
UNIVERSIDADE FEDERAL DO PARÁ

INSTITUTO DE CIÊNCIAS EXATAS E NATURAIS
FACULDADE DE MATEMÁTICA

FELIPE QUARESMA PIRES

# TEORIA DE GALOIS: TEOREMA FUNDAMENTAL E ALGUNS EXEMPLOS

Belém

2023

FELIPE QUARESMA PIRES

# TEORIA DE GALOIS: TEOREMA FUNDAMENTAL E ALGUNS EXEMPLOS

Trabalho de Conclusão de Curso, apresentado à Faculdade de Matemática do Instituto de Ciências Exatas e Naturais da Universidade Federal do Pará como requisito básico para a obtenção do título de Licenciado em Matemática.

Orientador(a) Prof(a) Dra. Juliana Silva Canella.

Belém

2023

FELIPE QUARESMA PIRES

# TEORIA DE GALOIS: TEOREMA FUNDAMENTAL E ALGUNS EXEMPLOS

Trabalho de Conclusão de Curso, apresentado à Faculdade de Matemática do Instituto de Ciências Exatas e Naturais da Universidade Federal do Pará como requisito básico para a obtenção do título de Licenciado em Matemática.

Data da Apresentação: 12/12/2023

gov.br Documento assinado digitalmente
JULIANA SILVA CANELLA
Data: 12/12/2023 19:42:18-0300
Verifique em https://validar.iti.gov.br

Prof. Dra. Juliana Silva Canella (Orientadora)
Faculdade de Matemática, UFPA

gov.br Documento assinado digitalmente
ALINE GOMES DA SILVA PINTO
Data: 12/12/2023 18:28:11-0300
Verifique em https://validar.iti.gov.br

Prof. Dra. Aline Gomes da Silva Pinto (Membro Externo)
Departamento de Matemática, UnB

gov.br Documento assinado digitalmente
MARCEL VINHAS BERTOLINI
Data: 12/12/2023 19:38:18-0300
Verifique em https://validar.iti.gov.br

Prof. Dr. Marcel Vinhas Bertolini (Membro Interno)
Faculdade de Matemática, UFPA

Dedico este à todos que me fizeram ser quem eu sou.

## AGRADECIMENTOS

Sim... a viagem neste grande navio *Licenciatura em Matemática* está findando. Contemplando a bela vista no horizonte, com o *Porto Formado* nítido a frente, vejo claramente os agentes que me auxiliaram ao longo de todo esse percurso.

Inicialmente, ao mar que possibilitou iniciar a grande viagem que é a minha vida, isto é, nosso querido e amado Bom Deus. Hoje, percebo alguns dos tantos amparos, bençãos, proteção e livramentos silenciosos que Ele proporcionou nesse meu caminhar.

Angústias, medos, incertezas... esses sentimentos podem se tornarem densas e perigosas neblinas. Todavia, quando se têm luzes pra iluminar tal caminho a densidade diminui, a trajetória fica mais nítida e os passos são mais seguros. Nesse sentido, dentre esses meus faróis luminosos estão:

Mãe e pai, Joana Maria e Orlando, os meus portos seguros essenciais, agradeço pela paciência, pelo olhar bondoso educador, por me ouvirem, compreenderem minhas escolhas e por estarem sempre ao meu lado dado-me preciosos conselhos no âmbito profissional e social que ajudaram profundamente em minha edificação humana. Grandes referenciais do meu viver.

Meu irmão, Orlando Neto, por se dispor a ser um guia em minha caminhada acadêmica. Os conselhos, indicações, cuidado, preocupação, zelo... decerto foi meu primeiro orientador nessa minha viagem da graduação. Não se contendo, hoje é um virtuoso guia espiritual. Ademais, nesse último ano uma rosa veio embelezar ainda mais essa minha aventura, minha pequena e doce irmã, Rosa Maria. Mesmo com certas semanas difíceis por vim, os fins de tarde de domingo tornaram-se uma nova fonte de energia para encara-las , o simples e sincero sorriso dessa menina. Sou extremamente grato aos dois.

Meu bem, Nádia Cardoso, assim como seus olhos claros e belos, você é veio para clarear e adornar o meu andar. Durante esses anos de viagem seu ombro amigo me acalentou diversas vezes e sua criatividade empolgante me cativou e instigou-me a refletir e expandir as possibilidades de aperfeiçoar e/ou utilizar recursos didáticos com o intuito de vivificar o processo de ensino e aprendizagem. No mais, sua torcida constante e fervorosa sempre me impulsionou e continua a me estimular a dar continuidade em meu sonhos.

Meus avós, Joana do Carmo e Sebastião, por me mostrarem, através de sua própria

vivência e em suas ricas histórias e palavras, o valor de levar a vida com leveza e a primordialidade da espiritualidade, de manter uma fé viva naquele que é a essência de tudo. Meus tios e tias, padrinho e madrinha, por estarem presentes ao longo de toda minha criação sempre dispostos a me ajudar e aconselhar. Meus primos e primas, por me alegrarem em suas particularidades e diversidades. Em síntese, a todos os meus familiares, por verem na Educação um caminho favorável a construção social e profissional.

Meus amigos, os da *República dos Filhos da Associada*, Victor, Luciana, Ayla, Leonardo, Arthur, Caio e Danilo pelos distintos momentos de risos (de nossas próprias atribulações) em nossos diálogos no café da tarde e os que fiz no navio *Licenciatura em Matemática*, Thatiana, Monique, Wallace, Lidiany, Emerson, Vinícius, Alisson, Williams, Júnior, Augusto e Rafael por me acolherem em seu meio, compartilharem suas experiências e me ajudarem em minhas dificuldades. Vocês são amados tripulantes na embarcação de minha vida.

Os *oficiais* do navio *Licenciatura em Matemática*. Em nome de todo corpo docente, agradeço ao professor João Rodrigues por me possibilitar desenvolver uma iniciação científica que foi fundamental a minha edificação acadêmica e, em especial, ao Almir, Janete, Alice e Marcilene que estavam sempre disponíveis para auxiliar nas questões administrativas.

Minha querida e admirável orientadora, professora Juliana Canella. Ao ver no horizonte a tempestade chamada de *Trabalho de Conclusão de Curso (TCC)* estava apreensivo, mas estava confiante que a prece para encara-la com seriedade e tranquilidade foi perfeitamente concedida, ao pôr em meu campo de visão a professora Juliana que estava ao longe contemplando a paisagem à vista. Como é bela a intercessão de Maria Santíssima ao seu filho, nosso senhor, Jesus Cristo. Antes mesmo de perguntar à professora, ela me surpreendeu com a proposta do trabalho. Com segurança e entusiasmo deu-se o desenvolvimento deste trabalho e a tempestade *TCC* foi atravessada pacificamente. Sentimento de gratidão pela confiança e paciência, professora Juliana.

Por fim, a estes *faróis* desta minha jornada neste grande e belo navio *Licenciatura em Matemática*, talvez eu não consiga retribuí-los dignamente, mas como singelo compensar tenham certeza de que vocês sempre estarão em minhas orações. Desejo tudo de bom à vocês e que, assim como ocorreu comigo, vocês possam iluminar os caminhos dos que estão aos seus arredores. Muito obrigado!

*Crer para compreender; compreender para crer.*

**Santo Agostinho**

## RESUMO

Analisar e compreender a possibilidade de resolver equações polinomiais é uma questão que acompanha há muitos séculos o ambiente matemático e está fortemente relacionada com muito dos desenvolvimentos do saber algébrico/matemático. Nesse sentido, tem-se como essencial as teorias Matemáticas que abordam, em seus distintos aspectos, esse conteúdo. Logo, o presente trabalho busca apreender a singularidade instigadora de um avanço significativo nos estudos das equações polinomiais que ecoaram a outros ramos da Matemática, a Teoria de Galois. Para isso, almeja-se, inicialmente expor os recursos algébricos básicos (grupos, anéis, homomorfismo de anéis, corpos, extensões de corpos) à assimilação edificadora das particularidades existentes na Teoria de Galois.



PALAVRAS-CHAVE: Equações polinomiais, Teoria de Galois.

**ABSTRACT**

Analyzing and understanding the possibility of solving polynomial equations is an question that has accompanied the mathematical environment for many centuries and is strongly related to many of the developments in algebraic/mathematical knowledge. In this sense, mathematical theories that address, in their different aspects, this content are essential. Therefore, the present work seeks to understand the singularity that instigated a significant advance in the studies of polynomial equations that echoed in other branches of Mathematics, the Galois Theory. To this end, the aim is to initially expose the basic algebraic resources (groups, rings, ring homomorphism, fields, field extensions) to the edifying assimilation of the particularities existing in Galois Theory.

KEY WORDS: Polynomial equations, Galois Theory.

# Sumário

# Introdução

O estudo para determinar as *raízes* (ou *zeros*) de equações polinomiais, frequentemente associadas a fórmulas explícitas que envolvem operações como adição, subtração, multiplicação, divisão e extração de raízes a partir dos coeficientes da equação polinomial, por exemplo

$$x = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}$$

é a fórmula bastante conhecida para resolver a equação quadrática $ax^2 + bx + c = 0$ com $a, b, c \in \mathbb{R}$ e $a \neq 0$, favoreceu profundamente ao desenvolvimento matemático. De acordo com [2], após o matemático italiano Scipione de Ferro (1456-1526) elaborar uma forma de resolver a equação cúbica $x^3 + px + q = 0$ a questão fundamental, nessa temática, a ser respondida por algebristas foi se seria possível calcular os zero de qualquer equação polinomial dessa maneira.

Buscando responder tal questão, [2] comenta ainda que o matemático ítalo-francês Joseph-Louis Lagrange (1736-1813) observou que uma via possível para isso estaria na teoria das permutações, isto é, as permutações envolvendo as raízes da equação. Nesse sentido, o matemático norueguês Niels Henrik Abel (1802-1829) mostraria a não existência de qualquer fórmula explícita dos coeficientes que resolva as equações de grau 5, como Lagrange já suspeitava, [2]. Logo, apesar dessa explicação, uma indagação ainda permanecia: como caracterizar matematicamente certas equações particulares de grau 5 que teriam uma fórmula desse tipo, conhecidas antes de Abel?

A explicação para esta pergunta fora dada pelo matemático francês Évariste Galois (1811-1832), cuja obra ressoou significativamente à edificação da teoria dos grupos na Matemática moderna, bem como influenciou áreas como a Álgebra Abstrata, a Geometria Algébrica e a Teoria de Corpos. Nesse sentido, a ideia central explanada por Galois, como

abordada em [5], foi associar a cada equação polinomial um grupo específico, conhecido como *grupo de Galois* formado por todas as permutações de suas raízes, e condicionar a possibilidade de determinação de tais artifícios a uma propriedade desse grupo preservando a estrutura algébrica da equação. Em outras palavras, Galois demonstrou a existência de uma correspondência direta entre o grupo de Galois associado a uma equação e a possibilidade de encontrar suas raízes por meio de fórmulas explícitas.

Diante disso, este trabalho se propõe a desenvolver todo o maquinário necessário para a discussão da possibilidade ou não da existência destas fórmulas para determinar estas raízes (zeros) de equações polinomiais, mas não mostrará efetivamente a solubilidade destes grupos como implicação direta na resolução.

Portanto, objetivando compreender esse pilar teórico fundamental da Matemática moderna que forneceu profundas análises sobre as soluções de equações polinomiais e clareou as conexões entre a Álgebra, a Teoria dos Números e a Teoria dos Grupos, o presente trabalho se dividirá em cinco capítulos, especificamente: o primeiro capítulo abordará as noções elementares de estruturas algébricas necessárias ao desenvolvimento do trabalho (grupos, anéis, corpos e espaços vetoriais); em seguida, no segundo capítulo serão estudados anéis de polinômios em virtude de sua relevância na construção das extensões de corpos; dando continuidade, no terceiro será explanado a respeito da teoria de extensões de corpos vinculada a adjunção de raízes de polinômios; já no quarto, se desenvolverá as ideias próprias da Teoria de Galois; por fim, o capítulo 5 tratará de alguns exemplos ilustrativos da Teoria de Galois (relação biunívoca das redes de corpos com seus respectivos grupos de Galois).

# Capítulo 1

# Preliminares

Buscando estabelecer uma configuração sólida à edificação deste trabalho, o presente capítulo abordará conceitos substanciais, a saber: Grupos, Anéis, Corpos e Espaços Vetoriais. Tendo como base as referência bibliográficas [1], [3], [4], [5] e [6], as respectivas seções de cada um desses tópicos apresentará, especialmente, as noções elementares e os pontos úteis ao desenvolvimento dos capítulos posteriores.

## 1.1 Grupos

Um *grupo* é uma estrutura algébrica que advém naturalmente no estudo de aspectos matemáticos como, por exemplo, na simetria, nas transformações geométricas, na análise das soluções de equações polinomiais e etc. Esse termo foi formalmente utilizado por Évariste Galois em seus estudos de equações polinomiais na década de 1830. Todavia, com avanço evolutivo comumente vivenciado dos conceitos matemáticos para se expressar, a definição moderna de grupos precisou, inicialmente, definir uma *operação binária*.

**Definição 1** [[3], Definition 2.1] *Seja $G$ um conjunto não vazio. Uma* ***Operação Binária*** $*$ *no conjunto $G$ é um mapeamento da forma*

$$\begin{aligned} * : G \times G &\longrightarrow G \\ (a, b) &\longmapsto a * b \end{aligned} .$$

Assim, resumidamente, uma **Operação Binária** em um conjunto não vazio $G$ é uma combinação entre elementos em um par ordenado de $G$ que produz um novo elemento de $G$.

Tal condição é denominada de **Fechamento**. Em exemplificação, a adição e multiplicação usuais em $\mathbb{Z} \setminus \{0\}$ são operações binárias, mas a divisão de números inteiros não o é, pois um inteiro dividido por um outro inteiro não produzirá necessariamente um inteiro.

**Definição 2** [[3], Definition 4.1] *Sejam $G$ um conjunto não vazio e $*$ uma operação binária em $G$. Um* ***Grupo*** *$(G, *)$ é o conjunto $G$, fechado sob a operação $*$, tal que as seguintes propriedades são satisfeitas:*

*(i) Associatividade: para todo $a, b, c \in G$, tem-se:*

$$(a * b) * c = a * (b * c).$$

*(ii) Existência do Elemento Identidade: existe um elemento $e_G \in G$ tal que, para todo $x \in G$:*

$$e_G * x = x * e_G = x.$$

*(iii) Existência do Elemento Inverso: para cada $a \in G$, existe um elemento $a' \in G$ tal que:*

$$a * a' = a' * a = e_G.$$

Ressaltamos que um grupo $G$ com a propriedade de que $a * b = b * a$, para todo par de elementos $a$ e $b$ em $G$ é dito ser um **Grupo Abeliano**. Além disso, almejando simplificar a notação, iremos apenas nos referir a um grupo $G$ sem usar a identificação binária $(G, *)$, mas sabendo que existe tal operação em $G$. Para haver clareza de qual operação binária está se trabalhando, usaremos a frase "o grupo $G$ sob a operação $*$".

