um homomorfismo.

Para os casos de homomorfismos injetores/sobrejetores, basta notarmos que, das propriedades de composição de funções, a composição de duas funções injetoras/sobrejetoras é injetora/sobrejetora. □

Definição 2.28. Dado um homomorfismo $f : G \longrightarrow J$. O conjunto:

$$\text{Ker}\, f = \{x \in G; f(x) = e_J\}$$

é chamado núcleo de f.

Exemplo 2.29. Dado um homomorfismo $f : G \longrightarrow J$, temos:

i - O conjunto $\text{Ker}\, f$ com a operação de G é um subgrupo normal de G;

ii - O conjunto $Imf = \{x \in G; f(x) \in J\}$ com a operação de J é um subgrupo de J;

iii - f é injetivo se, e somente se, $\text{Ker}\, f = \{e_G\}$.

O seguinte teorema, cuja demonstração encontramos em [4], [7] ou [13], serve como um método para encontrar um isomorfismo, e assim, fazer uso de suas consequências, já comentadas nesta seção.

Teorema 2.30. *(Teorema dos isomorfismos)*
Dados um homomorfismo de grupos $f : G \longrightarrow H$ e $N = \text{Ker}\, f$ seu núcleo. A aplicação:

$$\begin{array}{rccc} \iota: & G/N & \longrightarrow & H \\ & gN & \longmapsto & f(g) \end{array}$$

é injetiva. Em particular, G/N é isomorfo ao $f(G)$. Ou seja, se o homomorfismo dado for sobrejetivo teremos $G/N \simeq H$.

O exemplo a seguir, retirado de [7], contribuirá tanto para o entendimento do teorema acima como mostrará a utilidade do mesmo na identificação de um isomorfismo.

Exemplo 2.31. Seja $f : (\mathbb{Z}, +) \longrightarrow (\mathbb{U}_n, \cdot)$ dado por $f(k) = e^{\frac{2k\pi i}{n}}$. Temos que f é um homomorfismo sobrejetor e $\text{Ker}\, f = n\mathbb{Z}$. Portanto, pelo Teorema 2.30 (Teorema dos Isomorfismos), $(\mathbb{Z}/n\mathbb{Z}, +) \simeq (\mathbb{U}_n, \cdot)$.

Definição 2.32. Seja G um grupo. Um isomorfismo de G em G é dito um automorfismo.

"Automorfismos" serão vistos com maiores detalhes quando tratarmos de corpos, onde iremos estender o conceito para automorfismos de corpos e tratarmos dos grupos de automorfismos.

2.7 Grupos Cíclicos

Nesta seção, damos continuidade a resultados apresentados na Subseção 2.2.1 (onde tratamos dos subgrupos gerados por um elemento).

Definição 2.33. Um grupo G é cíclico se existe $a \in G$ tal que $G = \langle a \rangle$.

Pela Definição 2.10, verificamos que os dois exemplos a seguir mostram de fato grupos que são gerados por potências dos geradores apresentados.

Exemplo 2.34.

1 - $(\mathbb{Z}, +)$ é um grupo cíclico, pois, $(\mathbb{Z}, +) = \langle 1 \rangle = \langle -1 \rangle$;

2 - $(\mathbb{Z}_n, \oplus)$ é um grupo cíclico, pois, $(\mathbb{Z}_n, \oplus) = \langle \bar{1} \rangle$.

Na próxima proposição, cuja demonstração encontra-se em [13], há uma síntese de todos os grupos cíclicos existentes, a menos de isomorfismos. Assim, temos informações suficientes para nosso trabalho no que se refere a grupos cíclicos.

Proposição 2.35. *Seja G um grupo cíclico. Então:*

i - Se G é infinito, $G \simeq \mathbb{Z}$;

ii - Se G é finito de ordem n, $G \simeq \mathbb{Z}_n$.

Demonstração. Disponível em [13]. □

Proposição 2.36. *Todo subgrupo de um grupo cíclico é cíclico.*

Demonstração. Sejam G um grupo cíclico e H um subgrupo de G. Vamos analisar dois casos:

i - Se G é infinito:

Pela Proposição 2.35, $G \simeq \mathbb{Z}$, com isso, pode-se verificar que $H = a\mathbb{Z}$ para algum $a \geqslant 0$, onde $a\mathbb{Z}$ denota o subgrupo formado pelos múltiplos de a.

ii - Se G é finito:

Lembremos que por G ser cíclico $G = \langle g \rangle$ para algum $g \in G$. Dito isto, seja d o menor inteiro positivo tal que $g^d \in H$. Tomemos um $h \in H$, ou seja, $h = g^a$ para algum $a \in \mathbb{Z}$. Dividindo a por d, obtemos

$$a = qd + r, \text{com } 0 \leqslant r < d.$$

Notemos que $g^d, g^a \in H$ e, como H é subgrupo, $g^{-qd} \in H$ também, bem como $g^{a-qd} \in H$, ou seja, $g^r \in H$.

Este último resultado implica, pela minimalidade de d, que $r = 0$. Logo, $h = g^a = g^{qd} = (g^d)^q$, portanto, $H = \langle g^d \rangle$.

□

A seguir, fizemos uso do Teorema 2.14 (Teorema de Lagrange) para a demonstração de um resultado sobre grupos finitos de ordem p, onde p é primo.

Proposição 2.37. *Se G é um grupo finito de ordem p primo, então G é cíclico.*

Demonstração. Seja G um grupo finito tal que $|G| = p$, onde p é primo. Pelo Teorema 2.14 (Teorema de Lagrange), $|H|$, de um subgrupo H de G, divide $|G|$.

Por $|G|$ ser prima, temos $|H|$ igual a 1 ou p. Assim, G só admite os subgrupos triviais $\{e\}$ e G.

Agora tomemos um elemento $a \in G$, o subgrupo gerado por a (veja a Subseção 2.2.1) será $\{e\}$ ou G caso, respectivamente, $a = e$ ou $a \neq e$. Dessa forma, $G = \langle a \rangle$ para algum $a \in G$, $a \neq e$, esse resultado, pela Definição 2.33, implica que G é cíclico. □

Capítulo 3

Um pouco sobre os Números Complexos

Na capítulo 7 faremos uma análise da construtibilidade no plano complexo. Por isso, consideramos fundamental reservar este capítulo para descrever representações, operações e outros resultados que envolvem o corpo dos números complexos. Ao tempo, que relembramos uma bijeção entre números complexos e pontos do plano $\mathbb{R}^2$.

Para uma melhor associação entre as operações geométricas e algébricas que serão apresentadas recomendamos familiaridade com o conteúdo "operações entre vetores", que pode ser encontrado em [2] e [18].

3.1 Representações e Operações dos Complexos

3.1.1 Representação e Operações Aritméticas

O conjunto dos números da forma $z = a + bi$, com $a, b \in \mathbb{R}$ e i a unidade imaginária, onde $i^2 = -1$ é conhecido como o conjunto dos números complexos $\mathbb{C}$. Recordamos aqui as operações de soma e produto em $\mathbb{C}$, bem como, outros conceitos relacionadas a este corpo (maiores detalhes podem ser vistos em [18]).

Sejam $(a + bi), (c + di) \in \mathbb{C}$ definimos a soma $+$ e o produto $\cdot$ em $\mathbb{C}$ por:

$$\begin{cases} (a + bi) + (c + di) = (a + c) + (b + d)i \\ (a + bi) \cdot (c + di) = (ac - bd) + (ad + bc)i. \end{cases}$$

É pertinente agora, notarmos que o corpo $\mathbb{R}$ dos números reais é realmente um subcorpo do $\mathbb{C}$ dos números complexos, como vimos no Exemplo 5.1. De fato, os números reais r podem ser vistos como os números complexos da forma $r = r + 0i$.

Cada número $z = a + bi \in \mathbb{C}$ pode ser representado por um ponto $(a, b) \in \mathbb{R}^2$.

Outra representação de z é através do vetor u que vai da origem O de $\mathbb{R}^2$ ao ponto que o representa.

Uma outra maneira de representar um complexo z é através das chamadas coordenadas polares, pelo par (ρ, θ), onde ρ é o comprimento ou distância da origem O de $\mathbb{R}^2$ ao ponto

que o representa e θ é o ângulo formado no sentido anti-horário, a partir do chamado primeiro quadrante, pela reta horizontal de $\mathbb{R}^2$ que passa por O e pelo vetor u (veja na Figura 3.1 o ângulo α).

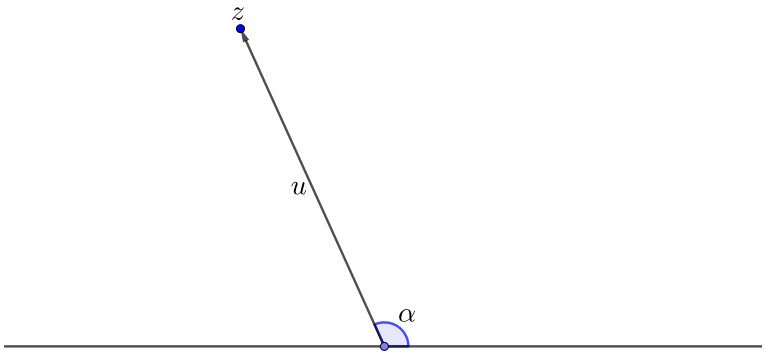

Figura 3.1: Coordenadas polares

O ρ que apresentamos, chamamos de módulo do número z, $|z|$. Já o θ chamamos de argumento de z.

Na Figura 3.2, notemos relações que existem entre essas representações. Do Teorema de Pitágoras, temos que $\rho = \sqrt{a^2 + b^2}$, assim $\rho \in \mathbb{R}$. Esse é um resultado interessante, pois, nos garante que o módulo de um número complexo é um número real.

Da definição de seno e cosseno, temos

$$\operatorname{sen}\theta = \frac{b}{\sqrt{a^2 + b^2}}.$$

$$\cos\theta = \frac{a}{\sqrt{a^2 + b^2}}.$$

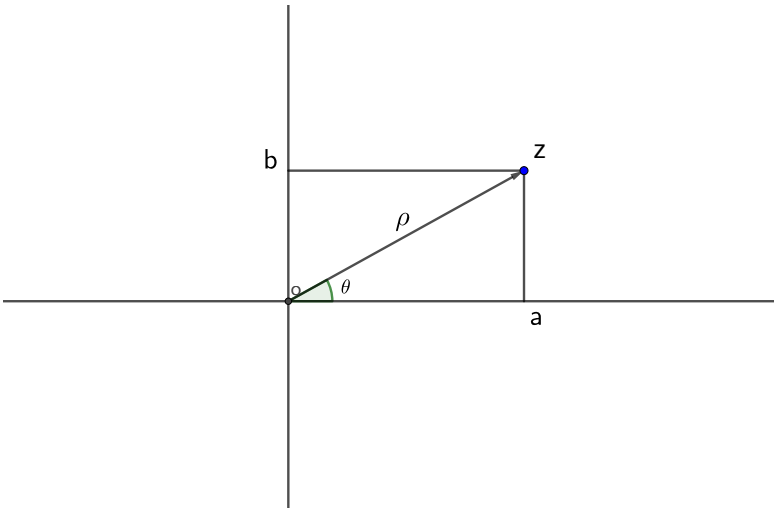

Figura 3.2: Relação entre coordenadas polares e cartesianas

Dito isto, podemos escrever:

$$z = a + bi = \rho(\cos\theta + i\,\mathrm{sen}\,\theta)$$

A multiplicação na forma polar fica:

Seja $z = \rho(\cos\theta + i\,\mathrm{sen}\,\theta)$ e $w = \eta(\cos\delta + i\,\mathrm{sen}\,\delta)$, então:

$$\begin{aligned} z \cdot w &= \rho(\cos\theta + i\,\mathrm{sen}\,\theta) \cdot \eta(\cos\delta + i\,\mathrm{sen}\,\delta) \\ &= \rho\eta[\cos\theta\cos\delta - \mathrm{sen}\,\theta\,\mathrm{sen}\,\delta + i(\mathrm{sen}\,\theta\cos\delta + \cos\theta\cos\delta)] \\ &= \rho\eta(\cos(\theta+\delta) + i\,\mathrm{sen}\,(\theta+\delta)). \end{aligned}$$

A última igualdade é resultante das conhecidas fórmulas de adição de arcos.

Do resultado acima, concluímos que na multiplicação de complexos na forma polar multiplicamos os módulos e somamos os argumentos. Lembremos disso, mais a frente, quando efetuarmos operações com régua e compasso.

Para descrevermos a divisão entre números complexos, vamos introduzir a descrição de inversos:

Dado um número complexo $z = \rho(\cos\theta + i\,\mathrm{sen}\,\theta)$, pela propriedade do inverso multiplicativo, um número w será inverso de z, se $z \cdot w = 1$. Seja $w = \eta(\cos\delta + i\,\mathrm{sen}\,\delta)$, teremos:

$$z \cdot w = \rho \cdot \eta[\cos(\theta+\delta) + i\,\mathrm{sen}\,(\theta+\delta)] = 1$$

Notemos que, $1 = \cos(2\pi) + i\,\mathrm{sen}(2\pi)$ e, assim,

$$\rho \cdot \eta[\cos(\theta+\delta) + i\,\mathrm{sen}\,(\theta+\delta)] = \cos(2\pi) + i\,\mathrm{sen}(2\pi)$$

Disso, obtemos $\rho \cdot \eta = 1$ e $\theta + \delta = 2k\pi$, para algum $k \in \mathbb{Z}$. Que nos fornece, $\eta = \dfrac{1}{\rho}$ e $\delta = 2k\pi - \theta$. Portanto,

$$w = \frac{1}{\rho}[\cos(-\theta) + \mathrm{sen}(-\theta)].$$

Denotamos o inverso de z por z^{-1}.

Para o quociente $\dfrac{z}{w}$, onde $w \neq 0$, temos $\dfrac{z}{w} = z \cdot w^{-1}$ que, pelo que vimos acima, resulta:

$$\frac{z}{w} = z \cdot w^{-1} = \frac{\rho}{\eta}(\cos(\theta-\delta) + i\,\mathrm{sen}\,(\theta-\delta)).$$

Seja um numero complexo $z = \rho(\cos\theta + i\,\mathrm{sen}\,\theta)$. Da multiplicação, recursivamente, fazendo $z^0 = 1$ e $z^n = z^{n-1} \cdot z$, podemos determinar a potência:

$$z^n = \rho^n(\cos(n\theta) + i\,\mathrm{sen}\,(n\theta)),$$

que no caso de $\rho = 1$, obtemos a chamada Fórmula de De Moivre:

$$(\cos\theta + i\,\mathrm{sen}\,\theta)^n = \cos(n\theta) + i\,\mathrm{sen}\,(n\theta).$$

De maneira análoga, determinamos a operação radiciação em complexos, que detalharemos na próxima subseção.

3.1.2 Radiciação Polar

Para a radiciação, destacamos aqui que a mesma tem um papel especial no transcorrer de nosso texto, especialmente a raiz quadrada.

Sejam $z = \rho(\cos\theta + i\,\mathrm{sen}\,\theta)$ e $w = \eta(\cos\delta + i\,\mathrm{sen}\,\delta)$ tais que $z^n = w$. Queremos determinar z.

Do resultado obtido na subseção anterior para a potenciação, temos

$$w = z^n = \rho^n(\cos(n\theta) + i\,\mathrm{sen}\,(n\theta)).$$

Logo,

$$\eta(\cos\delta + i\,\mathrm{sen}\,\delta) = w = \rho^n(\cos(n\theta) + i\,\mathrm{sen}\,(n\theta)).$$

E, assim

$$\eta\cos\delta = \rho^n(\cos(n\theta)),\ \text{enquanto que,}\ \eta\,\mathrm{sen}\,\delta = \rho^n(\mathrm{sen}\,(n\theta)).$$

Das duas últimas igualdades, concluímos por $\rho = \sqrt[n]{\eta}$ e $n\theta = \delta + 2k\pi$, $k \in \mathbb{Z}$ que resulta em $\theta = \frac{\delta+2k\pi}{n}$.

Finalmente, obtemos

$$z = \sqrt[n]{\eta}\left(\cos\frac{\delta+2k\pi}{n} + i\,\mathrm{sen}\,\frac{\delta+2k\pi}{n}\right).$$

Pode-se verificar que a variação em k acima produz exatamente n resultados distintos dados por $z_k = \sqrt[n]{\eta}\left(\cos\frac{\delta+2k\pi}{n} + i\,\mathrm{sen}\,\frac{\delta+2k\pi}{n}\right)$, com $k = \{0, 1, \ldots, n-1\}$. Ou seja, a equação $z^n = w$ tem exatamente n raízes, chamadas de raízes n-ésimas de w.

3.1.3 Raízes n-ésimas da Unidade

Em particular, quando $w = 1$ no último parágrafo da subseção anterior, utilizamos uma notação diferenciada, temos que $z^n = 1$ tem n raízes n-ésimas, chamadas raízes n-ésimas da unidade, dadas por:

$$z_k = \cos\frac{2k\pi}{n} + i\,\mathrm{sen}\,\frac{2k\pi}{n},\ \text{com}\ 0 \le k \le n-1.$$

Um resultado notório é que se tomarmos $z_1 = \cos\frac{2\pi}{n} + i\,\mathrm{sen}\,\frac{2\pi}{n}$, que denotamos por $z_1 = \zeta_n$, temos que $\zeta_n^k = z_k$, ou seja, as n-ésimas raízes da unidade são determinadas por potências sucessivas de ζ_n. Desta forma, o grupo das raízes n-ésimas da unidade (grupo 6 do Exemplo 2.4 $(U_n, \cdot)$) é gerado por ζ_n.

Definição 3.1. Seja ζ uma raiz n-ésima da unidade, ζ é dita uma raiz n-ésima primitiva da unidade se $U_n = \langle\zeta\rangle = \{\zeta^b; b \in \mathbb{Z}\}$, ou seja, ζ gera o grupo multiplicativo das raízes n-ésimas da unidade.

Observe que, na Definição 3.1, n é o menor inteiro positivo tal que $\zeta^n = 1$. Assim, ζ_n é uma raiz n-ésima primitiva da unidade.

As raízes n-ésimas primitivas da unidade serão muito úteis em nossos propósitos, como será visto em capítulos posteriores.

Seja $b \in \mathbb{Z}$. Dividindo b por n, obtemos $b = qn + r$, com $0 \leqslant r < n$. E com isso,

$$\zeta_n^b = \zeta_n^{qn+r} = \zeta_n^{qn} \cdot \zeta_n^r = (\zeta_n^n)^q \cdot \zeta_n^r = (1)^q \cdot \zeta_n^r = \zeta_n^r. \tag{3.1}$$

Da Equação 3.1, concluímos que realmente as raízes n-ésimas da unidade são determinadas pelas potências r com $0 \leqslant r < n$ de ζ_n. Ou seja, todas as potências de ζ_n nos inteiros gera resultados que estão no conjunto das potencias r, com r sendo os restos da divisão por n, mostrando a relevância da Definição 3.1.

Em resumo, obtivemos as soluções em $\mathbb{C}$ da equação $x^n = 1$ ou, equivalentemente, $x^n - 1 = 0$.

Mas quais das raízes n-ésimas da unidade são primitivas? Responderemos a essa pergunta na Proposição 3.3. Antes, porém, um pequeno lema auxiliar:

Lema 3.2. *Se ζ é uma raiz n-ésima primitiva da unidade, $m \in \mathbb{Z}$ e $\zeta^m = 1$, então $n|m$.*

Demonstração. Dividindo m por n, temos $m = qn + r$, com $0 \leqslant r < n$. E assim, como por hipótese $\zeta^m = 1$, temos que

$$\begin{aligned} 1 = \zeta^m &= \zeta^{qn+r} \\ &= \zeta^{qn} \cdot \zeta^r \\ &= (\zeta^n)^q \cdot \zeta^r \\ &= (1)^q \cdot \zeta^r \\ &= 1 \cdot \zeta^r \\ &= \zeta^r \end{aligned}$$

Da Definição 3.1, n é o menor inteiro positivo tal que $\zeta^n = 1$ e como $0 \leqslant r < n$, temos $r = 0$, logo $m = qn$, provando que $n|m$. □

Proposição 3.3. *Seja ζ uma raiz n-ésima primitiva da unidade e $m \in \mathbb{Z}$. Temos que ζ^m é uma raiz n-ésima primitiva da unidade se, e somente se,* $\operatorname{mdc}(m, n) = 1$.

Demonstração.

$\Rightarrow$)

Seja ζ^m uma raiz n-ésima primitiva da unidade. Por absurdo, suponhamos que $\operatorname{mdc}(m, n) = c \neq 1$, logo existe um $a \in \mathbb{N}$, tal que $n = c \cdot a$, disso:

$$(\zeta^m)^a = (\zeta^{\frac{m}{c} \cdot c})^a = (\zeta^{c \cdot a})^{\frac{m}{c}} = (\zeta^n)^{\frac{m}{c}} = (1)^{\frac{m}{c}} = 1$$

Chegamos que $(\zeta^m)^a = 1$, (com $1 < a < n$ pelo fato de $1 \neq c = \operatorname{mdc}(m, n)$), um absurdo pois n é o menor inteiro tal que $(\zeta^m)^n = 1$. Portanto, $\operatorname{mdc}(m, n) = 1$.

$\Leftarrow$)

Agora suponha que mdc $(m, n) = 1$. Seja um $b \in \mathbb{N}$ tal que $(\zeta^m)^b = 1$, então, temos $\zeta^{mb} = 1$. Pelo fato de ζ ser uma raiz n-ésima primitiva da unidade, temos que $n|mb$. Visto que mdc $(m, n) = 1$ então $n|b$. Então, o menor inteiro positivo b tal que $(\zeta^m)^b = 1$ é $b = n$. Pela Definição 3.1, implica que ζ^m é uma raiz n-ésima primitiva da unidade. □

Corolário 3.4. *Para todo $n \in \mathbb{N}$ temos $\varphi(n)$ raízes n-ésimas primitivas da unidade, onde $\varphi(n)$ é dada pela Definição 1.6.*

Demonstração. Resultado da junção da Equação 3.1 com a Proposição 3.3. De fato, pela Equação 3.1, obtemos n raízes n-ésimas e, destas, são primitivas, pela Proposição 3.3 e Definição 1.6, exatas $\varphi(n)$. □

Proposição 3.5. *Seja ζ uma raiz n-ésima primitiva da unidade e $m \in \mathbb{N}$. Então, $m|n$ se, e somente se, toda raiz m-ésima da unidade é raiz n-ésima da unidade.*

Demonstração.

⇒)

Seja $m \in \mathbb{N}$ tal que $m|n$, então $n = am$ para algum $a \in \mathbb{N}$.

Seja γ uma raiz m-ésima da unidade. Temos $\gamma^m = 1$ e, assim

$$\gamma^n = \gamma^{am} = (\gamma^m)^a = (1)^a = 1,$$

ou seja, $\gamma^n = 1$ e γ é uma raiz n-ésima da unidade. Como tomamos γ arbitrária, toda raiz m-ésima da unidade é raiz n-ésima da unidade.

⇐)

Supondo m tal que, toda raiz m-ésima da unidade é raiz n-ésima da unidade.

Seja $U_m = \langle\gamma\rangle$ e $U_n = \langle\zeta\rangle$ os grupos multiplicativos das raízes m-ésimas e n-ésimas da unidade, respectivamente, onde γ e ζ são respectivas raízes primitivas destes grupos.

Pela hipótese, $\gamma^i \in U_n$ para todo $1 \leqslant i \leqslant m$ e assim, U_m é subgrupo de U_n. Pelo Teorema 2.14 (Teorema de Lagrange), $|U_m|$ divide $|U_n|$, ou seja, $m|n$. □

3.1.4 Módulo e Conjugado

Nesta subseção, faremos uma exposição sucinta dos conceitos de módulo e conjugado, veremos algumas de suas propriedades, cujas demonstrações podem ser facilmente verificadas utilizando as operações apresentadas na Subseção 3.1.1.

Dado um número complexo $z = a + bi$, chamamos de conjugado de z, denotamos por $\overline{z}$, ao número complexo $\overline{z} = a - bi$.

O módulo de um número z já introduzimos na Subseção 3.1.1, momento em que descobrimos tratar-se de um número real. Como consequência disso, a distância entre dois pontos do plano complexo é um número real.

Proposição 3.6. *São válidas as seguintes propriedades do módulo e do conjugado:*

i - $z = \overline{z}$ *se, e somente se,* $z \in \mathbb{R}$*;*

ii - $\overline{z + w} = \overline{z} + \overline{w}$*;*

iii - $\overline{z \cdot w} = \overline{z} \cdot \overline{w}$*;*

iv - $\overline{\left(\frac{z}{w}\right)} = \frac{\overline{z}}{\overline{w}}$*;*

v - $|z|^2 = z \cdot \overline{z}$*;*

vi - $|z| = 1 \Leftrightarrow \frac{1}{z} = \overline{z}$*;*

Demonstração. Estas propriedades são de verificações imediatas a partir das operações definidas na Subseção 3.1.1. □

Capítulo 4

Polinômios

Na primeira seção deste capítulo introduziremos o conceito de corpo, para nas seções posteriores tratarmos de polinômios sobre um corpo. No próximo capítulo, retomaremos o estudo de corpos com maiores detalhes, utilizando para isso, inclusive, os resultados deste capítulo.

4.1 Corpos

Definição 4.1. Seja um conjunto C munido de duas operações que chamaremos de soma, $+$, e multiplicação, $\cdot$, que satisfazem as seguintes operações:

1- Associatividade da soma: sejam a, b, c elementos de C, então,

$$(a + b) + c = a + (b + c)$$

2- Existência de elemento neutro da adição, 0, tal que, para todo $a \in C$,

$$a + 0 = 0 + a = a$$

3- Existência de simétricos $-a$ para todo $a \in C$, tais que,

$$a + (-a) = (-a) + a = 0$$

4- Comutatividade da adição: para todos $a, b \in C$,

$$a + b = b + a$$

5- Associatividade da multiplicação: para todos $a, b, c \in C$,

$$a \cdot (b \cdot c) = (a \cdot b) \cdot c$$

6- Distributividade da multiplicação em relação a adição: para todos $a, b, c \in C$,

$$a \cdot (b + c) = (a \cdot b) + (a \cdot c)$$

e

$$(a + b) \cdot c = (a \cdot c) + (b \cdot c)$$

Nesta situação, diremos que C é um Anel.

Definição 4.2. Um corpo é um anel que satisfaz as seguintes propriedades:

7- É um anel com unidade: $\exists 1 \in C$, onde $0 \neq 1$, tal que,

$$a \cdot 1 = 1 \cdot a = a$$

8- É um anel comutativo: para todos $a, b \in C$,

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

9- É um anel sem divisores de zero:

$$a \cdot b = 0 \Rightarrow a = 0 \text{ ou } b = 0$$

10- Existência de inversos multiplicativos: $\forall a \neq 0$, existe a^{-1}, tal que,

$$a \cdot a^{-1} = 1$$

Definição 4.3. Se um anel A satisfaz as propriedades 7,8 e 9 diremos que A é um domínio de integridade.

Exemplo 4.4.

1 - $\mathbb{Z}$ com a soma e multiplicação usuais é um exemplo de domínio de integridade;

2 - $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ com as operações de soma e produto usuais são exemplos de corpos;

3 - $\mathbb{Z}_p$ com p primo é um exemplo de corpo com as operações de soma e produto $\mod p$.

Definição 4.5. Seja S um subconjunto de um corpo A. Diremos que S é um subanel, subdomínio de A, se S com as operações de A for, respectivamente, um anel, um domínio.

Definição 4.6. Seja S um subconjunto de um corpo $\mathbb{K}$. S é dito um subcorpo de $\mathbb{K}$ sempre que S, com as operações de soma e de multiplicação de $\mathbb{K}$, for um corpo. Neste caso, diremos que $\mathbb{K}$ é uma extensão de S.

Apresentamos condições necessárias e suficientes para identificar se determinado subconjunto de um corpo é um subcorpo.

Proposição 4.7. *Seja S um subconjunto de um corpo $\mathbb{K}$. Então, S é um subcorpo de $\mathbb{K}$ se, e somente se:*

i - 0 *e* $1 \in S$;

ii - $a, b \in S \Rightarrow a - b$ *e* $a \cdot b \in S$;

iii - $a \in S - \{0\} \Rightarrow a^{-1} \in S$.

Demonstração. As propriedades que citamos nesta demonstração são as contidas nas Definições 4.1 e 4.2 acima.

$\Rightarrow$)

Suponha que S seja um subcorpo de um corpo $\mathbb{K}$. Por S ser um corpo ele satisfaz as propriedade 2 e 7, e assim 0 e $1 \in S$.

Se tomarmos $a, b \in S$ e por S satisfazer tanto os fechamentos da multiplicação e da adição quanto a propriedade 3, teremos que $-b \in S$ e $a - b$ e $a \cdot b \in S$.

Ainda por ser corpo, S satisfaz a propriedade 10 e assim, se $a \in S - \{0\} \Rightarrow a^{-1} \in S$.