**Exemplo 1**

1. *Dizemos que $G$ é um* **Grupo Cíclico** *gerado por $a \in G$ se $G = \{a^n \mid n \in \mathbb{Z}\}$.*

2. *O conjunto dos números inteiros $\mathbb{Z}$ é um grupo sob a operação usual de adição, sendo $0$ o elemento identidade e $-a$ o inverso de $a \in \mathbb{Z}$. Já $\mathbb{Z} \setminus \{0\}$ sob a operação de multiplicação usual não é um grupo, pois o inverso de $3$, por exemplo, não está em $\mathbb{Z} \setminus \{0\}$ mesmo que a operação esteja definida.*

3. *O conjunto dos racionais positivos $\mathbb{Q}_+^*$ é um grupo sob a operação de multiplicação usual. O inverso de qualquer elemento $a \in \mathbb{Q}_+^*$ é $1/a = a^{-1}$.*

**4.** *O conjunto* $\mathbb{Z}_n = \{0, 1, \ldots, n-1\}$*, para* $n \geq 1$*, é um grupo sob a adição módulo* $n$*. Para qualquer* $a > 0$ *em* $\mathbb{Z}_n$*, o inverso de* $a$ *é* $n - a$*. Comumente esse grupo é denominado* ***Grupo dos Inteiros Módulo*** $n$*.*

**5.** *Seja* $A = \{1, 2, \ldots, n\}$ *um conjunto finito. O conjunto de todas as permutações (bijeções de* $A$ *em* $A$*) dos elementos de* $A$*,* $S_n$*, é um grupo sob a operação de composição de funções. Os elementos de* $S_n$ *têm a forma*

$$\begin{pmatrix} 1 & 2 & \ldots & n \\ \alpha(1) & \alpha(2) & \ldots & \alpha(n) \end{pmatrix},$$

*com* $\alpha(i)$ *a imagem de* $i \in A$ *via bijeção* $\alpha$*, para todo* $i \in A$*.*

*Ilustração: O conjunto* $S_3$ *é constituído por*

$$S_3 = \left\{ \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \right\}$$

*e*

$$\begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}.$$

*Esse grupo* $S_n$ *é chamado de* ***Grupo Simétrico*** *(ou* ***Grupo de Permutações****). Os elementos de* $S_n$ *podem ser escritos de maneira cíclica. Por exemplo, no conjunto* $S_3$ *acima, os elementos são, respectivamente, identificados por*

$$(1), (23), (13), (12), (123) \text{ e } (132).$$

**6.** *O conjunto dos quatérnios é uma extensão dos números complexos, sendo elementos da forma* $z = a + bi + cj + dk$*,* $a, b, c, d \in \mathbb{R}$ *e* $i$*,* $j$ *e* $k$ *são unidades imaginárias. O conjunto cujos elementos são identificados ao conjunto* $\{1,\ i,\ j,\ k,\ -1,\ -i,\ -j,\ -k\}$ *munido com o produto*

- $ij = -ji = k$
- $jk = -kj = i$
- $ki = -ik = j$

*é o* ***Grupo dos Quatérnios****, denotado frequentemente por* $Q_8$*.*

**7.** *O conjunto das simetrias de um polígono regular de n lados qualquer, geralmente representado por $D_n$, é um grupo denominado de* ***Grupo Diedral****.*

**8.** *Dizemos que o conjunto $K_4 = \{e, a, b, c\}$, munido com uma operação binária $*$, com e sendo o elemento neutro, é um* ***Grupo de Klein*** *se*

$$a * a = b * b = c * c = e$$

*e*

$$a * b = b * a = c, \quad b * c = c * b = a, \quad a * c = c * a = b.$$

*Observe que o grupo de Klein é abeliano.*

Listaremos, agora, dois teoremas que abordam as propriedades elementares de grupos.

**Teorema 1** [[5], Theorem 7.5] *Sejam $G$ um grupo e $a, b, c \in G$. Então:*

*i) $G$ tem um único elemento identidade.*

*ii) Lei de Cancelamento à Esquerda e à Direita:*

$$a * b = a * c \;\Rightarrow\; b = c; \qquad b * a = c * a \;\Rightarrow\; b = c.$$

*iii) Cada elemento de $G$ possui um único elemento inverso.*

Outrossim, ressalta-se uma terminologia própria dos grupos com relação a quantidade de seus elementos. O número de elementos de um grupo $G$ (finito ou infinito) é chamado **Ordem** de $G$ e é denotado por $|G|$. Aliás, se a operação em $G$ é a multiplicação e para um elemento $g \in G$ existe um menor inteiro positivo $n$ tal que $g^n = e_G$ ($ng = 0$ em notação aditiva), então esse inteiro $n$ é chamado de **Ordem do Elemento** $g$, cuja notação é $o(g)$. Se tal inteiro não existe, diremos que $g$ tem **Ordem Infinita**. Para mais, se $G$ tem ordem finita, então seus elementos terão ordem finita e a ordem de cada um deles divide a ordem de $G$.

**Exemplo 2**

**1.** *O grupo dos números inteiros $\mathbb{Z}$ (sob a operação usual de adição) e o grupo dos números racionais positivos $\mathbb{Q}_+^*$ (sob a operação de multiplicação usual) possuem ordem infinita.*

**2.** *O grupo* $\mathbb{Z}_n = \{0, 1, \ldots, n-1\}$*, sob adição módulo* $n$*, é um grupo cíclico finito,* $|Z_n| = n$*. Ademais, em* $\mathbb{Z}_6$*, notamos que*

$$1 \cdot 2 = 2, \quad 2 \cdot 2 = 4, \quad 3 \cdot 2 = 0,$$

*ou seja,* $o(2) = 3$*. Similarmente, temos que* $o(0) = 1$*,* $o(1) = 6$*,* $o(3) = 2$*,* $o(4) = 3$ *e* $o(5) = 6$*.*

**3.** *O grupo cíclico, simétrico, diedral, de Klein e dos quatérnios são finitos com ordem* $n$*,* $n!$*,* $2n$*,* $4$ *e* $8$*, respectivamente.*

## Subgrupos

Dando continuidade a abordagem sobre as propriedades básicas dos grupos, atentamos a certos subconjuntos desses grupos, os *subgrupos*:

**Definição 3** [[5], page 203] *Um subconjunto* $H$ *não vazio do grupo* $G$ *é um* ***Subgrupo*** *de* $G$ *se* $H$*, com relação a operação em* $G$*, forma um grupo, denotado por* $H \leq G$*. Um subgrupo* $H$ *de* $G$ *é dito próprio se* $H \neq G$*.*

**Exemplo 3**

**1.** *O subgrupo* $\{e_G\}$ *(elemento identidade de* $G$*) é chamado* ***Subgrupo Trivial*** *de* $G$*.*

**2.** *O conjunto dos inteiros* $\mathbb{Z}$ *sob a operação de adição é um subgrupo (próprio) de* $\mathbb{R}$ *sob a operação de adição.*

Uma maneira de verificar se um subconjunto $H \neq \emptyset$ é um subgrupo de um grupo $G$ é a seguinte:

**Teorema 2** [[3], Theorem 5.14] *Um subconjunto* $H$ *não vazio de um grupo* $G$ *é um subgrupo de* $G$ *se, e somente se,*

*i)* $H$ *é fechado sob a operação binária de* $G$*,*

*ii) o elemento identidade* $e$ *de* $G$ *está em* $H$*,*

*iii) para todo* $a \in H$ *o seu inverso* $a' \in H$ *também.*

## Classe Lateral

Agora, expõe-se uma ferramenta poderosa para analisar um grupo, a noção de *classe lateral*:

**Definição 4** [[3], Definition 10.2] *Sejam $H$ um subgrupo do grupo $G$ e $a \in G$. O subconjunto $aH = \{ah \mid h \in H\}$ de $G$ é chamado de* ***Classe Lateral à Esquerda*** *de $H$ em $G$ contendo $a$. Analogamente, o subconjunto $Ha = \{ha \mid h \in H\}$ de $G$ é chamado de* ***Classe Lateral à Direita*** *de $H$ em $G$ contendo $a$. O elemento $a$ é nomeado de* **Representante da Classe** *e o número de elementos da classe lateral $aH$ é denotado por $|aH|$ ou $|Ha|$, respectivamente.*

**Exemplo 4**

1. *Considere $G = \mathbb{Z}$ e $H = 2\mathbb{Z}$. Logo, considerando a notação de adição, as classes laterais à esquerda de $2\mathbb{Z}$ em $\mathbb{Z}$ contento o elemento qualquer $m \in \mathbb{Z}$ são da forma*

$$m + 2\mathbb{Z} = \{\ldots, m-6, m-4, m-2, 0, m+2, m+4, m+6, \ldots\}$$

*. Ou seja,*

- *Para $m = 0$*

$2\mathbb{Z} = \{\ldots, -6, -4, -2, 0, 2, 4, 6, \ldots\}$

- *Para $m = 1$*

$1+2\mathbb{Z} = \{\ldots, -5, -3, -1, 0, 3, 5, 7, \ldots\}$

2. *Seja $G = S_3$ e $H = \{(1), (13)\}$. Então, as classes laterais à esquerda de $H$ em $G$ são:*

$$\begin{aligned}
(1)H &= H, \\
(12)H &= \{(12), (12)(13)\} = \{(12), (132)\} = (132)H, \\
(13)H &= \{(13), (1)\} = H, \\
(23)H &= \{(23), (23)(13)\} = \{(23), (123)\} = (123)H.
\end{aligned}$$

3. *Tomando $H = \{0, 3, 6\}$ em $\mathbb{Z}_9$ sob a operação de adição. Assim, as classes laterais à esquerda de $H$ em $\mathbb{Z}_9$ são*

$$\begin{aligned}
0 + H &= \{0, 3, 6\} = 3 + H = 6 + H, \\
1 + H &= \{1, 4, 7\} = 4 + H = 7 + H, \\
2 + H &= \{2, 5, 8\} = 5 + H = 8 + H.
\end{aligned}$$

Algumas propriedades das classes laterais são exibidas no teorema abaixo:

**Teorema 3** [[4], Lemma 7.1] *Seja $H$ um subgrupo do grupo $G$ e os elementos $a, b \in G$. Então,*

*1)* $a \in aH$.

*2)* $aH = H$ *se, e somente se,* $a \in H$.

*3)* $(ab)H = a(bH)$ *e* $H(ab) = (Ha)b$.

*4)* $aH = bH$ *se, e somente se,* $a \in bH$.

*5)* $aH = bH$ *ou* $aH \cap bH = \emptyset$.

*6)* $aH = bH$ *se, e somente se,* $a'b \in H$.

*7)* $aH = Ha$ *se, e somente se,* $H = aHa'$.

*8)* $aH$ *é um subgrupo de* $G$ *se, e somente se,* $a \in H$.

Outro feito importante das classes laterais, observável no **Exemplo 4** é que, a união (disjunta) das classes laterais é igual ao grupo todo, como exibe um dos itens do resultado que segue:

**Teorema 4** [[5], Theorem 8.4] *Seja $H$ um subgrupo de um grupo $G$. Então,*

*i)* $G$ *é a união das classes laterias à esquerda de* $H$*:* $G = \bigcup_{a \in G} aH$ *(ou* $Ha$*).*

*ii) Para cada* $a \in G$*, existe uma bijeção* $f : H \longrightarrow aH$*. Por conseguinte, se* $H$ *é finito, quaisquer duas classes laterais à esquerda possuem o mesmo número de elementos (analogamente para classes laterais à direita).*

Ademais, destacamos que o número de classes laterais distintas (à esquerda ou à direita) do subgrupo $H$ do grupo $G$ é chamado de **Índice de $H$ em $G$** e é denotado por $[G : H]$. Se $G$ é um grupo finito, então pode haver apenas um número finito de classes laterais distintos de $H$. Dessa maneira, o índice $[G : H]$ é finito. Por outro lado, caso $G$ seja um grupo infinito, então o índice pode ser finito ou infinito. Como ilustração, no **Exemplo 4** os índices são finitos em cada um dos itens **4.1**, **4.2** e **4.3**.

O teorema seguinte expressa a relação entre a ordem de um subgrupo $H$ de um grupo finito $G$ com a ordem de $G$:

**Teorema 5 (Teorema de Lagrange)** [[5], Theorem 8.5] *Se $H$ é um subgrupo de um grupo finito $G$, então a ordem de $H$ divide a ordem de $G$. Particularmente,*

$$|G| = |H|[G : H].$$

No **Exemplo 4** item **4.3** podemos ver que $|H = \{0, 3, 6\}| = 3$ e que $[\mathbb{Z}_9 : H] = 3$. Logo, pelo **Teorema de Lagrange**, **Teorema 5**,

$$|\mathbb{Z}_9| = |H|[\mathbb{Z}_9 : H] = 3 \cdot 3 = 9,$$

como esperado.

## Subgrupo Normal e Grupo Quociente

Dentre as propriedade das classes laterais do **Teorema 3**, vimos que que $aH = Ha$ se, e somente se, $H = aHa'$ com $G$ grupo e $H$ subgrupo de $G$. Ou seja, nem sempre é válido que $aH = Ha$, para todo $a \in G$. Todavia, existe alguns cenários em que a igualdade é satisfeita. Subgrupos com essa propriedade desempenham papel ímpar na teoria dos grupos, sendo Galois o primeiro a reconhecer a importância de tais subgrupos:

**Definição 5** [[4], page 207] *Um subgrupo $N$ de um grupo $G$ é chamado* ***Subgrupo Normal*** *em $G$ se $aN = Na$, para todo $a \in G$. Iremos denotar isso por $N \lhd G$.*

**Exemplo 5**

1. *Todo subgrupo de um grupo abeliano é normal. De fato, se $N$ é um subgrupo de um grupo abeliano $G$ e $a \in G$, então*

   $$na = an, \ \forall \, n \in N,$$

   *de modo que a classe lateral à esquerda $aN$ é igual a classe lateral à direita $Na$.*

Uma forma viável de verificar se um subgrupo é normal em um grupo é através do resultado subsequente, uma versão mais fraca da propriedade *7)* do **Teorema 3**:

**Teorema 6** [[4], Theorem 9.1] *Um subgrupo $N$ de um grupo $G$ é normal em $G$ se, e somente se, $aHa' \subseteq H$, para todo $a \in G$.*

**Exemplo 6**

1. *O grupo $H = A_2(\mathbb{R})$ das matrizes $2 \times 2$ com entradas reais e determinante igual 1 formam um subgrupo normal no grupo das matrizes $2 \times 2$ com entradas reais e determinante não nulo, $G = M_2(\mathbb{R})$. De fato, dadas as matrizes $X \in M_2(\mathbb{R})$ e $Y \in A_2(\mathbb{R})$, notamos que*

$$\begin{aligned} \det(XYX^{-1}) &= (\det X)(\det Y)(\det X)^{-1} \\ &= (\det X)(\det X)^{-1} = 1. \end{aligned}$$

   *Então, $XYX^{-1} \in A_2(\mathbb{R})$, daí $X(A_2(\mathbb{R}))X^{-1} \subseteq A_2(\mathbb{R})$.*

Os subgrupos normais induzem um grupo, a saber, $G/N$, o conjunto das classes laterais à esquerda (ou à direita) de $N$ em $G$, desde que $N$ seja normal em um grupo $G$. O teorema abaixo verifica efetivamente que $G/N$ é um grupo:

**Teorema 7** [[4], Theorem 9.2] *Seja $G$ um grupo e $N$ um subgrupo normal de $G$. Então, o conjunto*

$$G/N = \{aH \mid a \in G\}$$

*é um grupo sob a operação $(aN)(bN) = abN$ com $a, b \in G$.*

O grupo $G/N$ é chamado de ***Grupo Quociente*** (ou ***Grupo Fator***) de $G$ por $N$. Ademais, o seguinte resultado elucida duas características do grupo quociente $G/N$, sendo a primeira delas obtida diretamente do *Teorema de Lagrange*:

**Teorema 8** [[5], Theorem 8.13] *Seja $N$ um subgrupo normal de um grupo $G$. Então:*

*i) Se $G$ for finito, então a ordem de $G/N$ é $|G|/|N|$.*

*ii) Se $G$ é um grupo abeliano, então $G/N$ também o é.*

## Homomorfismo entre Grupos

Frisa-se, agora, uma das ideias mais fundamentais em Álgebra, isto é, descobrir informações de um grupo ao examinar a sua interação com outros grupos via *homomorfismos*:

**Definição 6** [[5], page 220] *Sejam $(G, *)$ e $(L, \diamond)$ grupos. O mapeamento $\phi : G \longrightarrow L$ é dito ser um* ***Homomorfismo*** *se*

$$\phi(a * b) = \phi(a) \diamond \phi(b), \ \forall \, a, b \in G.$$

Desse modo, um homomorfismo entre grupos preserva sua estrutura.