$\Leftarrow$)

Supondo que um subconjunto S de um corpo $\mathbb{K}$ satisfaz (i), (ii) e (iii) acima. Por (i), $0 \in S$ e por (ii), dados $a, b \in S$, $0 - b = -b \in S$ e ainda $a - (-b) = a + b \in S$, logo S é fechado para a adição.

Por (ii), S é fechado para a multiplicação.

Naturalmente por S ser um subconjunto de $\mathbb{K}$ com as operações fechadas essas operações de adição e multiplicação satisfazem as propriedades 1,4,5,6,8 e 9.

Por (i), S satisfaz 2 e 7.

Por (i) e (ii), temos que $\forall a \in S$, $-a \in S$, satisfazendo 3.

Por (iii), S satisfaz 10, completando a demonstração de que S é um subcorpo de $\mathbb{K}$. □

Exemplo 4.8. $\mathbb{Q}$ é um subcorpo dos $\mathbb{R}$; $\mathbb{R}$ é um subcorpo dos $\mathbb{C}$; $\mathbb{Q}$ é um subcorpo dos $\mathbb{C}$.

Apresentamos, a seguir, um conceito que nos será útil quando introduzirmos os resultados sobre separabilidade.

Definição 4.9. (Característica de um corpo) Se em um corpo $\mathbb{K}$ tivermos um menor inteiro positivo n, tal que $na = 0$ para algum $a \neq 0$ diremos que $\mathbb{K}$ tem característica n. Se não existir tal n nesse corpo diremos que $\mathbb{K}$ tem característica 0.

Exemplo 4.10.

i - É possível provar que a característica de um corpo ou é p primo ou é 0;

ii - $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ são corpos de característica zero;

iii - Os corpos $\mathbb{Z}_p$ com p primo são corpos de característica p.

4.2 Algumas Definições sobre Polinômios

Precisamos introduzir o conceito de polinômios em uma indeterminada e apresentar mais uma série de informações relacionadas. Se $\mathbb{K}$ é um corpo, chamamos de polimômio sobre $\mathbb{K}$ na indeterminada x a toda expressão da forma $p(x) = a_0 + a_1x + \cdots + a_nx^n$,

onde $n \in \mathbb{N}$ e $a_i \in \mathbb{K}$ para todos $0 \leqslant i \leqslant n$. De maneira análoga, se tivermos $\mathbb{K}$ como um domínio de integridade diremos que $p(x)$ é um polinômio sobre o domínio $\mathbb{K}$. Englobamos, a seguir, uma gama de resultados iniciais sobre polinômios.

A igualdade entre dois polinômios é dada da seguinte forma:

Dois polinômios $p(x) = a_0 + a_1x + \cdots + a_kx^k$ e $q(x) = b_0 + b_1x + \cdots + b_lx^l$ são iguais se, e somente se, $k = l$ e $a_i = b_i$ para todos $0 \leqslant i \leqslant k$.

Um polinômio $p(x) = a_0 + a_1x + \cdots + a_kx^k$ sobre $\mathbb{K}$ tal que $a_0 = c \in \mathbb{K}$ e $a_i = 0, \forall i \geqslant 1$ chamamos de polinômio constante c. E mais, se $c = 0$ chamamos de polinômio nulo e denotamos por 0.

Se um polinômio $p(x) = a_0 + a_1x + \cdots + a_nx^n$ é tal que $a_n \neq 0$ dizemos que o polinômio $p(x)$ tem grau n, denotamos $\partial p(x) = n$. O grau do polinômio nulo damos como indefinido.

Definição 4.11. Diremos que um polinômio $p(x) = a_0 + a_1x + \cdots + a_nx^n$ é mônico se $a_n = 1$.

Denotamos por $\mathbb{K}[x]$ o conjunto de todos os polinômios na indeterminada x. Vamos definir uma soma e um produto em $\mathbb{K}[x]$:

Definição 4.12. Sejam $p(x) = a_0 + a_1x + \cdots + a_kx^k$ e $q(x) = b_0 + b_1x + \cdots + b_lx^l$ dois polinômios em $\mathbb{K}[x]$, definimos a soma e o produto entre $p(x)$ e $q(x)$ da seguinte forma:

A seguir, quando $k \neq l$, sem perda de generalidade, seja $k > l$ consideramos $b_i = 0$ para todos $l < i \leqslant k$.

$+$:

$$p(x) + q(x) = c_0 + c_1x + \cdots + c_kx^k,$$

onde $c_i = a_i + b_i$.

$\cdot$:

$$p(x) \cdot q(x) = c_0 + c_1x + \cdots + c_kx^k,$$

onde $c_i = a_0b_i + a_1b_{i-1} + \cdots + a_{i-1}b_1 + a_ib_0$, para todo $0 \leqslant i \leqslant k$.

Notação 4.13. Escrevemos $x^0 = 1$ e $x^1 = x$.

Se identificarmos os elementos $c \in \mathbb{K}$ como os polinômios constantes $p(x) = c$ podemos considerar que $\mathbb{K} \subset \mathbb{K}[x]$.

Na Definição 4.12, temos uma soma e um produto em $\mathbb{K}[x]$. Pode-se verificar que $\mathbb{K}[x]$ com essa soma e esse produto é um domínio, em particular um anel, onde 0 é o elemento neutro e o polinômio constante 1 é a unidade.

4.3 Álgebra do Anel de Polinômios

Apresentamos alguns resultados sobre os anéis de polinômios que fazem uma analogia ao anel dos inteiros. Estamos falando do Algoritmo da Divisão, Máximo Divisor Comum, e o Lema de Bézout.

A seguir temos uma demonstração, encontrada em [8], do Algoritmo da Divisão no anel dos polinômios.

Proposição 4.14. *(Algoritmo da Divisão) Sejam $f(x), g(x) \in \mathbb{K}[x]$ e $g(x) \neq 0$. Então, existem únicos $q(x), r(x) \in \mathbb{K}[x]$ tais que:*

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

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

Demonstração. Seja $f(x) = a_0 + a_1x + \cdots + a_nx^n$ e $g(x) = b_0 + b_1x + \cdots + b_mx^m$, com $\partial g(x) = m$.

i - Existência: Se $f(x) = 0$ basta tomar $q(x) = r(x) = 0$. Suponhamos $f(x) \neq 0$. Assim, $\partial f(x) = n$. Se $n < m$ basta tomar $q(x) = 0$ e $r(x) = f(x)$. Assim, assumindo $n \geqslant m$. Agora seja $f_1(x)$ o polinômio definido por:

$$f(x) = a_nb_m^{-1}x^{n-m} \cdot g(x) + f_1(x)$$

Note que $\partial f_1(x) < \partial f(x)$.

Vamos demonstrar por indução sobre n.

- Para $n = 0$: de $n \geqslant m$, temos $m = 0$, portanto, $f(x) = a_0 \neq 0$ e $g(x) = b_0 \neq 0$ e, teremos

$$f(x) = a_0b_0^{-1}g(x)$$

bastando tomar $q(x) = a_0b_0^{-1}$ e $r(x) = 0$.

- Sendo válido para $n - 1$, precisamos mostrar que é válido para n:

Temos

$$f_1(x) = f(x) - a_nb_m^{-1}x^{n-m} \cdot g(x).$$

E, $\partial f_1(x) < \partial f(x)$. Pela hipótese de indução, $\exists q_1(x), r_1(x) \in \mathbb{K}[x]$ tais que:

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

onde $r_1(x) = 0$ ou $\partial r_1(x) < \partial g(x)$.

Daí segue que:

$$f(x) = \left(q_1(x) + a_nb_m^{-1}x^{n-m}\right) g(x) + r_1(x).$$

E, portanto, tomando

$$q(x) = q_1(x) + a_nb_m^{-1}x^{n-m}$$

e

$$r(x) = r_1(x)$$

provamos a existência de polinômios $q(x)$ e $r(x)$ tais que $f(x) = q(x)g(x) + r(x)$, onde $r(x) = 0$ ou $\partial r(x) < \partial g(x)$.

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

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

onde $r_i(x) = 0$ ou $\partial r_i(x) < \partial g(x)$, $i = 1, 2$. Daí, segue que:

$$(q_1(x) - q_2(x)) \cdot g(x) = r_2(x) - r_1(x).$$

Mas, se $q_1(x) \neq q_2(x)$ o grau do polinômio do lado esquerdo da igualdade acima é maior ou igual que o grau de $g(x)$, enquanto que $\partial\left(r_2(x) - r_1(x)\right) < \partial g(x)$, uma contradição. Logo,

$$q_1(x) = q_2(x).$$

Daí temos que

$$r_1(x) = f(x) - q_1(x)g(x) = f(x) - q_2(x)g(x) = r_2(x).$$

□

Definição 4.15. (mdc) Sejam dois polinômios $p(x), q(x) \in \mathbb{K}[x]$, onde $q(x)$ é um polinômio não nulo. Dizemos que $q(x)|p(x)$ se existe algum polinômio $s(x) \in \mathbb{K}[x]$ tal que $p(x) = q(x) \cdot s(x)$.

Levando isso em consideração, dados dois polinômios $p(x), q(x) \in \mathbb{K}[x]$, um polinômio $m(x) \in \mathbb{K}[x]$ é dito máximo divisor comum de $p(x)$ e $q(x)$ se $m(x)|p(x)$, $m(x)|q(x)$ e, além disso, qualquer polinômio $n(x)$ que, da mesma forma, $n(x)|p(x)$ e $n(x)|q(x)$, tivermos $n(x)|m(x)$.

Os resultados desta seção começam a mostrar uma semelhança entre as Álgebras do anel dos inteiros e do anel de polinômios. Iremos apresentar mais resultados que elucidam essas semelhanças.

Proposição 4.16. *(Lema de Bézout) Sejam $p(x)$ e $q(x)$ dois polinômios não nulos sobre um corpo $\mathbb{K}$ que tem como* mdc *um polinômio $d(x) \in \mathbb{K}[x]$. Então, existem polinômios $r(x)$ e $s(x) \in \mathbb{K}[x]$ tais que*

$$d(x) = r(x) \cdot p(x) + s(x) \cdot q(x).$$

Demonstração. Pode ser encontrada em [17]. □

4.4 Raízes de Polinômios

Reservamos a seção para introduzir a definição de raízes de polinômios e alguns resultados envolvendo-as.

Se $p(x)$ é um polinômio não nulo em $\mathbb{K}[x]$ e $\alpha \in \mathbb{K}$ é tal que $p(\alpha) = 0 \in \mathbb{K}$ dizemos que α é raiz de $p(x)$ em $\mathbb{K}[x]$.

Proposição 4.17. *Sejam $\mathbb{K}$ um corpo e $p(x) \in \mathbb{K}[x]$, onde $p(x) \neq 0$ de grau n. Então, o número de raízes de $p(x)$ é no máximo n.*

Demonstração. Vamos provar por indução:

Para $n = 0$: temos que o polinômio $p(x)$ considerado, por ser não nulo e constante, não possui raiz e a proposição é trivialmente válida.

Consideremos o resultado válido para todos os polinômios com grau $\leqslant (n-1)$ e mostraremos que é válido também para n: tomemos $p(x)$ de grau n, se $p(x)$ não tiver raiz, nada há a considerar. Então, tomemos uma raiz α de $p(x)$. Notemos que o polinômio $f(x) = x - \alpha \in \mathbb{K}[x]$ e, assim, usando a Proposição 4.14 (Algoritmo da Divisão), temos

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

com $r(x) = 0$ ou $\partial r(x) < f(x)$. Então, $\partial r(x) < 1$, o que o torna um polinômio constante c. Agora devido α ser raiz de $p(x)$ e $f(x)$, temos

$$\begin{array}{rcl} p(\alpha) & = & q(\alpha) \cdot f(\alpha) + c \Leftrightarrow \\ 0 & = & q(\alpha) \cdot 0 + c. \end{array}$$

Logo, $r(x) = c = 0$ e $p(x) = q(x)(x - \alpha)$.

Disso, obtemos que $\partial q(x) = n-1$, assim, por hipótese de indução, $q(x)$ tem no máximo $n-1$ raízes. Como $p(x)$ tem como raízes α e as raízes de $q(x)$, $p(x)$ tem no máximo n raízes. □

A Proposição 4.17 é generalizada no corolário a seguir, onde, pelo grau de um polinômio determinamos seu número máximo de raízes em qualquer extensão do corpo onde o polinômio foi tomado inicialmente.

Corolário 4.18. *Seja $p(x)$ um polinômio não nulo em $\mathbb{K}[x]$. Então, $p(x)$ possui no máximo n raízes em qualquer extensão $\mathbb{L}$ de $\mathbb{K}$.*

Demonstração. Como $\mathbb{K} \subseteq \mathbb{L}$, podemos considerar $p(x) \in \mathbb{L}[x]$. Assim, pela Proposição 4.17, terminamos a demonstração. □

4.5 Polinômios Irredutíveis

O estudo e determinação da irredutibilidade de polinômios relaciona-se com o estudo de extensões de corpos, isto será evidenciado no desenrolar do texto, principalmente por esse motivo, apresentamos nesta seção resultados relacionados com a irredutibilidade.

Definição 4.19. Seja $p(x)$ um polinômio não constante sobre $\mathbb{K}[x]$, dizemos que $p(x)$ é irredutível sobre $\mathbb{K}$ se inexistem $q(x), r(x)$ tais que $1 \leqslant \partial q(x), \partial r(x) < \partial p(x)$ e $p(x) = q(x) \cdot r(x)$. Caso contrário, dizemos que $p(x)$ é redutível.

Exemplo 4.20. O polinômio $p(x) = x^2 - 2$ é irredutível sobre $\mathbb{Q}$. Já se considerarmos $p(x) \in \mathbb{R}[x]$, temos $p(x) = (x + \sqrt{2})(x - \sqrt{2})$, e assim $p(x)$ é redutível sobre $\mathbb{R}$.

A seguir, um resultado atribuído a Gauss que facilita as demonstrações de diversos critérios de verificação de irredutibilidade de polinômios, alguns destes critérios serão apresentados posteriormente.

Lema 4.21. *(Gauss) Seja $p(x) \in \mathbb{Z}[x]$. Se $p(x)$ é irredutível sobre $\mathbb{Z}$, então $p(x)$ é irredutível sobre $\mathbb{Q}$.*

Demonstração. Pode ser consultada em [8] ou [17]. □

Apresentamos, a seguir, outro lema que nos será muito útil em demonstrações futuras.

Lema 4.22. *Sejam $p(x), q(x) \in \mathbb{Q}[x]$ mônicos tais que $p(x) \cdot q(x) \in \mathbb{Z}[x]$, então $p(x), q(x) \in \mathbb{Z}[x]$.*

Demonstração. Pode ser vista em [7]. □

Exemplo 4.23. $p(x) = x^3 - 2$ é irredutível sobre $\mathbb{Q}$. De fato, se existisse um $a \in \mathbb{Z}$ tal que $p(a) = 0$, teríamos que $a^3 = 2$, um absurdo: não existe inteiro com essa propriedade. Assim, como $p(x)$ não tem raiz em $\mathbb{Z}$, $p(x)$ não pode ser reescrito como produto de polinômios de grau maior que 1 e menor que 3. Logo, $p(x)$ é irredutível sobre $\mathbb{Z}$ que, pelo Lema 4.21, implica $p(x)$ irredutível sobre $\mathbb{Q}$.

Proposição 4.24. *(Critério de Eisenstein) Seja $f(x) = a_0 + a_1 x + \cdots + a_n x^n \in \mathbb{Z}[x]$. Se tivermos um primo p, tal que:*

i - $p \nmid a_n$;

ii - $p \mid a_i, \forall i \in \{0, 1, \ldots, n-1\}$;

iii - $p^2 \nmid a_0$.

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

Demonstração. Pelo Lema 4.21 (Lema de Gauss), é suficiente mostrarmos que $f(x)$ é irredutível sobre $\mathbb{Z}$: Supondo que não. Pela Definição 4.19, existem $g(x), h(x) \in \mathbb{Z}[x]$, tais que $f(x) = g(x)h(x)$, onde

$$g(x) = b_0 + b_1 x + \cdots + b_r x^r$$

$$h(x) = c_0 + c_1 x + \cdots + c_s x^s$$

com $1 \leqslant \partial g(x), \partial h(x) < \partial p(x)$.

Utilizando propriedades do produto de polinômios, temos que $r + s = n$. E mais, $b_0c_0 = a_0$ e, por (ii), $p \mid a_0$ e, por p ser primo, $p \mid b_0$ ou $p \mid c_0$, porém, pelo item (iii), não pode dividir ambos. Assim, sem perda de generalidade, digamos que $p \mid b_0$ e $p \nmid c_0$.

Sabemos que $p \mid b_0$, mas p não divide todos os b_j, pois se dividisse, dividiria a_n, contrariando (i). Então, tomando b_j como o primeiro coeficiente de $g(x)$ que não é divisível por p, temos

$$a_j = b_jc_0 + \cdots + b_0c_j,$$

onde $j < n$.

Como $p \mid a_j$ (por (ii)), divide $b_0, b_1, \ldots, b_{j-1}$ e não divide b_j (pela forma como tomamos b_j), então $p \mid c_0$, um absurdo, pois supomos que não dividia. Concluindo que $f(x)$ é irredutível sobre $\mathbb{Z}$. □

Proposição 4.25. *Sejam $\mathbb{K}$ um corpo, $p(x) \in \mathbb{K}[x]$ e $a \in \mathbb{K}$. Se $p(x + a)$ for irredutível sobre $\mathbb{K}$, então $p(x)$ é irredutível sobre $\mathbb{K}$.*

Demonstração. É suficiente verificarmos que a seguinte função é um automorfismo.

$$\begin{array}{rccc} f: & \mathbb{K}[x] & \longrightarrow & \mathbb{K}[x] \\ & p(x) & \longmapsto & p(x+a). \end{array}$$

Então, vamos a isso.

Afirmação: f é um homomorfismo. De fato, sejam $p(x)$ e $q(x)$ polinômios em $\mathbb{K}[x]$, então,

$$f(p(x) + q(x)) = p(x + a) + q(x + a) = f(p(x)) + f(q(x))$$

e

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

Temos que f é injetiva:

Pelo item (iii) do Exemplo 2.29, f é injetivo se, e somente se, $\operatorname{Ker} f = \{0\}$. Agora, notemos que,

$$f(p(x)) = 0 \Leftrightarrow p(x) = 0.$$

Pois, $\partial f(p(x)) = \partial p(x)$, assim $\partial p(x) = 0$ e, o único polinômio constante c tal que $f(c) = 0$ é o polinômio 0, portanto $\operatorname{Ker} f = \{0\}$ e f é injetiva.

Temos que f é sobrejetiva. De fato, tomando um polinômio $p(x) \in \mathbb{K}[x]$. Temos, que o polinômio $q(x) = p(x - a) \in \mathbb{K}[x]$ e, é tal que, $q(x + a) = p(x)$, ou seja, existe $q(x)$, onde $f(q(x)) = p(x)$, mostrando que f é sobrejetiva.

Terminando a prova, pois temos um homomorfismo bijetivo em $\mathbb{K}[x]$. □

Exemplo 4.26. Seja $q(x) \in \mathbb{Z}[x]$, $q(x) = x^{p-1} + x^{p-2} + \cdots + x + 1$, onde p é primo. Então, $q(x)$ é irredutível sobre $\mathbb{Z}$.

De fato, temos que

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

A última igualdade ocorre em virtude da Proposição 1.2.

Daí,

$$q(x+1) = \frac{(x+1)^p - 1}{(x+1) - 1} = \frac{(x+1)^p - 1}{x}.$$

que desenvolvendo o binômio, utilizando a Proposição 1.3, temos

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

Do Lema 1.4, $p \Big| \binom{p}{i}$ para todo $0 < i < p$. E sabemos que $p^2 \nmid p = \binom{p}{p-1}$.

Aplicando o Critério de Eisenstein em $q(x+1)$, com relação ao primo p, temos $q(x+1)$ irredutível sobre $\mathbb{Z}$. Pela Proposição 4.25, $q(x)$ também é irredutível sobre $\mathbb{Z}$.

Exemplo 4.27. O polinômio $p(x) = x^3 - 3x - 1$ é irredutível sobre $\mathbb{Q}$.

De fato,

$$\begin{aligned} p(x+1) = (x+1)^3 - 3(x+1) - 1 = \\ = (x^3 + 3x^2 + 3x + 1) + (-3x - 3) - 1 = \\ = x^3 + 3x^2 - 3 \end{aligned}$$

Aplicando o Critério de Eisenstein ao polinômio $p(x+1) = x^3 + 3x^2 - 3$, para $p = 3$, provamos que $p(x+1)$ é irredutível sobre $\mathbb{Z}$ e, pela Proposição 4.25, $p(x)$ também é irredutível sobre $\mathbb{Z}$.

Pelo Lema 4.21 (Lema de Gauss), $p(x)$ é irredutível sobre $\mathbb{Q}$.

Veremos agora, mais um critério interessante que nos permite identificar a irredutibilidade de polinômios.

Proposição 4.28. *Se tivermos um corpo $\mathbb{Z}_p$, com p primo, $\mathbb{Z}_p = \{\bar{0}, \bar{1}, \ldots, \overline{p-1}\}$, para um polinômio $p(x) = a_0 + a_1x + \cdots + a_nx^n$ podemos definir o polinômio $\overline{p}(x) = \overline{a}_0 + \overline{a}_1x + \cdots + \overline{a}_nx^n$ em $\mathbb{Z}_p[x]$, onde $\overline{a}_i$ é a classe de equivalência de a_i modulo p, em que a_i é o representante. Se p não divide a_n e $\overline{p}(x)$ é irredutível sobre $\mathbb{Z}_p$, então $p(x)$ é irredutível sobre $\mathbb{Q}$.*

Demonstração. Suponhamos, por absurdo, que $p(x)$ seja redutível sobre $\mathbb{Q}$. Pela contrapositiva do Lema 4.21 (Lema de Gauss), $p(x)$ é redutível sobre $\mathbb{Z}$, ou seja, existem polinômios $f(x), g(x) \in \mathbb{Z}[x]$, onde $\partial f(x) = r$ e $\partial g(x) = s$ com $1 \leqslant r, s \leqslant n$, tais que $p(x) = f(x) \cdot g(x)$.

Pela forma como definimos $\overline{p}(x)$, temos $\overline{p}(x) = \overline{f}(x) \cdot \overline{g}(x)$, onde $\overline{f}(x), \overline{g}(x) \in \mathbb{Z}_p[x]$. Sejam $f(x) = b_0 + b_1x + \cdots + b_rx^r$ e $g(x) = c_0 + c_1x + \cdots c_sx^s$, pelo produto de polinômios, $a_n = b_r \cdot c_r$ e por $p \nmid a_n$, temos que $p \nmid b_r$ e $p \nmid c_r$, que resulta em $\partial\overline{f}(x) = r$ e $\partial\overline{g}(x) = s$, logo $p(x)$ é redutível sobre $\mathbb{Z}_p[x]$, um absurdo. □

Capítulo 5

Extensões de Corpos

Se tivermos um subcorpo $\mathbb{K}$ de um corpo $\mathbb{L}$ dizemos que $\mathbb{L}$ é uma extensão de $\mathbb{K}$, denotamos por $\mathbb{L}|\mathbb{K}$, e $\mathbb{K}$ é dito o corpo base da extensão.

Exemplo 5.1.
$\mathbb{C}|\mathbb{R}$, $\mathbb{R}|\mathbb{Q}$ e $\mathbb{C}|\mathbb{Q}$ são exemplos de extensões.

5.1 Extensões Algébricas

Definição 5.2. Sejam $\mathbb{L}$ uma extensão de $\mathbb{K}$ e $\alpha \in \mathbb{L}$. dizemos que α é algébrico sobre $\mathbb{K}$ se existe $p(x) \in \mathbb{K}[x]$, um polinômio não nulo, tal que $p(\alpha) = 0$. Caso o contrário, dizemos que α é transcendente sobre $\mathbb{K}$.

Notação 5.3. Se um número α é algébrico/transcendente sobre o corpo $\mathbb{Q}$, dizemos simplesmente que α é algébrico/transcendente, a menos que deixemos explícito que estamos falando de outro corpo.

Exemplo 5.4.

i) $\sqrt{2}$ é algébrico. De fato, $p(\sqrt{2}) = 0$, onde $p(x) = x^2 - 2$;

ii) O número complexo i é algébrico, pois $p(i) = 0$, onde $p(x) = x^2 + 1$;

iii) π é transcendente. Ferdinand Lindemann provou a transcedência de π em 1982, veja [6]. Uma prova da transcedência de π encontramos em [17];

iv) Dada uma extensão $\mathbb{L}|\mathbb{K}$. Se $\alpha \in \mathbb{K}$, então α é algébrico sobre $\mathbb{K}$. De fato, $p(\alpha) = 0$, onde $p(x) \in \mathbb{K}[x]$ é o polinômio $p(x) = x - \alpha$.

Definição 5.5. Uma extensão $\mathbb{L}|\mathbb{K}$ é dita algébrica sobre $\mathbb{K}$ se, $\forall \alpha \in \mathbb{L}$, α for algébrico sobre $\mathbb{K}$. Caso contrário dizemos que $\mathbb{L}|\mathbb{K}$ é transcendente sobre $\mathbb{K}$.

5.2 Polinômio Minimal

Definição 5.6. Sejam $\mathbb{L}|\mathbb{K}$ uma extensão e $\alpha \in \mathbb{L}$ um elemento algébrico sobre $\mathbb{K}$. Chamamos de polinômio minimal de α sobre $\mathbb{K}$, o único polinômio mônico e de menor grau não nulo $m(x) \in \mathbb{K}[x]$, tal que $m(\alpha) = 0$. O denotamos por $m(x) = p_{min}(\alpha, \mathbb{K})$.

Na Definição 5.6, o polinômio descrito é de fato único. Pois, se existisse um outro, digamos $q(x) \in \mathbb{K}[x]$, satisfazendo as mesmas condições, como os dois são irredutíveis, eles não possuem fator comum em $\mathbb{K}[x]$ logo, pelo Lema 4.16 (Lema de Bézout), teríamos que existem $r(x), s(x) \in \mathbb{K}[x]$ tais que,

$$r(x)p(x) + s(x)q(x) = 1.$$

Logo,

$$1 = r(\alpha)p(\alpha) + s(\alpha)q(\alpha) = r(\alpha) \cdot 0 + s(\alpha) \cdot 0 = 0.$$

Absurdo.

Proposição 5.7. *Numa extensão $\mathbb{L}|\mathbb{K}$, sejam $\alpha \in \mathbb{L}$ e $m(x) = p_{min}(\alpha, \mathbb{K})$. Então, $m(x)$ divide todos os polinômios $p(x) \in \mathbb{K}[x]$ tais que $p(\alpha) = 0$.*

Demonstração. Seja um polinômio $p(x) \in \mathbb{K}[x]$, tal que $p(\alpha) = 0$. Pela Proposição 4.14 (Algoritmo da Divisão), existem $q(x)$ e $r(x) \in \mathbb{K}[x]$ tais que $p(x) = q(x) \cdot m(x) + r(x)$, com $0 \leqslant \partial r(x) < \partial m(x)$.

Disso, temos

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

Mas, como $m(\alpha) = 0$ e $p(\alpha) = 0$, temos $r(\alpha) = 0$.

Desta última igualdade, e da definição de polinômio minimal (o fato de ser o de menor grau que tem α como raiz), afirmamos que $r(x) = 0$. E, então $p(x) = q(x)m(x)$, mostrando que, pela Definição 4.15, $m(x)|p(x)$. □

Proposição 5.8. *Sejam $\mathbb{L}|\mathbb{K}$ uma extensão, $\alpha \in \mathbb{L}$ algébrico sobre $\mathbb{K}$ e $p(x) \in \mathbb{K}[x]$ um polinômio mônico, tal que $p(\alpha) = 0$. Então, $p(x)$ é o polinômio minimal de α se, e somente se, $p(x)$ é irredutível sobre $\mathbb{K}$.*

Demonstração.

$\Rightarrow$)

Seja $p(x) = p_{min}(\alpha, \mathbb{K})$. Por absurdo, suponhamos que existem $f(x), g(x) \in \mathbb{K}[x]$ tais que $f(x)g(x) = p(x)$, com $1 \leqslant \partial f(x), \partial g(x) < \partial p(x)$. Como $p(\alpha) = 0$ temos

$$f(\alpha)g(\alpha) = p(\alpha) = 0$$

Como $f(\alpha), g(\alpha) \in \mathbb{K}$ e $\mathbb{K}$ é um corpo, temos que $f(\alpha) = 0$ ou $g(\alpha) = 0$, mas isso é um absurdo, pois, $\partial f(x), \partial g(x) < \partial p(x)$ e $p(x)$ é o polinômio de menor grau que tem α como raiz, portanto, $p(x)$ é irredutível sobre $\mathbb{K}$.