**Exemplo 7**

1. *O mapa entre grupos $Id : G \longrightarrow G$ dado por $Id(a) = a$, para todo $a \in G$, é o* ***homomorfismo identidade****.*

2. *O mapeamento de grupos $e : G \longrightarrow L$ dado por $e(a) = e_L$ (elemento identidade de $L$), para todo $a \in G$, é o* ***homomorfismo trivial****.*

3. *A função $f : \mathbb{R}^* \longrightarrow \mathbb{R}^*$ dada por $f(x) = x^2$ é um homomorfismo de grupos sob a operação de multiplicação de número reais, pois*

$$f(ab) = (ab)^2 = a^2b^2 = f(a)f(b), \ \forall \, a, b \in \mathbb{R}^*.$$

*Por outro lado, sob a adição de números reais, a função $\bar{f} : \mathbb{R} \longrightarrow \mathbb{R}$ dada por $\bar{f}(x) = x^2$ não é um homomorfismo, justamente por*

$$\bar{f}(a + b) = (a + b)^2 = a^2 + 2ab + b^2$$

*que é distinto de*

$$\bar{f}(a) + \bar{f}(b) = a^2 + b^2.$$

Enfatizamos que, caso um homomorfismo entre os grupos $G$ e $L$ seja bijetor, ele será chamado de ***Isomorfismo*** entre grupos. Assim, $G$ e $L$ são grupos *Isomorfos* (algebricamente idênticos) e representaremos essa relação por $G \cong L$. Ressalta-se, ainda, um tipo de isomorfismo cujo domínio coincide com o contradomínio e que terá papel fundamental

no Capítulo 4, isto é, os **Automorfismos**. Ademais, o seguinte resultado é bastante útil ao se trabalhar com isomorfismos, pois ele, de forma geral, expõe uma propriedade dos mapeamentos bijetivos.

**Teorema 9** [[5], Theorem B.1] *Um mapeamento $f : A \to B$, com $A$ e $B$ conjuntos não vazios, é bijetivo se, e somente se, existe uma mapa $g : B \to A$ tal que*

$$g \circ f = \iota_A \quad e \quad f \circ g = \iota_B,$$

*onde $\iota_A$ e $\iota_B$ são os mapas identidade dados, respectivamente, por*

$$\begin{array}{rcl} \iota_A : A & \longrightarrow & A \\ a & \longmapsto & a \end{array} \qquad e \qquad \begin{array}{rcl} \iota_B : B & \longrightarrow & B \\ b & \longmapsto & b \end{array}$$

**Exemplo 8**

1. *Considere $P$ o grupo dos números inteiros pares sob a operação de adição usual. O mapa*

$$\begin{array}{rcl} f : \mathbb{Z} & \longrightarrow & P \\ a & \longmapsto & 2a \end{array}$$

*é um isomorfismo. De fato, para mostrar a injetividade, seja $a, b \in \mathbb{Z}$ e suponha que $f(a) = f(b)$ em $P$. Logo,*

$$\begin{array}{rcll} f(a) & = & f(b) & \\ 2a & = & 2b & \textit{(definição de } f\textit{)} \\ a & = & b & \text{(dividindo ambos os lados por 2).} \end{array}$$

*Assim, $f$ é injetivo. Ainda mais, para todo $n \in P$ temos que $n = 2k$ (inteiro par) para algum $k \in \mathbb{Z}$. Desse modo, $f(k) = 2k = n$, em outras palavras $f$ é sobrejetivo. Por fim, para todo $a, b \in \mathbb{Z}$,*

$$f(a + b) = 2(a + b) = 2a + 2b = f(a) + f(b).$$

*Portanto, $f$, como definido, é um isomorfismo de grupos e $\mathbb{Z} \cong P$.*

2. *De maneira geral, todo grupo cíclico de ordem infinita é isomorfo ao grupo $\mathbb{Z}$ e todo grupo cíclico de ordem finita $n$ é isomorfo ao grupo $\mathbb{Z}_n$.*

Antes de apresentar o próximo resultado, recorde que o conjunto ***Imagem*** de um mapeamento $f : X \longrightarrow Y$ é um subconjunto de $Y$, cuja notação é $\mathrm{Im}f$, dado por

$$\mathrm{Im}f = \{y \in Y \mid y = f(x), \text{ para algum } x \in X\}.$$

Aliás, o mapa $f$ poder ser considerado como um mapeamento sobrejetivo de $X$ em $\mathrm{Im}f$.

**Teorema 10** [[5], Theorem 7.20] *Sejam $G$ e $L$ grupos com elementos identidades $e_G$ e $e_L$, respectivamente. Se $\phi : G \longrightarrow L$ é um homomorfismo, então:*

*1)* $\phi(e_G) = e_L$.

*2)* $\phi(a') = \phi(a)'$, *para todo* $a \in G$.

*3)* $\mathrm{Im}\phi$ *é um subgrupo de* $L$.

*4) Se* $\phi$ *é injetivo, então* $G \cong \mathrm{Im}f$.

O próximo resultado estabelece a importância dos grupos de permutação para Teoria de Grupos, pois permite representar qualquer grupo, a menos de isomorfismo, como um grupo de permutações.

**Teorema 11 (Teorema de Cayley)** [[5], Theorem 7.21] *Todo grupo $G$ é isomórfico a um grupo de permutações. Em particular, se $G$ for finito de ordem $n$ então $G$ é isomorfo a um subgrupo de $S_n$*

Logo, grupos de permutação são um modelo universal para todos os grupos possíveis. Salienta-se, também, que a partir da classificação dos grupos finitos é possível identificar todos os grupos, a menos de isomorfismo, de ordem 8. Esse caso, elucidado no teorema abaixo, será útil ao Capítulo 5 para determinar os elementos de certos subgrupos.

**Teorema 12** [[6], Teorema 3.1.2] *Os únicos grupos não abelianos de ordem* 8 *são $D_4$ e $Q_8$.*

Destacamos, ainda, um conceito fundamental à associação estreita dos subgrupos normais, grupos quocientes e homomorfismo - o *kernel* (ou *Núcleo*) de um homomorfismo:

**Definição 7** [[5], page 263] *Seja $\phi : G \longrightarrow L$ um homomorfismo de grupos. Então, o* ***kernel*** *(ou* ***Núcleo****) de $\phi$ é o conjunto*

$$\ker(\phi) = \{a \in G \mid \phi(a) = e_L\}.$$

Logo, o kernel é um subconjunto de $G$ cujo elementos de $G$ são mapeados no elemento identidade de $L$ por um homomorfismo $\phi$.

**Exemplo 9**

1. *Vimos que o mapa $f : \mathbb{R}^* \longrightarrow \mathbb{R}^*$ dada por $f(x) = x^2$ é um homomorfismo de grupos sob a operação de multiplicação de número reais no* ***Exemplo 7.3****. Seu kernel é o conjunto de todos os números reais $x$ tais que $x^2 = 1$, ou seja, $\{1, -1\}$.*

Os dois teoremas seguintes mostram a relação de um homomorfismo injetor com um kernel específico e uma caracterização de grupos para o kernel.

**Teorema 13** [[5], Theorem 8.17] *Sejam $G$ e $L$ grupos e $\phi : G \longrightarrow L$ um homomorfismo. Então, $\ker(\phi) = \{e_G\}$ se, e somente se, $\phi$ é injetor.*

**Teorema 14** [[5], Theorem 8.16] *Sejam $G$ e $L$ grupos e $\phi : G \longrightarrow L$ um homomorfismo. Então, $\ker(\phi)$ é um subgrupo normal de $G$.*

Finalmente, elucidamos o teorema que relaciona estreitamente os subgrupos normais, grupos quocientes e homomorfismos:

**Teorema 15 (1º Teorema de Isomorfismo para Grupos)** [[5], Theorem 8.20] *Sejam $G$ e $L$ grupos e $\phi : G \longrightarrow L$ um homomorfismo sobrejetor. Então,*

$$G/\ker(\phi) \cong L.$$

## 1.2 Anéis

Vimos que os grupos são conjuntos não vazios munidos de uma única operação binária. No entanto, nos conjuntos numéricos, matrizes e polinômios, por exemplo, salvos as devidas

considerações, podemos definir duas operações binárias, como a adição e a multiplicação. Estamos interessados, agora, em uma estrutura algébrica na qual possamos definir, simultaneamente, duas operações binárias, chamados *anel*.

**Definição 8** [[5], page 44] *Um* ***Anel*** *é um conjunto não vazio $R$ munido com duas operações binárias, $(R, +, \cdot)$, que satisfazem as seguintes propriedades, para todo $a, b, c \in R$:*

- $(R, +)$ :

- *Fechamento: se $a, b \in R$, então $a + b \in R$.*

- *Associatividade: $a + (b + c) = (a + b) + c$.*

- *Comutatividade: $a + b = b + a$.*

- *Existência do Elemento Neutro: existe um elemento $0_R \in R$ tal que*

$$a + 0_R = a = 0_R + a, \ \forall \ a \in R.$$

- *Existência do Elemento Oposto: para cada $a \in R$, existe um elemento $-a \in R$ tal que:*

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

- $(R, +, \cdot)$ :

- *Fechamento: se $a, b \in R$, então $a \cdot b \in R$.*

- *Associatividade: $a \cdot (b \cdot c) = (a \cdot b) \cdot c$.*

- *Distributividade: $a \cdot (b + c) = (a \cdot b) + (a \cdot c)$ e $(a + b) \cdot c = (a \cdot c) + (b \cdot c)$.*

Desse modo, um anel é um grupo abeliano sob adição, possuindo também uma multiplicação associativa que é distributiva à esquerda e à direita sobre a adição.

Note que, em relação a operação de multiplicação, não temos necessariamente a comutatividade. Caso o anel $(R, +, \cdot)$ seja comutativo, diremos que $R$ é um ***Anel Comutativo***. Além disso, quando um anel $R$ contém um elemento $1_R$ satisfazendo a propriedade

$$a \cdot 1_R = a = 1_R \cdot a, \ \forall \ a \in R \qquad \text{(Identidade Multiplicativa)}$$

esse anel será chamado de ***Anel com Identidade***.

**Exemplo 10**

1. *Com a adição e multiplicação usual, o conjuntos dos números inteiros* $\mathbb{Z}$ *e dos números reais* $\mathbb{R}$ *são anéis comutativos com identidade.*

2. *O conjunto* $\mathbb{Z}_n = \{0, 1, \ldots, n-1\}$ *sob a adição e multiplicação módulo* $n$ *é um anel comutativo com identidade.*

3. *O conjunto* $M_2(\mathbb{Z})$ *das matrizes* $2 \times 2$ *sobre os inteiros é um anel com identidade* $\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$, *mas não é um anel comutativo.*

4. *Seja* $T$ *o conjunto de todas as funções de* $\mathbb{R}$ *em* $\mathbb{R}$. *Como no cálculo,* $f+g$ *e* $fg$ *são funções definidas por*

$$(f+g)(x) = f(x) + g(x) \quad e \quad (fg)(x) = f(x)g(x).$$

   *Então,* $T$ *é um anel comutativo com identidade* $e(x) = 1$ *e o elemento nulo para adição é a função* $h(x) = 0$, *para todo* $x \in \mathbb{R}$.

Outro aspecto interessante dos anéis, fundamental para certas análises posteriores, é sobre sua *característica*:

**Definição 9** [[4], page 288] *Um anel* $R$ *possui* ***Característica*** $n$ *se* $n$ *é o menor inteiro positivo tal que* $nx = 0$, *para todo* $x \in R$. *Se tal inteiro não existe, dizemos que* $R$ *tem característica* $0$.

Uma forma prática de identificar a característica de um anel $R$ com identidade multiplicativa é a seguinte:

**Teorema 16** [[3], Theorem 19.15] *Seja* $R$ *um anel com identidade multiplicativa. Suponha que* $n \cdot 1_R \neq 0_R$, *para todo inteiro positivo* $n$. *Então,* $R$ *tem característica* $0$. *Por outro lado, se* $n \cdot 1_R = 0_R$, *para algum inteiro positivo* $n$, *então o menor inteiro positivo* $n$ *com essa propriedade é a característica de* $R$.

**Exemplo 11**

1. *Os conjuntos dos números inteiros $\mathbb{Z}$, dos racionais $\mathbb{Q}$ e dos reais $\mathbb{R}$ são anéis de característica 0.*

2. *O anel $\mathbb{Z}_n$ possui característica $n$.*

Abaixo, seguem algumas as propriedade básicas de qualquer anel:

**Teorema 17** [[5, 4], Theorem 3.3, Theorem 12.2] *Seja $R$ um anel. Para todo elemento $a \in R$, seu elemento oposto (inverso aditivo) é único e, caso $a \in R$ possua inverso multiplicativo em $R$, também será único.*

**Definição 10** [[5], page 64] *Um elemento $a \neq 0_R$ em um anel $R$ é um **Divisor de Zero** desde que exista um elemento não nulo $b \in R$ tal que*

$$a \cdot b = 0_R \ \ ou \ \ b \cdot a = 0_R.$$

**Definição 11** [[5], page 48] *Um **Domínio de Integridade** é um anel comutativo $R$ com identidade $1_R \neq 0_R$ se, para quaisquer $a, b \in R$ não nulos*

$$a \cdot b = 0_R \ \ implica \ que \ \ a = 0_R \ \ \ ou \ \ \ b = 0_R.$$

*Em outras palavras, um domínio de integridade é um anel sem divisores de zero.*

**Exemplo 12**

1. *O anel $\mathbb{Z}_p$ de inteiros módulo um primo $p$ é um domínio de integridade. Por outro lado, o anel $\mathbb{Z}_n$ de inteiros módulo $n$ não é um domínio de integridade quando $n$ não é primo.*

**Teorema 18** [[5], Theorem 3.4] *Para quaisquer elementos $a$ e $b$ no anel $R$,*

*1)* $a \cdot 0_R = 0_R = 0_R \cdot a$. *Em particular,* $0_R \cdot 0_R = 0_R$.

*2)* $a \cdot (-b) = -a \cdot b = (-a) \cdot b$.

*3)* $-(-a) = a$.

*4)* $-(a + b) = (-a) + (-b)$.

*5)* $-(a-b) = (-a) + b$.

*6)* $(-a) \cdot (-b) = a \cdot b$.

*Se $R$ tem uma identidade, então*

*7)* $(-1_R) \cdot a = -a$.

## Subanéis

Semelhante à teoria de grupos onde tem-se alguns subconjuntos com propriedades algébricas herdadas, temos também, na teoria dos anéis, os chamados *subanéis*:

**Definição 12** [[4], page 274] *Um subconjunto não vazio $S$ de um anel $R$ é um* ***Subanel*** *se $S$, sob as operações de $R$, é um anel.*

Assim como nos subgrupos, existe um teste simples para determinar se um subconjunto é um subanel.