$\Leftarrow$)

Seja $p(x)$ irredutível sobre $\mathbb{K}$, mônico e tal que $p(\alpha) = 0$ e $m(x) = p_{min}(\alpha, \mathbb{K})$, pela Proposição 5.7, $m(x)|p(x)$, como $m(x)$ é irredutível sobre $\mathbb{K}$ e também é mônico, temos que $p(x) = m(x) = p_{min}(\alpha, \mathbb{K})$. □

5.3 Extensões Finitas

Notemos que podemos considerar $\mathbb{L}$ como um espaço vetorial sobre $\mathbb{K}$. Ou seja, as operações de adição dos elementos de $\mathbb{L}$ e a multiplicação de elementos de $\mathbb{L}$ por elementos de $\mathbb{K}$ (multiplicação por escalar) obedecem as definições de espaço vetorial (cabe neste momento uma revisão de conceitos de Algébra Linear, sugerimos [10]).

Definição 5.9. A dimensão (e assim o número de elementos de uma base) de $\mathbb{L}$ como um $\mathbb{K}$-Espaço Vetorial chamamos de grau da extensão $\mathbb{L}$ sobre $\mathbb{K}$ e denotamos por $[\mathbb{L} : \mathbb{K}]$. Uma extensão $\mathbb{L}|\mathbb{K}$ será dita finita se tem grau finito e, caso o contrário, infinita.

Exemplo 5.10. $[\mathbb{C} : \mathbb{R}] = 2$. Pois, $\mathbb{C}$ é um espaço vetorial sobre $\mathbb{R}$, onde temos $\{1, i\}$ como uma base deste espaço.

Teorema 5.11. *(Teorema da Torre) Sejam $\mathbb{K}, \mathbb{L}$ e $\mathbb{M}$ corpos tais que $\mathbb{K} \subseteq \mathbb{L} \subseteq \mathbb{M}$ são extensões finitas. Então,* $[\mathbb{M} : \mathbb{K}] = [\mathbb{M} : \mathbb{L}][\mathbb{L} : \mathbb{K}]$.

Demonstração. Sejam $(a_i)_{i\in I}$ uma base do espaço vetorial de $\mathbb{L}$ sobre $\mathbb{K}$ e $(b_j)_{j\in J}$ uma base do espaço vetorial de $\mathbb{M}$ sobre $\mathbb{L}$, onde I, J são conjuntos. Para todo $i \in I$ e todo $j \in J$, temos $a_i \in \mathbb{L}$ e $b_j \in \mathbb{M}$. Basta mostrarmos que $(a_i b_j)_{i\in I, j\in J}$ é uma base para o espaço vetorial de $\mathbb{M}$ sobre $\mathbb{K}$.

Vamos inicialmente mostrar que $(a_i b_j)_{i\in I, j\in J}$ é linearmente independente. Para isso, tomemos

$$\sum_{i,j} k_{ij} a_i b_j = 0, \text{ com } k_{ij} \in \mathbb{K}.$$

E, assim

$$\sum_{i,j} k_{ij} a_i b_j = 0 \Leftrightarrow \sum_j \left(\sum_i k_{ij} a_i \right) b_j = 0.$$

Como $(b_j)_{j\in J}$ é L.I., temos

$$\sum_j m_j b_j = 0 \Leftrightarrow m_j = 0.$$

Logo, voltando ao nosso caso,

$$\sum_i k_{ij} a_i = 0, \forall j \in J.$$

Temos também que $(a_i)_{i\in I}$ é L.I., então

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

Vamos agora mostrar que $(a_i b_j)_{i\in I, j\in J}$ gera $\mathbb{M}$ sobre $\mathbb{K}$. Tomemos um elemento $v \in \mathbb{M}$ que podemos escrever da seguinte forma:

$$v = \sum_j n_j b_j, \text{ com } n_j \in \mathbb{L}.$$

E com isso, para cada j, temos que existem $r_{ij} \in \mathbb{K}$ tais que

$$n_j = \sum_i r_{ij} a_i.$$

Assim, o elemento $v \in \mathbb{M}$, pode ser escrito como:

$$v = \sum_j \left(\sum_i r_{ij} a_i \right) b_j = \sum_{ij} r_{ij} a_i b_j.$$

Portanto, $(a_i b_j)_{i\in I, j\in J}$ é uma base de $\mathbb{M}$ sobre $\mathbb{K}$. □

Definição 5.12. Sejam $\mathbb{L}|\mathbb{K}$ uma extensão e $\alpha \in \mathbb{L}$. Denotamos por $\mathbb{K}[\alpha]$ ao subdomínio de $\mathbb{L}$ formado por todos os polinômios de $\mathbb{K}[x]$ em α, ou seja, $\mathbb{K}[\alpha] = \{p(\alpha) : p(x) \in \mathbb{K}[x]\}$.

Note que como $\alpha \in \mathbb{L}$, temos que os elementos de $\mathbb{K}[\alpha]$ pertencem a $\mathbb{L}$, e mais, pode-se mostrar que $\mathbb{K}[\alpha]$, como definido, é realmente um domínio.

A partir de um domínio, podemos construir o "corpo de frações", como podemos ver em [8]. Sendo assim, denotamos por $\mathbb{K}(\alpha)$ o corpo de frações do domínio $\mathbb{K}[\alpha]$. Dessa forma,

$$\mathbb{K}(\alpha) = \left\{ \frac{f(\alpha)}{g(\alpha)}; \text{ com } f(x), g(x) \in \mathbb{K}[x] \text{ e } g(\alpha) \neq 0 \right\}.$$

Proposição 5.13. *Se α for algébrico sobre $\mathbb{K}$, então $\mathbb{K}[\alpha] = \mathbb{K}(\alpha)$.*

Demonstração. Sejam $p(x) = p_{min}(\alpha, \mathbb{K})$ e $\beta \in \mathbb{K}(\alpha)$. Temos que $\beta = \dfrac{g(\alpha)}{h(\alpha)}$ onde $g(x), h(x) \in \mathbb{K}[x], h(\alpha) \neq 0$.

Como $h(\alpha) \neq 0$, pela Proposição 5.7, $p(x)$ não divide $h(x)$, e como $p(x)$ é irredutível temos que o $\text{mdc}\,(p(x), h(x)) = 1$. Assim, pelo Lema 4.16 (Lema de Bézout), existem $a(x), b(x) \in \mathbb{K}[x]$ tais que

$$a(x)p(x) + b(x)h(x) = 1.$$

Dessa forma,

$$a(\alpha)p(\alpha) + b(\alpha)h(\alpha) = 1.$$

Logo,

$$a(\alpha) \cdot 0 + b(\alpha)h(\alpha) = 1.$$

Portanto, $h(\alpha)$ é invertível e podemos escrever: $\beta = g(\alpha)b(\alpha)$, ou seja, os elementos de $\mathbb{K}(\alpha)$ são escritos como polinômios em $\mathbb{K}[\alpha]$. Provando que $\mathbb{K}(\alpha) = \mathbb{K}[\alpha]$. □

A Proposição 5.13 nos permite escrever indistintamente $\mathbb{K}[\alpha]$ ou $\mathbb{K}(\alpha)$ quando α for algébrico sobre $\mathbb{K}$.

Definição 5.14. Sejam $\alpha_1, \alpha_2, \ldots, \alpha_n$ elementos algébricos sobre $\mathbb{K}$. A partir da Proposição 5.13, podemos definir, recursivamente:

$$\mathbb{K}(\alpha_1, \alpha_2, \ldots, \alpha_n) = \mathbb{K}(\alpha_1, \alpha_2, \ldots, \alpha_{n-1})(\alpha_n).$$

Definição 5.15. Seja $\mathbb{L}|\mathbb{K}$ uma extensão. Dizemos que $\mathbb{L}|\mathbb{K}$ é uma extensão simples se $\mathbb{L} = \mathbb{K}(\alpha)$ para algum $\alpha \in \mathbb{L}$.

Proposição 5.16. *Sejam $\mathbb{L}|\mathbb{K}$ uma extensão simples, $\mathbb{L} = \mathbb{K}(\alpha)$, onde $\alpha \in \mathbb{L}$ é algébrico sobre $\mathbb{K}$ e n é o grau do polinômio minimal $m(x)$ de α sobre $\mathbb{K}$. Então, $[\mathbb{L} : \mathbb{K}] = n$ e uma base de $\mathbb{K}(\alpha)$ sobre $\mathbb{K}$ é $\{1, \alpha, \alpha^2, \ldots, \alpha^{n-1}\}$.*

Demonstração. Por α ser algébrico sobre $\mathbb{K}$ e pela Proposição 5.13, temos $\mathbb{K}(\alpha) = \mathbb{K}[\alpha]$. Ou seja, os elementos de $\mathbb{L}$ são escritos como polinômios em $\mathbb{K}[\alpha]$.

Seja $v \in \mathbb{L}$ arbitrário, então $v = g(\alpha)$, para algum $g(x) \in \mathbb{K}[x]$. Pela Proposição 4.14 (Algoritmo da Divisão), existem $q(x), r(x) \in \mathbb{K}[x]$ tais que

$$g(x) = q(x)m(x) + r(x),$$

com $0 \leqslant \partial r(x) < \partial m(x) = n$. Daí,

$$\begin{aligned} g(\alpha) &= q(\alpha)m(\alpha) + r(\alpha) \\ &= q(\alpha) \cdot 0 + r(\alpha) \\ &= r(\alpha). \end{aligned}$$

Isto significa que $g(\alpha) = r(\alpha) = a_0 + a_1\alpha + \cdots + a_{n-1}\alpha^{n-1}$ com $a_0, a_1, \ldots, a_{n-1} \in \mathbb{K}$, provando que $\{1, \alpha, \alpha^2, \ldots, \alpha^{n-1}\}$ gera $\mathbb{L}$.

Provemos que esse conjunto é linearmente independente: sejam $b_j \in \mathbb{K}, 0 \leqslant j \leqslant n-1$ tais que

$$b_0 \cdot 1 + b_1\alpha + \cdots + b_{n-1}\alpha^{n-1} = 0.$$

Se os b_j não forem todos nulos, então o polinômio

$$h(x) = b_0 + b_1x + \cdots + b_{n-1}x^{n-1},$$

é tal que $h(\alpha) = 0$ com $\partial h(x) < n$, contrariando a minimalidade do grau de $m(x)$, logo os b_j são todos nulos e $\{1, \alpha, \alpha^2, \ldots, \alpha^{n-1}\}$ é L.I.

Portanto, $\{1, \alpha, \alpha^2, \ldots, \alpha^{n-1}\}$ é uma base de $\mathbb{L}|\mathbb{K}$ e $[\mathbb{L} : \mathbb{K}] = n$. □

As duas próximas proposições relacionam extensões algébricas e finitas: a primeira mostra que toda extensão finita é algébrica e a segunda apresenta as condições que uma extensão algébrica deve satisfazer para que possamos garantir sua finitude.

Proposição 5.17. *Se uma extensão $\mathbb{L}|\mathbb{K}$ é finita, então $\mathbb{L}|\mathbb{K}$ é algébrica.*

Demonstração. Seja uma extensão $\mathbb{L}|\mathbb{K}$ finita. Tomando $\alpha \in \mathbb{L}$, temos que $\mathbb{K} \subseteq \mathbb{K}(\alpha) \subseteq \mathbb{L}$, pelo Teorema 5.11 (Teorema da Torre), $\mathbb{K}(\alpha)|\mathbb{K}$ é finita. Seja n o grau da extensão $\mathbb{K}(\alpha)|\mathbb{K}$, então se tomarmos o conjunto $\{1, \alpha, \alpha^2, \ldots, \alpha^n\}$, como este conjunto tem $n+1$ elementos, ele é L.D., daí existem elementos $b_j \in \mathbb{K}$, $0 \leqslant j \leqslant n$, não todos nulos, tais que

$$b_0 \cdot 1 + b_1\alpha + b_2\alpha^2 + \cdots + b_n\alpha^n = 0.$$

E α é raiz do polinômio não nulo $p(x) = b_0 + b_1x + b_2x^2 \cdots + b_nx^n$, mostrando que α é algébrico e, como foi tomado arbitrário, temos que $\mathbb{L}|\mathbb{K}$ é algébrica. □

Proposição 5.18. *Se uma extensão $\mathbb{L}|\mathbb{K}$ é algébrica e existe um número finito de elementos $\alpha_1, \alpha_2, \ldots, \alpha_n \in \mathbb{L}$, tais que $\mathbb{L} = \mathbb{K}(\alpha_1, \alpha_2, \ldots, \alpha_n)$, então $\mathbb{L}|\mathbb{K}$ é finita.*

Demonstração. Pela Definição 5.14,

$$\mathbb{L} = \mathbb{K}(\alpha_1, \alpha_2, \ldots, \alpha_n) = \mathbb{K}(\alpha_1, \alpha_2, \ldots, \alpha_{n-1})(\alpha_n)$$

E pela Proposição 5.16, $[\mathbb{L} : \mathbb{K}(\alpha_1, \alpha_2, \ldots, \alpha_{n-1})]$ é finito. Finalmente, pelo Teorema 5.11 (Teorema da Torre), $[\mathbb{L} : \mathbb{K}]$ é finito. □

Terminamos a seção com o belíssimo Teorema do Elemento Primitivo:

Teorema 5.19. *(Teorema do Elemento Primitivo).*
Sejam $\mathbb{Q} \subseteq \mathbb{K} \subseteq \mathbb{L} \subseteq \mathbb{C}$ corpos. Se $\mathbb{L} = \mathbb{K}(\delta_1, \delta_2, \ldots, \delta_n)$, então existe um $\gamma \in \mathbb{L}$ tal que $\mathbb{L} = \mathbb{K}(\gamma)$.

Demonstração. Notemos que, por indução, basta mostrarmos que é válido para $n = 2$, pois, o caso $n = 1$ é trivial e os demais é resolvido de maneira recursiva, se provarmos para $n = 2$.

Dito isto, seja $\mathbb{L}$ um subcorpo $\mathbb{C}$ tal que $\mathbb{L} = \mathbb{K}(\delta_1, \delta_2)$, vamos reescrever $\mathbb{L} = \mathbb{K}(\alpha, \beta)$. Basta mostrarmos que existe $\gamma \in \mathbb{L}$ tal que $\mathbb{L} = \mathbb{K}(\gamma)$.

Sejam $p(x) = p_{min}(\alpha, \mathbb{K})$ e $q(x) = p_{min}(\beta, \mathbb{K})$, com $\partial p(x) = m$ e $\partial q(x) = n$. Pela Proposição 6.4, $p(x)$ e $q(x)$ tem, respectivamente, m e n raízes distintas em $\mathbb{C}$. Sejam $\alpha = \alpha_1, \ldots, \alpha_m$ as m raízes distintas de $p(x)$ e $\beta = \beta_1, \ldots, \beta_n$ as n raízes distintas de $q(x)$. Para $1 \leqslant i \leqslant m$ e $2 \leqslant j \leqslant n$, sejam λ_{ij} os seguintes números complexos:

$$\lambda_{ij} = \frac{\alpha_i - \alpha}{\beta - \beta_j}$$

Agora, tomemos um $\lambda \in \mathbb{K}$, onde $\lambda \neq \lambda_{ij}$ para todos i, j considerados, observe que, por $\mathbb{K}$ ser um conjunto infinito, garantimos a existência de tal λ. Definimos $\gamma = \alpha + \lambda\beta$ e seja $h(x) \in \mathbb{K}(\gamma)$ o polinômio $h(x) = p(\gamma - \lambda x)$.

Temos que β é raiz de $h(x)$, de fato, $h(\beta) = p(\gamma - \lambda\beta) = p(\alpha) = 0$.

E mais, $h(\beta_j) \neq 0$ para todo $2 \leqslant j \leqslant n$, provemos:

Supondo, por absurdo, que $h(\beta_j) = 0$ para algum j dos considerados, teremos $p(\gamma - \lambda\beta_j) = 0$, logo $\gamma - \lambda\beta_j = \alpha_i$ para algum $1 \leqslant i \leqslant m$.

Pela forma que definimos γ, temos

$$\begin{aligned} \alpha_i &= \gamma - \lambda\beta_j \\ &= \alpha + \lambda\beta - \lambda\beta_j \end{aligned}$$

que resulta em

$$\lambda = \frac{\alpha_i - \alpha}{\beta - \beta_j},$$

um absurdo, pois, contraria a hipótese estabelecida sobre λ.

Desta forma, podemos afirmar que o $\mathrm{mdc}_{\mathbb{C}[x]}(p(x), h(x)) = (x - \beta)$, pois, das raízes de $p(x)$ (lembrando que são todas simples) apenas β é raiz de $h(x)$.

Temos, também, que o $\mathrm{mdc}_{\mathbb{K}(\gamma)[x]}(p(x), h(x)) = (x - \beta)$. De fato, por $\mathbb{K}(\gamma) \subseteq \mathbb{C}$, o $\mathrm{mdc}_{\mathbb{K}(\gamma)[x]}(p(x), h(x))$ divide o $\mathrm{mdc}_{\mathbb{C}[x]}(p(x), h(x))$ e,

$$\partial[\mathrm{mdc}_{\mathbb{K}(\gamma)[x]}] \leqslant \partial[\mathrm{mdc}_{\mathbb{C}[x]}].$$

Assim, o $\mathrm{mdc}_{\mathbb{K}(\gamma)[x]}(p(x), h(x))$ é igual 1 ou $x - \beta$. Se $\mathrm{mdc}_{\mathbb{K}(\gamma)[x]}(p(x), h(x))$ fosse igual à 1 teríamos o absurdo de $\mathrm{mdc}_{\mathbb{C}[x]}(p(x), h(x)) = 1$, portanto, $\mathrm{mdc}_{\mathbb{K}(\gamma)[x]}(p(x), h(x)) = x - \beta$. Isto garante que $\beta \in \mathbb{K}(\gamma)$, pelo fato de mostrar que $x - \beta$ é um polinômio em $\mathbb{K}(\gamma)$. E isso implica que $\alpha \in \mathbb{K}(\gamma)$, pois $\alpha = \gamma - \lambda\beta$ e, $\gamma \in \mathbb{K}(\gamma)$, $\lambda \in \mathbb{K} \subseteq \mathbb{K}(\gamma)$ e $\beta \in \mathbb{K}(\gamma)$.

Disso tudo:

$$\mathbb{L} = \mathbb{K}(\alpha, \beta) \subseteq \mathbb{K}(\gamma). \tag{5.1}$$

E, juntando o fato de $\gamma \in \mathbb{L}$ (pela forma como o definimos) com o fato de $\mathbb{K} \subseteq \mathbb{L}$, temos,

$$\mathbb{K}(\gamma) \subseteq \mathbb{L}. \tag{5.2}$$

De (5.1) e (5.2), $\mathbb{L} = \mathbb{K}(\gamma)$. □

Capítulo 6

Teoria de Galois e Extensões Ciclotômicas

Neste capítulo, apresentamos um estudo da Teoria de Galois, onde expomos resultados que são necessários em demonstrações sobre construtibilidade feitas nos próximos capítulos.

Na Seção 6.5, introduzimos aplicações dos resultados da Teoria de Galois no estudo de Extensões Ciclotômicas.

6.1 Corpo de Decomposição de um Polinômio

Pelo Teorema Fundamental da Álgebra, veja [17], todo polinômio com coeficientes complexos de uma variável e de grau $n \geqslant 1$ tem todas as suas raízes em $\mathbb{C}$. Desta forma, um polinômio $p(x) \in \mathbb{K}[x]$, sendo $\mathbb{K}$ um subcorpo dos complexos, é tal que

$$p(x) = k(x-a_1)^{m_1}(x-a_2)^{m_2}\cdots(x-a_n)^{m_n},$$

onde $n, m_1, m_2, \ldots, m_n$ são inteiros positivos, $k \in \mathbb{K}$ e $a_1, a_2, \ldots, a_n$ são as raízes complexas de $p(x)$. Dizemos que m_i é a multiplicidade da raiz a_i. Quando $m_i = 1$, a raiz a_i é dita simples.

Definição 6.1. (Corpo de decomposição de um polinômio) Seja um polinômio $p(x) \in \mathbb{K}[x]$. O menor corpo $\mathbb{L}$ que contém $\mathbb{K}$ e todas as raízes de $p(x)$ é dito corpo de decomposição de $p(x)$, denotaremos por $\mathbb{L} = \mathrm{Gal}(p(x), \mathbb{K})$. E assim, um corpo $\mathbb{L}$ é o corpo de decomposição do polinômio $p(x) \in \mathbb{K}[x]$ se ele satisfaz:

i - $p(x)$ decompõe-se em $\mathbb{L}$ da seguinte forma

$$p(x) = k(x-a_1)(x-a_2)\cdots(x-a_n),$$

onde $k, a_1, a_2, \ldots, a_n \in \mathbb{L}$ e $a_1, a_2, \ldots, a_n$ são as raízes de $p(x)$;

ii - Se $p(x)$ decompõe-se em um corpo $\mathbb{L}'$ onde $\mathbb{K} \subseteq \mathbb{L}' \subseteq \mathbb{L}$, então $\mathbb{L}' = \mathbb{L}$. E temos, $\mathbb{L} = \mathbb{K}(a_1, a_2, \ldots, a_n)$.

Precisamos do conceito de derivada e algumas de suas propriedades.

Definição 6.2. Seja $p(x) = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n \in \mathbb{K}[x]$, onde $\mathbb{K}$ é um corpo. Temos que $p'(x) = a_1 + 2a_2x + \cdots + na_nx^{n-1}$ é dita a derivada de $p(x)$. Podem ser facilmente verificadas as seguintes propriedades:

Sejam $p(x), q(x) \in \mathbb{K}[x]$, então:

i - $((p(x) + q(x))' = p'(x) + q'(x)$;

ii - $((p(x) \cdot q(x))' = p'(x) \cdot q(x) + p(x) \cdot q'(x)$;

iii - $[p(q(x))]' = [p(y)]' \cdot q'(x)$, onde $y = q(x)$.

6.2 Extensões Separavéis, Normais, de Galois

Introduzimos o conceito de separabilidade com a seguinte definição:

Definição 6.3. Seja $\mathbb{L}|\mathbb{K}$ uma extensão algébrica. Um polinômio $p(x) \in \mathbb{K}[x]$ irredutível sobre $\mathbb{K}$ é dito separável sobre $\mathbb{K}$ se ele não tiver raízes múltiplas em nenhum corpo de decomposição. Caso o contrário, dizemos que ele é inseparável. Um $\alpha \in \mathbb{L}$ algébrico sobre $\mathbb{K}$ é dito separável se seu polinômio minimal sobre $\mathbb{K}$ for separável sobre $\mathbb{K}$. $\mathbb{L}|\mathbb{K}$ é dita uma extensão separável se todos seus elementos forem separáveis sobre $\mathbb{K}$.

Proposição 6.4. *Sejam $\mathbb{K}$ um subcorpo de $\mathbb{C}$ e $p(x) \in \mathbb{K}[x]$ um polinômio de grau $n \geqslant 1$. Então:*

i - $p(x)$ é separável $\Leftrightarrow \text{mdc}(p(x), p'(x)) = 1$.

ii - Se $p(x)$ é irredutível sobre $\mathbb{K}$, então todas as raízes de $p(x)$ são simples.

Demonstração.

i - $\Rightarrow$) Suponha $\text{mdc}(p(x), p'(x)) = d(x) \neq 1$. Então, $p(x) = p_1(x)d(x)$ e $p'(x) = p_2(x)d(x)$ para alguns $p_1(x), p_2(x) \in \mathbb{K}[x]$. Agora, seja $\alpha \in \mathbb{C}$ tal que $d(\alpha) = 0$. Temos que $p(\alpha) = p'(\alpha) = 0$, portanto podemos escrever $p(x) = (x - \alpha)g(x)$. Derivando $p(x)$, pela forma como escrevemos, chegamos a $p'(x) = (x-\alpha)g'(x)+g(x)$, assim, $p'(\alpha) = g(\alpha) = 0$. Temos que, $g(x) = (x - \alpha)f(x)$, que substituindo em $p(x)$, obtemos $p(x) = (x - \alpha)^2 f(x)$, logo α não é uma raiz simples de $p(x)$, portanto $p(x)$ não é separável, um absurdo.

$\Leftarrow$) Suponha que $p(x)$ não seja separável. Então, $p(x)$ possui uma raiz com multiplicidade $k > 1$. Seja α essa raiz. Podemos escrever $p(x) = (x-\alpha)^k g(x)$. Derivando $p(x)$, obtemos

$$p'(x) = (x - \alpha)^{k-1}[kg(x) + (x - \alpha)g'(x)].$$

Portanto, $p(x)$ e $p'(x)$ têm pelo menos um fator em comum em $\mathbb{C}[x]$, a saber $(x-\alpha)$, logo

$$\text{mdc}(p(x), p'(x)) \neq 1.$$

ii - Seja α uma raiz de $p(x)$. Se α tem multiplicidade maior do que 1, então, $p'(\alpha) = 0$, assim $\text{mdc}(p(x), p'(x)) \neq 1$, pelo item (i), $p(x)$ não é separável, absurdo.

□

Proposição 6.5. *Seja $\mathbb{L}|\mathbb{K}$ uma extensão algébrica. Se $\mathbb{K}$ é um corpo de característica 0, então $\mathbb{L}|\mathbb{K}$ é separável.*

Demonstração.

Tomando um $\alpha \in \mathbb{L}$, por $\mathbb{L}|\mathbb{K}$ ser algébrica, existe $m(x) = p_{min}(\alpha, \mathbb{K})$. E seja $m'(x)$ sua derivada.

Seja $\partial m(x) = n$, por $\mathbb{K}$ ser de característica 0, temos $\partial m'(x) = n - 1$.

Assim, $m'(\alpha) \neq 0$, pois caso contrário, teríamos um absurdo, diante da minimalidade de grau de $m(x)$.

Suponha que $m(x)$ não seja separável, então, pela Proposição 6.4, $\text{mdc}\,(m(x), m'(x)) = d(x) \neq 1$. Portanto, $d(x)|m(x)$ o que contraria a hipótese de que $m(x)$ é irredutível. □

Definição 6.6. Uma extensão $\mathbb{L}|\mathbb{K}$ é dita normal se todo polinômio irredutível $p(x) \in \mathbb{K}[x]$ que tem ao menos uma raiz em $\mathbb{L}$ se decompõe linearmente em $\mathbb{L}$, ou seja, se $p(x)$ tem uma raiz em $\mathbb{L}$, então todas as raízes de $p(x)$ estão em $\mathbb{L}$.

Apresentamos a seguir uma situação onde a extensão é normal. O exemplo nos ajuda a melhor compreender a definição de extensão normal e nos mostra um processo de identificação de extensões deste tipo.

Exemplo 6.7. Se uma extensão $\mathbb{L}|\mathbb{K}$ é tal que $[\mathbb{L} : \mathbb{K}] = 2$, então $[\mathbb{L} : \mathbb{K}]$ é normal.

De fato, para todo $\alpha \in \mathbb{L}$, com $\alpha \notin \mathbb{K}$, temos, pelo fato de $[\mathbb{L} : \mathbb{K}] = 2$, que $\mathbb{L} = \mathbb{K}(\alpha)$. E, da Proposição 5.16, o grau de $p(x) = p_{min}(\alpha, \mathbb{K}) = 2$. Então, $p(x) = (x - \alpha)q(x)$ para algum $q(x) \in \mathbb{L}[x]$ com $\partial q(x) = \partial p(x) - 1 = 1$, daí, $q(x) = x - \beta$ para algum $\beta \in \mathbb{L}$. Ou seja, a outra raiz de $p(x)$ está em $\mathbb{L}$, mostrando que $\mathbb{L}|\mathbb{K}$ é normal, pela Definição 6.6.

Definição 6.8. Sejam $\mathbb{K}, \mathbb{K}'$ subcorpos de $\mathbb{C}$, $\sigma : \mathbb{K} \longrightarrow \mathbb{K}'$ um isomorfismo e $p(x) = a_0 + a_1x + \cdots + a_nx^n$ um polinômio em $\mathbb{K}[x]$. Definimos $p^\sigma(x)$ por:

$$p^\sigma(x) = a'_0 + a'_1x + \cdots + a'_nx^n,$$

onde $a'_i = \sigma(a_i)$ para $0 \leqslant i \leqslant n$.

Usamos a Definição 6.8, na apresentação de dois importantes lemas, cujas demonstrações podem ser encontradas em [8], [11] ou [17], que serão necessários em uma gama de demonstrações no transcorrer de todo o capítulo.

Lema 6.9. *Sejam $\mathbb{K}, \mathbb{K}'$ subcorpos de $\mathbb{C}$, $\sigma : \mathbb{K} \longrightarrow \mathbb{K}'$ um isomorfismo e $p(x)$ um polinômio irredutível sobre $\mathbb{K}$. Se α é uma raíz de $p(x)$ e β é uma raiz de $p^\sigma(x)$. Então, existe um único isomorfismo $\tilde{\sigma} : \mathbb{K}(\alpha) \longrightarrow \mathbb{K}(\beta)$ tal que $\tilde{\sigma}(\alpha) = \beta$ e $\tilde{\sigma}|_{\mathbb{K}} = \sigma$.*

Lema 6.10. *Sejam $\mathbb{K}, \mathbb{K}'$ subcorpos de $\mathbb{C}$, $\sigma : \mathbb{K} \longrightarrow \mathbb{K}'$ um isomorfismo e $p(x) \in \mathbb{K}[x]$. Se $\mathbb{L} = \mathrm{Gal}(p(x), \mathbb{K})$ e $\mathbb{L}' = \mathrm{Gal}(p^\sigma(x), \mathbb{K}')$. Então, existe um isomorfismo $\hat{\sigma} : \mathbb{L} \longrightarrow \mathbb{L}'$ tal que $\hat{\sigma}|_{\mathbb{K}} : \sigma$.*

A seguinte proposição mostra um critério menos restritivo sobre extensões finitas que implica em suas normalidades. O resultado nos poupa de termos que verificar as condições da Definição 6.6 sobre todos os polinômios irredutíveis citados, bastando que a extensão seja o corpo de decomposição de um polinômio separável sobre o corpo base.

Proposição 6.11. *Seja $\mathbb{L}|\mathbb{K}$ uma extensão finita. $\mathbb{L}|\mathbb{K}$ é normal e separável se, e somente se, $\mathbb{L}$ for o corpo de decomposição de algum polinômio separável $p(x) \in \mathbb{K}[x]$.*

Demonstração.

$\Rightarrow$) Seja $\mathbb{L}|\mathbb{K}$ normal e separável. Pelo Teorema 5.19, $\exists \alpha \in \mathbb{L}$ tal que $\mathbb{L} = \mathbb{K}(\alpha)$. Como a extensão é finita, pela Proposição 5.17, é também algébrica. Seja $m(x) = p_{min}(\alpha, \mathbb{K})$, temos que $m(x)$ é separável, pelo fato de $\mathbb{L}|\mathbb{K}$ ser separável. Por $\alpha \in \mathbb{L}$ e $\mathbb{L}|\mathbb{K}$ ser normal, temos que todas as raízes de $m(x)$ estão em $\mathbb{L}$. Assim,

$$\mathrm{Gal}(m(x), \mathbb{K}) \subseteq \mathbb{L} = \mathbb{K}(\alpha) \subseteq \mathrm{Gal}(m(x), \mathbb{K}).$$

Portanto, $\mathbb{L} = \mathrm{Gal}(m(x), \mathbb{K})$, ou seja, $\mathbb{L}|\mathbb{K}$ é o corpo de decomposição do polinômio separável $m(x)$.

$\Leftarrow$) Seja $\mathbb{L}$ um corpo de decomposição de um polinômio separável $p(x) \in \mathbb{K}[x]$, ou seja, $\mathbb{L} = \mathrm{Gal}(p(x), \mathbb{K})$. Seja $f(x)$ um polinômio irredutível sobre $\mathbb{K}$ e $\alpha \in \mathbb{L}$ uma raiz de $f(x)$. Seja β uma outra raiz de $f(x)$, é suficiente mostrarmos que $\beta \in \mathbb{L}$. Vejamos:

No Lema 6.9, consideremos σ como o isomorfismo identidade de $\mathbb{K}$, $\mathrm{Id}_{\mathbb{K}}$, ou seja, $\sigma(a) = a$ para todo $a \in \mathbb{K}$. Então, esse lema garante a existência de um único isomorfismo $\tilde{\sigma} : \mathbb{K}(\alpha) \longrightarrow \mathbb{K}(\beta)$ tal que $\tilde{\sigma}(\alpha) = \beta$ e $\tilde{\sigma}|_{\mathbb{K}} = \mathrm{Id}_{\mathbb{K}}$.

Enquanto que, pelo Lema 6.10, existe um isomorfismo

$$\hat{\sigma} : \mathrm{Gal}(p(x), \mathbb{K}(\alpha)) \longrightarrow \mathrm{Gal}(p(x), \mathbb{K}(\beta))$$

tal que $\hat{\sigma}|_{\mathbb{K}(\alpha)} = \tilde{\sigma}$ e, restringindo mais, temos $\hat{\sigma}|_{\mathbb{K}} = \mathrm{Id}_{\mathbb{K}}$.

De $\alpha \in \mathbb{L}$, temos $\mathrm{Gal}(p(x), \mathbb{K}(\alpha)) = \mathbb{L} = \mathrm{Gal}(p(x), \mathbb{K})$. Chamemos $\mathrm{Gal}(p(x), \mathbb{K}(\beta))$ de $\mathbb{L}'$.

Assim, $\hat{\sigma}$ é um isomorfismo entre dois $\mathbb{K}$-espaços vetoriais e, portanto,

$$[\mathbb{L} : \mathbb{K}] = [\mathbb{L}' : \mathbb{K}]$$

Notemos que, como $\mathbb{K} \subseteq \mathbb{K}(\beta)$, temos $\mathbb{L} = \mathrm{Gal}(p(x), \mathbb{K}) \subseteq \mathrm{Gal}(p(x), \mathbb{K}(\beta)) = \mathbb{L}'$.

E, assim, juntando as informações $\mathbb{L} \subseteq \mathbb{L}'$ com $[\mathbb{L} : \mathbb{K}] = [\mathbb{L}' : \mathbb{K}]$, temos, pelo Teorema da Torre 5.11,

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

Logo, $[\mathbb{L}' : \mathbb{L}] = 1$, que equivale a $\mathbb{L}' = \mathbb{L}$, portanto, $\beta \in \mathbb{L}$, mostrando que $\mathbb{L}|\mathbb{K}$ é normal.

A separabilidade é imediata, pois $\mathbb{L} = \mathrm{Gal}(p(x), \mathbb{K})$, e assim, todos os elementos da extensão são separáveis, uma vez que, $\mathbb{L} = \mathbb{K}[\alpha_1, \alpha_2, \ldots, \alpha_n]$, onde $\alpha_1, \alpha_2, \ldots, \alpha_n$ são as raízes do polinômio separável $p(x)$. □

Definição 6.12. Uma extensão finita $\mathbb{L}|\mathbb{K}$ é dita de Galois se ela for normal e separável.

Proposição 6.13. *Seja $\mathbb{K} \subseteq \mathbb{M} \subseteq \mathbb{L}$ uma cadeia de corpos. Se a extensão $\mathbb{L}|\mathbb{K}$ é de Galois, então $\mathbb{L}|\mathbb{M}$ é de Galois.*

Demonstração. Seja $\mathbb{L}|\mathbb{K}$ uma extensão de Galois. Pela Proposição 6.11, juntamente com a Definição 6.12, é suficiente mostrarmos que $\mathbb{L}|\mathbb{M}$ é o corpo de decomposição de um polinômio $q(x) \in \mathbb{M}[x]$ separável.

Como $\mathbb{L}|\mathbb{K}$ é de Galois, pela Proposição 6.11, $\mathbb{L} = \mathrm{Gal}(q(x), \mathbb{K})$, ou seja, é o corpo de decomposição de um polinômio $q(x)$ separável sobre $\mathbb{K}$.

Agora, por $\mathbb{K} \subseteq \mathbb{M}$, temos que, $q(x) \in \mathbb{M}[x]$ e $\mathrm{Gal}(q(x), \mathbb{K}) \subseteq \mathrm{Gal}(q(x), \mathbb{M})$ que equivale a

$$\mathbb{L} \subseteq \mathrm{Gal}(q(x), \mathbb{M}). \tag{6.1}$$

Por outro lado, por $\mathbb{L}$ ser o corpo de decomposição de $q(x)$, $\mathbb{L}$ contém todas as raízes de $q(x)$. Além disso, $\mathbb{M} \subseteq \mathbb{L}$, portanto,

$$\mathrm{Gal}(q(x), \mathbb{M}) \subseteq \mathbb{L}. \tag{6.2}$$

De (6.1) e (6.2), $\mathbb{L} = \mathrm{Gal}(q(x), \mathbb{M})$, terminando a demonstração. □

6.3 Grupo de Galois

Como citado no Capítulo 2, estenderemos o conceito de automorfismo de grupos para automorfismo de corpos e falaremos sobre grupos de automorfismos.

Definição 6.14. (Automorfismo) Seja uma função f de um corpo $\mathbb{K}$ nele próprio. Se f for tal que

$$f(a \cdot b) = f(a) \cdot f(b) \text{ e}$$

$$f(a + b) = f(a) + f(b)$$

$$\forall a, b \in \mathbb{K}$$

e, além disso, f ser bijetiva, f é dito um automorfismo de $\mathbb{K}$.

Proposição 6.15. *O conjunto dos automorfismos de um corpo* $\mathbb{K}$*, que denotaremos por* $\operatorname{Aut}\mathbb{K}$*, com a operação* $\circ$ *composição de funções é um grupo.*

Demonstração. Precisamos mostrar que o par $(\operatorname{Aut}\mathbb{K}, \circ)$ obedece as condições da Definição 2.1. Vejamos:

Sejam $\sigma, \rho, \tau \in \operatorname{Aut}\mathbb{K}$. Da Definição 6.14,

$$(\sigma \circ \rho)(x) = \sigma(\rho(x)) = \sigma(y), \text{ para } \rho(x) = y, \text{ tal que } x, y \in \mathbb{K}.$$

Com isso, a composição de automorfismos é também um automorfismo, garantindo que a operação está bem definida.

Notemos que pela definição de automorfismo, todo automorfismo é homomorfismo, sendo assim,

$$\tau \circ (\sigma \circ \rho)(x) = \tau(x) \circ (\sigma \circ \rho)(x) = \tau(x) \circ \sigma(x) \circ \rho(x) = (\tau \circ \sigma)(x) \circ \rho(x) = (\tau \circ \sigma) \circ \rho(x).$$

Ou seja,

$$\tau \circ (\sigma \circ \rho)(x) = (\tau \circ \sigma) \circ \rho(x).$$

O que mostra a associatividade da operação.

Agora, seja $\epsilon \in \operatorname{Aut}\mathbb{K}$ tal que $\epsilon(x) = x$, para todo $x \in \mathbb{K}$, chamamos ϵ de identidade de $\operatorname{Aut}\mathbb{K}$, e como

$$(\sigma \circ \epsilon)(x) = \sigma(\epsilon(x)) = \sigma(x) = \epsilon(\sigma(x)) = (\epsilon \circ \sigma)(x),$$

temos ϵ como o elemento neutro de $\operatorname{Aut}\mathbb{K}$.

Ainda da Definição 6.14, todo automorfismo é bijetivo. Como toda aplicação bijetiva admite inversa, isto nos garante a existência dos inversos. □

Definição 6.16. Seja uma extensão $\mathbb{L}|\mathbb{K}$. Um automorfismo ϕ dessa extensão é dito um $\mathbb{K}$-automorfismo se ele preserva os elementos de $\mathbb{K}$, ou seja,

$$\phi(a) = a, \forall a \in \mathbb{K}.$$

O conjunto dos $\mathbb{K}$-automorfismos de $\mathbb{L}$ denotaremos por $\operatorname{Aut}_{\mathbb{K}}\mathbb{L}$.

Proposição 6.17. *Seja uma extensão* $\mathbb{L}|\mathbb{K}$*. O conjunto dos* $\mathbb{K}$*-automorfismos forma um grupo com a operação* $\circ$ *composição de funções. O qual denotaremos por* $\Gamma(\mathbb{L}|\mathbb{K})$*, Grupo de Galois da extensão* $\mathbb{L}|\mathbb{K}$*.*

Demonstração. Da Proposição 6.15, sabemos que $\operatorname{Aut}\mathbb{L}$ é um grupo com a operação composição de funções. Mostraremos que $\Gamma(\mathbb{L}|\mathbb{K})$ é um subgrupo de $\operatorname{Aut}\mathbb{K}$. Pela Proposição 2.7, devemos mostrar que sempre que $\sigma, \rho \in \operatorname{Aut}_{\mathbb{K}}\mathbb{L}$, temos $\sigma \circ \rho^{-1} \in \operatorname{Aut}_{\mathbb{K}}\mathbb{L}$, vejamos:

Seja $x \in \mathbb{L}$, da definição de automorfismo e da definição de $\mathbb{K}$-automorfismo,

$$(\sigma \circ \rho)(x) = \sigma(\rho(x)) = \sigma(x) = x,$$

o que nos mostra que, sempre que $\sigma, \rho \in \mathrm{Aut}_{\mathbb{K}}\,\mathbb{L}$, temos $\sigma \circ \rho \in \mathrm{Aut}_{\mathbb{K}}\,\mathbb{L}$.

Resta-nos mostrar que $\rho^{-1} \in \mathrm{Aut}_{\mathbb{K}}\,\mathbb{L}$. Ora,

$$x = (\rho^{-1} \circ \rho)(x) = \rho^{-1}(\rho(x)) = \rho^{-1}(x).$$

Portanto, $\mathrm{Aut}_{\mathbb{K}}\,\mathbb{L} < \mathrm{Aut}\,\mathbb{L}$. □

Proposição 6.18. *Sejam $\mathbb{L}|\mathbb{K}$ uma extensão, σ um $\mathbb{K}$-automorfismo da extensão $\mathbb{L}|\mathbb{K}$ e $\alpha \in \mathbb{L}$ uma raiz do polinômio $p(x) \in \mathbb{K}[x]$. Então, $\sigma(\alpha) = \alpha_i$, onde α_i é raiz de $p(x)$. E mais, pelo fato de σ ser bijetivo, σ permuta as raízes de $p(x)$.*

Demonstração. Sejam $\sigma \in \mathrm{Aut}_{\mathbb{K}}\,\mathbb{L}$ e $p(x) \in \mathbb{K}[x]$, tal que $p(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$.

$$\begin{aligned}
\sigma(p(x)) &= \sigma(a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0) \\
&= \sigma(a_n x^n) + \sigma(a_{n-1}x^{n-1}) + \cdots + \sigma(a_1 x) + \sigma(a_0) \\
&= \sigma(a_n)\sigma(x^n) + \sigma(a_{n-1})\sigma(x^{n-1}) + \cdots + \sigma(a_1)\sigma(x) + \sigma(a_0) \\
&= a_n\sigma(x^n) + a_{n-1}\sigma(x^{n-1}) + \cdots + a_1\sigma(x) + a_0 \\
&= p(\sigma(x)).
\end{aligned}$$

Assim,

$$\sigma(p(x)) = p(\sigma(x)).$$

Logo, se α_i é raiz de $p(x)$, ou seja, $p(\alpha_i) = 0$, temos:

$$p(\sigma(\alpha_i)) = \sigma(p(\alpha_i)) = \sigma(0) = 0 \Longrightarrow p(\sigma(\alpha_i)) = 0.$$

Portando, $\sigma(\alpha_i)$ é raiz de $p(x)$ e podemos concluir que um automorfismo leva uma raiz de $p(x)$ em outra que esteja em $\mathbb{L}$. □

Proposição 6.19. *Seja $\mathbb{L}|\mathbb{K}$ uma extensão finita e separável. Então, $|\Gamma(\mathbb{L}|\mathbb{K})| \leqslant [\mathbb{L} : \mathbb{K}]$.*

Demonstração. Seja $\alpha \in \mathbb{L}, \alpha \notin \mathbb{K}$, e tomemos a extensão $\mathbb{K}(\alpha)|\mathbb{K}$. Por $\mathbb{L}|\mathbb{K}$ ser finita, é algébrica. Assim, α é algébrico sobre $\mathbb{K}$ e seja $m(x) = p_{min}(\alpha, \mathbb{K})$. Seja R_m o conjunto de raízes de $m(x)$ e tomemos a seguinte aplicação:

$$\begin{array}{rccc} f: & \Gamma(\mathbb{L}|\mathbb{K}) & \longrightarrow & R_m \cap \mathbb{L} \\ & \sigma & \longmapsto & \sigma(\alpha). \end{array}$$

Pela Proposição 6.18, f está bem definida, pois cada $\mathbb{K}$-automorfismo da extensão $\mathbb{L}|\mathbb{K}$ leva uma raiz de $m(x)$ em outra que esteja em $\mathbb{L}$.

Temos que f é injetiva. De fato, se tivermos $\sigma(\alpha) = \rho(\alpha) = \alpha_i$, como a extensão é separável, as raízes do conjunto R_m são distintas, logo, existe um único automorfismo que leva α em α_i, portanto, $\sigma = \rho$. E, assim,

$$|\Gamma(\mathbb{L}|\mathbb{K})| \leqslant |R_m \cap \mathbb{L}| \leqslant \partial m(x) = [\mathbb{K}(\alpha) : \mathbb{K}] \leqslant [\mathbb{L} : \mathbb{K}], \tag{6.3}$$

onde $|R_m \cap \mathbb{L}|$ denota a ordem do conjunto $R_m \cap \mathbb{L}$, e $m(x) = [\mathbb{K}(\alpha) : \mathbb{K}]$ pela Proposição 5.16. □

Proposição 6.20. *Seja $\mathbb{L}|\mathbb{K}$ uma extensão finita e separável. $\mathbb{L}|\mathbb{K}$ é de Galois se, e somente se, $\Gamma(\mathbb{L}|\mathbb{K}) = [\mathbb{L} : \mathbb{K}]$.*

Demonstração.

Como $\mathbb{L}|\mathbb{K}$ é finita e separável, pelo Teorema 5.19 (Teorema do Elemento Primitivo), $\exists \alpha \in \mathbb{L}$ tal que $\mathbb{L} = \mathbb{K}(\alpha)$. Seja $m(x) = p_{min}(\alpha, \mathbb{K})$, com $\partial m(x) = n$.

$\Rightarrow$) Seja $\mathbb{L}|\mathbb{K}$ de Galois, pela Definição 6.12, $\mathbb{L}|\mathbb{K}$ é normal. Daí, todas as raízes de $m(x)$ estão em $\mathbb{L}$, pelo fato de $\alpha \in \mathbb{L}$ e pela Definição 6.6. Logo,

$$\mathbb{L} = \mathbb{K}(\alpha) \subseteq \mathrm{Gal}(m(x), \mathbb{K}) \subseteq \mathbb{L}.$$

Ou seja, $\mathbb{L}$ é o corpo de decomposição de $m(x)$, $\mathbb{L} = \mathrm{Gal}(m(x), \mathbb{K})$. Por $m(x) = p_{min}(\alpha, \mathbb{K})$, temos $m(x)$ irredutível e, pelo item (ii) da Proposição 6.4, $m(x)$ tem n raízes distintas (lembrando que todas estão em $\mathbb{L}$). Sejam $\alpha = \alpha_1, \ldots, \alpha_n$ as n raízes de $m(x)$.

Tomando, no Lema 6.9, $\sigma = \mathrm{Id}_{\mathbb{K}}$ o isomorfismo identidade em $\mathbb{K}$, obtemos que, para todo $1 \leqslant i \leqslant n$, existe o isomorfismo $\sigma_i : \mathbb{K}(\alpha) \longrightarrow \mathbb{K}(\alpha_i)$ tal que $\sigma_i(\alpha) = \alpha_i$ e $\sigma|_{\mathbb{K}} = \mathrm{Id}_{\mathbb{K}}$. Como $\mathbb{K}(\alpha) = \mathbb{L}$, temos o isomorfismo σ_i reescrito como $\sigma_i : \mathbb{L} \longrightarrow \mathbb{K}(\alpha_i)$, mostrando que $\mathbb{K}(\alpha_i) \subseteq \mathbb{L}$ e, pela Definição 6.14 (Definição de Automorfismo), $\sigma_i \in \mathrm{Aut}\,\mathbb{L}$. Lembramos que σ_i preserva $\mathbb{K}$, logo $\sigma_i \in \mathrm{Aut}_{\mathbb{K}}\,\mathbb{L}$ que equivale à $\sigma_i \in \Gamma(\mathbb{L}|\mathbb{K})$. Desta forma, obtemos n automorfismos de $\Gamma(\mathbb{L}|\mathbb{K})$ e, assim, usando a Proposição 5.16,

$$|\Gamma(\mathbb{L}|\mathbb{K})| \geqslant n = [\mathbb{K}(\alpha) : \mathbb{K}] = [\mathbb{L} : \mathbb{K}]. \tag{6.4}$$

Por outro lado, pela Proposição 6.19,

$$|\Gamma(\mathbb{L}|\mathbb{K})| \leqslant [\mathbb{L} : \mathbb{K}]. \tag{6.5}$$

De (6.4) e (6.5), $|\Gamma(\mathbb{L}|\mathbb{K})| = [\mathbb{L} : \mathbb{K}]$.

$\Leftarrow$) Seja $|\Gamma(\mathbb{L}|\mathbb{K})| = [\mathbb{L} : \mathbb{K}]$. Pela demonstração da Proposição 6.19, em particular, pela Equação 6.3, temos $|R_m \cap \mathbb{L}| = \partial m(x) = [\mathbb{K}(\alpha) : \mathbb{K}] = [\mathbb{L} : \mathbb{K}]$.

Assim todas as raízes de $m(x)$ estão em $\mathbb{L}$ e,

$$\mathrm{Gal}(m(x), \mathbb{K}) \subseteq \mathbb{L} = \mathbb{K}(\alpha) \subseteq \mathrm{Gal}(m(x), \mathbb{K}).$$

Ou seja, $\mathbb{L} = \mathrm{Gal}(m(x), \mathbb{K})$, estamos dizendo que $\mathbb{L}$ é o corpo de decomposição do polinômio separável $m(x)$ e, daí, pela Proposição 6.11 e Definição 6.12, $\mathbb{L}|\mathbb{K}$ é de Galois. □

Proposição 6.21. *O corpo de decomposição de $x^n - 1$ sobre $\mathbb{Q}$ é dado por $\mathbb{Q}[\zeta]$, onde ζ é uma raiz n-ésima primitiva da unidade em $\mathbb{C}$.*

Demonstração. De fato, vimos na Subseção 3.1.3 que, as raízes de $x^n - 1$ são as do conjunto:

$$\left\{\zeta_n, \zeta_n^2, \ldots, \zeta_n^{n-1}, \zeta_n^n = 1\right\},$$

onde $\zeta_n = \cos\frac{2\pi}{n} + i\,\mathrm{sen}\,\frac{2\pi}{n}$.

Vimos também que, ζ_n é uma raiz n-ésima primitiva da unidade e que, uma característica marcante de uma raiz n-ésima primitiva da unidade é a propriedade que ela tem de "gerar" as demais raízes n-ésimas da unidade, por potências sucessivas.

Desta forma, seja ζ uma raiz n-ésima primitiva da unidade e $\zeta^2, \ldots, \zeta^{n-1}$ as demais raízes n-ésimas da unidade. Pelo que vimos acima, obviamente, $\mathbb{Q}[\zeta] \subseteq \mathbb{Q}[\zeta, \zeta^2, \ldots, \zeta^{n-1}]$ e, como $\zeta^i \in \mathbb{Q}[\zeta]$ para todo $1 \leqslant i \leqslant n$, $\mathbb{Q}[\zeta, \zeta^2, \ldots, \zeta^{n-1}] \subseteq \mathbb{Q}[\zeta]$. Logo,

$$\mathbb{Q}[\zeta, \zeta^2, \ldots, \zeta^{n-1}] = \mathbb{Q}[\zeta].$$

Pela Definição 6.1, $\mathbb{Q}[\zeta] = \mathrm{Gal}(p(x), \mathbb{Q})$, onde $p(x) = x^n - 1$. □

6.4 Correspondência de Galois

Devido a grandiosidade do Teorema da Correspondência de Galois, é interessante que sua demonstração seja fracionada. Desta forma, faremos as demonstrações de proposições que, em conjunto, culminam com o referido teorema.

Seja uma extensão $\mathbb{L}|\mathbb{K}$. Chamamos um corpo $\mathbb{M}$ tal que $\mathbb{K} \subseteq \mathbb{M} \subseteq \mathbb{L}$ de corpo intermediário. Notemos que todo $\mathbb{M}$-automorfismo de $\mathbb{L}$ é também um $\mathbb{K}$-automorfismo de $\mathbb{L}$ e, assim $\Gamma(\mathbb{L}|\mathbb{M})$ é um subgrupo de $\Gamma(\mathbb{L}|\mathbb{K})$.

Proposição 6.22.

Seja H um subgrupo de $\Gamma(\mathbb{L}|\mathbb{K})$, o conjunto ${}_{fix}\mathbb{H} = \{a \in \mathbb{L} : \sigma(a) = a, \forall \sigma \in H\}$ é uma extensão intermediária $\mathbb{K} \subseteq {}_{fix}\mathbb{H} \subseteq \mathbb{L}$. Denominamos o corpo ${}_{fix}\mathbb{H}$ como "corpo fixo de H".

Demonstração.

Verificaremos os itens (i), (ii) e (iii) da Proposição 4.7:

i - Temos que 0 e 1 pertencem a ${}_{fix}\mathbb{H}$, pois, para todo $\sigma \in H$, $\sigma(0) = 0$ e $\sigma(1) = 1$, uma vez que, os automorfismos de H fixam os elementos de $\mathbb{K}$ e por $\mathbb{K}$ ser corpo já contém 0 e 1;

ii - Sejam $a, b \in {}_{fix}\mathbb{H}$, então $\forall \sigma \in H$, pelas propriedades de homomorfismo de σ:

Como $\sigma(0) = 0$,

$$\sigma(b + (-b)) = \sigma(b) + \sigma(-b) = 0$$

Logo, $\sigma(-b) = -\sigma(b)$.

Agora,

$$\sigma(a - b) = \sigma(a) + \sigma(-b) = a - b$$

e,

$$\sigma(a \cdot b) = \sigma(a) \cdot \sigma(b) = a \cdot b$$

Assim, $a - b$ e $a \cdot b \in {}_{fix}\mathbb{H}$;

iii - Seja $0 \neq a \in {}_{fix}\mathbb{H}$, pelas propriedades de homomorfismo de σ dadas na Proposição 2.26, temos que,

$$\sigma(a^{-1}) = [\sigma(a)]^{-1} = a^{-1}.$$

Portanto, $a^{-1} \in {}_{fix}\mathbb{H}$.

Por satisfazer estes itens, temos ${}_{fix}\mathbb{H}$ é um subcorpo de $\mathbb{L}$. Agora, como H é um subgrupo de $\Gamma(\mathbb{L}|\mathbb{K})$ temos que, $\forall x \in \mathbb{K}$ e $\forall \sigma \in H, \sigma(x) = x$, logo, $\mathbb{K} \subseteq {}_{fix}\mathbb{H}$. Concluindo que, $\mathbb{K} \subseteq {}_{fix}\mathbb{H} \subseteq \mathbb{L}$. □

Proposição 6.23. *Sejam $\mathbb{L}|\mathbb{K}$ uma extensão, $\Gamma(\mathbb{L}|\mathbb{K})$ o grupo de Galois da extensão e H_1, H_2 dois subgrupos de $\Gamma(\mathbb{L}|\mathbb{K})$. Se $H_1 < H_2$, então ${}_{fix}\mathbb{H}_2 \subseteq {}_{fix}\mathbb{H}_1$.*

Demonstração. Seja $x \in {}_{fix}\mathbb{H}_2$. Assim, $x \in \mathbb{L}$ e $\sigma(x) = x$ para todo $\sigma \in H_2$ e, em particular, como $H_1 < H_2$, temos $\sigma(x) = x$ para todo $\sigma \in H_1$. Portanto, $x \in {}_{fix}\mathbb{H}_1$, logo, ${}_{fix}\mathbb{H}_2 \subseteq {}_{fix}\mathbb{H}_1$. □

Apresentamos a seguir um lema (encontrado em [11]) central nesta seção, o qual apresenta resultados que são necessários na demonstração do teorema principal da seção.

Lema 6.24. *Seja $\mathbb{L}|\mathbb{K}$ uma extensão finita, separável e simples que, por ser simples, $\exists \alpha \in \mathbb{L}$ tal que $\mathbb{L} = \mathbb{K}(\alpha)$. Se $H = \{\sigma_1, \ldots, \sigma_n\}$ é um subgrupo de $\Gamma(\mathbb{L}|\mathbb{K})$ e seja o polinômio $p(x) = (x - \sigma_1(\alpha)) \cdots (x - \sigma_n(\alpha))$. Então, $p(x) \in {}_{fix}\mathbb{H}[x]$ e $[\mathbb{L} : {}_{fix}\mathbb{H}] \leqslant |H|$.*

Demonstração.

$\forall \sigma \in H$, tomando $p^\sigma(x)$, nos moldes da Definição 6.8, temos,

$$p^\sigma(x) = (x - \sigma \circ \sigma_1(\alpha)) \cdots (x - \sigma \circ \sigma_n(\alpha)) = p(x). \tag{6.6}$$

Isso acontece porque $\{\sigma \circ \sigma_1, \ldots, \sigma \circ \sigma_n\} = \{\sigma_1, \ldots, \sigma_n\}$ para todo $\sigma \in H$ (isso pode ser verificado considerando que H é um grupo finito de automorfismos).

Escrevendo $p(x) = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n$, da Equação 6.6 e Definição 6.8, temos,

$$p(x) = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n = \sigma(a_0) + \sigma(a_1)x + \sigma(a_2)x^2 + \cdots + \sigma(a_n)x^n.$$

Ou seja, $\sigma(a_i) = a_i$, para todo $\sigma \in H$ e $0 \leqslant i \leqslant n$, então, $p(x) \in {}_{fix}\mathbb{H}[x]$.