**Teorema 19** [[5], Theorem 3.6] *Seja $S$ um subconjunto não vazio de um anel $R$ tal que*

*i) $S$ é fechado sob a subtração, isto é, se $a, b \in S$, então $a - b \in S$;*

*ii) $S$ é fechado sob a multiplicação, ou seja, se $a, b \in S$, então $a \cdot b \in S$.*

*Então, $S$ é um subanel de $R$.*

**Exemplo 13**

1. $\{0\}$ *e $R$ são subanéis de qualquer anel $R$, eles são chamados de Subanéis Triviais de $R$.*

2. *Para cada inteiro positivo $n$, o conjunto*

$$n\mathbb{Z} = \{0, \pm n, \pm 2n, \pm 3n, \dots\}$$

*é um subanel dos inteiros $\mathbb{Z}$.*

**3.** *O conjunto das matrizes diagonais sobre* $\mathbb{Z}$*, isto é,*

$$\left\{ \begin{bmatrix} a & 0 \\ 0 & b \end{bmatrix} \mid a, b \in \mathbb{Z} \right\}$$

*é um subanel do anel* $M_2(\mathbb{Z})$ *das matrizes* $2 \times 2$ *sobre os inteiros.*

## Ideais e Anéis Quocientes

Na seção anterior sobre grupos, observamos que os subgrupos normais permitiram construir grupos quocientes. Veremos, nesse momento, conceitos que desempenham papeis análogos para anéis, os *ideais* e os *anéis quocientes*.

A partir deste momento, omitiremos "$\cdot$" da operação, $a \cdot b = ab$, quando não for de interpretação dúbia.

**Definição 13** [[4], page 298] *Um subanel* $I$ *de um anel* $R$ *é chamado de* ***Ideal*** *de* $R$ *se, para todo* $r \in R$ *e, para todo,* $a \in I$ *temos que* $ra$ *e* $ar$ *estão em* $I$*.*

Em outras palavras, um subanel $I$ de um anel $R$ é um ideal de $R$ se $I$ "absorve"os elementos de $R$.

**Exemplo 14**

**1.** *Para qualquer anel* $R$*,* $\{0\}$ *e* $R$ *são os ideias triviais de* $R$*.*

**2.** *Sejam* $R$ *um anel comutativo com identidade e* $a \in R$*. O conjunto* $\langle a \rangle = \{ra \mid r \in R\}$ *é um ideal de* $R$ *denominado de* ***Ideal Principal gerado por*** $a$*. Em* $\mathbb{Z}$*, todo ideal é principal.*

**3.** *Seja* $T$ *o anel de todas as funções de* $\mathbb{R}$ *em* $\mathbb{R}$*, como descrito no item* **4.** *do* ***Exemplo 10*** *com* $f(x) = x^2$*. Considere* $I$ *um subconjunto de* $T$ *constituído pelas funções* $g$ *tais que* $g(2) = 0$*. Então,* $I$ *é um subanel de* $T$*. Mais ainda, para qualquer função* $f \in T$ *e* $g \in I$*, temos que*

$$(f \cdot g)(2) = f(2)g(2) = f(2)g(0) = 0.$$

*Logo,* $f \cdot g \in I$ *e, similarmente,* $g \cdot f \in I$*. Portanto,* $I$ *é um ideal de* $T$*.*

Ademais, um ideal $I$ de $R$ é chamado de ***Ideal Próprio*** de $R$ se $I$ for um subconjunto próprio de $R$. Para mais, um ideal próprio $N$ de um anel comutativo $R$ é dito ser um ***Ideal Primo***, se

$$ab \in N \Rightarrow a \in N \text{ ou } b \in N.$$

Aliás, quando um ideal próprio $M$ de um anel comutativo $R$ é tal que, para qualquer ideal $A$ de $R$ com $M \subseteq A \subseteq R$, temos $A = M$ ou $A = R$, então $M$ é nomeado ***Ideal Maximal*** de $R$.

Outrossim, buscando identificar se um subanel é um ideal, é comum utilizar o teorema seguinte que é uma consequência imediata da definição de ideal e do **Teorema 19**:

**Teorema 20** [[4], Theorem 14.1] *Sejam $R$ um anel e $I$ um subconjunto não vazio de $R$. $I$ é um ideal de $R$ sempre que:*

*i) Para quaisquer $a, b \in I$, então $a - b \in I$;*

*ii) Se $r \in R$ e $a \in I$, então $ra \in I$ e $ar \in I$.*

Bem como os subgrupos normais induzem os grupos quocientes, os ideais levam a certos anéis, os das classes laterais à esquerda (ou à direita) de $I$ em $R$ denotado por $R/I$, sendo $I$ um ideal de um anel $R$. O resultado seguinte averigua, concretamente que $R/I$ é um anel:

**Teorema 21** [[5], Theorem 6.9 item (1)] *Sejam $R$ um anel e $I$ um ideal de $R$. Então, o conjunto*

$$R/I = \{r + I \mid r \in R\}$$

*é um anel sob as operações:*

$$(a + I) + (b + I) = (a + b) + I \quad e \quad (a + I)(b + I) = ab + I,$$

*para quaisquer $a, b \in R$.*

O anel $R/I$ é chamado de **Anel Quociente** (ou **Anel Fator**) de $R$ por $I$.

**Exemplo 15**

1. *Se $I$ é o ideal principal $\langle 5\rangle$ em $\mathbb{Z}$, então a adição e a multiplicação de classes laterais é igual a soma e produto usuais de classes de congruência (mais detalhes veja Hungerford [5] Seção 2.2). Logo, $Z/I$ é o anel $Z_5$. De modo geral, se $I$ for o ideal principal, para algum inteiro positivo $n$, $\langle n\rangle$, em $\mathbb{Z}$, então*

$$\mathbb{Z}/\langle n\rangle = \mathbb{Z}_n.$$

Além disso, o teorema abaixo apresenta duas particularidades comuns dos anéis quocientes:

**Teorema 22** [[5], Theorem 6.9, [(2),(3)]] *Sejam $R$ um anel e $I$ um ideal de $R$. Então,*

*i) Se $R$ é comutativo, então $R/I$ também o é.*

*ii) Se $R$ tem identidade, então o mesmo acontece com $R/I$.*

Antes de finalizarmos essa seção, definamos um conceito que é bastante significativo para anéis arbitrários e será de grande valia para este trabalho, as *unidades*.

**Definição 14** [[5], page 63] *Um elemento $a$ de um anel $R$ com identidade é uma* ***Unidade*** *se existe um elemento $u \in R$ tal que*

$$au = 1_R = ua.$$

*Neste caso, o elemento $u$ é chamado de* **Inverso** *de $a$ e é denotado por $a^{-1}$, por vezes também pode ser nomeado* **Inverso Multiplicativo**.

**Exemplo 16**

1. *No conjunto dos números inteiros $\mathbb{Z}$, as únicas unidades são os inteiros $1$ e $-1$.*

2. *No anel dos números reais $\mathbb{R}$, todo elemento não nulo é uma unidade: se $a \in \mathbb{R}$ e $a \neq 0$, então*

$$a \cdot \frac{1}{a} = 1.$$

O **Exemplo 16.2.** vai ser válido, de forma geral, à próxima estrutura algébrica a ser explorada - os *Corpos*.

## Homomorfismo de Anéis

Sabemos que, através dos homomorfismos, podemos compreender as peculiaridades de um grupo ao avaliar sua relação com outros grupos. Esse conceito pode ser definido para anéis com resultados igualmente importantes.

**Definição 15** [[4], page 316] *Sejam $(R,+,\cdot)$ e $(S,+,\cdot)$ anéis. Um mapeamento $\varphi$ entre $R$ e $S$ é dito ser um* ***Homomorfismo de Anéis*** *se ele preserva as duas operações dos anéis. Isto é, se, para todo $a,b \in R$*

$$\varphi(a+b) = \varphi(a) + \varphi(b) \quad e \quad \varphi(ab) = \varphi(a)\varphi(b).$$

*Um homomorfismo de anéis que é bijetor é chamado de* ***Isomorfismo*** *e diremos que os anéis são isomorfos com notação $R \cong S$.*

Como em grupos, na definição anterior, as operações à esquerda dos sinais de igualdade são em $R$, enquanto as operações à direita são em $S$.

**Exemplo 17**

1. *Para quaisquer anéis $R$ e $S$, o mapeamento nulo $z : R \longrightarrow S$ dado por $z(r) = 0_S$ para todo $r \in R$ é um homomorfismo de anéis, pois para todos $a,b \in R$*

   - $z(a+b) = 0_S = 0_S + 0_S = z(a) + z(b)$
   - $z(ab) = 0_S = 0_S \cdot 0_S = z(a)z(b)$.

2. *Se um anel qualquer $R$ e $\iota : R \longrightarrow R$ é o mapa identidade dado por $\iota(r) = r$, então para todo $a,b \in R$*

   - $\iota(a+b) = a+b = \iota(a) + \iota(b)$
   - $\iota(ab) = ab = \iota(a)\iota(b)$.

   *Como $\iota$ é claramente bijetivo, segue que ele é um isomorfismos de anéis.*

3. *O mapa $f : \mathbb{C} \longrightarrow \mathbb{C}$ dado por $f(a+bi) = a-bi$ é um isomorfismo. De fato, ele é um homomorfismos: para quaisquer números complexos $a+bi$ e $c+di$*

   - $\begin{aligned} f((a+bi)+(c+di)) &= f((a+c)+(b+d)i) \\ &= (a+c)-(b+d)i \\ &= (a-bi)+(c+di) = f(a+bi)+f(c+di); \end{aligned}$

$$\bullet\ f((a+bi)(c+di)) = f((ac-bd)+(ad+bc)i)$$
$$= (ac-bd)-(ad+bc)i$$
$$= (a-bi)(c-di) = f(a+bi)f(c+di).$$

*Para verificar a injetividade de $f$, note que se $f(a+bi) = f(c+di)$ teremos*

$$a - bi = c - di.$$

*Logo, pela igualdade de números complexos, tem-se que $a = b$ e $c = d$. Agora, a sobrejetividade de $f$ é garantida em razão de todo número complexo possuir um conjugado. Portanto, o mapeamento $f$ como definido é um isomorfismo.*

**Observação 1**

**i)** *Se $g : R \longrightarrow S$ e $f : S \longrightarrow T$ são homomorfismos de anéis, então $f \circ g : R \longrightarrow T$ é um homomorfismo de anéis.*

*Verificação:* *Precisamos mostrar que, para quaisquer $a, b \in R$*

$$(f \circ g)(a+b) = (f \circ g)(a) + (f \circ g)(b) \quad e \quad (f \circ g)(ab) = (f \circ g)(a)(f \circ g)(b).$$

*Logo,*

$$\begin{aligned}
(f \circ g)(a+b) &= f(g(a+b)) && \Big(\text{definição de composição de função}\Big)\\
&= f(g(a)+g(b)) && (g \text{ é um homomorfismo})\\
&= f(g(a)) + f(g(b)) && \Big(g(a), g(b) \in S \text{ e } f \text{ homomorfismo}\Big)\\
&= (f \circ g)(a) + (f \circ g)(b); && \Big(\text{definição composição de função}\Big)
\end{aligned}$$

*Similarmente, é possível verificar para a multiplicação. Portanto, $f \circ g : R \longrightarrow T$ é um homomorfismo de anéis.*

**ii)** *Se $f$ e $g$ são isomorfismos de anéis, então $f \circ g$ também será um isomorfismo de anéis.*

*Verificação:* *Pelo item anterior, $f \circ g$ é um homomorfismo de anéis. Resta ver que ele é bijetor. Assim,*

- *Injetor: para todo $a, b \in R$*

$$\begin{aligned}
(f \circ g)(a) &= (f \circ g)(b) \\
(f(g(a)) &= (f(g(a)) \qquad \Big(\textit{definição de composição de função}\Big) \\
g(a) &= g(b) \qquad (f \textit{ é um isomorfismo}) \\
a &= b. \qquad (g \textit{ é um isomorfismo})
\end{aligned}$$

• *Sobrejetor: Note que por $f$ ser, em particular, sobrejetivo, todo $t \in T$ é imagem de algum $s \in S$, ou seja, $f(s) = t$. Ademais, como $g$ é também sobrejetivo, todo $s \in S$ é imagem de algum $r \in R$, isto é, $g(r) = s$. Logo, para todo $t \in T$ temos que*

$$t = f(s) = f(g(r)) = (f \circ g)(r).$$

*Mostrando, desse modo, a sobrejetividade. Portanto, $f \circ g$ é um isomorfismo de anéis.*

**iii)** *Sejam $R$ e $S$ anéis com $f : R \longrightarrow S$ um isomorfismo e $g : S \longrightarrow R$ um mapeamento inverso de $f$, isto é,*

$$g \circ f = \iota_R \qquad e \qquad f \circ g = \iota_S,$$

*com $\iota_R$ e $\iota_S$ sendo, respectivamente, os mapas identidade de $R$ e $S$. Então, $g$ é também um isomorfismo de anéis.*

*Verificação: Como $f$ é um isomorfismo, isto é, um homomorfismo bijetor, segue que sua inversa $g$ também é bijetora (**Teorema 9**). Agora, vamos certificar que $g$ é um homomorfismo. Por definição,*

$$(f \circ g)(s) = f(g(s)) = s \; \forall \; s \in S.$$

*Além disso, para todo $a, b \in S$*

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

*pois $f$ é um homomorfismo. Consequentemente, como $f$ é injetivo, temos que*

$$g(a + b) = g(a) + g(b).$$

*De forma análoga, tem-se para o produto. Portanto, $g$ é um isomorfismo de anéis.*

Outrossim, similarmente como foi abordado em grupos, a ***Imagem*** de um homomorfismo entre anéis $R$ e $S$, $\varphi : R \longrightarrow S$, é um subconjunto de $S$ dado por

$$\text{Im}\varphi = \{s \in S \mid s = \varphi(r) \text{ para algum} r \in R\}.$$

E o ***kernel*** de $\varphi$ é um subconjunto de $R$ da forma

$$\ker(\varphi) = \{r \in R \mid \varphi(r) = 0_S\}.$$

Os teoremas que seguem ilustram algumas das propriedades gerais dos homomorfismos de anéis.

**Teorema 23** [[5], Theorem 3.10] *Seja $\varphi : R \longrightarrow S$ um homomorfismo de anéis. Então, para todo $a, b \in R$*

*1)* $\varphi(0_R) = 0_S$.

*2)* $\varphi(-a) = -\varphi(a)$.

*3)* $\varphi(a - b) = \varphi(a) - \varphi(b)$.

*Se $R$ é um anel com identidade e $\varphi$ é sobrejetiva, então*

*4) $S$ é um anel com identidade $f(1_R)$.*

*5) Quando $u$ é uma unidade em $R$, então $f(u)$ é uma unidade em $S$ e $f(u)^{-1} = f(u^{-1})$.*

**Teorema 24** [[5], Theorem 3.10] *Se $\varphi : R \longrightarrow S$ é um homomorfismo de anéis, então a imagem de $\varphi$ é um subanel de $S$.*

**Teorema 25** [[4], Theorem 15.2] *Seja $\varphi : R \longrightarrow S$ um homomorfismo de anéis. Então,*

$$\ker(\varphi) = \{r \in R \mid \varphi(r) = 0_S\}$$

*é um ideal de $R$.*

Novamente, de maneira similar aos grupos, caso o kernel de um homomorfismo contenha apenas o elemento $0_R$ temos:

**Teorema 26** [[5], Theorem 6.11] *Seja $\varphi : R \longrightarrow S$ um homomorfismo de anéis. Então,*

$$\ker(\varphi) = \{0_R\}$$

*se, e somente se, $\varphi$ é injetivo.*

Destacamos também o seguinte resultado o qual afirma que todo ideal é o núcleo de um homomorfismo:

**Teorema 27** [[5], Theorem 6.12] *Sejam $R$ um anel e $I$ um ideal de $R$. Então, o mapa $\psi : R \longrightarrow R/I$ dado por $\psi(r) = r + I$ é um homomorfismo sobrejetor com $ker(\psi) = I$.*

O mapeamento $\psi$ é chamado de ***Homomorfismo Natural*** de $R$ para $R/I$. Por fim, o próximo teorema nos exibe precisamente como $R$, $S$ e o kernel estão relacionados:

**Teorema 28 (1º Teorema de Isomorfismo para Anéis)** [[5], Theorem 6.13] *Sejam $R$ e $S$ anéis e considere $\varphi : R \longrightarrow S$ um homomorfismo sobrejetor de anéis. Então, o anel quociente*

$$\frac{R}{\ker(\varphi)} \cong S.$$

O **1º Teorema de Isomorfismo para Anéis** é demasiadamente útil para determinar a estrutura de anéis quocientes.