Para a última afirmação, notemos que, utilizando a Proposição 6.22, temos

$$\mathbb{K} \subseteq {}_{fix}\mathbb{H} \subseteq \mathbb{L}.$$

Logo,

$$\mathbb{L} = \mathbb{K}(\alpha) \subseteq {}_{fix}\mathbb{H}(\alpha) \subseteq \mathbb{L}.$$

Assim, $\mathbb{L} = {}_{fix}\mathbb{H}(\alpha)$.

E, como $p(x) \in {}_{fix}\mathbb{H}[x]$ e $p(\alpha) = 0$, combinando a Proposição 5.7 com a Proposição 5.16, chegamos a

$$[\mathbb{L} : {}_{fix}\mathbb{H}] = [{}_{fix}\mathbb{H}(\alpha) : {}_{fix}\mathbb{H}] \leqslant \partial p(x) = |H|.$$

□

Vamos a mais um resultado auxiliar na busca de completarmos a demonstração do Teorema da Correspondência de Galois.

Lema 6.25. *Seja $\mathbb{L}|\mathbb{K}$ uma extensão finita e separável, $G = \Gamma(\mathbb{L}|\mathbb{K})$ e $\alpha \in \mathbb{L}$ tal que $\alpha \notin \mathbb{K}$. Se $\mathbb{L}|\mathbb{K}$ é de Galois, então $\exists \sigma \in G$ tal que $\sigma(\alpha) \neq \alpha$.*

Demonstração.

Por $\mathbb{L}|\mathbb{K}$ ser finita, é algébrica e, por $\alpha \in \mathbb{L}$, existe $m(x) = p_{min}(\alpha, \mathbb{K})$. Como $\alpha \notin \mathbb{K}$, temos que, $\partial m(x) \geqslant 2$.

Por $\mathbb{L}|\mathbb{K}$ ser separável e $\partial m(x) \geqslant 2$, garantimos a existência de $\beta \in \mathrm{Gal}(m(x), \mathbb{K})$, $\beta \neq \alpha$. Pela Proposição 6.11, $\mathbb{L}|\mathbb{K}$ é normal e, assim, $\beta \in \mathbb{L}$, uma vez que $\alpha \in \mathbb{L}$.

Pelos Lemas 6.9 e 6.10 (para auxiliar no entendimento da aplicação destes lemas considere o isomorfismo σ do Lema 6.9 como sendo $\sigma = \mathrm{Id}_{\mathbb{K}}$) existe um isomorfismo $\sigma : \mathbb{L} \longrightarrow \mathbb{L}$ tal que $\sigma(\alpha) = \beta$ e $\sigma|_{\mathbb{K}} = \mathrm{Id}_{\mathbb{K}}$. Sendo assim, $\sigma \in G$ e $\sigma(\alpha) = \beta \neq \alpha$, terminando a prova. □

Proposição 6.26. *Seja $\mathbb{L}|\mathbb{K}$ uma extensão finita e seperável e $G = \Gamma(\mathbb{L}|\mathbb{K})$. Então, $\mathbb{L}|\mathbb{K}$ é de Galois se, e somente se, $\mathbb{K} = {}_{fix}\mathbb{G}$.*

Demonstração.

$\Rightarrow$) Seja $\mathbb{L}|\mathbb{K}$ de Galois. É suficiente mostrarmos que $\mathbb{K} \subseteq {}_{fix}\mathbb{G}$ e ${}_{fix}\mathbb{G} \subseteq \mathbb{K}$.

Pela própria definição de Grupo de Galois, G fixa os elementos de $\mathbb{K}$, logo, $\mathbb{K} \subseteq {}_{fix}\mathbb{G}$.

Para provarmos que ${}_{fix}\mathbb{G} \subseteq \mathbb{K}$: suponhamos, por absurdo, que ${}_{fix}\mathbb{G} \nsubseteq \mathbb{K}$. Assim, $\exists \alpha \in {}_{fix}\mathbb{G}$, onde $\alpha \notin \mathbb{K}$. Isso significa que $\alpha \in \mathbb{L}\backslash\mathbb{K}$ e, pelo Lema 6.25, existe $\sigma \in G$ tal que $\sigma(\alpha) \neq \alpha$, ou seja, α não é preservado por σ, logo, $\alpha \notin {}_{fix}\mathbb{G}$, contrariando o que supomos no início e, assim, ${}_{fix}\mathbb{G} \subseteq \mathbb{K}$. Portanto, podemos concluir que $\mathbb{K} = {}_{fix}\mathbb{G}$.

$\Leftarrow$) Seja $\mathbb{K} = {}_{fix}\mathbb{G}$. Pela Proposição 6.19,

$$|G| = |\Gamma(\mathbb{L}|\mathbb{K})| \leqslant [\mathbb{L} : \mathbb{K}]. \tag{6.7}$$

Notemos que $[\mathbb{L} : \mathbb{K}] = [\mathbb{L} : {}_{fix}\mathbb{G}]$ e, pelo Lema 6.24,

$$[\mathbb{L} : \mathbb{K}] = [\mathbb{L} : {}_{fix}\mathbb{G}] \leqslant |G|. \tag{6.8}$$

Das Equações (6.7) e (6.8), $|G| = [\mathbb{L} : \mathbb{K}]$ que, pela Proposição 6.20, $\mathbb{L}|\mathbb{K}$ é de Galois. □

Proposição 6.27. *Seja $\mathbb{L}|\mathbb{K}$ uma extensão de Galois e $G = \Gamma(\mathbb{L}|\mathbb{K})$. Se H é um subgrupo de G, então $[\mathbb{L} : {}_{fix}\mathbb{H}] = |H|$ e $H = \Gamma(\mathbb{L}|_{fix}\mathbb{H})$.*

Demonstração.

Da cadeia de subgrupos $\{\mathrm{Id}_{\mathbb{L}}\} \subseteq H \subseteq G$, utilizando a Proposição 6.23, obtemos a cadeia de subcorpos ${}_{fix}\mathbb{G} \subseteq {}_{fix}\mathbb{H} \subseteq {}_{fix}\{\mathrm{Id}_{\mathbb{L}}\}$. Notemos que, trivialmente, ${}_{fix}\{\mathrm{Id}_{\mathbb{L}}\} = \mathbb{L}$ e, pela Proposição 6.26, como $\mathbb{L}|\mathbb{K}$ é de Galois, ${}_{fix}\mathbb{G} = \mathbb{K}$.

Por $\mathbb{L}|\mathbb{K}$ ser de Galois e, pela Proposição 6.13, temos que $\mathbb{L}|_{fix}\mathbb{H}$ é de Galois.

$\mathbb{L}|_{fix}\mathbb{H}$ sendo de Galois, pela Proposição 6.20,

$$[\mathbb{L} : {}_{fix}\mathbb{H}] = |\Gamma(\mathbb{L}|_{fix}\mathbb{H})|. \tag{6.9}$$

Agora, afirmamos que $H \subseteq \Gamma(\mathbb{L}|_{fix}\mathbb{H})$. De fato, tomando $\sigma \in H$, pela definição de ${}_{fix}\mathbb{H}$, para todo $\alpha \in {}_{fix}\mathbb{H}$, $\sigma(\alpha) = \alpha$, que equivale a dizer que,

$$\sigma|_{{}_{fix}\mathbb{H}} = \mathrm{Id}_{{}_{fix}\mathbb{H}}\,.$$

Ou seja, $\sigma \in \Gamma(\mathbb{L}|_{fix}\mathbb{H})$ (pois, por $H < G$, $\sigma \in \mathrm{Aut}\,\mathbb{L}$ e, como vimos, σ preserva ${}_{fix}\mathbb{H}$). E, como σ foi tomado arbitrário, $H \subseteq \Gamma(\mathbb{L}|_{fix}\mathbb{H})$.

Desta nossa afirmação, tiramos que $|H| \leqslant |\Gamma(\mathbb{L}|_{fix}\mathbb{H})|$.

Agrupamos, agora, algumas informações que nos permitirá concluir a demonstração:

Vimos que $|H| \leqslant |\Gamma(\mathbb{L}|_{fix}\mathbb{H})|$ e isso, pela Equação 6.9, significa que,

$$|H| \leqslant [\mathbb{L} : {}_{fix}\mathbb{H}]. \tag{6.10}$$

Só que, pelo Lema 6.24 (Observe que $\mathbb{L}|_{fix}\mathbb{H}$, por ser de Galois, satisfaz as condições do Teorema 5.19 e completa as hipóteses do Lema 6.24), então,

$$|H| \geqslant [\mathbb{L} : {}_{fix}\mathbb{H}]. \tag{6.11}$$

Assim, pelas Equações (6.10) e (6.11), $|H| = [\mathbb{L} : {}_{fix}\mathbb{H}]$ e, (como vimos acima que $H \subseteq \Gamma(\mathbb{L}|_{fix}\mathbb{H})$), temos $H = \Gamma(\mathbb{L}|_{fix}\mathbb{H})$. □

Proposição 6.28. *Sejam $\mathbb{K} \subseteq \mathbb{M} \subseteq \mathbb{L}$ corpos, com $\mathbb{L}|\mathbb{K}$ uma extensão de Galois e $G = \Gamma(\mathbb{L}|\mathbb{K})$. Então,*

A extensão $\mathbb{M}|\mathbb{K}$ é de Galois se, e somente se, $\Gamma(\mathbb{M}|\mathbb{K}) \lhd G$ e $\dfrac{G}{\Gamma(\mathbb{L}|\mathbb{M})} \simeq \Gamma(\mathbb{M}|\mathbb{K})$.

Demonstração.

$\Rightarrow$) Seja $\mathbb{M}|\mathbb{K}$ de Galois. Assim, $\mathbb{M}|\mathbb{K}$ é o corpo de decomposição de algum polinômio separável, logo, $[\mathbb{M} : \mathbb{K}] < \infty$ e, pelo Teorema 5.19, $\exists \alpha \in \mathbb{M}$ tal que $\mathbb{M} = \mathbb{K}(\alpha)$. Seja $m(x) = p_{min}(\alpha, \mathbb{K})$. Como $\mathbb{M}|\mathbb{K}$ ser de Galois implica ser Normal, então, todas as raízes de $m(x)$ estão em $\mathbb{M}$ (pela Definição 6.6, uma vez que $\alpha \in \mathbb{M}$).

Tomando $\sigma \in G$, pela Proposição 6.18, $\sigma(\alpha)$ é raiz de $m(x)$, então, pelo parágrafo anterior, $\sigma(\alpha) \in \mathbb{M}$.

Isto equivale a dizer que $\sigma(x) \in \mathbb{M}$ para todo $x \in \mathbb{M}$. De fato, como $\mathbb{M} = \mathbb{K}(\alpha)$ e σ preserva os elementos de $\mathbb{K}$ e $\sigma(\alpha)$ já vimos que pertence a $\mathbb{M}$, então, realmente, $\sigma(\mathbb{M}) \subseteq \mathbb{M}$.

Assim, podemos definir o seguinte homomorfismo:

$$\begin{array}{rccc} h: & G & \longrightarrow & \Gamma(\mathbb{M}|\mathbb{K}) \\ & \sigma & \longmapsto & \sigma|_{\mathbb{M}} \end{array}$$

(Alertamos que o desenvolvimento da demonstração fará uso do Teorema 2.30).

O núcleo de f, $\operatorname{Ker} f = \Gamma(\mathbb{L}|\mathbb{M})$, vejamos:

Pela Definição 2.28,

$$\sigma \in \operatorname{Ker} f \Leftrightarrow \sigma|_{\mathbb{M}} = \mathrm{Id}_{\mathbb{M}} \tag{6.12}$$

Só que $\sigma \in \operatorname{Aut}\mathbb{L}$ e como, pela Equação 6.12, se $\sigma \in \operatorname{Ker} f$ ele preserva os elementos de $\mathbb{M}$, $\sigma \in \Gamma(\mathbb{L}|\mathbb{M})$.

Lembramos que, pelo item (i) do Exemplo 2.29,

$$\Gamma(\mathbb{L}|\mathbb{M}) = \operatorname{Ker} f \lhd G.$$

Afirmamos que h é sobrejetiva. De fato, seja $\rho \in \Gamma(\mathbb{M}|\mathbb{K})$, de $\mathbb{M} = \mathbb{K}(\alpha)$ temos que, ρ é um isomorfismo de $\mathbb{K}(\alpha)$ que preserva $\mathbb{K}$, ou seja, $\rho : \mathbb{K}(\alpha) \longrightarrow \mathbb{K}(\alpha)$, com $\sigma|_{\mathbb{K}} = \mathrm{Id}_{\mathbb{K}}$.

Como $\mathbb{L}|\mathbb{K}$ é de Galois, pela Proposição 6.13, $\mathbb{L}|\mathbb{K}(\alpha)$ também é de Galois.

Por $\mathbb{L}|\mathbb{K}(\alpha)$ ser de Galois e pela Proposição 6.11, $\mathbb{L} = \operatorname{Gal}(p(x), \mathbb{K}(\alpha))$ de algum polinômio separável $p(x) \in \mathbb{K}(\alpha)$, logo, pelo Lema 6.10, existe um isomorfismo $\sigma : \mathbb{L} \longrightarrow \mathbb{L}$ tal que $\sigma|_{\mathbb{K}(\alpha)} = \rho$.

Agora, veja o que temos:

$\sigma \in \operatorname{Aut}\mathbb{L}$, $\sigma|_{\mathbb{K}(\alpha)=\mathbb{M}} = \rho$ e $\rho|_{\mathbb{K}} = \mathrm{Id}_{\mathbb{K}}$, ou seja, σ é um automorfismo de $\mathbb{L}$ que preserva $\mathbb{K}$, que equivale a $\sigma \in G$, e $h(\sigma) = \rho$, provando a sobrejetividade de h.

Neste momento, percebam a aplicabilidade do Teorema 2.30, mostrando que,

$$\frac{G}{\Gamma(\mathbb{L}|\mathbb{M})} \simeq \Gamma(\mathbb{M}|\mathbb{K}).$$

$\Leftarrow$) Seja $\Gamma(\mathbb{M}|\mathbb{K}) \lhd G$ e $\dfrac{G}{\Gamma(\mathbb{L}|\mathbb{M})} \simeq \Gamma(\mathbb{M}|\mathbb{K})$. Suponhamos, por absurdo, que $\mathbb{M}|\mathbb{K}$ não seja de Galois. Assim, $\mathbb{M}|\mathbb{K}$ não é normal.

Vimos que $\mathbb{M} = \mathbb{K}(\alpha)$. Seja $m(x) = p_{min}(\alpha, \mathbb{K})$, como $\mathbb{M}|\mathbb{K}$ não é normal, garantimos a existência de β raiz de $m(x)$ tal que $\beta \notin \mathbb{M}$.

Já $\mathbb{L}|\mathbb{K}$ é normal. E, como $\alpha \in \mathbb{M}$ e $\mathbb{M} \subseteq \mathbb{L}$, $\alpha \in \mathbb{L}$, ou seja, como uma raiz de $m(x)$ está em $\mathbb{L}$ todas estão, em particular, β. Com isso, pelos Lemas 6.9 e 6.10, $\exists \sigma \in G$ tal que $\sigma(\alpha) = \beta$.

Como $\beta \in \mathbb{L}$ e $\beta \notin \mathbb{M}$, pelo Lema 6.25, $\exists \rho \in \Gamma(\mathbb{L}|\mathbb{M})$ tal que $\rho(\beta) \neq \beta$.

Agora, vamos utilizar o resultado da Definição 2.15 para verificar a normalidade de $\Gamma(\mathbb{L}|\mathbb{M})$:

Já temos, que $\sigma, \rho \in \Gamma(\mathbb{L}|\mathbb{M})$, como $\Gamma(\mathbb{L}|\mathbb{M})$ é um grupo, temos a garantia da existência de inversos, daí $\sigma^{-1} \in \Gamma(\mathbb{L}|\mathbb{M})$, também. Dito isto,

$$(\sigma^{-1} \circ \rho \circ \sigma)(\alpha) = \sigma^{-1} \circ \rho(\sigma(\alpha)) = \sigma^{-1}(\rho(\beta)) \neq \sigma^{-1}(\beta) = \alpha$$

Assim, $(\sigma^{-1} \circ \rho \circ \sigma)$ não preserva α e, portanto, $(\sigma^{-1} \circ \rho \circ \sigma)|_{\mathbb{M}} \neq \mathrm{Id}_{\mathbb{M}}$, logo,

$$(\sigma^{-1} \circ \rho \circ \sigma) \notin \Gamma(\mathbb{L}|\mathbb{M}).$$

Este último resultado, contraria a hipótese de que $\Gamma(\mathbb{M}|\mathbb{K})$ é um subgrupo normal de G, um absurdo, portanto, $\mathbb{M}|\mathbb{K}$ é de Galois. □

Estes resultados que apresentamos culminam com uma correspondência, entre corpos intermediários de uma extensão $\mathbb{L}|\mathbb{K}$ e subgrupos do $\Gamma(\mathbb{L}|\mathbb{K})$, a esta correspondência damos o nome de "Correspondência de Galois".

Teorema 6.29. *(Teorema da Correspondência de Galois) Sejam $\mathbb{L}|\mathbb{K}$ uma Extensão Galoisiana e $G = \Gamma(\mathbb{L}|\mathbb{K})$. Então:*

1 - $|G| = [\mathbb{L} : \mathbb{K}]$*;*

2 - Seja um corpo intermediario $\mathbb{M}$. A extensão $\mathbb{M}|\mathbb{K}$ é de Galois se, e somente se, $\Gamma(\mathbb{M}|\mathbb{K}) \lhd G$ *e* $\dfrac{G}{\Gamma(\mathbb{L}|\mathbb{M})} \simeq \Gamma(\mathbb{M}|\mathbb{K})$*;*

3 - Dado um corpo intermediário $\mathbb{M}$, temos:

$$[\mathbb{L} : \mathbb{M}] = |\Gamma(\mathbb{L}|\mathbb{M})|$$

e

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

Demonstração.

1. Feita na Proposição 6.20.

2. Feita na Proposição 6.28.

3. Pela Proposição 6.13, a extensão $\mathbb{L}|\mathbb{M}$ é de Galois e, pelo item 1 acima

$$[\mathbb{L} : \mathbb{M}] = |\Gamma(\mathbb{L}|\mathbb{M})|.$$

Pelo Teorema da Torre 5.11,

$$|G| = [\mathbb{L} : \mathbb{K}] = [\mathbb{L} : \mathbb{M}] \cdot [\mathbb{M} : \mathbb{K}].$$

Portanto,

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

□

6.5 Extensões Ciclotômicas

Definição 6.30. Seja $\mathbb{K}$ um subcorpo dos complexos. Chamamos de extensão ciclotômica uma extensão $\mathbb{K}(\zeta)|\mathbb{K}$, onde $\zeta^n = 1$ para algum $n \in \mathbb{N}$.

Lema 6.31. *Seja $U_n = \{1, \zeta, \zeta^2, \ldots, \zeta^{n-1}\}$ o grupo das raízes n-ésimas da unidade. Todo homomorfismo de U_n em U_n é dado por:*

$$\begin{array}{rccc} a^* : & U_n & \longrightarrow & U_n \\ & \gamma & \longmapsto & \gamma^a, \end{array}$$

onde $a \in \mathbb{Z}$.

Demonstração. Seja σ um homomorfismo de U_n em U_n, e ζ uma raiz primitiva n-ésima da unidade. Tomemos $x \in U_n$, então $x = \zeta^k$, para algum $k \in \mathbb{Z}$. Das propriedades de homomorfismo:

$$\sigma(x) = \sigma(\zeta^k) = (\sigma(\zeta))^k$$

Seja $\sigma(\zeta) = \beta \in U_n$. Assim, $\beta = \zeta^a$, para algum $a \in \mathbb{Z}$. Portanto,

$$\sigma(x) = (\sigma(\zeta))^k = \beta^k = (\zeta^a)^k = (\zeta^k)^a = x^a$$

Como tomamos x arbitrário, o resultado é válido para todo $x \in U_n$. □

Lema 6.32. *Seja $U_n = \{1, \zeta, \zeta^2, \ldots, \zeta^{n-1}\}$ o grupo das raízes n-ésimas da unidade e $a \in \mathbb{Z}$. A aplicação:*

$$\begin{array}{rccc} a^* : & U_n & \longrightarrow & U_n \\ & \gamma & \longmapsto & \gamma^a \end{array}$$

é um automorfismo se, e somente se, $\text{mdc}\,(a, n) = 1$.

Demonstração.

A aplicação a^* é um homomorfismo. De fato,

Sejam $x, y \in U_n$,

$$a^*(x \cdot y) = (x \cdot y)^a = x^a \cdot y^a = a^*(x)b^*(y)$$

Portanto, $a^*(x \cdot y) = a^*(x)b^*(y)$.

$\Rightarrow$)

Seja a^* automorfismo. Suponha por absurdo que $\text{mdc}\,(a, n) = d \neq 1$.

Como a^* é automorfismo, a^* é homomorfismo, então $a^*(1) = 1$.

De $\text{mdc}\,(a, n) = d$, tiramos que, $a = a'd$ e $n = n'd$ para alguns $a', n' \in \mathbb{Z}$. Onde, $n' < n$, pois $d \neq 1$.

Agora, seja ζ uma raiz n-ésima primitiva da unidade. Tomemos $x = \zeta^{n'} \in U_n$. Notemos que $\zeta^{n'} \neq 1$, pelo fato de $n' < n$ e ζ ser uma n-ésima primitiva da unidade.

Dito isto,

$$a^*(x) = a^*(\zeta^{n'}) = (\zeta^{n'})^a = (\zeta^{n'})^{a'd} = \zeta^{n'a'd} = \zeta^{(n'd)a'} = \zeta^{(n)a'} = (\zeta^n)^{a'} = 1^{a'} = 1$$

Descobrimos que $a^*(1) = 1$ e $a^*(x) = 1$ com $1 \neq x$, o que nos permite constatar que a^* não é injetiva, contrariando a hipótese de a^* é automorfismo. E assim $\text{mdc}\,(a, n) = 1$.

$\Leftarrow$)

Tomemos $a \in \mathbb{Z}$ tal que $\text{mdc}\,(a, n) = 1$. Já vimos no início da demonstração que a^* é um homomorfismo, e assim, é um homomorfismo entre conjuntos finitos. Portanto, é suficiente mostrarmos que $a*$ é sobrejetiva que concluirmos que é um automorfismo.

Seja ζ uma raiz n-ésima primitiva da unidade. Pela Proposição 3.3, ζ^a também é uma raiz primitiva n-ésima da unidade.

Tomemos $y \in U_n$, ou seja, $y = (\zeta^a)^k$ para algum $1 \leqslant k \leqslant n$. Assim,

$$y = (\zeta^a)^k = \zeta^{ak} = (\zeta^k)^a$$

Portanto, existe $\zeta^k \in U_n$ tal que $a^*(\zeta^k) = y$, o que demonstra que a^* é sobrejetiva e termina a prova. □

Lema 6.33. *A ordem do grupo* $\text{Aut}\, U_n$ *é* $\varphi(n)$.

Demonstração. Pela própria definição de automorfismo, todo automorfismo é homomorfismo. Pelo Lema 6.31, todo homomorfismo de U_n é dado por a^* da forma que apresentamos. Pelo Lema 6.32, a aplicação a^* é automorfismo se, e somente se, $\text{mdc}\,(a, n) = 1$. Pela Definição 1.6, $|\,\text{Aut}\, U_n| = \varphi(n)$. □

Proposição 6.34. *Seja uma extensão* $\mathbb{Q}(\zeta)|\mathbb{Q}$. *Então,* $\Gamma(\mathbb{Q}(\zeta)|\mathbb{Q})$ *é abeliano e, além disso,* $|\Gamma(\mathbb{Q}(\zeta)|\mathbb{Q})|$ *divide* $\varphi(n)$.

Demonstração. Basta mostrarmos que $\Gamma(\mathbb{Q}(\zeta_n)|\mathbb{Q})$, que vamos denotar simplesmente por Γ, é isomorfo à um subgrupo de $\mathbb{Z}_n^*$, pois, $\mathbb{Z}_n^*$ é abeliano e tem ordem $\varphi(n)$ e, pelo Teorema de Lagrange 2.14, qualquer subgrupo seu, deve dividir sua ordem, ou seja, $|\Gamma(\mathbb{Q}(\zeta)|\mathbb{Q})|$ deve dividir $|\mathbb{Z}_n^*|$.

Seja $\phi_n = p_{min}(\zeta, \mathbb{Q})$ o polinômio minimal de ζ sobre $\mathbb{Q}$. Pela Proposição 6.18, cada $\sigma \in \Gamma(\mathbb{Q}(\zeta)|\mathbb{Q})$ leva uma raiz de ϕ em outra, ou seja, permuta suas raízes. Assim, σ restrito ao grupo dos automorfismos de U_n (grupo dos automorfismos das raízes n-ésimas da unidade) é um automorfismo deste grupo. E assim, temos um homomorfismo injetivo dado por:

$$\begin{array}{rccc} f: & \Gamma & \longrightarrow & S_n \\ & \sigma & \longmapsto & \sigma|_{\text{Aut}\, U_n} \end{array}$$

Onde S_n é o grupo de todas as permutações dos elementos de U_n.

Só que o grupo $\text{Aut}\, U_n$ é isomorfo a $\mathbb{Z}_n^*$. De fato, tomemos a aplicação g dada por:

$$\begin{array}{rccc} g: & \mathbb{Z}_n^* & \longrightarrow & \text{Aut}\, U_n \\ & a & \longmapsto & a^* \end{array}$$

Onde a^* é um automorfismo de $\text{Aut}\, U_n$ definido como no Lema 6.32. Temos que, g é um isomorfismo, vejamos:

g é homomorfismo, de fato,

Seja $a, b \in \mathbb{Z}_n^*$, temos que $g(a \cdot b) = (a \cdot b)^*$. Agora tomando um $\alpha \in U_n$,

$$(a \cdot b)^*(\alpha) = \alpha^{a \cdot b} = \alpha^{b \cdot a} = (\alpha^b)^a = b^*(\alpha^a) = (a^* \circ b^*)(\alpha)) = a^*(\alpha) \circ b^*(\alpha)$$

Assim, $(a \cdot b)^* = (a^* \circ b^*)$, ou seja, $g(a \cdot b) = g(a) \circ g(b)$.

Pelo Lema 6.33, $|\operatorname{Aut} U_n| = \varphi(n)|$. E como a ordem de $\mathbb{Z}_n^*$ também é $\varphi(n)$, g é um homomorfismo entre conjuntos de mesma ordem. Bastando, mostrar a injetividade de g para concluir que a aplicação é um isomorfismo.

Pelo item (iii) do Exemplo 2.29, g é injetivo se, e somente se, $\operatorname{Ker} g = 1$.

Pela Definição 2.28, $\operatorname{Ker} g = \{a \in \mathbb{Z}; g(a) = \mathrm{Id}_{\operatorname{Aut} U_n}\}$, onde $\mathrm{Id}_{\operatorname{Aut} U_n}$ é o automorfismo identidade de U_n.

Seja $a \in \mathbb{Z}_n^*$, onde $a \in \operatorname{Ker} g$, tomemos ζ uma raiz n-ésima primitiva da unidade.

$g(a) = a^* = \mathrm{Id}_{\operatorname{Aut} U_n}$ assim,

$$g(a)(\zeta) = a^*(\zeta) = \mathrm{Id}_{\operatorname{Aut} U_n}(\zeta) = \zeta$$

Portanto, $a^*(\zeta) = \zeta$ e, pela definição de a^*, $\zeta^a = \zeta$. Dividindo ambos os lados desta última igualdade por ζ, obtemos $\zeta^{a-1} = 1$.

Pela Proposição 3.2, $n|a-1$. Lembremos que $1 \leqslant a \leqslant n-1$, pois, $a \in \mathbb{Z}_n^*$. E, assim $a - 1 = 0$, concluindo que $a = 1$, logo, g é injetiva e mostramos o isomorfismo.

Utilizando a Proposição 2.27, ao fazermos a composição de funções $g \circ f$, obtemos que $g \circ f$ é um homomorfismo injetivo de Γ para $\mathbb{Z}_n^*$, terminando a prova. □

Lema 6.35. *Seja p um número primo e $q(x)$ um polinômio. Então,*

$$[q(x)]^p \equiv q(x^p) \mod p$$

Demonstração.

Faremos por indução em n.

Para $n = 0$: $q(x) = a_0$. Logo, pelo Pequeno Teorema de Fermat 1.5,

$$q(x)^p \equiv a_0^p \equiv a_0 \equiv q(x^p) \mod p$$

Suponha que o resultado seja válido para todo polinômio de grau $n \leqslant k$, para algum $k \geqslant 0$. Seja $q(x) = a_{k+1}x^{k+1} + f(x)$, onde $\partial f(x) \leqslant k$.

Assim, $q(x)^p = (a_{k+1}x^{k+1} + f(x))^p$, pela Proposição 1.3, temos

$$[a_{k+1}x^{k+1} + f(x)]^p =$$

$$a_{k+1}^p x^{k+1p} + \binom{p}{1} a_{k+1}^{(p-1)} x^{k+1(p-1)} [f(x)]^1 + \binom{p}{2} a_{k+1}^{(p-2)} x^{k+1(p-2)} [f(x)]^2 + \cdots$$

$$\cdots + \binom{p}{p-1} a_{k+1}x^{k+1}[f(x)]^{p-1} + [f(x)]^p$$

Pelo Lema 1.4,

$$[a_{k+1}x^{k+1} + f(x)]^p \equiv a_{k+1}^p x^{k+1p} + [f(x)]^p \mod p$$

Por hipótese de indução $(f(x))^p \equiv f(x^p)$ e pelo Pequeno Teorema de Fermat 1.5,

$$a_{k+1}^p x^{k+1p} + [f(x)]^p \equiv a_{k+1}(x^p)^{k+1} f(x^p) \equiv q(x^p) \mod p$$

Portanto, o resultado é válido para $n = k + 1$.

□

Lema 6.36. *Sejam o polinômio $q(x) = x^n - 1 \in \mathbb{Z}[x]$ e p um primo tal que $p \nmid n$, então $\overline{q(x)} = \overline{x^n - 1}$ é separavél em $\mathbb{Z}_p[x]$.*

Demonstração. Seja $\overline{q(x)} = \overline{x^n - 1} = \overline{x^n} - \overline{1}$. A derivada de $\overline{q(x)}$ é $\overline{q'(x)} = \overline{n}x^{n-1}$. Como $p \nmid n$, $\overline{q'(x)}$ não é $\overline{0}$, assim, o único fator que divide $\overline{q'(x)}$ é x, e sabemos que x não divide $\overline{q(x)}$. Então, $\overline{q(x)}$ e $\overline{q'(x)}$ não têm fator comum. Pela Proposição 6.4, temos o resultado desejado. □

Teorema 6.37. *Se ζ é uma raiz n-ésima primitiva da unidade em $\mathbb{C}$, então,*

$$[\mathbb{Q}(\zeta) : \mathbb{Q}] = \varphi(n)$$

Demonstração.

Inicialmente, tomemos um p primo tal que $p \nmid n$.

Tomemos $m(x) = p_{min}(\zeta, \mathbb{Q})$ e $q(x) = p_{min}(\zeta^p, \mathbb{Q})$. Queremos mostrar que $m(x) = q(x)$. Suponha $m(x) \neq q(x)$. Da Proposição 5.7, temos que $m(x)|x^n - 1$ e $q(x)|x^n - 1$, e como $m(x)$ e $q(x)$ são distintos, $x^n - 1 = m(x)q(x)f(x)$ para algum $f(x) \in \mathbb{Q}[x]$. Do Lema 4.22, $m(x), q(x), f(x) \in \mathbb{Z}[x]$.

Notemos que ζ é raiz de $q(x^p) = 0$, logo, pela Proposição 5.7, $m(x)|q(x^p)$ e, assim, $q(x^p) = m(x)h(x)$ para algum $h(x) \in \mathbb{Q}[x]$ que, novamente, pelo Lema 4.22, $h(x) \in \mathbb{Z}[x]$.

Pelo Lema 6.35, temos que $\overline{m(x)} \cdot \overline{h(x)} = \overline{q(x^p)} = \overline{q(x)}^p$. Com isso, $\overline{m(x)}$ tem um fator irredutível que divide $\overline{q(x)}$, ou seja, eles tem um fator comum e como $\overline{x^n - 1} = \overline{m(x)} \cdot \overline{q(x)} \cdot \overline{f(x)}$, temos que $\overline{x^n - 1}$ têm raízes múltiplas, o que o torna inseparável, contrariando o Lema 6.36. Assim, $m(x) = q(x)$.

Agora, generalizando, se tomarmos um s não necessariamente primo, mas ainda com $\text{mdc}(s, n) = 1$, temos que $s = r_1 r_2 \dots r_t$ onde $r_1 r_2 \dots r_t$ são primos, não necessariamente distintos, $r_i \nmid n$ para todo $1 \leqslant i \leqslant t$. Com isso, aplicando recursivamente o resultado acima aos números $\zeta, \zeta^{r_1}, \zeta^{r_1 r_2}, \dots, \zeta^{r_1 r_2 \cdots r_t}$ obtemos que o resultado é válido, também, para s. Desta forma, pela Definição 1.6 (Função Phi de Euler), já conseguimos determinar $\varphi(n)$ raízes distintas para $m(x)$. Ou seja, $\partial m(x) \geqslant \varphi(n)$.

Sendo assim, pela Proposição 5.16, $\partial m(x) = [\mathbb{Q}(\zeta) : \mathbb{Q}] \geqslant \varphi(n)$.

Já, pela Proposição 6.34, $[\mathbb{Q}(\zeta) : \mathbb{Q}] \leqslant \varphi(n)$.

Portanto, $[\mathbb{Q}(\zeta) : \mathbb{Q}] = \varphi(n)$. □

6.5.1 Polinômio Ciclotômico

Falamos mais sobre esta classe especial de polinômios: os Polinômios Ciclotômicos.

Definição 6.38. (Polinômios ciclotômicos) Seja $n \in \mathbb{N}$ e ζ uma raiz n-ésima primitiva da unidade. Chamamos de n-ésimo polinômo ciclotômico o polinômio dado por

$$\phi_n(x) = p_{min}(\zeta, \mathbb{Q}).$$

Observe que, em virtude, do Teorema 6.37,

$$\phi_n(x) = \prod_{a=1,(mdc(a,n)=1)}^{n} (x - \zeta^a).$$

Proposição 6.39. *Para todo inteiro positivo n,*

$$x^n - 1 = \prod_{d|n} \phi_d(x).$$

Demonstração. Seja ζ uma raiz n-ésima da unidade. Pela Proposição 3.5, ζ será raiz d-ésima da unidade se, e somente se, $d|n$.

Isto significa que $\phi_d(x)$ divide $x^n - 1$ para todo d divisor de n. Ou seja,

$$x^n - 1 = \prod_{d|n} \phi_d(x).$$

Concluindo a demonstração. □

Na Proposição 6.39, se $n = p$ primo, temos

$$x^p - 1 = \phi_p(x) \cdot \phi_1(x)$$

e, como $\phi_1(x) = x - \zeta_1^1 = x - 1$, concluímos que

$$\phi_p(x) = \frac{x^p - 1}{\phi_1(x)} = \frac{x^p - 1}{x - 1} = x^{p-1} + x^{p-2} + \cdots + x + 1. \tag{6.13}$$

A última igualdade é fruto da Proposição 1.2.

Capítulo 7

A Construbilidade no Plano Complexo

Desde tempos remotos que os problemas de construção usando régua não graduada e compasso intrigam os matemáticos. Observamos aqui que, utilizaremos sempre o termo "régua" para denotar "régua não graduada". Construções como as que serão vistas no Capítulo 9 reforçaram a dedicação na busca por respostas para questões de construtibilidade ou não de determinados objetos geométricos.

O problema de descobrir quais polígonos regulares são construtíveis por régua não graduada e compasso suscita naturalmente a dúvida de como isso pode ser respondido, ou seja, quais instrumentos, quais teorias da Matemática devem ser utilizadas para a apresentação de um resultado nítido. Concomitante a isso, surge a expectativa de que essa resposta apresente uma abstração, (em virtude de ser uma questão de "possibilidade geométrica"), que não deixe os resultados evidentes. Porém, ao mesmo tempo, há uma confiança na objetividade da Matemática e de que as relações entre os instrumentos e teorias da mesma possam explanar uma resposta consistente, convincente e que, apesar da abstração necessária, deixe nítida a validade real dos resultados.

Uma resposta com essas características foi feita por Johann Carl Friedrich Gauss, surpreendemente aos 19 anos, em 1796, veja [6]. Apresentaremos o teorema que responde essa perguntra no Capítulo 8. Uma análise da teoria que envolve esse feito nos permitirá um entendimento amplo e um reconhecimento da magnitude dos resultados obtidos com a Teoria de Galois.

7.1 Retas e Circunferências

Na Seção 7.7 utilizaremos equações de retas e circunferências com coeficientes nos complexos. Preparando-se para esse encontro, expomos aqui, a descrição de tais objetos geométricos.

Voltemos a utilizar noções do estudo de vetores. Sabemos que uma reta é determinada por dois pontos. Seja r a reta determinada pelos pontos a e b. Três pontos a, b e c são colineares se o ângulo formado entre $b-a$ e $c-a$ for 0 ou π, ou seja, o $\text{Arg}\left(\dfrac{c-a}{b-a}\right)$ for

igual a 0 ou π, que equivale a $\dfrac{c-a}{b-a} \in \mathbb{R}$.

Do paragrafo anterior, tiramos que um ponto x vai pertencer a r se

$$\frac{x-a}{b-a} \in \mathbb{R}$$

Pelo item (i) da Proposição 3.6,

$$\frac{x-a}{b-a} = \overline{\left(\frac{x-a}{b-a}\right)}$$

e dos itens (iv) e (ii) da Proposição 3.6, chegamos à

$$\frac{x-a}{b-a} = \frac{\overline{x}-\overline{a}}{\overline{b}-\overline{a}}$$

Finalmente, temos como equação da reta r:

$$r : (x-a)\frac{(\overline{b}-\overline{a})}{(b-a)} - (\overline{x}-\overline{a}) = 0 \tag{7.1}$$

Sabemos que uma circunferência é determinada pelos seus centro e raio. Seja c a circunferência determinada pelo centro a e raio r. Temos que um ponto x vai pertencer a c se $|x-c| = r$, elevando ambos os lados ao quadrado obtemos $|x-c|^2 = r^2$. Sabemos que o quadrado do módulo de um número complexo é igual ao produto dele pelo seu conjugado, o que resulta em $(x-c)\cdot\overline{(x-c)} = r^2$. Que, novamente das operações com conjugado, chegamos à equação da circunferência c:

$$c : (x-c)\cdot(\overline{x}-\overline{c}) - r^2 = 0 \tag{7.2}$$

Reforçamos a importância do conhecimento de alguns conceitos relacionados à "operações entre vetores" para um melhor entendimento dos resultados tratados aqui. Em particular, notemos que a reta r descrita pela Equação 7.1 acima, pode ser reescrita como:

$$r = \{a + (b-a)t; t \in \mathbb{R}\}$$

De fato, se $x \in r$, então x é tal que,

$$\begin{aligned} x &= a + (b-a)t \\ x - a &= (b-a)t \end{aligned}$$

Como os pontos a e b foram tomados distintos, $b - a \neq 0$ e, podemos fazer,

$$\frac{x-a}{b-a} = t$$

onde $t \in \mathbb{R}$. Agora, do item (i) da Proposição 3.6, obtemos o resultado da Equação (7.1).

Proposição 7.1. *Sejam duas retas não-paralelas r e s dadas por:*

$$r = u_1 + (v_1 - u_1)g$$

$$s = u_2 + (v_2 - u_2)h$$

Onde $g, h \in \mathbb{R}$ e u_1, v_1, u_2, v_2 são pontos do plano complexo. Então, $v_2 - u_2 \neq t(v_1 - u_1)$ para todo $t \in \mathbb{R}$.

Demonstração. Por absurdo, supondo que existe algum $t' \in \mathbb{R}$, tal que

$$v_2 - u_2 = (v_1 - u_1)t'$$

Assim,

$$s = u_2 + (v_2 - u_2)h = u_2 + (v_1 - u_1)t'h$$

Note que $t'h \in \mathbb{R}$, logo s é uma reta determinada pelo mesmo vetor, $(v_1 - u_1)$, que determina r, indicando que r e s são paralelas, um absurdo, pois, por hipótese r e s são não-paralelas. □

Corolário 7.2. *Dadas duas retas não-paralelas r e s, sendo r determinada pelos pontos a e b e s determinada pelos pontos c e d. Então, temos:*

$$\left(\frac{(\overline{b} - \overline{a})}{(b-a)} - \frac{(\overline{d} - \overline{c})}{(d-c)}\right) \neq 0.$$

Demonstração.

As retas r e s são dadas pelas equações:

$$r : (x-a)\frac{(\overline{b} - \overline{a})}{(b-a)} - (\overline{x} - \overline{a}) = 0$$
$$s : (x-c)\frac{(\overline{d} - \overline{c})}{(d-c)} - (\overline{x} - \overline{c}) = 0$$

Supondo, por absurdo,

$$\left(\frac{(\overline{b} - \overline{a})}{(b-a)} - \frac{(\overline{d} - \overline{c})}{(d-c)}\right) = 0$$

Então,

$$\frac{(\overline{b} - \overline{a})}{(b-a)} = \frac{(\overline{d} - \overline{c})}{(d-c)}$$

Que resulta,

$$\frac{(d-c)}{(b-a)} = \frac{(\overline{d} - \overline{c})}{(\overline{b} - \overline{a})}$$

Esta última igualdade significa, pelo item (i) da Proposição 3.6, que $\dfrac{(d-c)}{(b-a)} = t \in \mathbb{R}$, o que contraria a proposição anterior, e termina a prova. □

7.2 Números Complexos Construtíveis

Iniciamos fazendo uma explanação das regras que regem as construções com régua e compasso. Esta régua é uma régua não-graduada. Segundo [6], nos Postulados de Euclides, essas construções seguem as seguintes regras: com a régua podemos construir uma reta passando por dois pontos dados; com o compasso podemos construir uma circunferência com centro e um de seus pontos dados, chamemos de "compasso fixo". Nos usos

mais modernos das construções com régua e compasso temos construções de circunferências com centro em um ponto dado e raio definido pela distância entre dois pontos dados, onde um destes não necessariamente é o centro. Nesse segundo uso o compasso pode "transportar" distâncias. Chamemos este de "compasso móvel". Essas aparentes diferenças são excluídas quando mostra-se que esse transporte de distâncias é possível de ser feito também com o compasso fixo, faremos isso no exemplo a seguir.

Exemplo 7.3. Acompanhando na Figura 7.1, a seguir, queremos construir uma circunferência de centro A e raio igual a distância de B para C. Com o compasso das regras mais atuais isso é permitido de imediato. Provaremos que isso é também possível com o compasso fixo.

De posse do compasso fixo, construímos uma circunferência de centro A passando por C, e outra de centro C passando por A. Essas circunferências se intersectam nos pontos D e E da figura. Agora construimos mais duas circunferências de centro D e E passando por B. Essas novas duas circunferências se intersectam em B, naturalmente, e no ponto F da figura. Finalmente, a circunferência que queremos é a centrada em A passando por F.

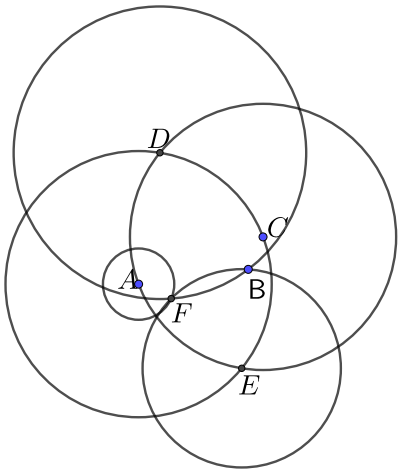

Figura 7.1: Equivalência entre compassos

Diante deste exemplo, acaba por torna-se semelhante utilizarmos o que chamamos de "compasso fixo" ou "compasso móvel". Semelhante no sentido que todas as construções possíveis com um são possível com outro. Optamos aqui para o uso do "compasso móvel".

A partir daí, como já mencionado, surge questionamentos sobre quais objetos geométricos podem ser construídos utilizando esses instrumentos. Ou seja, utilizando régua e compasso, para construir retas e circunferências, obtendo com isso pontos de intercessão que posteriormente poderão ser utilizados em conjunto com os já existentes para a construção de novas retas e circunferências e possíveis novos pontos de intercessão e assim sucessivamente.

Dado um segmento que define a aresta de um cubo, podemos construir um outro segmento que define a aresta de um cubo com o dobro do volume do cubo anterior? Dado um ângulo podemos construir um outro medido $\frac{1}{3}$ de sua medida? Podemos construir um quadrado com área igual a de uma circunferência dada? Esses são os conhecidos três problemas gregos clássicos, que estão entre as perguntas que podem ser feitas sobre a questão da construtibilidade com régua e compasso. Responderemos elas no Capítulo 9.

Outro problema, que inclusive é o foco principal neste trabalho, é o de dividir uma circunferência em $n \in \mathbb{N}$ partes iguais ou, equivalentemente, construir um n-ágono regular, veja na Figura Ilustrativa 7.2, que realmente são equivalentes esses problemas. Para quais n isso é possível? e por quê? Debruçaremos-nos sobre essas questões fazendo um destrinchamento das teorias envolvidas nas suas respostas.

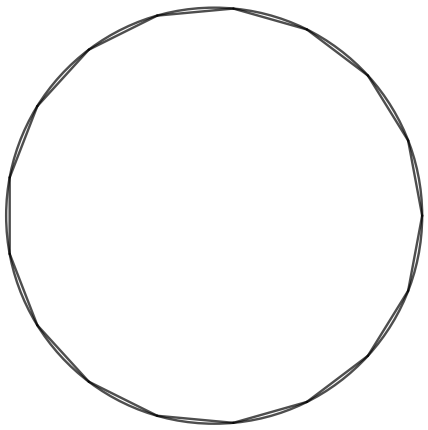

Figura 7.2: Heptadecágono regular inscrito em circunferência

Agora que vimos como se dão as construções com régua e compasso, apresentamos algumas definições iniciais que levam em consideração as possibilidades e limitações desses processos de construção.

Reescrevemos as duas regras que devem ser seguidas nas construções com régua e compasso, na forma de definições.

Nas definições que seguem percebemos a necessidade da preexistência de pelo menos dois pontos. Diante disso, até por unidade de medida, consideramos os pontos $(0,0)$ e $(1,0)$, ou seja, os números complexos 0 e 1 como pilar de nossas construções.

Definição 7.4. (Reta Construtível) Dado um subconjunto A com pelo menos dois pontos, podemos traçar uma reta passando por dois pontos de A. Diremos que essa reta é construtível.

Exemplo 7.5. A reta determinada pelos pontos 0 e 1 (a reta real) é construtível.

Definição 7.6. (Circunferência Construtível) Dado um subconjunto A com pelo menos

dois pontos, podemos traçar uma circunferência com centro em um ponto de A e com raio igual a distancia entre dois pontos de A. Diremos que essa circunferência é construtível.

Chamemos de $\mathcal{RC}(A)$ ao conjunto de todas as retas e circunferências construtíveis a partir de pontos de A, nos moldes das duas definições anteriores.

Para continuarmos a análise do processo de construção com régua e compasso, faremos a seguinte definição:

Definição 7.7. Definimos como "operações elementares com régua e compasso" as três operações abaixo:

- ⋆ Intercessão entre duas retas construtíveis;
- ⋆ Intercessão entre uma reta e uma circunferência construtíveis;
- ⋆ Intercessão entre duas circunferências construtíveis.

Usaremos neste momento um termo utilizado por [5] para definir pontos obtidos a partir de uma das três operações elementares no conjunto A.

Definição 7.8. (Ponto Simplesmente Construtível) Um ponto será dito simplesmente construtível a partir de um subconjunto A, se ele pertencer ao conjunto de todos os pontos de intercessão dos elementos do conjunto $\mathcal{RC}(A)$.

Seja A um conjunto de pontos do plano complexo. Denotaremos por $c_1(A)$, o conjunto de todos os pontos simplesmente construtíveis a partir de A. Note que, trivialmente, temos $A \subset c_1(A)$. Recursivamente, denotaremos por $c_{n+1}(A)$ o conjunto de todos os pontos construtíveis a partir de $c_n(A)$. Por conveniência, denotaremos por $c_0(A)$ o próprio A e $c_\infty(A) = \bigcup_{n\in\mathbb{N}} c_n(A)$. Então, temos a seguinte cadeia:

$$A = c_0(A) \subset c_1(A) \subset c_2(A) \subset \cdots \subset c_\infty(A) \tag{7.3}$$

O conjunto $c_\infty(A)$ é o conjunto de todos os pontos construtíveis a partir de A.

Generalizando esses resultados, podemos dizer que um objeto geométrico (ponto, segmento, polígono, etc.) é dito "construtível" se ele for obtido por um processo finito de *operações elementares* (que são as operações apresentadas na Definição 7.7) a partir de um conjunto com pelo menos dois pontos.

Vimos, na Subseção 3.1.1, uma evidente associação entre os números complexos e pontos do plano $\mathbb{R}^2$. Diante disso, poderemos falar em pontos ou números construtíveis indistintamente.

Definição 7.9. (Número Construtível) Seja o conjunto $A = \{0, 1\}$. Diremos que um número é construtível se ele pertencer a algum dos conjuntos $c_n(A)$ da cadeia 7.3. Denotaremos por $\mathbb{C}_c$ o conjunto $c_\infty(\{0, 1\})$ que é o conjunto de todos os números construtíveis a partir do conjunto $\{0, 1\}$.

7.3 Algumas Construções Possíveis

Faremos agora algumas construções possíveis, em algumas apresentaremos apenas algoritmos, o leitor interessado nas demonstrações da validade destas, pode consultar [14].

Reta Perpendicular

Dados uma reta r e um ponto P construtíveis podemos construir uma reta s perpendicular a r passando por P. Temos dois casos a considerar:

Caso 1: Se $P \in r$ temos que r é determinada por P e um Q construtível, $Q \neq P$. Acompanhe na Figura 7.3, tracemos a circunferência c de centro P e passando por Q. Como interseção entre c e r temos Q e R. Agora traçamos as circunferências c_1 com centro em Q passando por R e c_2 com centro em R passando por Q. As circunferências c_1 e c_2 tem como interseção S e T. Finalmente, por S e T traçamos a reta p que queríamos.

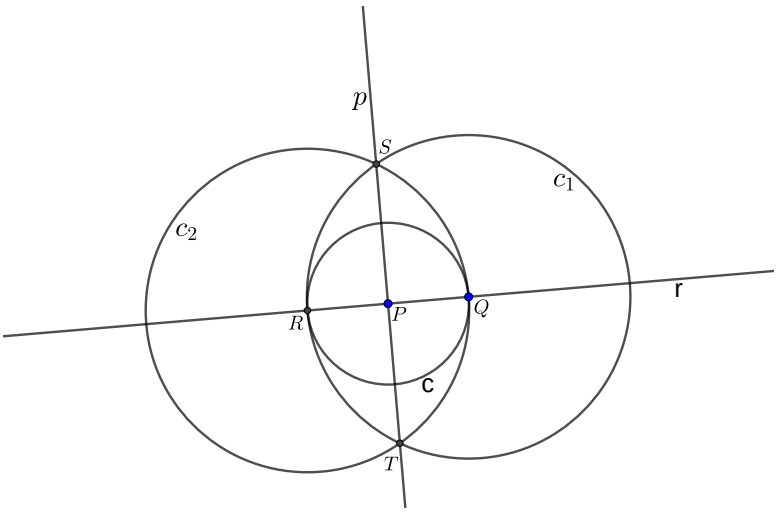

Figura 7.3: Construção de reta perpendicular: $P \in r$

Caso 2: Se $P \notin r$. Acompanhe na Figura 7.4, notemos primeiro que r é determinada por dois pontos z_1, z_2 construtíveis. Tracemos a circunferência c de centro z_1 passando por P e a circunferência d de centro z_2 passando por P. A interseção entre c e d são os pontos P e Q. Finalmente, por P e Q traçamos s, que é a reta que queríamos.

Exemplo 7.10. Pelo Caso 1 acima, temos como construtível a reta perpendicular a reta real, passando pelo ponto 0, que chamamos de reta imaginária.

Reta Paralela

Dados uma reta r e um ponto P construtíveis podemos contruir uma reta s, paralela a r, passando por P.

Caso 1: Se $P \in r$, então s é a própria r.

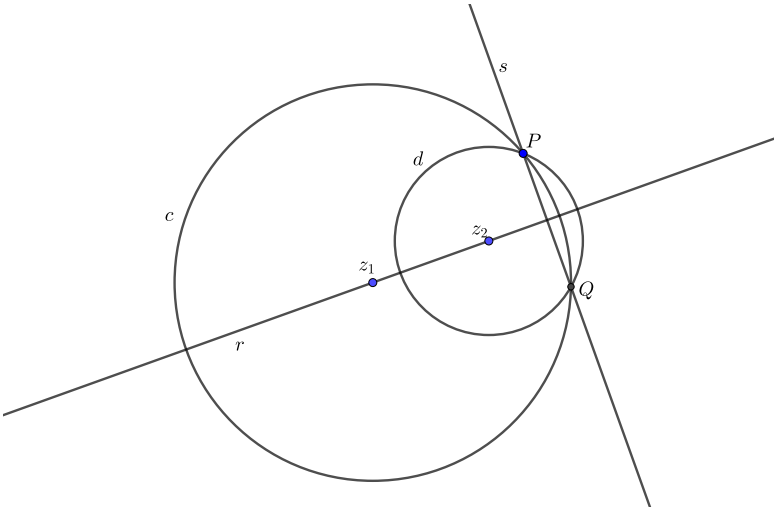

Figura 7.4: Construção de perpendicular: $P \notin r$

Caso 2: Se $P \notin r$. Na Figura 7.5, temos que r é determinada por z_1, z_2 construtíveis. Tracemos a circunferência c de centro P e raio $|z_1 - z_2|$ e a circunferência d de centro z_2 e raio $|P - z_1|$. Construímos a reta s que queremos passando por P e pelo ponto da interseção entre c e d que fica no mesmo semiplano que P em relação a r.

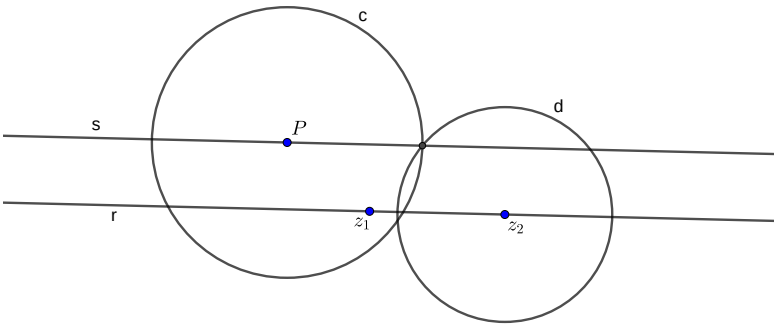

Figura 7.5: Construção de paralela

Bissecção

Lema 7.11. *Dado um ângulo α podemos construir sua bissetriz, ou seja, fazer sua bissecção com régua e compasso.*

Demonstração. Seja um ângulo α. Naturalmente ele é determinado por dois segmentos de reta e, com isso, determinado por três pontos. Sejam A, B e C três pontos que determinam o ângulo α (veja a Figura 7.6). Traçamos uma circunferência c de centro no ponto A passando por B ou C, sem perda de generalidade, façamos passando por B. A interseção

entre c e os segmentos de reta que determinam α são os pontos B e D. Seja $E \neq A$ o ponto de interseção entre as circunferências c_1 e c_2 com centros em B e D, respectivamente, passando por A.

A reta determinada por A e E é a bissetriz de α. De fato, $ABED$ é um losango e AE uma de suas diagonais, portanto, $B\widehat{A}E = D\widehat{A}E = \dfrac{\alpha}{2}$.

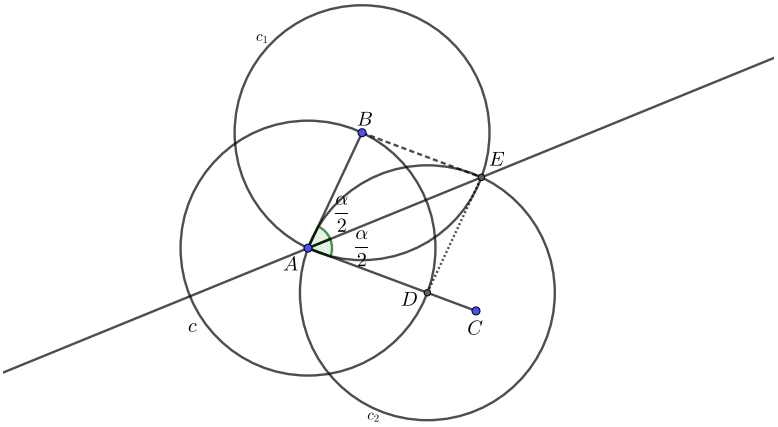

Figura 7.6: Bissecção de ângulo

□

Transporte de Ângulos

Em construções posteriores falaremos em transportar um ângulo com naturalidade em virtude do próximo resultado:

Dado um ângulo α podemos transporta-lo, ou seja, podemos construir um ângulo α "rente" a uma reta r com centro num ponto $D \in r$.

Acompanhe na Figura 7.7. Dado um ângulo α, centrado em A, podemos determinar segmentos $AB = AC$ como visto na demonstração do lema anterior. Traçamos a circunferência c_1 de centro D e raio $|A-B|$ obtendo o ponto B' como um dos pontos de interseção entre c_1 e r. Agora, C' é um dos pontos de interseção entre a circunferência c_2 de centro B' e raio $|B-C|$ com c_1. O ângulo $\widehat{B'DC'} = \alpha' = \alpha$ é o ângulo que queríamos.