**Exemplo 18**

1. *Para determinar as imagens homomórficas do anel $\mathbb{Z}$, isto é, os possíveis contra-domínios de qualquer homomorfismo sobrejetor cujo domínio é $\mathbb{Z}$, suponhamos que $f : \mathbb{Z} \longrightarrow S$ seja um homomorfismo sobrejetivo. Se $f$ for, na realidade, um isomorfismo, então $S$ é, sob olhar de estruturas algébricas, similar a $\mathbb{Z}$. Caso $f$ seja apenas sobrejetivo, então o $Ker(f)$ é um ideal diferente de zero em $\mathbb{Z}$, pelo* ***Teorema 26****.*

   *Como $ker(f)$ é um ideal em $\mathbb{Z}$, então $ker(f)$ deve ser um ideal principal, digamos $ker(f) = \langle n \rangle$), para algum $n \neq 0$, pelo* ***Exemplo 14.2.****. Logo, pelo* ***Teorema 28****, $S$ é isomorfo a*

$$\begin{aligned} S \cong \mathbb{Z}/\mathrm{Ker}(f) &= \mathbb{Z}/\langle n \rangle \\ &= \mathbb{Z}_n. \qquad (\textit{pelo } \textbf{\textit{Exemplo 15.1.}}) \end{aligned}$$

   *Portanto, toda imagem homomórfica de $\mathbb{Z}$ é isomórfica a $\mathbb{Z}$ ou a $\mathbb{Z}_n$, para algum $n$.*

## 1.3 Corpos

Uma estrutura algébrica com aplicações diversas e primordial a este trabalho é um tipo particular de domínio de integridade, os *corpos*.

**Definição 16** [[4], page 286] *Um **Corpo** $F$ é um anel comutativo com unidade em que todo elemento não nulo é uma unidade e todo elemento diferente de zero possui inverso.*

**Exemplo 19**

1. *Para todo inteiro primo $p$, o anel $\mathbb{Z}_p$ de inteiros módulo $p$ é um corpo.*
2. *O conjunto dos números inteiros $\mathbb{Z}$ não é um corpo, pois, as únicas unidades em $\mathbb{Z}$ são $1$ e $-1$.*
3. *O conjunto dos números racionais $\mathbb{Q}$, dos reais $\mathbb{R}$ e dos complexo $\mathbb{C}$ são corpos sob as operações de adição e multiplicação usuais.*

Os dois teoremas seguintes certificam da correlação de corpos com domínios de integridade, **Definição 11**, previamente citada no início desta seção.

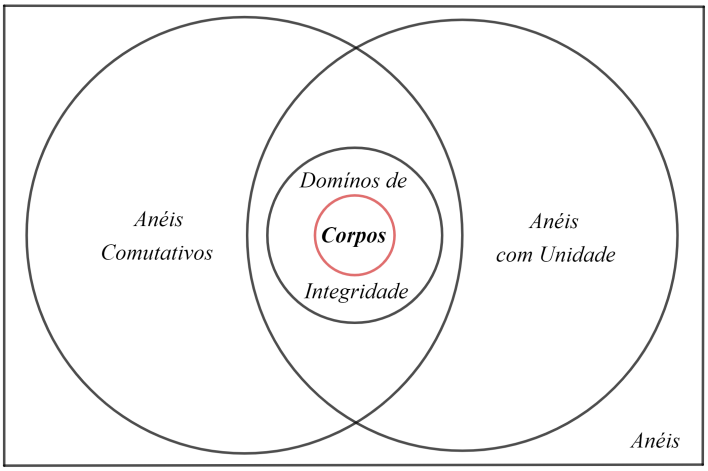
**Teorema 29** [[5], Theorem 3.8] *Todo corpo é um domínio de integridade.*

O recíproca deste teorema não é válida em geral, pois, $\mathbb{Z}$ é um domínio de integridade mas não é um corpo. Contudo, a recíproca é verdadeira para o caso de domínios de integridade finitos:

**Teorema 30** [[5], Theorem 3.9] *Todo domínio de integridade finito é um corpo.*

Tal como os subgrupos e os subanéis, um ***Subcorpo*** é um subconjunto de um corpo $K$ que, sob as operações de $K$, é visto com um corpo. Ademais, a Figura 5.1 fornece um diagrama de Venn ilustrativo contendo para os corpos.

Figura 1.1: Uma coleção de anéis.




Fonte: De autoria própria.

## 1.4 Espaços Vetoriais

Os saberes envolvendo espaços vetoriais (vetores, escalares, independência linear, base, etc.) são bastante familiares e para os estudos de *extensões de corpos*, objetos que serão estudados no Capítulo 3, e portanto são um instrumento crucial.

A partir deste momento, $F$ denotará um corpo.

**Definição 17** [[5], page 366] *Seja $F$ um corpo. Um conjunto não vazio $V$, munido de duas operações binárias*

$$\begin{array}{rcl} +: V \times V & \longrightarrow & V \\ (u, v) & \longmapsto & u + v \end{array} \qquad e \qquad \begin{array}{rcl} \text{“ ”}: F \times V & \longrightarrow & V \\ (\alpha, u) & \longmapsto & \alpha u \end{array}$$

*é dito* ***Espaço Vetorial sobre*** *$F$, ou $F$-espaço vetorial se, para quaisquer $\alpha, \beta \in F$ e $u, v \in V$:*

*i)* $(V, +)$ *é um grupo abeliano;*

*ii)* $\alpha(\beta v) = (\alpha\beta)v$;

*iii)* $(\alpha + \beta)v = \alpha v + \beta v$;

*iv)* $\alpha(u + v) = \alpha u + \alpha v$

*v)* $(1_F)u = u$

A operação "" é chamada **Multiplicação por Escalar**. Os elementos de $V$ são denominados ***Vetores*** e os de $F$ são chamados de ***Escalares***.

**Exemplo 20**

**1.** *Todo corpo $F$ é um $F$-espaço vetorial, pois as duas operações internas de $F$ podem ser vistas como a soma de vetores e a multiplicação por escalares.*

**2.** *De forma geral, para um inteiro positivo $n$, o conjunto*

$$F^n = \underbrace{F \times \cdots \times F}_{n} = \{(a_1, \ldots, a_n) \mid a_i \in F, \, \forall \, i = 1, \ldots, n\}$$

*tem uma estrutura de estrutura de espaço vetorial sobre $F$ com as operações:*

- $(a_1, \ldots, a_n) + (b_1, \ldots, b_n) = (a_1 + b_1, \ldots, a_n + b_n)$
- $\lambda \cdot (a_1, \ldots, a_n) = (\lambda a_1, \ldots, \lambda a_n)$,

*para todo $(a_1, \ldots, a_n), (b_1, \ldots, b_n) \in F^n$ e, para todo $\lambda \in F$. Logo, $\mathbb{R}^n$ é um espaço vetorial sobre $\mathbb{R}$, $\mathbb{C}^n$ é um espaço vetorial sobre $\mathbb{C}$, $(\mathbb{Z}_p)^n$, $p$ primo, é um espaço vetorial sobre $\mathbb{Z}_p$.*

**Proposição 1** [[3], Theorem 30.5] *Sejam $F$ um corpo e $V$ um $F$-espaço vetorial. Então, para todo $\alpha \in F$ e $v \in V$:*

*i)* $0_F v = 0_V$;

*ii)* $\alpha 0_V = 0_V$

*iii)* $(-\alpha)v = \alpha(-v) = -(\alpha v)$

## Independência Linear e Base

Seja $V$ um $F$-espaço vetorial. Um vetor $v \in V$ é uma ***Combinação Linear*** dos vetores $v_1, \ldots, v_n \in V$ se existirem escalares $\alpha_1, \ldots \alpha_n \in F$ tais que

$$v = \alpha_1 v_1 + \cdots + \alpha_n v_n = \sum_{i=1}^{n} \alpha_i v_i.$$

Além disso, se cada elemento de $V$ for uma combinação linear dos $v_1, \ldots, v_n$, diremos que o conjunto $\{v_1, \ldots, v_n\}$ ***Gera*** $V$ sobre $F$.

**Exemplo 21**

**1.** *O conjunto*

$$\{(1, 0, \ldots, 0), (0, 1, 0, \ldots, 0), \ldots, (0, 0, \ldots, 1)\}$$

*gera o espaço vetorial* $\mathbb{R}^n$ *sobre* $\mathbb{R}$*, pois todo elemento* $(a_1, a_2, \ldots, a_n) \in \mathbb{R}^n$ *pode ser escrito como*

$$(a_1, a_2, \ldots, a_n) = a_1(1, 0, \ldots, 0) + a_2(0, 1, 0, \ldots, 0) + \cdots + a_n(0, 0, \ldots, 1).$$

Enfatizamos, também, que é comum um espaço vetorial possuir mais de um conjunto gerador seja com um número infinito ou finito de elementos, esse último chamado *finitamente gerado*. Todavia, muitas vezes, um cenário ideal é que esse conjunto gerador seja o menor possível e que cada elemento de espaço vetorial possa ser escrito de maneira única como combinação linear dos elementos do gerador. Porém, por trás dessa ideia encontra-se um importante conceito descrito abaixo.

**Definição 18** [[5], page 368] *Um subconjunto* $\{v_1, v_2, \ldots, v_n\}$ *do espaço vetorial* $V$ *sobre um corpo* $F$ *é dito* ***Linearmente Independente*** *sobre* $F$ *se*

$$\alpha_1 v_1 + \alpha_2 v_2 + \cdots + \alpha_n v_n = 0_V,$$

*com cada* $\alpha_i \in F$*, implica que* $\alpha_i = 0_F$*, para todo* $i = 1, \ldots, n$*. Um conjunto que não é linearmente independente é chamado* ***Linearmente Dependente****.*

Observe, assim, que um conjunto $\{v_1, v_2, \ldots, v_n\}$ é linearmente dependente sobre $F$ se existem elementos $\alpha_i \in F$, $1 \leq i \leq n$, nem todos nulos tais que

$$\alpha_1 v_1 + \alpha_2 v_2 + \cdots + \alpha_n v_n = 0_V.$$

Ademais, enfatiza-se que todo conjunto contendo o vetor nulo é linearmente dependente, pois seu coeficiente em qualquer combinação linear que seja igual a zero (vetor) poderá ser diferente de zero.

**Exemplo 22**

1. *Seja o subconjunto* $B = \{(1,0),(i,0),(0,1),(0,i)\}$ *de* $\mathbb{C}^2$. *Considere* $\mathbb{C}^2$ *como espaço vetorial sobre* $\mathbb{C}$. *Então* $B$ *é linearmente dependente, pois*

$$(0,0) = 1(1,0) + i(i,0) + 0(0,1) + 0(0,i).$$

*Entretanto, se considerarmos* $\mathbb{C}^2$ *como espaço vetorial sobre* $\mathbb{R}$, $B$ *é linearmente independente, em virtude de que, para* $a,b,c,d \in \mathbb{R}$

$$\begin{aligned}(0,0) &= a(1,0) + b(i,0) + c(0,1) + d(0,i)\\ &= (a+bi, c+di)\end{aligned}$$

*o que implica em*

$$\begin{cases} a+bi &= 0\\ c+di &= 0\end{cases} \quad \Rightarrow \quad a=b=c=d=0.$$

Agora, a partir do exposto, elucidaremos o conceito importante para o estudo de extensões de corpos que aglutina a ideia de gerador e independência linear:

**Definição 19** [[1], página 49] *Um subconjunto* $\{v_1, v_2, \ldots, v_n\}$ *de um espaço vetorial* $V$ *sobre um corpo* $F$ *é uma* ***Base*** *para* $V$ *se gera* $V$ *e é linearmente independente sobre* $F$.

**Exemplo 23**

1. *O subconjunto* $\{(1,0,\ldots,0),(0,1,0,\ldots,0),\ldots,(0,0,\ldots,1)\}$ *de* $\mathbb{R}^n$ *é uma base para* $\mathbb{R}^n$ *sobre* $\mathbb{R}$, *pois já vimos que ele gera* $\mathbb{R}^n$ *e, para* $\alpha_1, \alpha_2, \ldots, \alpha_n \in \mathbb{R}$

$$\begin{aligned}(0,0,\ldots,0) &= \alpha_1(1,0,\ldots,0) + \alpha_2(0,1,0,\ldots,0) + \cdots + \alpha_n(0,0,\ldots,1)\\ &= (\alpha_1, \alpha_2, \ldots, \alpha_n).\end{aligned}$$

*Ou seja,* $\alpha_1 = \alpha_2 = \cdots = \alpha_n = 0$.

2. *Vimos anteriormente no* ***Exemplo 22.1.*** *que considerando* $\mathbb{C}^2$ *como espaço vetorial sobre* $\mathbb{R}$ *o subconjunto* $B = \{(1,0),(i,0),(0,1),(0,i)\}$ *de* $\mathbb{C}^2$ *é linearmente independente. Mas note que para quaisquer números complexos* $a+bi$ *e* $c+di$, *com* $a,b,c,d \in \mathbb{R}$, *temos*

$$\begin{aligned}(a+bi, c+di) &= (a+bi, 0) + (0, c+di)\\ &= a(1,0) + b(i,0) + c(0,1) + d(0,i).\end{aligned}$$

*Em outras palavras, $B$ gera $\mathbb{C}^2$. Portanto, $B$ é uma base para $\mathbb{C}^2$ sobre $\mathbb{R}$.*

Os dois resultados que seguem expõem uma característica dos conjuntos linearmente independentes (um limite superior do tamanho desse conjunto) e outra sobre a base de um espaço vetorial:

**Proposição 2** [[1], Proposição 2.3.4] *Sejam $F$ corpo e $V$ um $F$-espaço vetorial não nulo. Assuma que o conjunto $\{v_1, v_2, \ldots, v_m\}$ seja um gerador de $V$. Então, todo conjunto linearmente independente de vetores em $V$ tem no máximo $m$ elementos.*

**Teorema 31** [[1], Corolário 2.3.5] *Sejam $F$ corpo e $V$ um $F$-espaço vetorial não nulo finitamente gerado. Então, duas bases quaisquer de $V$ têm o mesmo número de elementos.*

O **Teorema 31** mostra que o número de elementos em uma base de um espaço vetorial sobre um corpo independe da base escolhida. Dessa maneira, tal valor é uma propriedade do espaço vetorial em questão:

**Definição 20** [[1], página 53] *Seja $V$ um espaço vetorial sobre um corpo $F$. Se $V$ admite uma base finita, então $V$ é dito ter* ***Dimensão Finita*** *sobre $F$ e chamamos de* ***Dimensão de $V$ sobre $F$*** *o número de elementos de tal base cuja notação será $[V : F]$. Caso contrário, dizemos que $V$ possui* ***Dimensão Infinita*** *sobre $F$.*

**Exemplo 24**

1. *A dimensão de $\mathbb{R}^n$ sobre $\mathbb{R}$ é $n$, pois, o subconjunto com $n$ elementos*

$$\{(1, 0, \ldots, 0), (0, 1, 0, \ldots, 0), \ldots, (0, 0, \ldots, 1)\}$$

   *de $\mathbb{R}^n$ é uma base.*

2. *Como observável no* ***Exemplo 23.2.****, a dimensão de $\mathbb{C}^n$ sobre $\mathbb{R}$ é $2n$. Enquanto se considerado sobre $\mathbb{C}$ a dimensão será $n$ como exposto no* ***Exemplo 20.2.****.*

É importante perceber que os espaços vetoriais considerados nesta seção foram com a operação soma usual, apesar de em certos casos ser possível obter espaços vetoriais com o

produto de dois vetores como, por exemplo, no espaço vetorial $M_n(F)$ da matrizes $n \times n$ sobre o corpo $F$. Para esses tipos de espaços vetoriais temos uma terminologia própria, são chamados de **Álgebra sobre um corpo**.