Ponto Médio

Dados dois pontos z_1 e z_2 construtíveis, podemos construir o ponto M, médio entre eles.

Na Figura 7.8, traçamos as circunferências c_1 de centro z_1 passando por z_2 e c_2 de centro z_2 passando por z_1. A interseção entre c_1 e c_2 determinam os pontos z_3 e z_4.

A interseção entre a reta r, determinada por z_1 e z_2, com a reta s, determinada por z_3 e z_4 é o ponto médio M.

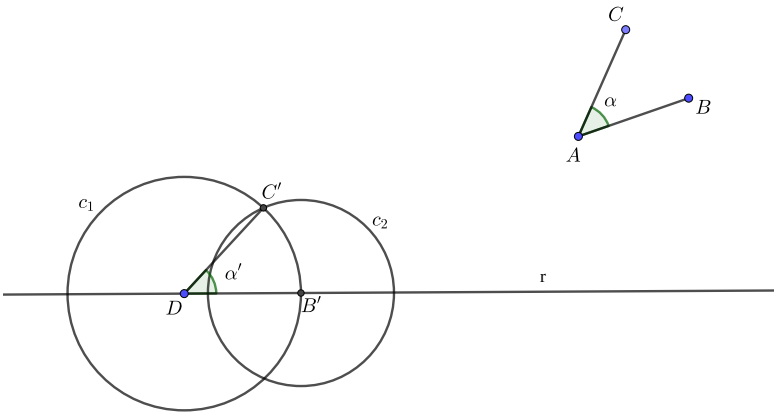

Figura 7.7: Transporte de ângulo

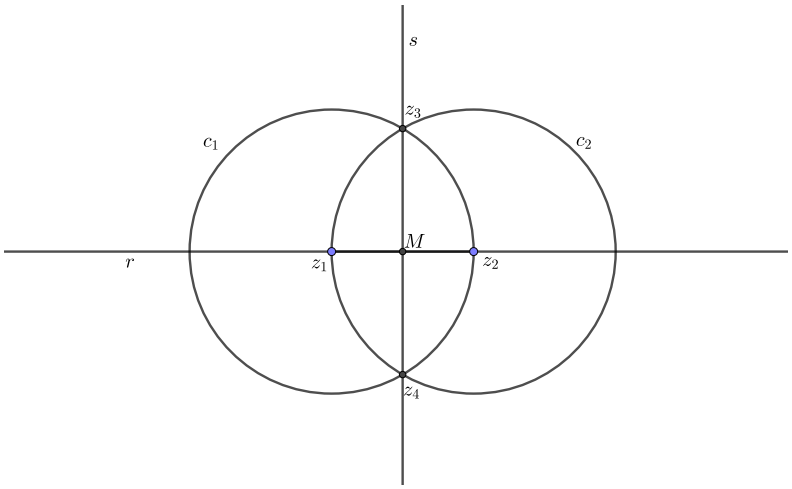

Figura 7.8: Ponto Médio

7.4 Soma, Subtração, Produto, Quociente

Agrupamos nesta seção uma série de resultados que comprovam o fechamento das operações de soma, subtração, produto e quociente de números construtíveis.

Proposição 7.12. *Sejam z_1 e z_2 dois números complexos construtíveis, então $z_1 + z_2$ é construtível.*

Demonstração. Dados dois números complexos $z_1 = a + bi$ e $z_2 = c + di$ contrutíveis, utilizando sua representação pelos vetores u e v, respectivamente, (veja a Figura 7.9). Traçamos com régua e compasso uma paralela ao vetor v passando por z_1 e uma paralela ao vetor u passando por z_2, obtendo o ponto z_3, na interseção entre essas duas retas. A partir do conceito da soma de vetores, temos $z_3 = z_1 + z_2$. Com isso a soma de dois números complexos construtíveis é construtível.

□

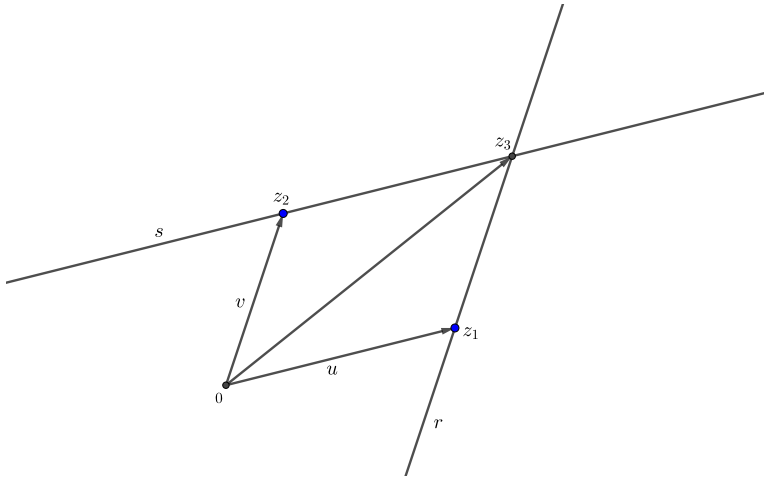

Figura 7.9: Soma $z_1 + z_2$

Proposição 7.13. *Sejam z_1 e z_2 dois números complexos construtíveis, então $z_1 - z_2$ é construtível.*

Demonstração. Dados dois números complexos construtíveis z_1 e z_2. Observe na Figura 7.10, traçamos uma circunferência c com centro na origem passando por z_2 e a reta r passando por 0 e por z_2. A interseção entre c e d são os pontos z_2 e $-z_2$. Da proposição anterior, podemos construir a soma $z_1 + (-z_2) = z_1 - z_2$. Portanto, podemos concluir que a subtração de dois números complexos construtíveis é construtível.

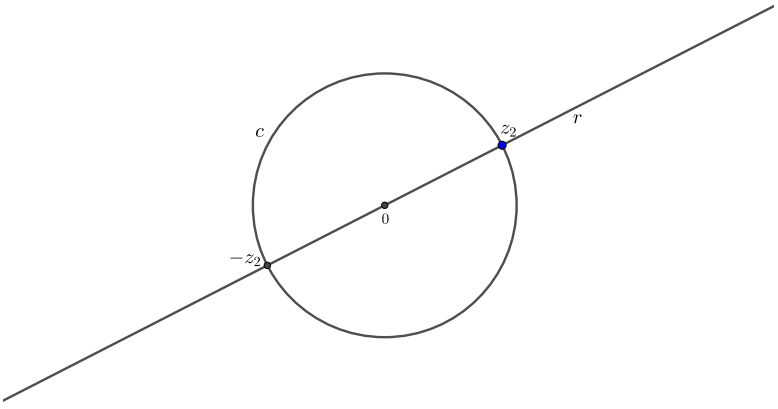

Figura 7.10: Simétrico de z_2

□

Para a prova da construtibilidade do produto e do quociente utilizaremos, em determinados momentos, a representação de números complexos em coordenadas polares.

Para a demonstração da próxima proposição precisaremos do seguinte lema:

Lema 7.14. *Dados dois números complexos construtíveis z_1 e z_2 com $|z_1| = u$ e $|z_2| = v$. O produto de seus módulos $u \cdot v$ é construtível.*

Demonstração. Na Figura 7.11, traçamos as circunferências c_1 e c_2 de centro em $O = (0, 0)$ e raio, respectivamente, u e v.

Um dos pontos de interseção de c_1 com a reta imaginária é o ponto A, e um dos pontos de interseção de c_2 com a reta real é o ponto B.

Traçamos um segmento ligando A ao ponto $(0, 1) = U$ e, em seguida, construímos a paralela a este segmento f passando por B.

A interseção de f com a reta imaginária é o ponto C. Finalmente, $|C - O| = u \cdot v$, isto é válido pela semelhança entre os triângulos OUA e OBC, vejamos,

$$\frac{u}{1} = \frac{|C - O|}{v} \Leftrightarrow |C - O| = u \cdot v$$

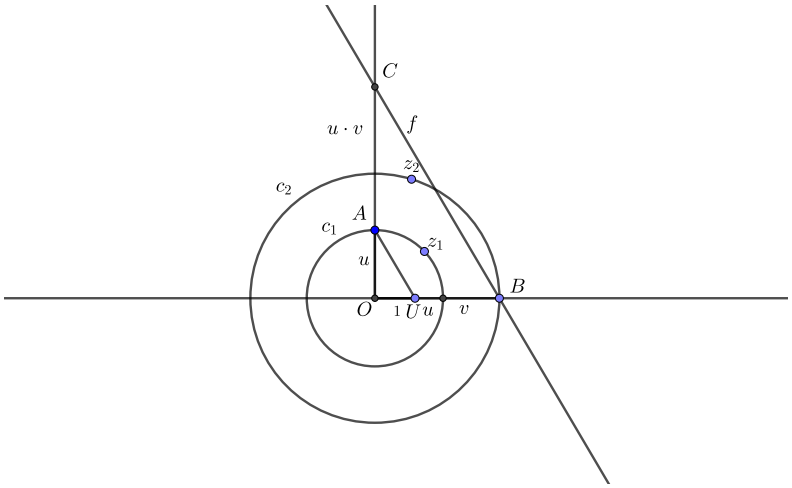

Figura 7.11: Produto de módulos

□

Proposição 7.15. *Sejam z_1 e z_2 dois números complexos construtíveis, então $z_1 \cdot z_2$ é construtível.*

Demonstração. Dados dois números complexos construtíveis $z_1 = (u; \alpha)$ e $z_2 = (v; \beta)$, onde u e v são as normas e α e β são os argumentos de z_1 e z_2, respectivamente.

Vimos na Subseção 3.1.1, que o produto de números complexos é obtido através do produto das normas e soma dos argumentos.

Agora, acompanhe na Figura 7.12, a reta f é a reta real do plano de Argand-Gauss. Pelo que foi visto na Seção 7.3 sobre transporte de ângulos, podemos transportar o ângulo α para a região externa ao ângulo β, de modo que, esteja com suporte na origem e na reta que passa por z_2 e pela origem. Calculamos o produto das normas $u \cdot v$, como mostramos

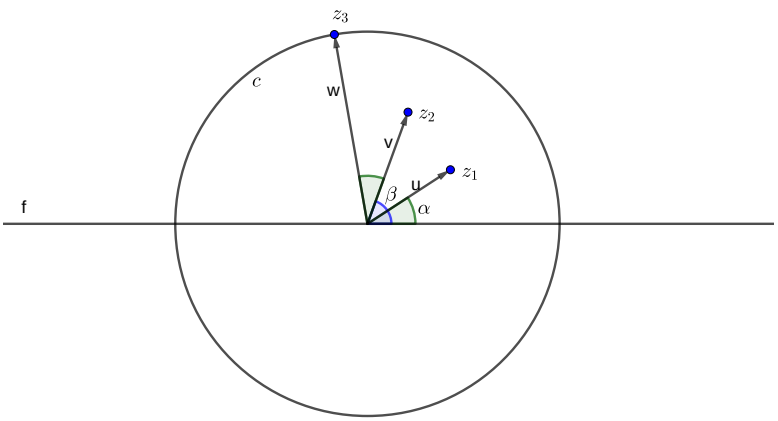

Figura 7.12: $z_1 \cdot z_2$

no Lema 7.14, e construimos uma circunferência c, centrada em $(0,0)$ com raio $u \cdot v$. O ponto de interseção de c com a outra semirreta suporte do ângulo transportado é o ponto z_3. Pelo parágrafo anterior $z_3 = z_1 \cdot z_2$. E podemos concluir que o produto de dois números complexos construtíveis é construtível.

□

Lema 7.16. *Dados dois números complexos construtíveis z_1 e z_2 com $|z_1| = u$ e $|z_2| = v$, sendo $z_2 \neq 0$. O quociente de seus módulos $\frac{u}{v}$ é construtível.*

Demonstração. Na Figura 7.13, traçamos a circunferência c_1 de centro na origem O e raio 1. Uma dos pontos de interseção de c_1 com a reta imaginária é o ponto $(1,0) = E$.

Traçamos as circunferências c_2 e c_3 de centro em O e raio, respectivamente, v e u.

Um dos pontos de interseção de c_2 com a reta real é o ponto $(v,0) = A$ e um dos pontos de interseção de c_3 com a reta real é o ponto $(u,0) = B$.

Traçamos um segmento ligando $(1,0) = E$ a $(v,0) = A$ e, em seguida, construímos a paralela f a este segmento passando por $(u,0) = B$.

A interseção de f com a reta imaginária é o ponto C. Finalmente, $|C - O| = \frac{u}{v}$. Isto é válido devido a semelhança entre os triângulos OAE e OBC, vejamos,

$$\frac{1}{v} = \frac{|C-O|}{u} \Leftrightarrow |C-O| = \frac{u}{v}$$

□

Proposição 7.17. *Sejam z_1 e z_2 dois números complexos construtíveis, então $\frac{z_1}{z_2}$ é construtível.*

Demonstração. Sejam dois números complexos construtíveis $z_1 = (u;\alpha)$ e $z_2 = (v;\beta)$, onde $z_2 \neq 0$, u e v são as normas e α e β são os argumentos de z_1 e z_2, respectivamente.

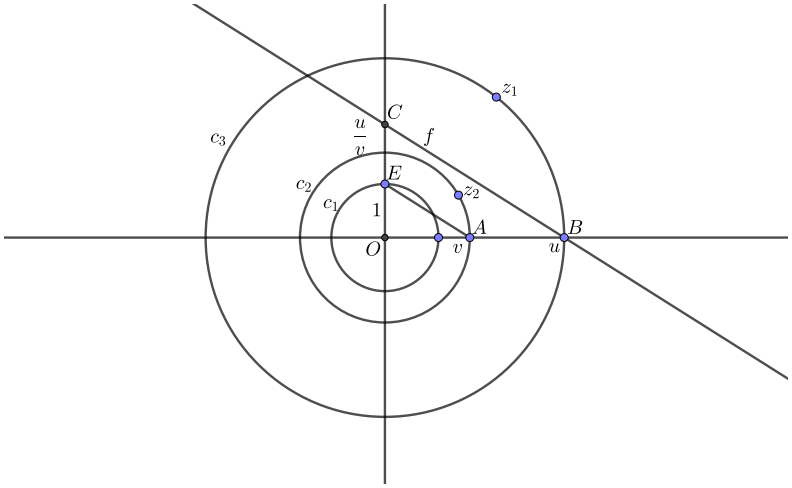

Figura 7.13: Quociente de módulos

Vimos na Subseção 3.1.1, que o quociente de números complexos é obtido através do quociente das normas e diferença dos argumentos.

Novamente, a reta f é a reta real do plano de Argand-Gauss. Notemos que na Figura 7.14, o ângulo $\alpha - \beta$ é precisamente o ângulo formado pelos segmentos de reta dos pontos z_1 e z_2. Transportamos esse ângulo, de modo que fique com reta suporte na reta f e no sentido anti-horário, obtemos o ângulo γ da figura. Calculamos o quociente $\frac{u}{v}$, como mostrado no Lema 7.16, e construímos uma circunferência c de centro em $(0,0)$ e raio $\frac{u}{v}$. A interseção entre c e a outra semirreta suporte de γ é o ponto z_3. Pelo parágrafo anterior, $z_3 = \frac{z_1}{z_2}$. E podemos concluir que o quociente de dois números complexos construtíveis, o divisor não nulo, é construtível.

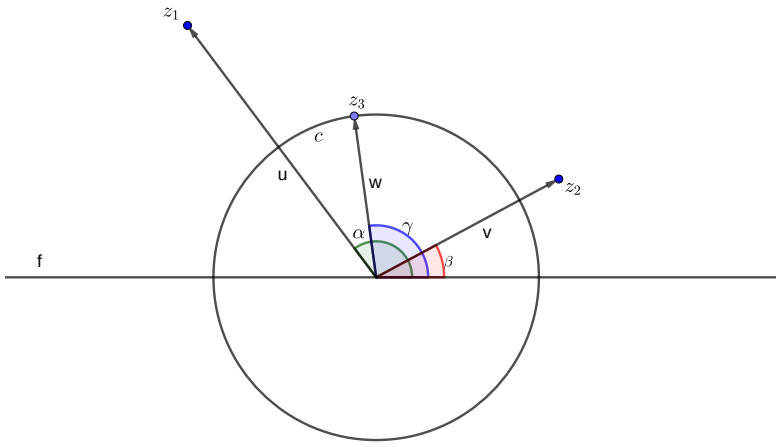

Figura 7.14: $\frac{z_1}{z_2}$

□

Nesta seção mostramos que é possível com régua e compasso efetuar as operações de

soma, subtração, produto e quociente (por número não nulo) de números construtíveis. Diante disso, ao partirmos de $c_0 = \{0, 1\}$, provamos que todos os números racionais são construtíveis, e temos que $\mathbb{Q} \subset \mathbb{C}_c$.

Para garantirmos o tratamento do conjunto $\mathbb{C}_c$ como um corpo, provemos este fato.

Proposição 7.18. *O conjunto $\mathbb{C}_c$ dos números construtíveis a partir de $c_0 = \{0, 1\}$ é um subcorpo dos complexos.*

Demonstração. Como os pontos de $\mathbb{C}_c$ estão no plano complexo, então $\mathbb{C}_c$ é um subconjunto de $\mathbb{C}$. De 0 e $1 \in \mathbb{C}_c$ temos que $\mathbb{C}_c \neq \varnothing$ e, além disso, garantimos também o item (i) da Proposição 4.7. Os itens (ii) e (iii) da mesma proposição são garantidos pelos resultados desta seção, terminando a prova. □

7.5 Módulo e Conjugado

Vamos mostrar mais construções possíveis que nos serão fundamentais na determinação do corpo $\mathbb{C}_c$.

Lema 7.19. *Seja $z = (u; \alpha)$ construtível, então seu módulo u e seu conjugado $\overline{z}$ são construtíveis.*

Demonstração.

Dado um número z construtível. Traçamos a circunferência c de centro 0 passando por z. A interseção entre c com a reta real é u.

Traçamos a circunferência d de centro em 1 passando por z. A interseção de c com d são os pontos z e $\overline{z}$.

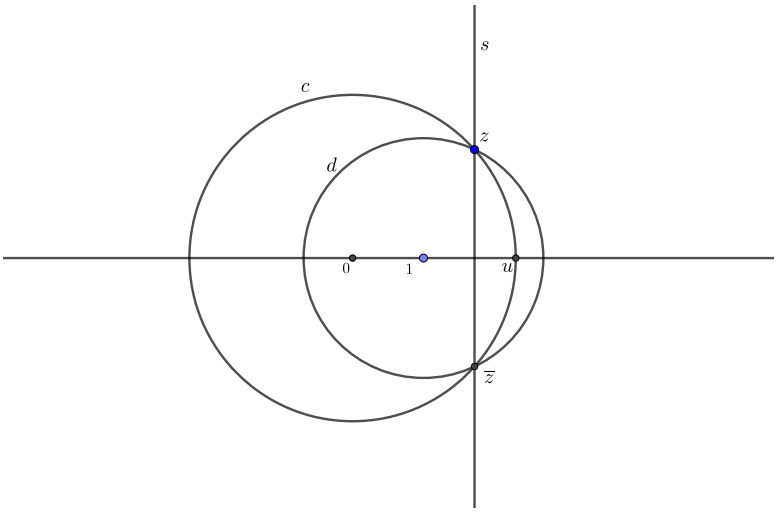

Figura 7.15: Construção de conjugado

De fato, o ponto $\overline{z}$ na Figura 7.15, é realmente o conjugado de z, pois, sendo o ponto A a interseção entre a reta real e a reta perpendicular a reta real passando por z, temos que $|z - A| = |\overline{z} - A|$.

□

Lema 7.20. *Dado um número real positivo u, construtível, então, $\sqrt{u}$ é construtível.*

Demonstração.

Traçamos uma circunferência c_1, de centro em 0 passando por 1. Um dos pontos de interseção de c com a reta real é o ponto: -1.

Determinamos o ponto médio M entre -1 e u.

Traçamos a circunferência c_2 de centro em M passando por u. Um dos pontos de interseção de c_2 com a reta imaginária é o ponto C.

Finalmente, $|C-0| = \sqrt{u}$. De fato, chamaremos de A o ponto -1 e de B o ponto u, então o triângulo ACB é retângulo em C, pois o ângulo $A\widehat{C}B$ é inscrito em c_2, portanto, mede metade do ângulo central $A\widehat{M}B = 180°$, detalhes sobre ângulos inscritos em [14]. Pelo fato de ACB ser retângulo em C, valem as relações trigonométricas num triângulo retângulo, que também podem ser consultadas em [14]:

$$\begin{aligned} |C-0|^2 &= 1 \cdot u \\ |C-0|^2 &= u \\ |C-0| &= \sqrt{u} \end{aligned}$$

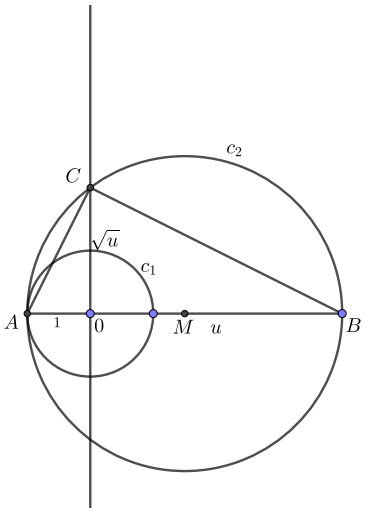

Figura 7.16: Raiz quadrada de módulo

□

7.6 Números $x^2 = z$

Proposição 7.21. *Seja z_1 um número complexo construtível, então são construtíveis os números x tais que $x^2 = z_1$.*

Demonstração. Dado um número complexo construtível: $z_1 = (u; \alpha)$, onde u é a norma e α é o argumento. Vimos na Subseção 3.1.2, quais os números x, tais que $x^2 = z_1$.

Pelo Lema 7.19, u é construtível. Pelo Lema 7.20, $\sqrt{u}$ é construtível. Pelo Lema 7.11, a bissetriz de α é construtível. Traçamos uma circunferência c, com centro em 0 e raio igual a $\sqrt{u}$. A interseção de c com a bissetriz de α são os pontos z_2 e z_3, que são os números x procurados (notemos que o argumento de z_3 é $\frac{\alpha}{2} + 180°$, o que confirma nosso resultado). Desta forma, podemos concluir que os números x tais que $x^2 = z_1$ são construtíveis.

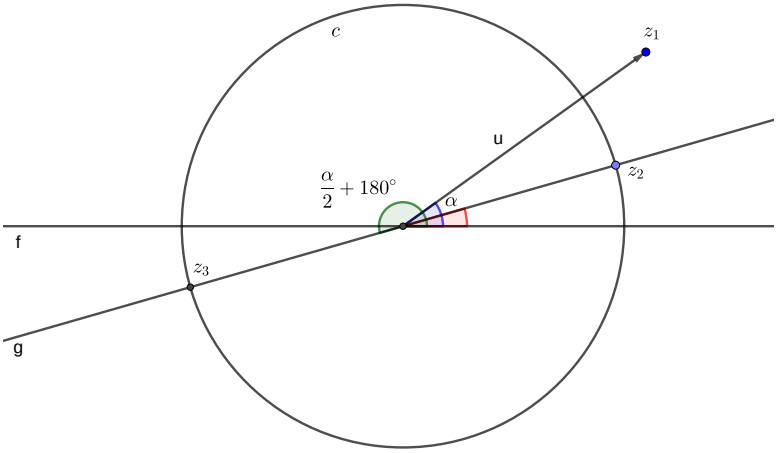

Figura 7.17: $z_2^2 = z_1$ e $z_3^2 = z_1$

□

7.7 Grau de um Número Construtível

Neste momento utilizaremos fortemente conceitos de extensões de corpos como auxílio na busca da identificação do corpo $\mathbb{C}_c$. Nesta seção denotaremos o conjunto $c_i(\{0,1\})$ apresentado na cadeia (7.3) por $\mathcal{C}_i$.

Proposição 7.22. *Seja $z \in \mathcal{C}_i$, então $\overline{z} \in \mathcal{C}_i$.*

Demonstração.

É imediato. Visto que todos os $\mathcal{C}_i$'s são obtidos a partir do conjunto $\{0,1\}$. □

Já vimos que $\mathbb{C}_c$ é um subcorpo dos complexos que contém os racionais, ou seja, $\mathbb{Q} \subset \mathbb{C}_c \subset \mathbb{C}$. Assim um número construtível z pertencerá a um corpo da forma $\mathbb{Q}(\mathcal{C}_i)$, para algum $i \in \mathbb{N}$. Para simplificar a notação, vamos denotar $\mathbb{Q}(\mathcal{C}_i)$ por $\mathbb{K}_i$.

A próxima proposição determina o grau de um elemento $z \in \mathcal{C}_{i+1}$ sobre $\mathbb{K}_i$.

Proposição 7.23. *Seja $z \in \mathcal{C}_{i+1}$, então $[\mathbb{K}_i(z) : \mathbb{K}_i] \leqslant 2$.*

Demonstração. Pela definição de ponto simplesmente construtível, sabemos que z foi obtido pela interseção entre duas retas, ou uma reta e uma circunferência, ou duas circunferência construídas a partir de pontos de $\mathcal{C}_i$. Diante disso, naturalmente, temos três casos a considerar.

As equações de retas e circunferências apresentadas aqui foram vistas na Seção 7.1.

i) (Interseção entre duas retas) Sejam r_1 e r_2 duas retas construídas a partir de pontos de $\mathcal{C}_i$ tal que $z \in (r_1 \bigcap r_2)$. Então, z deve ser solução do seguinte sistema de equações:

$$\begin{cases} r_1 : (x-a)\dfrac{(\overline{b}-\overline{a})}{(b-a)} - (\overline{x}-\overline{a}) = 0 \\ r_2 : (x-c)\dfrac{(\overline{d}-\overline{c})}{(d-c)} - (\overline{x}-\overline{c}) = 0 \end{cases}$$

Onde $a, b, c, d \in \mathcal{C}_i$. Subtraindo os termos da segunda igualdade da primeira, obtemos:

$$x\left(\frac{(\overline{b}-\overline{a})}{(b-a)} - \frac{(\overline{d}-\overline{c})}{(d-c)}\right) - a\frac{(\overline{b}-\overline{a})}{(b-a)} + c\frac{(\overline{d}-\overline{c})}{(d-c)} + \overline{a} - \overline{c} = 0$$

Que é uma equação da forma

$$\alpha x - \beta = 0$$

com $\alpha, \beta \in \mathbb{K}_i$. Pelo Corolário 7.2, temos que $\alpha \neq 0$.

Portanto, z é raiz de uma equação polinomial de grau 1 com coeficientes em $\mathbb{K}_i$, logo, $z \in \mathbb{K}_i$ e $[\mathbb{K}_i(z) : \mathbb{K}_i] = 1$;

ii) (Interseção entre uma reta e uma circunferência) Sejam r uma reta e c uma circunferência construídas a partir de pontos de $\mathcal{C}_i$. Suponha que $z \in (r \bigcap c)$, então z deve ser solução do seguinte sistema de equações:

$$\begin{cases} r : (x-a)\dfrac{(\overline{b}-\overline{a})}{(b-a)} - (\overline{x}-\overline{a}) = 0 \\ c : (x-c)\cdot(\overline{x}-\overline{c}) - (d-e)(\overline{d}-\overline{e}) = 0 \end{cases}$$

Onde a, b, c, d e $e \in \mathcal{C}_i$. Isolando o $\overline{x}$ na primeira equação obtemos

$$\overline{x} = (x-a)\frac{(\overline{b}-\overline{a})}{(b-a)} + \overline{a}$$

Substituindo o $\overline{x}$ na segunda equação obtemos:

$$(x-c)\cdot\left((x-a)\frac{(\overline{b}-\overline{a})}{(b-a)} + \overline{a} - \overline{c}\right) - (d-e)(\overline{d}-\overline{e}) = 0$$

Que desenvolvendo chegamos a uma equação da forma:

$$\alpha x^2 + \beta x + \gamma = 0$$

Onde $\alpha, \beta, \gamma \in \mathbb{K}_i$ e $\alpha = \dfrac{(\overline{b}-\overline{a})}{(b-a)} \neq 0$, pois $b \neq a$, uma vez que são os pontos que determinam a reta r. Dessa forma, z é um zero de um polinômio $p(x) \in \mathbb{K}_i[x]$ de grau 2. Pela Proposição 5.7, o polinômio minimal de z sobre $\mathbb{K}_i$ divide $p(x)$. Logo, $[\mathbb{K}_i(z) : \mathbb{K}_i] \leqslant 2$;

iii) (Interseção entre duas circunferências) Sejam c_1 e c_2 circunferências não-concêntricas construídas a partir de pontos de $\mathcal{C}_i$, tal que $z \in (c_1 \bigcap c_2)$. Então, z é solução do seguinte sistema de equações:

$$\begin{cases} c_1 : (x-a)\cdot(\overline{x}-\overline{a}) - (d-e)(\overline{d}-\overline{e}) = 0 \\ c_2 : (x-b)\cdot(\overline{x}-\overline{b}) - (f-g)(\overline{f}-\overline{g}) = 0 \end{cases}$$

Onde $a, b, d, e, f, g \in \mathcal{C}_i$.