Precisamente, seja $F$ um corpo e $A$ um espaço vetorial sobre $F$ munido com a seguinte operação binária (por vezes chamada de *multiplicação* em $A$)

$$\begin{aligned} \cdot : A \times A &\longrightarrow A \\ (x, y) &\longmapsto x \cdot y \end{aligned} \quad .$$

Então, $A$ é uma ***Álgebra*** sobre $F$, ou simplesmente uma **$F$-álgebra**, se satisfaz as seguintes condições para todo $x, y, z \in A$ e todos os escalares $\alpha, \beta \in F$:

*(i) Distributividade à direita:* $(x + y) \cdot z = x \cdot z + y \cdot z$;

*(ii) Distributividade à esquerda:* $z \cdot (x + y) = z \cdot x + z \cdot y$;

*(iii) Compatibilidade com escalares:* $(\alpha x) \cdot (\beta y) = (\alpha\beta)(x \cdot y)$.

As três propriedades acima são outra forma de dizer que a operação binária é bilinear. Ademais, caso

*(iv) Associatividade:* $x \cdot (y \cdot z) = (x \cdot y) \cdot z$

seja satisfeita, para todo $x, y, z \in A$, dizemos que a $F$-álgebra é *Associativa*.

# Capítulo 2

# Anel de Polinômios

A ideia do que se constitui um polinômio é bastante familiar, isto é, a noção de ser uma expressão algébrica envolvendo as potências de uma *variável* ou *indeterminada*. Neste capítulo, estaremos dedicados, na Seção 2.1, em trabalhar com esses polinômios como sendo elementos de um anel, em particular no anel $F[x]$ com $F$ sendo um corpo, e estudar, em cada situação, as suas propriedades algébricas, especialmente a divisibilidade e a irredutibilidade, por vezes, análogas ao anel dos inteiros $\mathbb{Z}$.

Outrossim, na Seção 2.2, analisaremos conceitos de congruência e aritmética de classe de congruência em $F[x]$ que nos levarão a um resultado fundamental: dado qualquer polinômio sobre qualquer corpo, é possível determinar uma raiz dele em algum corpo maior. Em síntese, tendo como principais referências [3], [5], [4] e [7], destaca-se que a relevância de apreender tais saberes decorre do fato deles nos levarem, naturalmente, a uma discussão sobre extensões de corpos, tema do Capítulo 3.

## 2.1 Arimética Polinomial

A aritmética de polinômios engloba a existência de noções análogas aos conceitos baseados em números inteiros como, por exemplo, divisibilidade, primos, fatoração primária e máximos divisores comuns e iremos desenvolvê-las nesta seção. Entretanto, é necessário ter claramente a definição de anel de *polinômios*.

**Definição 21** [[4], page 334] *Considere $R$ um anel. O conjunto*

$$R[x] = \{f(x) = a_n x^n + \cdots + a_2 x^2 + a_1 x + a_0 \mid a_i \in R \text{ e algum } n \in \mathbb{Z}_+\}$$

*é chamado de* ***Anel de Polinômios*** *sobre $R$ na indeterminada $x$.*

**Exemplo 25**

1. *Os conjuntos $\mathbb{Z}[x]$, $\mathbb{Q}[x]$ e $\mathbb{R}[x]$ são anéis de polinômios familiares. Veja que o polinômio $2x^3 + x^2 + 3x + 5$ está nos três anéis, mas $\frac{5}{2}x^2 + 1$ pertence somente a $\mathbb{Q}[x]$ e $\mathbb{R}[x]$, pois o coeficiente $\frac{5}{2} \notin \mathbb{Z}$.*

Sejam $f(x) = a_n x^n + \cdots + a_1 x + a_0$ e $g(x) = b_m x^m + \cdots + b_1 x + b_0$ elementos em $R[x]$. Note que $f(x) = g(x)$ se, e somente se, $a_i = b_i$, para todo $i \in \mathbb{Z}_+$. Aliás, $f(x) = 0_R$ se, e somente se, $a_i = 0_R$, para todo $i$.

É significativo ressaltar algumas terminologias sobre os polinômios. Seja

$$f(x) = a_n x^n + \cdots + a_2 x^2 + a_1 x + a_0$$

um polinômio em $R[x]$. Chamamos $a_i \in R$ de **Coeficientes** de $f$. Se $a_n \neq 0$, com $n$ a maior potência de $x$ com essa propriedade, então diremos que $f(x)$ tem ***Grau*** $n$ e será denotado por $\partial f(x)$ e o termo $a_n$ é chamado de ***Coeficiente Líder*** de $f(x)$. Se o coeficiente líder é o elemento identidade multiplicativo de $R$, $1_R$, então dizemos que $f(x)$ é um ***Polinômio Mônico***. O polinômio $f(x) = 0_R$ não possui grau, pois não há potência de $x$ que apareça com coeficiente diferente de zero. Por fim, polinômios da forma $f(x) = a_0$, isto é, os elementos de $R$ são denominados ***Polinômios Constantes***, sendo seu grau igual a $0_R$.

O fato de $R$ ser um anel nos permite definir, entre $f(x), g(x) \in R[x]$, $\partial f(x) = n$ e $\partial g(x) = m$:

***Adição de Polinômios***:

$$\begin{aligned} f(x) + g(x) &= (a_t + b_t)x^t + \cdots + (a_2 + b_2)x^2 + (a_1 + b_1)x + (a_0 + b_0) \\ &= \sum_{i=0}^{t} (a_i + b_i)x^i \end{aligned}$$

com $t$ o máximo entre $n$ e $m$, $a_i = 0$ se $n < i$, e $b_i = 0$ se $m < i$.

***Multiplicação de Polinômios***:

$$\begin{aligned} f(x)g(x) &= d_{m+n}x^{m+n} + d_{m+n-1}x^{m+n-1} + \cdots + d_2x^2 + d_1x + d_0 \\ &= \sum_{i=0}^{m+n} d_i x^i \end{aligned}$$

sendo

$$d_i = a_ib_0 + a_{i-1}b_1 + \cdots + a_1b_{i-1} + a_0b_i = \sum_{i=0}^{m+n} a_ib_{n-i}.$$

**Exemplo 26**

**1.** *Considere os polinômios* $f(x) = 2x^3 + x^2 + 5x + 2$ *e* $g(x) = 3x^2 + 2x + 4$ *em* $\mathbb{Q}[x]$. *Então:*

- $$\begin{aligned} f(x) + g(x) &= (2x^3 + x^2 + 5x + 2) + (0x^3 + 3x^2 + 2x + 4) \\ &= (2+0)x^3 + (1+3)x^2 + (5+2)x + (2+4) \\ &= 2x^3 + 4x^2 + 7x + 6. \end{aligned}$$

- $$\begin{aligned} f(x)g(x) &= (2x^3 + x^2 + 5x + 2)(3x^2 + 2x + 4) \\ &= (0\cdot 4 + 0\cdot 2 + 2\cdot 3 + 1\cdot 0 + 5\cdot 0 + 2\cdot 0)x^5 \\ &\quad +(0\cdot 4 + 2\cdot 2 + 1\cdot 3 + 5\cdot 0 + 2\cdot 0)x^4 \\ &\quad +(2\cdot 4 + 1\cdot 2 + 5\cdot 3 + 2\cdot 0)x^3 \\ &\quad +(1\cdot 4 + 5\cdot 2 + 2\cdot 3)x^2 \\ &\quad +(5\cdot 4 + 2\cdot 2)x + (2\cdot 4) \\ &= 6x^5 + 7x^4 + 25x^2 + 24x + 8 \end{aligned}$$

A partir dessa formulação das operações de adição e multiplicação de polinômios, observe que a primeira disporá da comutativa e associativa, enquanto a multiplicação será distributiva sobre a adição. Logo, tomando os polinômios $0(x) = 0_R$ e $-f(x) = -\sum_{i=}^{n} a^i x^i$ segue-se que $R[x]$ é, de fato, um anel.

Salienta-se, ainda, se $R$ é comutativo, temos diretamente da definição de multiplicação de polinômios acima, que $R[x]$ é um anel comutativo. Além disso, caso $R$ tenha uma identidade multiplicativa $1_R$, então a identidade multiplicativa em $R[x]$ é $1_R$, pois considerando o

polinômio constante $s(x) = 1_R$ em $R[x]$ temos

$$f(x)s(x) = \sum_{i=0}^{n}(a_i \cdot 1_R)x^i = \sum_{i=0}^{n}(1_R \cdot a_i)x^i = s(x)f(x) = f(x),$$

para qualquer $f(x) \in R[x]$.

Desse modo, com definição da adição e multiplicação de polinômios dada, concluímos o seguinte resultado para o grau da soma e do produto de quaisquer dois polinômios em um anel.

**Teorema 32** [[5], [Corollary 4.3, Exercise 12 Section 4.1]] *Seja $R$ um anel. Se $f(x)$, $g(x)$, $f(x)g(x)$ e $f(x) + g(x)$ são polinômios não nulos em $R[x]$, então:*

*i)* $\partial[f(x)g(x)] \leq \partial f(x) + \partial g(x)$;

*ii)* $\partial[f(x) + g(x)] \leq \max\{\partial f(x), \partial g(x)\}$.

**Exemplo 27**

**1.** *Considere os polinômios $f(x) = 2x^3 + 3$ e $g(x) = x^2 + 5$ em $\mathbb{Z}_3[x]$. Logo,*

$$f(x)g(x) = (2x^3 + 3)(x^2 + 5) = (2 \cdot 1)x^5 + (2 \cdot 5)x^3 + (3 \cdot 1)x^2 + (3 \cdot 5) = 2x^5 + x^3,$$

*ou seja, $\partial[f(x)g(x)] = \partial f(x) + \partial g(x)$. Todavia, se $g(x) = 3x^2 + 4x$, teremos*

$$f(x)g(x) = (2x^3 + 3)(3x^2 + 4x) = (2 \cdot 3)x^5 + (2 \cdot 4)x^4 + (3 \cdot 3)x^2 + (3 \cdot 4)x = 2x^4,$$

*que possui grau 4. Porém, $\partial f(x) + \partial g(x) = 5$. Portanto, $\partial[f(x)g(x)] < \partial f(x) + \partial g(x)$.*

Frisamos também que, caso $R$ seja um domínio de integridade, é fácil verificar que $\partial[f(x)g(x)] = \partial f(x) + \partial g(x)$, por [[5], Teorema 4.2]. Além disso, outro aspecto básico a ser ponderado é sobre os elementos que são *unidades*, elementos inversos, em $R[x]$. Nesse sentido, o corolário que segue elucida a caracterização das unidades de $R[x]$:

**Corolário 1** [[5], Corollary 4.5] *Seja $R$ um domínio de integridade e $f(x) \in R[x]$. Então, $f(x)$ é uma **unidade** em $R[x]$ se, somente se, $f(x)$ é um polinômio constante que é uma unidade em $R$. Particularmente, se $R$ é um corpo, as unidades em $R[x]$ são as constantes não nulas em $R$.*

Para mais, assim como a comutatividade em $R$ é transferida para $R[x]$, o teorema abaixo é outra propriedade em que isso ocorre.

**Teorema 33** [[4], Theorem 16.1] *Se $R$ é um domínio de integridade, então $R[x]$ é um domínio de integridade.*

## Algoritmo da Divisão e Divisibilidade em F[x]

Consideraremos, a partir de agora, os polinômios com coeficientes em um corpo $F$. Nesse sentido, serão expostas algumas propriedades de $F[x]$ que, com certas modificações, são transferidas de $\mathbb{Z}$. Inicialmente, a primeira delas a ser apresentada é a afirmação para polinômios sobre um corpo $F$, análoga ao algoritmo da divisão dos números inteiros: se $a$ e $b$ são inteiros e $b \neq 0_{\mathbb{Z}}$, então existem inteiros únicos $q$ e $r$ tais que $a = bq + r$, com $0 \leq r < |b|$.

**Teorema 34 (Algoritmo da Divisão em $F[x]$)** [[4], Theorem 16.2] *Seja $F$ um corpo e os polinômios $f(x), g(x) \in F[x]$ com $g(x) \neq 0_F$. Então, existem únicos polinômios $q(x)$ e $r(x)$ em $F[x]$ tais que $f(x) = g(x)q(x) + r(x)$ sendo $r(x) = 0_F$ ou $\partial r(x) < \partial g(x)$.*

Os polinômios $q(x)$ e $r(x)$ no algoritmo de divisão são denominados de **Quociente** e **Resto** na divisão de $f(x)$ por $g(x)$. Ademais, quando consideramos os coeficientes do anel de polinômios em um corpo, podemos usar o processo de divisão longa, "método da chave", para determinar esses valores como no exemplo abaixo:

**Exemplo 28**

1. *A divisão de $f(x) = 3x^4 + x^3 + 2x^2 + x - 4$ por $g(x) = x^2 - 2x + 1$ em $\mathbb{Q}[x]$ é dada por*

$$\begin{array}{rrrrr|l} 3x^4 & +x^3 & +2x^2 & +x & -4 & x^2-2x+1 \\ \cline{6-6} -3x^4 & +6x^3 & -3x^2 & & & 3x^2+7x+13 \\ \cline{1-3} & 7x^3 & -x^2 & +x & & \\ & -7x^3 & +14x^2 & -7x & & \\ \cline{2-4} & & 13x^2 & -6x & -4 & \\ & & -13x^2 & +26x & -13 & \\ \cline{3-5} & & & 20x & -17 & \end{array}$$

*Logo,* $q(x) = 3x^2 + 7x + 13$ *e* $r(x) = 20x - 17$.

Além disso, outra característica similar ao anel do inteiros $\mathbb{Z}$ é a divisibilidade e, por conseguinte, a noção de *máximo divisor comum* (mdc).

**Definição 22** [[5], page 96] *Seja* $F$ *um corpo e* $f(x)$ *e* $g(x)$ *polinômios em* $F[x]$ *com* $g(x) \neq 0$. *Diremos que* $g(x)$ ***Divide*** $f(x)$ *se existe* $h(x) \in F[x]$ *tal que* $f(x) = g(x)h(x)$. *Nesse caso, a notação empregada será* $g(x) \mid f(x)$ *e também podemos dizer que* $g(x)$ *é um* ***Fator*** *de* $f(x)$.

**Exemplo 29**

1. *Sejam* $f(x) = x^3 + 4x^2 + x - 6$ *e* $g(x) = x + 2$ *polinômios em* $\mathbb{Q}[x]$. *Temos que* $g(x) \mid f(x)$, *pois*

$$x^3 + 4x^2 + x - 6 = (x + 2)(x^2 + 2x - 3).$$

*Aliás, todo múltiplo constante não nulo de* $x + 2$ *também divide* $x^3 + 4x^2 + x - 6$, *justamente por*

$$x^3 + 4x^2 + x - 6 = \lambda(x + 2)\left[\frac{1}{\lambda}(x^2 + 2x - 3)\right] \text{ com } \lambda \in \mathbb{Q},\ \lambda \neq 0.$$

*Observe, ainda, que* $\partial g(x) < \partial f(x)$.

O **Exemplo 29.1.** também explana os itens do seguinte resultado.

**Teorema 35** [[5], Theorem 4.7] *Seja* $F$ *um corpo e* $f(x), g(x) \in F[x]$ *com* $g(x) \neq 0_F$.

*i) Se* $g(x) \mid f(x)$, *então* $\lambda g(x) \mid f(x)$, *para qualquer* $\lambda \neq 0_F$;

*ii) Todo divisor de* $f(x)$ *tem grau menor ou igual ao* $\partial f(x)$.

Sabemos que o máximo divisor comum de dois números inteiros é o maior número inteiro que divide ambos. De maneira similar, o máximo divisor comum de dois polinômios $f(x)$ e $g(x)$ em $F[x]$ deve ser o polinômio de maior grau que divide ambos. Todavia, pelo item $i$) do **Teorema 35**, esse máximo divisor comum não seria único, pois cada um de seus múltiplos constantes não nulos teria o mesmo grau e também dividiria $f(x)$ e $g(x)$. Logo, um meio

de garantir a unicidade do mdc é considerá-lo como sendo um polinômio mônico, isto é, seu coeficiente líder é $1_F$.

Atentamos que a existência de ao menos um divisor comum mônico de $f(x)$ e $g(x)$ se dá em razão do grau desse divisor não poder exceder o $\partial f(x)$ ou $\partial g(x)$, como mostra o **Teorema 35**, devendo haver, assim, pelo menos um divisor comum mônico de maior grau.

**Definição 23** [[5], page 96] *Seja $F$ um corpo e $f(x)$ e $g(x)$ polinômios em $F[x]$. O **Máximo Divisor Comum (mdc)** de $f(x)$ e $g(x)$ é o polinômio mônico de maior grau que divide $f(x)$ e $g(x)$. De outro modo, $d(x) \in F[x]$ é o mdc de $f(x)$ e $g(x)$ se provado que $d(x)$ é mônico e*

*i) $d(x) \mid f(x)$ e $d(x) \mid g(x)$;*

*ii) Se $s(x) \mid f(x)$ e $s(x) \mid g(x)$, então $\partial s(x) \leq \partial d(x)$, com $s(x) \in F[x]$.*

**Exemplo 30**

**1.** *Em $\mathbb{Q}[x]$, observe que*

- $f(x) = 3x^4 + 13x^3 - 10x^2 = x^2(3x^2 - 2x + 15x - 10) = x^2(x + 5)(3x - 2)$,
- $g(x) = 3x^3 - 2x^2 - 3x + 2 = (3x - 2)(x^2 - 1) = (3x - 2)(x - 1)(x + 1)$.

*Notamos que $3x-2$ é um divisor comum de maior grau de $f(x)$ e $g(x)$. Nesse âmbito, o múltiplo constante não nulo $\frac{1}{3}(3x - 2) = x - \frac{2}{3}$ é um divisor comum mônico de maior grau, isto é, o mdc de $f(x)$ e $g(x)$.*

No teorema abaixo assegura a unicidade do divisor comum mônico, justificando então o uso do artigo definido "o" na definição de máximo divisor comum e no exemplo acima.

**Teorema 36** [[5], Theorem 4.8] *Sejam $F$ um corpo e $f(x), g(x) \in F[x]$, ambos não nulos. Então, existe um único máximo divisor comum $d(x)$ entre $f(x)$ e $g(x)$. Ademais, existem, não necessariamente únicos, polinômios $u(x)$ e $v(x)$ tais que*

$$d(x) = f(x)u(x) + g(x)v(x).$$

**Corolário 2** [[5], Corollary 4.9] *Sejam $F$ um corpo e $f(x), g(x) \in F[x]$, ambos não nulos. Um polinômio mônico $d(x) \in F[x]$ é o máximo divisor comum de $f(x)$ e $g(x)$ se, e somente se, $d(x)$ satisfazer as condições:*

*i) $d(x) \mid f(x)$ e $d(x) \mid g(x)$;*

*ii) Se $s(x) \mid f(x)$ e $s(x) \mid g(x)$, então $s(x) \mid d(x)$, com $s(x) \in F[x]$.*

Outro conceito importante a ser mencionado é o de *primos relativos* em $F[x]$. Os polinômios $f(x)$ e $g(x)$ são ditos ser ***Relativamente Primos*** se o máximo divisor comum entre eles é $1_F$.

**Corolário 3** [[5], Theorem 4.10] *Considere o corpo $F$ e $f(x), g(x), h(x) \in F[x]$. Se $f(x) \mid g(x)h(x)$ com $f(x)$ e $g(x)$ sendo primos relativos, então $f(x) \mid h(x)$.*

## Irredutibilidade e Fatoração Única

Ainda no contexto de analisar as propriedades do anel de polinômios $F[x]$, veremos que existem certos polinômios desempenham função semelhante aos números primos no anel dos inteiros, os *irredutíveis*.

**Definição 24** [[4], page 343] *Seja $F$ um corpo. Um polinômio $p(x) \in F[x]$ não nulo e que não seja uma unidade em $F[x]$ é dito ser* ***Irredutível*** *se, toda vez que $p(x)$ for expresso como um produto $p(x) = f(x)g(x)$, como $f(x), g(x) \in F[x]$, então $f(x)$ ou $g(x)$ é uma unidade em $F[x]$. Ou seja, $p(x) = \lambda g(x)$ (ou $p(x) = \lambda f(x)$) com $\lambda \in F$. Um elemento em $F[x]$ não sendo uma unidade, não nulo e que não é irredutível é chamado de* ***Redutível****.*

**Exemplo 31**

1. *Todo polinômio de grau 1 em $F[x]$ é irredutível. Certamente, seja $ax+b$ um polinômio em $F[x]$. Se $f(x) \mid (ax+b)$, $f(x) \in F[x]$, então*

$$ax + b = f(x)g(x)$$

*com $g(x) \in F[x]$. Como, em particular, $F$ é um domínio de integridade, segue do* ***Teorema 32****, que*

$$\partial(ax + b) = \partial f(x) + \partial g(x) \Rightarrow 1 = \partial f(x) + \partial g(x).$$

*Logo, as únicas possibilidades são* $\partial f(x) = 1$ *e* $\partial g(x) = 0$ *ou* $\partial f(x) = 0$ *e* $\partial g(x) = 1$. *Em ambos os casos ou* $f(x)$ *ou* $g(x)$ *é um polinômio constante não nulo, isto é, uma unidade em* $F[x]$. *Portanto, por definição, todo polinômio de grau* 1 *em* $F[x]$ *é irredutível.*

Em alguns casos, os polinômios irredutíveis são definidos como os que não são possíveis de serem escritos como um produto de polinômios de grau menor. O próximo teorema mostra que essa e a **Definição 24** são equivalentes.

**Teorema 37** [[5], Theorem 4.11] *Considere um corpo* $F$. *Um polinômio não nulo* $f(x)$ *é redutível em* $F[x]$ *se, e somente se,* $f(x)$ *pode ser escrito como o produto de dois polinômios de grau maior do que zero e menor do que* $\partial f$.

Ainda sob a ótica da semelhança entre as propriedades de $F[x]$ com $\mathbb{Z}$, o teorema seguinte nos mostra que polinômios irredutíveis em $F[x]$ têm essencialmente as mesmas características de divisibilidade que os primos em $\mathbb{Z}$.

**Teorema 38** [[5], Theorem 4.12] *Sejam* $F$ *um corpo e* $p(x)$ *um polinômio não constante em* $F[x]$. *Então, as condições abaixo são equivalentes:*

*i)* $p(x)$ *é irredutível.*

*ii) Se* $f(x)$ *e* $g(x)$ *são quaisquer dois polinômios em* $F[x]$ *tais que* $p(x) \mid f(x)g(x)$, *então* $p(x) \mid f(x)$ *ou* $p(x) \mid g(x)$.

*iii) Se* $r(x)$ *e* $s(x)$ *são quaisquer dois polinômios em* $F[x]$ *tais que* $p(x) = r(x)s(x)$, *então* $r(x)$ *ou* $s(x)$ *é um polinômio constante não nulo.*

**Corolário 4** [[5], Theorem 4.13] *Seja* $F$ *um corpo e* $p(x)$ *um polinômio irredutível em* $F[x]$. *Se*

$$p(x) \mid f_1(x)f_2(x)\dots f_n(x)$$

*com cada um dos* $f_i(x) \in F[x]$, *com* $1 \leq i \leq n$, *então* $p(x)$ *divide pelo menos um dos* $f_i(x)$.

Outrossim, tal como um inteiro pode ser escrito como um produto de números primos de maneira única, o mesmo acontece com os polinômios em $F[x]$, ou seja, eles podem ser

fatorados em um produto de polinômios irredutíveis em $F[x]$ de uma forma essencialmente única. Este fato é abordado no resultado que segue:

**Teorema 39** [[3], Theorem 23.20] *Seja $F$ um corpo. Todo polinômio não constante $f(x) \in F[x]$ é um produto de polinômios irredutíveis. Tal fatoração é única a menos de fatores de ordem e unidades.*

**Exemplo 32**

1. *Observe que uma fatoração de $f(x) = 2x^4 + 5x^3 - 5x - 2$ em $\mathbb{Q}[x]$ é $(2x+1)(x+2)(x+1)(x-1)$. Esses fatores são irredutíveis por terem grau 1 em $\mathbb{Q}[x]$ e são únicos a menos de unidade (constate não nula em $\mathbb{Q}$). Por exemplo,*

$$2x + 1 = \frac{1}{2}(4x + 2).$$

## Raízes de Polinômios e Redutibilidade

Ao estudar polinômios temos como essencial destacar um conceito chave, as *raízes* (*zeros*) desses elementos. A princípio, é fundamental compreender o fato de que todo polinômio em $R[x]$, $R$ um anel comutativo, induz uma função de $R$ em $R$.

Nesse contexto, sendo $R$ um anel comutativo, temos que, associada a cada polinômio

$$a_n x^n + \cdots + a_2 x^2 + a_1 x + a_0$$

em $R[x]$ está uma função $f : R \longrightarrow R$ da forma

$$\begin{aligned} f : R &\longrightarrow R \\ r &\longmapsto f(r) = \sum_{i=0}^{n} a_i r^i \end{aligned} \quad .$$

Tal função $f$ induzida por um polinômio é chamada de ***Função Polinomial***. Como exemplo, o polinômio $x^3 - 2x + 5$ em $\mathbb{R}[x]$ induz a função $f : \mathbb{R} \longrightarrow \mathbb{R}$ cuja regra é $f(\lambda) = \lambda^3 - 2\lambda + 5$, para todo $\lambda \in \mathbb{R}$.

Percebemos, apesar de clara a distinção conceitual, que a notação pode acarretar ambiguidades. Buscando evitá-las, é viável assegurar que afirmações sobre a variável $x$ ocorrem no anel $R$, enquanto as sobre a indeterminada $x$ (elemento especial do anel) acontecem no

anel polinomial $R[x]$. Assim, distanciamo-nos de sentenças falsas como $x^2 + 2x + 4 = 0$ em $\mathbb{R}$ onde $x$ é uma indeterminada (nesse caso, tal igualdade só seria verdadeira se todos os coeficientes fossem iguais a $0_R$). Por outro lado, caso $x$ seja uma variável na regra da função polinomial $f(x) = x^2 + 2x + 4$, perguntamos quais elementos de $R$ são mapeados para $0_R$ por essa função polinomial.

Esclarecidos estes detalhes, segue abaixo a definição de *raiz* de um polinômio, fundamental às respostas sobre redutibilidade ou irredutibilidade polinomial:

**Definição 25** [[5], page 106] *Seja $R$ um anel comutativo e $f(x)$ um polinômio em $R[x]$. Um elemento $a \in R$ é dito ser uma **Raiz** (ou **Zero**) do polinômio $f(x)$ se $f(a) = 0_R$, isto é, se a função polinomial induzida $f : R \longrightarrow R$ mapeia $a$ em $0_R$.*

**Exemplo 33**

1. *O polinômio $f(x) = x^2 - x - 6$ em $\mathbb{R}[x]$ tem como raízes os valores da variável $x$ para os quais $f(x) = 0_{\mathbb{R}}$, ou seja, a solução da equação $x^2 - x - 6 = 0$. De maneira usual para equações quadrática, temos que $3$ e $-2$ são as raízes de $f(x)$.*

2. *O polinômio $g(x) = x^2 - 5$ em $\mathbb{Q}[x]$ não possui raízes em $\mathbb{Q}$, pois não existe uma solução racional da equação $x^2 - 5 = 0_{\mathbb{Q}}$. Porém, se $g(x) = x^2 - 5$ é considerado como um polinômio em $\mathbb{R}[x]$, então $\sqrt{5}$ e $-\sqrt{5}$ são as suas raízes, justamente por esses valores serem solução de $x^2 - 5 = 0_{\mathbb{R}}$ em $\mathbb{R}$.*

Os próximos três resultados, provenientes do **Algoritmo da Divisão em** $F[x]$, **Teorema 34**, dão informações sobre as raízes de um polinômio, sendo o primeiro comumente visto no período do Ensino Médio como um caso especial quando $F[x] = \mathbb{R}[x]$.

**Teorema 40 (Teorema do Resto)** [[5], Theorem 4.15] *Seja $F$ um corpo, $f(x)$ um polinômio em $F[x]$ e $a \in F$. Então o resto quando $f(x)$ é dividido pelo polinômio $x - a$ é $f(a)$.*

**Exemplo 34**

1. *Para calcular o resto quando $f(x) = 6x^3 + 10x^2 - 7x + 3$ é dividido por $x + 3$, devemos observar que, no **Teorema 40**, é $x - a$ e não $x + a$. Logo, deve-se reescrever $x + 3$*

*como* $x-(-3)$ *e aplicar o Teorema do Resto com* $a=-3$. *Portanto, temos que*

$$f(-3)=6(-3)^3+10(-3)^2-7(-3)+3=-162+90+21+3=-48.$$

**Teorema 41 (Teorema do Fator)** [[5], Theorem 4.16] *Seja* $F$ *um corpo,* $f(x)$ *um polinômio em* $F[x]$ *e* $a\in F$. *Então* $a$ *é uma raiz do polinômio* $f(x)$ *se, e somente se,* $x-a$ *é um fator de* $f(x)$ *em* $F[x]$.

**Exemplo 35**

1. *Note que* 2 *é uma raiz do polinômio* $f(x)=x^5-4x^4+9x^3-14x^2+23x-30$ *em* $\mathbb{Q}[x]$. *Logo,* $x-2$ *é um fator de* $f(x)$ *em* $\mathbb{Q}[x]$, *ou seja,* $f(x)$ *é redutível em* $\mathbb{Q}[x]$.

**Corolário 5** [[5], Corollary 4.17] *Considere um corpo* $F$ *e* $f(x)$ *um polinômio não nulo de grau* $n$ *em* $F[x]$. *Então,* $f(x)$ *tem no máximo* $n$ *raízes em* $F$.

Por vezes, de maneira geral, determinar se um polinômio específico é redutível ou irredutível em um domínio de integridade pode não ser trivial, mas há casos especiais em que isso pode ser facilmente observável. Os resultados seguintes são exemplos disso:

**Teorema 42** [[4], Theorem 17.1] *Seja* $F$ *um corpo. Se* $f(x)$ *é um polinômio em* $F[x]$ *e* $\partial f(x)$ *é* 2 *ou* 3, *então* $f(x)$ *é redutível em* $F[x]$ *se, e somente se,* $f(x)$ *tem uma raiz em* $F$. *De outro modo,* $f(x)$ *é irredutível em* $F[x]$ *se, e somente se,* $f(x)$ *não tem raízes em* $F$.