Vamos reescrever as equações acima da seguinte forma:

$$\begin{cases} \overline{x}-\overline{a} = \dfrac{(d-e)(\overline{d}-\overline{e})}{(x-a)} \\ \overline{x}-\overline{b} = \dfrac{(f-g)(\overline{f}-\overline{g})}{(x-b)} \end{cases}$$

Subtraindo os termos da segunda igualdade da primeira, obtemos:

$$-\overline{a}+\overline{b} = \frac{(d-e)(\overline{d}-\overline{e})}{x-a} - \frac{(f-g)(\overline{f}-\overline{g})}{x-b}$$

Que é uma equação que não depende de $\overline{x}$. Desenvolvendo, obtemos uma equação da forma

$$\alpha x^2 + \beta x + \gamma = 0$$

Onde $\alpha, \beta, \gamma \in \mathbb{K}_i$ e $\alpha = -\overline{a}+\overline{b} \neq 0$, pois as circunferências não são concêntricas. Portanto, de forma análoga ao item ii), obtemos $[\mathbb{K}_i(z) : \mathbb{K}_i] \leqslant 2$.

□

De posse da proposição anterior podemos demonstrar o seguinte teorema:

Teorema 7.24. *Se $z \in \mathbb{C}_c$, então existe uma cadeia finita $\mathbb{Q} \subset \mathbb{K}_1 \subset \mathbb{K}_2 \subset \cdots \subset \mathbb{K}_n$ de subcorpos dos complexos, tais que $z \in \mathbb{K}_n$ e $[\mathbb{K}_i : \mathbb{K}_{i-1}] = 2$, com $i \in \{1, 2, \ldots, n\}$. E assim, $[\mathbb{Q}(z) : \mathbb{Q}] = 2^m$ para algum $m \in \mathbb{N}$.*

Demonstração.

Sendo $z \in \mathbb{C}_c$, pela Definição 7.9, $z \in \mathcal{C}_n$ para algum $n \in \mathbb{N}$. Faremos a demonstração por indução em n.

Seja $z \in \mathcal{C}_1$, então pela proposição anterior o grau da extensão $\mathbb{Q}(z)|\mathbb{Q}$ é 1 ou 2, portanto $[\mathbb{Q}(z) : \mathbb{Q}]$ é uma potência de 2 e o teorema é válido para $n = 1$.

Suponha que o teorema é válido para $n = k$ para algum $k \geqslant 1$.

Seja $z \in \mathcal{C}_{k+1}$, então z é construído a partir de duas retas ou uma reta e uma circunferência ou duas circunferências, onde essa(s) reta(s) e/ou circunferência(s) são construídas a partir de pontos de um conjunto finito $\{a_1, a_2, \ldots, a_s\} \subset \mathcal{C}_k$. Note que esse conjunto precisa ter no máximo 6 pontos. Por hipótese de indução, $[\mathbb{Q}[a_i] : \mathbb{Q}]$ é uma

potência de 2 para todo $1 \leqslant i \leqslant s$. Então, $[\mathbb{Q}[a_1, a_2, \ldots, a_s] : \mathbb{Q}]$ é uma potência de 2. Note que z é construído a partir de pontos da extensão $[\mathbb{Q}[a_1, a_2, \ldots, a_s] : \mathbb{Q}]$. Portanto, $[\mathbb{Q}(z) : \mathbb{Q}[a_1, a_2, \ldots, a_s]] \leqslant 2$ pela proposição anterior.

Logo, pelo Teorema 5.11 (Teorema da Torre):

$$[\mathbb{Q}(z) : \mathbb{Q}] = [\mathbb{Q}(z) : \mathbb{Q}[a_1, a_2, \ldots, a_s]] \cdot [\mathbb{Q}[a_1, a_2, \ldots, a_s] : \mathbb{Q}]$$

Portanto, $[\mathbb{Q}(z) : \mathbb{Q}]$ é uma potência de 2 para todo $z \in \mathbb{C}_c$. □

Teorema 7.25. *Se $\mathbb{K}|\mathbb{Q}$ é uma extensão normal com $[\mathbb{K} : \mathbb{Q}] = 2^n$, $n \in \mathbb{N}$. Então, $\mathbb{K} \subseteq \mathbb{C}_c$.*

Demonstração.

Faremos por indução em n.

Para $n = 0$ é válido trivialmente, pois, neste caso $\mathbb{K} = \mathbb{Q}$ e, como sabemos, $\mathbb{Q} \subseteq \mathbb{C}_c$.

Agora, suponha que o teorema seja válido para $n = k$ para algum $k \geqslant 0$.

Seja uma extensão $\mathbb{K}|\mathbb{Q}$ normal com $[\mathbb{K} : \mathbb{Q}] = 2^{k+1}$ e seja $\Gamma(\mathbb{K}|\mathbb{Q})$ seu Grupo de Galois. Pelo item 1 do Teorema 6.29, $|\Gamma(\mathbb{K}|\mathbb{Q})| = [\mathbb{K} : \mathbb{Q}] = 2^{k+1}$.

Pelo Teorema de Lagrange 2.14, qualquer subgrupo de $\Gamma(\mathbb{K}|\mathbb{Q})$ tem ordem que divide 2^{k+1}. Pela Proposição 2.22, o centro de $\Gamma(\mathbb{K}|\mathbb{Q})$ tem ordem 2^j onde $1 \leqslant j \leqslant k+1$. Pelo item iii) do Exemplo 2.16, qualquer subgrupo do centro de $\Gamma(\mathbb{K}|\mathbb{Q})$ é normal em relação a $\Gamma(\mathbb{K}|\mathbb{Q})$. Pela Proposição 2.21, existe um subgrupo H do centro de $\Gamma(\mathbb{K}|\mathbb{Q})$ de ordem 2.

Pelo Teorema 6.29, existe uma extensão $\mathbb{M}|\mathbb{Q}$ normal associada a H e

$$[\mathbb{M} : \mathbb{Q}] = \frac{|\Gamma(\mathbb{K}|\mathbb{Q})|}{|H|} = \frac{2^{k+1}}{2} = 2^k$$

Pela hipótese de indução $\mathbb{M} \subset \mathbb{C}_c$. Agora, pelo Teorema 5.11 (Teorema da Torre)

$$\begin{aligned} [\mathbb{K} : \mathbb{Q}] &= [\mathbb{K} : \mathbb{M}] \cdot [\mathbb{M} : \mathbb{Q}] \\ 2^{k+1} &= [\mathbb{K} : \mathbb{M}] \cdot 2^k \end{aligned}$$

Assim, $[\mathbb{K} : \mathbb{M}] = 2$ que, pela Proposição 5.17, por ser uma extensão finita é algébrica. Pelo Teorema do Elemento Primitivo 5.19, existe $\beta \in \mathbb{C}$ tal que $\mathbb{K} = \mathbb{M}(\beta)$, onde β tem grau 2 sobre $\mathbb{M}$, ou seja, β é raiz de um polinômio minimal de grau 2 sobre $\mathbb{M}$. Seja $m(x) = p_{min}(\beta, \mathbb{M})$, onde $m(x) = x^2 + ax + b$ com $a, b \in \mathbb{M}$. Tomemos $\gamma = \beta + \frac{a}{2}$, temos que $\gamma^2 = -b + \frac{a^2}{4}$, logo, $\gamma \in \mathbb{M}$ e $\mathbb{K} = \mathbb{M}(\gamma)$. Pela Proposição 7.21, $\gamma \in \mathbb{C}_c$. Como já vimos que $\mathbb{M} \subset \mathbb{C}_c$ e $\mathbb{K} = \mathbb{M}(\gamma)$, então $\mathbb{K} \subset \mathbb{C}_c$. □

Corolário 7.26. *Seja $z \in \mathbb{C}$ um elemento de uma extensão normal $\mathbb{K}|\mathbb{Q}$ tal que $[\mathbb{K} : \mathbb{Q}] = 2^n, n \in \mathbb{N}$, então z é construtível.*

Demonstração. Imediato do teorema acima, pois z pertence a uma extensão onde todos os pontos são construtíveis. □

Capítulo 8

Polígonos Regulares Construtíveis

Neste capítulo, de posse dos resultados apresentados no capítulo anterior sobre construtibilidade, apresentamos um belíssimo teorema, devido a Gauss, que caracteriza os polígonos regulares construtíveis com régua e compasso.

Proposição 8.1. *As raízes de $x^n - 1$ quando marcadas no plano complexo formam os vértices de um polígono regular de n lados inscrito num círculo unitário.*

Demonstração. Vimos a descrição das raízes n-ésimas da unidade na Subseção 3.1.3, que reescrevendo-as na forma polar temos $\left(1; \frac{2k\pi}{n}\right)$, com $0 \leqslant k \leqslant n-1$. Obviamente todas as raízes tem módulo 1 o que garante que estão todas no círculo unitário. Notamos que a diferença dos argumentos de duas raízes consecutivas é igual a $\frac{2k\pi}{n} - \frac{2(k-1)\pi}{n} = \frac{2\pi}{n}$, o que mostra que as raízes estão igualmente espaçadas no círculo unitário, comprovando que elas realmente são os vértices de um n-ágono regular inscrito no círculo unitário. □

Proposição 8.2. *Seja $n \in \mathbb{N}$, $n \geqslant 3$. Um n-ágono regular é construtível se, e somente se, uma n-ésima raiz primitiva da unidade é construtível.*

Demonstração.

$\Rightarrow$) Seja um n-ágono construtível. Se o considerarmos no plano complexo e utilizarmos uma unidade de medida de forma que ele esteja inscrito na circunferência unitária com centro 0, com um dos vértices sobre o ponto 1, pela Proposição 8.1, todas as raízes n-ésimas primitivas da unidade são construtíveis.

$\Leftarrow$) Seja ζ uma raiz n-ésima primitiva da unidade construtível. Vimos na Subseção 3.1.3, que uma raíz primitiva da unidade gera $U_n = \{\zeta, \zeta^2, \ldots, \zeta^{n-1}, \zeta^n = 1\}$, por potenciação, operação que, como já vimos, é possível efetuar com régua e compasso. Novamente, pela Proposição 8.1, U_n são os vértices do n-ágono, provando sua construtibilidade. □

Proposição 8.3. *Se $r, s \in \mathbb{N}$ são tais que $\text{mdc}(r, s) = 1$, se o r-ágono e o s-ágono regulares são construtíveis, então o rs-ágono regular é construtível.*

Demonstração. Visto que $\text{mdc}\,(r,s)=1$, existem $a,b\in\mathbb{Z}$ tais que $ar+bs=1$. Multiplicando esta última equação por $\dfrac{2\pi}{rs}$ obtemos

$$a\frac{2\pi}{s}+b\frac{2\pi}{r}=\frac{2\pi}{rs}$$

Com isso, chegamos que o ângulo $\dfrac{2\pi}{rs}$ pode ser obtido como combinação linear com coeficientes inteiros entre os ângulos $\dfrac{2\pi}{s}$ e $\dfrac{2\pi}{r}$. Ou seja, podemos obter o ângulo $\dfrac{2\pi}{rs}$ através de operações de somas e subtrações entre os ângulos $\dfrac{2\pi}{s}$ e $\dfrac{2\pi}{r}$ (que, como vimos, são possíveis com régua e compasso), os quais, por hipótese, são construtíveis. □

Proposição 8.4. *O 2^n-ágono regular é construtível, para todo $n\in\mathbb{N}$ tal que $n\geqslant 2$.*

Demonstração.

Por indução. Para $n=2$ mostremos que o quadrado é construtível.

Dado um segmento AB. Traçamos as circunferências c_1 e c_2 de centros em A e B, respectivamente, e raio $|A-B|$. Traçamos a reta r, determinada pelos pontos de intercessão entre as circunferências c_1 e c_2. A reta r intersecta o segmento AB em seu ponto médio C. Traçamos a circunferência c_3 de centro C e raio $|C-A|$. A reta r intersecta c_3 nos pontos D e E. O quadrado é determinado traçando os segmentos: BD, DA, AE e EB.

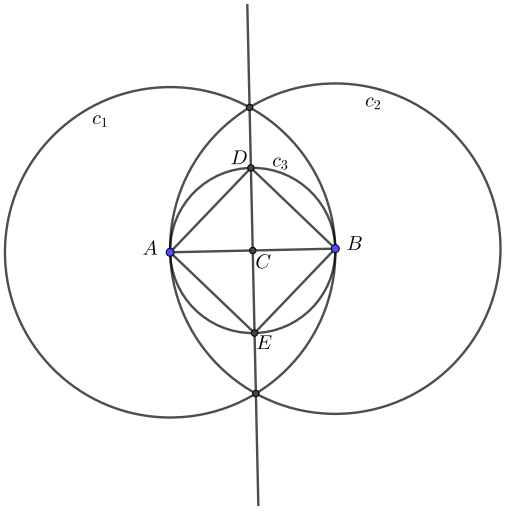

Figura 8.1: Quadrado

Supondo que o resultado é válido para um $n\geqslant 2$, mostraremos ser válido para $n+1$. Seja um 2^n-ágono construtível. Pelo visto na Seção 7.3, podemos fazer a bissecção de qualquer ângulo. Então, fazemos a bissecção dos ângulos centrais do 2^n-ágono. Os vértices do 2^n-ágono mais os pontos de intercessão entre a circunferência que circunscreve este polígono e as bissetrizes seus ângulos centrais formam os vértices do 2^{n+1}-ágono. □

Antes do resultado principal do capítulo, precisamos de um resultado importante de Aritmética:

Proposição 8.5. *Seja $p \in \mathbb{N}$ tal que $p = 2^n + 1$. Se p é primo, então $n = 2^r$ para algum $r \in \mathbb{N}$.*

Demonstração.

Supondo, por absurdo, que n tivesse algum fator ímpar em sua decomposição, digamos j, e com isso, teríamos $n = aj$ com $a \in \mathbb{N}$, e j ímpar. Logo,

$$p = 2^n + 1 = 2^{aj} + 1 = (2^a)^j + 1$$

Agora, pela Proposição 1.2, temos,

$$p = (2^a)^j + 1 = (2^a + 1)((2^a)^{j-1} - (2^a)^{j-2} + (2^a)^{j-3} - + \cdots - (2^a) + 1)$$

Desta forma, teríamos p divisível por $(2^a + 1)$, um absurdo, pois p é primo. □

Os números naturais $F_n = 2^{2^n} + 1$ são chamados de números de Fermat. Esses números nem sempre são primos, conforme conjecturou Fermat, veja [6]. Quando um número de Fermat é primo chamamos ele de *Primo de Fermat*. Os números $F_0 = 3, F_1 = 5, F_2 = 17, F_3 = 257, F_4 = 65537$ são primos. Euler mostrou que $F_5 = 4.294.967.297$ é divisível por 641.

Até a atualidade sabe-se que F_n é composto, para $5 \leqslant n \leqslant 32$ e, não se tem conhecimento de nenhum primo de Fermat além de F_0, F_1, F_2, F_3, F_4, mais informações sobre essa pesquisa em [3].

Teorema 8.6. *(Gauss) Seja n um número natural. Podemos construir um polígono regular de n lados com régua e compasso se, e somente se, $n = 2^k$ ou $n = 2^k p_0 p_1 \dots p_s$, onde $k, s \in \mathbb{Z}_+$, e $p_0, p_1, \dots, p_s$ são Primo de Fermat distintos.*

Demonstração.

$\Rightarrow$)

Seja um n-ágono regular construtível. Pelo Teorema 1.1 (Teorema Fundamental da Aritmética), $n = 2^k p_0^{m_0} p_1^{m_1} \dots p_s^{m_s}$ onde $k, m_0, m_1, \dots, m_s \in \mathbb{Z}_+$ e $p_0, p_1, \dots, p_s$ são primos ímpares. Da Definição 1.6 (Função Phi de Euler) e de suas propriedades elencadas nas Proposições 1.7 e 1.10,

$$\begin{aligned} \varphi(n) &= \varphi(2^k p_0^{m_0} p_1^{m_1} \dots p_s^{m_s}) \\ &= \varphi(2^k)\varphi(p_0^{m_0})\varphi(p_1^{m_1}) \dots \varphi(p_s^{m_s}) \\ &= 2^{k-1}(p_0 - 1)(p_0^{m_0-1})(p_1 - 1)(p_1^{m_1-1}) \dots (p_s - 1)(p_s^{m_s-1}) \end{aligned} \tag{8.1}$$

Por outro lado, pela Proposição 8.2, uma vez que o n-ágono regular é construtível, então, uma raiz n-ésima primitiva da unidade ζ é construtível. Pela Proposição 6.37, $[\mathbb{Q}(\zeta) : \mathbb{Q}] = \varphi(n)$. Pelo Teorema 7.24, $[\mathbb{Q}(\zeta) : \mathbb{Q}] = 2^r$ para algum $r \in \mathbb{Z}_+$. Logo,

$$\varphi(n) = 2^{k-1}(p_0 - 1)(p_0^{m_0-1})(p_1 - 1)(p_1^{m_1-1}) \dots (p_s - 1)(p_s^{m_s-1}) = 2^r$$

E assim, para todo $0 \leqslant i \leqslant s$, temos $p_i - 1 = 2^{t_i}$ para algum $t_i \in \mathbb{Z}_+$ e $m_i = 1$.

Como $p_i - 1 = 2^{t_i}$, logo $p_i = 2^{t_i} + 1$.

Portanto, temos $n = 2^k p_0 p_1 \dots p_s$. Pela Proposição 8.5, t_i é uma potência de 2 para todo $1 \leqslant i \leqslant s$. Portanto, $p_i = 2^{2^{r_i}} + 1$, com $r_i \in \mathbb{Z}_+$.

$\Leftarrow$)

Se $n = 2^k$, pela Proposição 8.4, o 2^k-ágono regular é construtível.

Seja $p_i = 2^{2^{r_i}} + 1$ um Primo de Fermat e ζ_{p_i} uma p_i-ésima raiz primitiva da unidade em $\mathbb{C}$. Pela Proposição 6.21, $\mathbb{Q}(\zeta_{p_i})$ é o corpo de decomposição do polinômio $x^{p_i} - 1$. Pela Proposição 6.11, $\mathbb{Q}(\zeta_{p_i})|\mathbb{Q}$ é uma extensão normal e, pelo Teorema 6.37, temos:

$$[\mathbb{Q}(\zeta_{p_i}) : \mathbb{Q}] = \varphi(p_i) = p_i - 1 = (2^{2^{r_i}} + 1) - 1 = 2^{2^{r_i}}$$

Diante disso, pelo Corolário 7.26, ζ_{p_i} é construtível. Portanto, pela Proposição 8.2, todos os p_i-ágonos regulares são construtíveis.

Se $n = 2^k p_0 p_1 \dots p_s$, onde $k, s \in \mathbb{Z}_+$, e $p_0, p_1, \dots, p_s$ são *Primos de Fermat* distintos, então, pela Proposição 8.3, temos que o n-ágono é construtível e finalizamos a demonstração. □

Capítulo 9

Os Três Problemas Gregos Clássicos

Dedicamos este capítulo ao tratamento dos três problemas clássicos gregos, onde veremos que diante de todos os resultados apresentados e de todo o desdobramento feito da teoria, estamos em condições de se debruçarmos sobre as provas das impossibilidades das resoluções de tais problemas.

Os resultados que apresentaremos reforçam que as teorias trabalhadas aqui servem para responder muitas perguntas sobre questões de possibilidades e impossibilidades geométricas.

9.1 Duplicação do Cubo

Dado um cubo de aresta qualquer a e assim volume a^3, podemos construir um cubo com o dobro de seu volume, portanto $2a^3$?

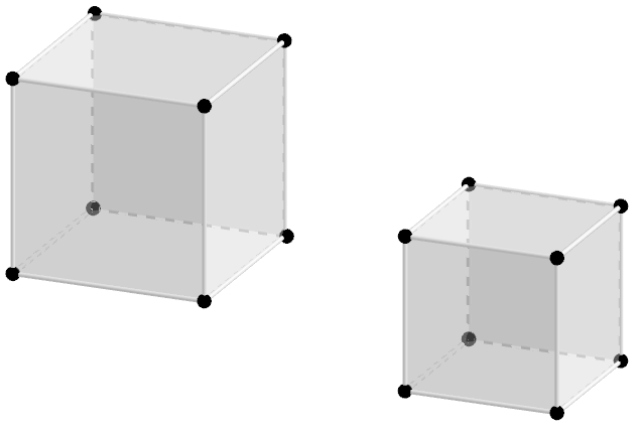

Figura 9.1: Duplicação do Cubo

Se isto fosse possível então poderíamos duplicar o cubo de aresta $a = 1$.

Tomemos um cubo de aresta medido 1, seu volume é $1^3 = 1$. Se pudéssemos construir um cubo com o dobro do seu volume, este cubo teria volume $v = 2 \cdot 1 = 2$ e sua aresta α seria tal que $\alpha^3 = 2$.

Agora tomemos o polinômio $p(x) = x^3 - 2$ pertencente a $\mathbb{Q}[x]$. Temos que $p(\alpha) = 0$ e, pelo Exemplo 4.23, $p(x)$ é irredutível sobre racionais, logo, pela Proposição 5.8, $p(x) = p_{min}(\alpha, \mathbb{Q})$. E assim, pela Proposição 5.16, $[\mathbb{Q}(\alpha) : \mathbb{Q}] = \partial p(x) = 3$. E então, α pertence a uma extensão $\mathbb{Q}(\alpha)$ de grau 3 sobre racionais que, obviamente não é uma potência de 2 e assim, pelo Teorema 7.24, α não é construtível.

9.2 Trissecção do Ângulo

Dado um ângulo de medida qualquer θ podemos construir o ângulo de medida $\frac{\theta}{3}$?

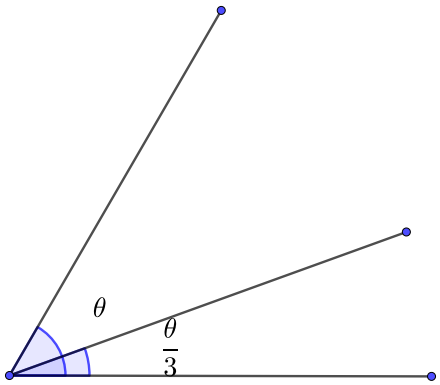

Figura 9.2: Trissecção do Ângulo

Se isso fosse possível, poderíamos fazer a trissecção do ângulo $\theta = 60°$, que é o mesmo que construir o ângulo de $\frac{\theta}{3} = 20°$. É através destes valores que provaremos esta impossibilidade.

Primeiramente vejamos três informações que utilizaremos:

i - Notemos, na Figura 9.3, (onde temos um ângulo μ inscrito no círculo unitário), que construir um ângulo μ é equivalente a construir o $\cos \mu$:

ii - Temos como válida a seguinte identidade trigonométrica, que pode ser facilmente verificada utilizando a relação trigonométrica fundamental $\cos^2 \theta + \text{sen}^2 \theta = 1$:

$$\cos(3\theta) = 4\cos^3 \theta - 3\cos \theta$$

iii - Relembremos que $\cos 60° = \frac{1}{2}$.

Dito isto, voltemos ao nosso contra-exemplo, onde aplicaremos estes resultados:

Se fosse construtível o ângulo $\frac{\theta}{3} = 20°$, teríamos que $\cos 20°$ seria construtível e, naturalmente, $2\cos 20°$ também seria. Só que, pela identidade acima,

$$\cos 60° = 4\cos^3 20° - 3\cos 20°$$

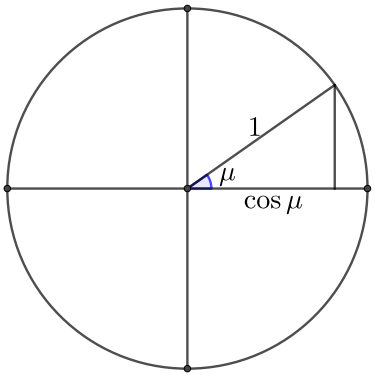

Figura 9.3: Equivalência entre construção de ângulo e seu cosseno.

E assim, $4\cos^3 20° - 3\cos 20° = \frac{1}{2}$.

Fazendo $2\cos 20° = \gamma$, descobrimos que γ é raiz do polinômio $q(x) = x^3 - 3x - 1$. E mais, pelo Exemplo 4.27, temos que $q(x)$ é irredutível sobre racionais. Portanto, pela Proposição 5.8, $q(x) = p_{min}(\gamma, \mathbb{Q})$. Com isso, pela Proposição 5.16, $[\mathbb{Q}[\gamma] : \mathbb{Q}] = \partial q(x) = 3$ e, com final semelhante à duplicação do cubo, podemos concluir pela impossibilidade da trissecção do ângulo.

9.3 Quadratura do Círculo

Dado um círculo de área igual a um A qualquer, ou seja, sua área é $\pi \cdot r^2 = A$, onde r é o raio deste círculo, podemos construir um quadrado de área igual a A?

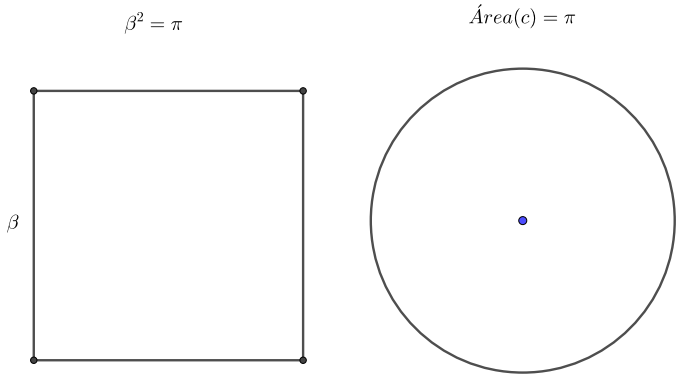

Figura 9.4: Quadratura do Círculo

Se isto fosse possível, poderíamos "quadrar" um circulo de raio 1, e assim de área $A = \pi \cdot 1^2 = \pi$. E mais, esse quadrado teria como lado β tal que $\beta \cdot \beta = \beta^2 = \pi$. E com isso, π seria construtível e desta forma algébrico, um absurdo, uma vez que, pelo item (iii) do Exemplo 5.4, π é transcendente.

Para contato com o autor:
kleklinho@hotmail.com

Referências Bibliográficas

[1] CHAMIZO, L. F. ¡Qué bonita es la teoría de Galois!. Notas de curso: 2004-2005.

[2] DELGADO, J, FRENSEL, K, CRISSAFF, L. Geometria Analitica: 2^a edição. Rio de Janeiro: SBM, 2017. (Coleção PROFMAT).

[3] DISTRIBUTED SEARCH FOR FERMAT NUMBER DIVISORS. Disponível em <http://www.fermatsearch.org/> Acesso em 19 de Agosto de 2019.

[4] DOMINGUES, H. D, IEZZI, G. Álgebra Moderna: 4^a edição. São Paulo: Atual, 2003.

[5] ENDLER, O. Teoria dos Corpos. Monografia de Matemática n44. Rio de Janeiro: IMPA, 1987.

[6] EVES, H. Introdução à História da Matemática: Tradução Hygino H. Domingues: 5^a edição. Campinas, SP: Editora da Unicamp, 2011.

[7] GARCIA, A, LEQUAIN, Y. Elementos de Álgebra. Rio de Janeiro: IMPA, 2001.(Projeto Euclides).

[8] GONÇALVES, A. Introdução à Álgebra. Rio de Janeiro: IMPA, 2006. (Projeto Euclides).

[9] HEFEZ, A. Aritmética. Rio de Janeiro: SBM, 2016. (Coleção PROFMAT).

[10] HEFEZ, A, FERNANDEZ, C. S. Introdução à Álgebra Linear. Rio de Janeiro: SBM, 2016. (Coleção PROFMAT).

[11] KAKUTA, N, SALEHYAN, P. Introdução à Teoria de Galois. São Paulo: Cultura Acadêmica Editora, 2013.

[12] MEDEIROS, N. Teoria de Galois: Notas de Curso. UFF: 2016.

[13] MEDEIROS, N. Teoria dos Grupos: Notas de Curso. UFF: 2016.

[14] NETO, A. C. M. Geometria: 1^a edição. Rio de Janeiro: SBM, 2013. (Coleção PROFMAT).

[15] PICADO, J. Corpos e Equações Algébricas. Universidade de Coimbra: Departamento de Matemática, 2009.

[16] REZENDE, J. C. Um Estudo sobre as Raízes da Unidade e suas Aplicações em Matemática: Dissertação. Universidade Estadual Paulista: Rio Claro, 2017.

[17] STEWART, I. Galois Theory: 4^a edição. Coventry, UK, University of Warwick: A Chapman & Hall/CRC, 1972.

[18] VIEIRA, E. S. Funções Holomorfas de uma Variável. Universidade Federal de Sergipe: I Colóquio de Matemática da Região Nordeste, 2011.

[19] WAGNER, E. Uma Introdução às Construções Algébricas. Rio de Janeiro: IMPA, 2015.