**Exemplo 36**

1. *De posse do* ***Teorema 42*** *é fácil identificar se um polinômio* $f(x)$ *de grau* $\partial f(x)=2,3$ *é ou não redutível quando o corpo é* $\mathbb{Z}_p$ *(*$p\in\mathbb{Z}$ *primo), pois, nesse caso, podemos testar se* $f(a)=0$, *para* $a=0,1,\ldots,p-1$ *em* $\mathbb{Z}_p$. *Por exemplo,* 4 *é um zero de* $x^2-1$ *em* $\mathbb{Z}_3$, *assim* $x^2-1$ *é redutível em* $\mathbb{Z}_3$. *De outro modo, uma vez que* $0,1,2,3,4,5,6$ *não são zeros de* $x^2+2$ *em* $\mathbb{Z}_5$, *tem-se que* $x^2+2$ *é irredutível em* $\mathbb{Z}_5$.

**Teorema 43** [[5], Theorem 4.23] *Seja* $f(x)$ *um polinômio com coeficientes inteiros, isto é, em* $\mathbb{Z}[x]$. *Então,* $f(x)$ *é redutível em* $\mathbb{Q}[x]$ *se, e somente se,* $f(x)$ *é redutível em* $\mathbb{Z}[x]$.

A contra-positiva do **Teorema 43**, isto é, "*se $f(x)$ é um polinômio irredutível em $\mathbb{Z}[x]$, então considerando-o com um polinômio sobre $\mathbb{Q}$, ele também será irredutível*" é denominada, em algumas referências, como ***Lema de Gauss***. Por exemplo, $x^2 - 11$ em $\mathbb{Z}[x]$ é irredutível, consequentemente, esse polinômio é irredutível em $\mathbb{Q}[x]$.

Ademais, para certos polinômios de grau elevado, buscando minimizar e/ou evitar cálculos extensos, podemos verificar sua irredutibilidade através do seguinte critério:

**Teorema 44 (Critério de Eisenstein)** [[7], Theorem 3.21] *Seja*

$$f(x) = a_n x^n + \cdots + a_2 x^2 + a_1 x + a_0$$

*um polinômio em $\mathbb{Z}[x]$. Suponha que exista um primo $p$ tal que:*

*i)* $p \nmid a_n$;

*ii)* $p \mid a_i$ *com* $i = 0, \ldots, n-1$;

*iii)* $p^2 \nmid a_0$.

*Então, $f(x)$ é irredutível em $\mathbb{Q}[x]$.*

**Exemplo 37**

1. *O polinômio $x^7 - 10x^5 + 5x^4 - 25x^3 + 15x - 20$ é irredutível em $\mathbb{Q}[x]$ pelo* **Critério de Eisenstein** *com $p = 5$.*

O teorema que segue possibilita, sem a necessidade de testes ou critérios elaborados como vistos em $\mathbb{Q}[x]$, descrever explicitamente todos os polinômios irredutíveis em $\mathbb{R}[x]$ e $\mathbb{C}[x]$:

**Teorema 45 (Teorema Fundamental da Álgebra)** [[5], Theorem 4.26] *Todo polinômio não constante em $\mathbb{C}[x]$ tem uma raiz em $\mathbb{C}$.*

Logo, de imediato temos o seguinte corolário:

**Corolário 6** [[5], Corollary 4.28] *Todo polinômio não contante $f(x)$ de grau $n$ em $\mathbb{C}[x]$ pode ser escrito na forma*

$$f(x) = c(x - a_1)(x - a_2) \cdots (x - a_n),$$

*para certos* $c, a_1, a_2, \ldots, a_n \in \mathbb{C}$. *Essa fatoração é única a menos de ordem dos fatores.*

Outrossim, para identificar a redutibilidade ou não de um polinômio sobre o corpo dos números reais $\mathbb{R}$ exibimos os dois resultados abaixo que são consequências do **Teorema Fundamental da Álgebra, Teorema 45**.

**Corolário 7** [[5], Theorem 4.30] *Um polinômio* $f(x)$ *é irredutível em* $\mathbb{R}[x]$ *se, e somente se,* $f(x)$ *tem grau* 1 *ou* $f(x) = a^2 + bx + c$ *com* $b^2 - 4ac < 0$.

**Exemplo 38** *Observe que o polinômio* $f(x) = x^4 - 2x^3 + 8x^2 - 10x + 15$ *em* $\mathbb{R}[x]$ *tem como fatores os polinômios* $x^2 - 2x + 3$ *e* $x^2 + 5$ *que são irredutíveis em* $\mathbb{R}[x]$.

**Corolário 8** [[5], Corollary 4.31] *Todo polinômio* $f(x)$ *de grau ímpar em* $\mathbb{R}[x]$ *tem uma raiz em* $\mathbb{R}$.

Destacamos o termo *uma* do **Corolário 8**, pois as outras raízes podem estar em um corpo maior, neste caso $\mathbb{C}$. Por exemplo, o polinômio $f(x) = 2x^3 - 13x^2 + 17x - 10$ em $\mathbb{R}[x]$ pode ser reescrito como

$$f(x) = 2x^3 - 13x^2 + 17x - 10 = (x - 5)(2x^2 - 3x + 2)$$

em $\mathbb{R}[x]$. Logo, uma de suas raízes é o número real 5, mas o seu fator $2x^2 - 3x + 2$ não possui raízes reais, pelo **Corolário 7**. Todavia, em $\mathbb{C}$ tal fator tem os valores

$$\frac{3}{4} + \frac{\sqrt{7}}{4}i \qquad \text{e} \qquad \frac{3}{4} - \frac{\sqrt{7}}{4}i$$

como raízes em $\mathbb{C}$.

Um caso particular e importante de raízes de polinômios sobre $\mathbb{C}$ são as daqueles que são escritos na forma $x^n - 1$, denominadas *Raízes n-ésimas da Unidade*, mas ressalta-se aquelas ditas *primitivas* da unidade.

**Definição 26** [[7], Definition 1.5] *Uma* ***Raiz n-ésima Primitiva da Unidade*** *é uma raiz n-ésima de* 1 *(unidade em* $\mathbb{C}$*) que não é uma raiz m-ésima de* 1*, para qualquer divisor próprio* $m$ *de* $n$ $(m < n)$.

Como exemplo temos que $i$ é uma raiz oitava da unidade ($i^8 = 1$), mas não é uma raiz oitava primitiva da unidade, pois $i^4 = 1$, ou seja, $i$ é uma raiz quarta primitiva da unidade. Destacamos que, sobre $\mathbb{C}$, como ilustra [7], a escolha padrão oriunda da *fórmula de Moivre* para uma raiz $n$-ésima primitiva de unidade, ou seja, de $x^n = 1$ é

$$\omega = \cos\frac{2\pi}{n} + i\sin\frac{2\pi}{n}.$$

Utilizando esta fórmula e lembrando da periodicidade das funções seno e cosseno, obtemos as demais raízes $n$-ésimas primitivas da unidade dadas por $1, \omega, \omega^2, \ldots, \omega^{n-1}$, com $\omega^k \neq 1$, para $1 \leq k < n$. Observe que $\{1, \omega, \omega^2, \ldots, \omega^{n-1}\}$ são as potências de $\omega$, consequentemente esse conjunto é o grupo cíclico gerado por $\langle\omega\rangle$, ou seja,

$$\langle\omega\rangle = \{1, \omega, \omega^2, \ldots, \omega^{n-1}\}.$$

Outrossim, veja que, caso $x^n = c$, $c \in \mathbb{C}$, as raízes do polinômio $x^n - c$, isto é, as raízes $n$-ésima de $c$ serão

$$\sqrt[n]{c},\ \sqrt[n]{c}\,\omega,\ \sqrt[n]{c}\,\omega^2, \ldots,\ \sqrt[n]{c}\,\omega^{n-1}.$$

**Exemplo 39**

1. *Seja o polinômio $f(x) = x^3 - 2$ em $\mathbb{R}[x]$. Notamos, a princípio, que $a = \sqrt[3]{2}$ é uma raiz de $f(x)$. Pelas observações anteriores, vemos que as suas outras duas raízes estão em $\mathbb{C}$ e são $a\omega$ e $a\omega^2$, onde*

$$\omega = \cos\frac{2\pi}{3} + i\sin\frac{2\pi}{3} = -\frac{1}{2} + i\frac{\sqrt{3}}{2}.$$

Diante disto, vemos que todo polinômio tem suas raízes em $\mathbb{C}$. Entretanto, um questionamento natural é se necessariamente precisamos "chegar"ao corpo $\mathbb{C}$ para termos todas as raízes de um determinado polinômio. Tal questão irá ser respondida na próxima seção e está intimamente relacionada com o Capítulo 3.

## 2.2 Congruência em $F[x]$ e Classes de Congruência

Para demonstrar o principal teorema desta seção (**Teorema 53**) a noção de congruência e classe de congruência em $F[x]$, sendo $F$ um corpo, são essenciais (possuindo bastante semelhança com as da relação de congruência nos inteiros).

**Definição 27** [[5], page 125] *Seja $F$ um corpo e $f(x), g(x), p(x) \in F[x]$ com $p(x)$ não nulo. Se $p(x)$ divide $f(x) - g(x)$ diremos que $f(x)$ é* ***Congruente a*** *$g(x)$* ***módulo*** *$p(x)$ cuja notação será $f(x) \equiv g(x)(mod\ p(x))$.*

**Exemplo 40**

1. *Em $\mathbb{R}[x]$, $2x^4 + 5x^3 - 14x - 6 \equiv 9x^3 - 7x^2 + 6x - 18\ (mod\ x - 2)$, pois temos que*

$$\begin{aligned}(2x^4 + 5x^3 - 14x - 6) - (9x^3 - 7x^2 + 6x - 18) &= 2x^4 - 4x^3 + 7x^2 - 20x + 12 \\ &= (x - 2)(2x^3 + 7x - 6).\end{aligned}$$

Os dois resultados adiante expressam propriedades básicas da relação de congruência em $F[x]$.

**Teorema 46** [[5], Theorem 5.1] *Seja $F$ um corpo e $p(x)$ um polinômio em $F[x]$. Então, a relação de congruência módulo $p(x)$ é, para todo $f(x), g(x), h(x) \in F[x]$:*

*i) reflexiva: $f(x) \equiv f(x)\ (mod\ p(x))$;*

*ii) simétrica: se $g(x) \equiv f(x)\ (mod\ p(x))$, então $f(x) \equiv g(x)\ (mod\ p(x))$;*

*iii) transitiva: se $f(x) \equiv g(x)\ (mod\ p(x))$ e $g(x) \equiv h(x)\ (mod\ p(x))$, então $f(x) \equiv h(x)\ (mod\ p(x))$.*

**Teorema 47** [[5], Theorem 5.2] *Seja $F$ um corpo e $f(x)$, $g(x)$, $h(x)$, $k(x)$ e $p(x)$ polinômios em $F[x]$ com $p(x)$ não nulo. Se $f(x) \equiv g(x)\ (mod\ p(x))$ e $h(x) \equiv k(x)\ (mod\ p(x))$, então*

*i) $f(x) + h(x) \equiv g(x) + k(x)\ (mod\ p(x))$;*

*ii) $f(x)h(x) \equiv g(x)k(x)\ (mod\ p(x))$.*

A partir da compreensão da relação de congruência em $F[x]$, um conjunto surge naturalmente, o que abrange todos os polinômios congruentes a $f(x) \in F[x]$ módulo $p(x) \in F[x]$. Esse conjunto dispõe de uma notação específica, como explicitada a seguir:

**Definição 28** [[5], page 126] *Sejam $F$ um corpo e $f(x)$, $g(x)$ e $p(x)$ polinômios em $F[x]$ com $p(x)$ não nulo. A* ***Classe de Congruência*** *(ou* ***Classe de Resíduo****) de $f(x)$ módulo*

*$p(x)$ é denotada por $[f(x)]$ e consiste de todos os polinômios em $F[x]$ que são congruentes a $f(x)$ módulo $p(x)$, ou seja,*

$$[f(x)] = \{g(x) \mid g(x) \in F[x] \text{ e } g(x) \equiv f(x) \ (mod\ p(x))\}.$$

Sabemos que $g(x) \equiv f(x) \ (mod\ p(x))$ significa que $p(x)$ divide $g(x) - f(x)$, isto é,

$$g(x) - f(x) = h(x)p(x) \text{ para algum } h(x) \in F[x].$$

Ou ainda,

$$g(x) = f(x) + h(x)p(x).$$

Logo,

$$\begin{aligned} [f(x)] &= \{g(x) \mid g(x) \in F[x] \text{ e } g(x) \equiv f(x) \ (mod\ p(x))\} \\ &= \{f(x) + h(x)p(x) \mid h(x) \in F[x]\}, \end{aligned}$$

ou seja, a classe de congruência de $f(x)$ módulo $p(x)$ é constituída de todos os polinômios em $F[x]$ que possuem $f(x)$ como resto quando divididos por $p(x)$.

**Exemplo 41**

**1.** *A classe de congruência de $3x + 2$ módulo $x^2 + 5$ em $\mathbb{R}[x]$ é o conjunto*

$$\{(3x + 2) + h(x)(x^2 + 5) \mid h(x) \in \mathbb{R}[x]\},$$

*pois o **Algoritmo da Divisão** exibe que os elementos desse conjunto são todos os polinômios em $\mathbb{R}[x]$ que possuem resto $3x + 2$ quando divididos por $x^2 + 5$.*

Salientamos, também, as duas características abaixo das classes de congruência:

**Teorema 48** [[5], Theorem 5.3] *Sejam $F$ um corpo e $f(x)$, $g(x)$ e $p(x)$ polinômios em $F[x]$ com $p(x)$ não nulo. Diremos que $f(x) \equiv g(x) \ (mod\ p(x))$ se, e somente se, $[f(x)] = [g(x)]$.*

**Exemplo 42**

1. *Considere o módulo de congruência* $x^3 + x^2 + 1$ *em* $\mathbb{Z}_2[x]$*. Ao determinar a classe de congruência de* $x^2$*, notamos que*

$$x^3 \equiv x^2 + 1 \ (mod\ x^3 + x^2 + 1),$$

*pois* $x^3 - (x^2 + 1) = x^3 - x^2 - 1 = (x^3 + x^2 + 1)$ *uma vez que*

$$1 + 1 = 0 \text{ em } \mathbb{Z}_2 \Rightarrow 1 = -1.$$

*Portanto, pelo* ***Teorema 48****,* $[x^2 + 1] = [x^3]$ *em* $\mathbb{Z}_2[x]$*.*

**Corolário 9** [[5], Corollary 5.4] *Duas classes de congruência módulo* $p(x) \in F[x]$ *são disjuntas ou idênticas.*

O resultado seguinte ilustra, em $F[x]$, com $F$ corpo, a relação entre a classe $[f(x)]$ e a dos possíveis restos de $f(x)$ quando dividido por um polinômio $p(x)$ de grau $n$, além de descrever as classes de congruência módulo $p(x)$:

**Corolário 10** [[5], Corollary 5.5] *Sejam* $F$ *um corpo,* $p(x)$ *um polinômio de grau* $n$ *em* $F[x]$ *e considere o módulo de congruência* $p(x)$*.*

*i) Se* $f(x) \in F[x]$ *e* $r(x)$ *é o resto quando* $f(x)$ *é dividido por* $p(x)$*, então* $[f(x)] = [r(x)]$*.*

*ii) Considere* $S$ *como o conjunto constituído pelo polinômio nulo e todos aqueles de grau menor que* $n$ *em* $F[x]$*. Então, toda classe de congruência módulo* $p(x)$ *é a classe de algum polinômio em* $S$*, e as classes de congruência de polinômios diferentes em* $S$ *são distintas.*

**Exemplo 43**

1. *Seja* $p$ *um inteiro primo tal que* $\mathbb{Z}_p$ *seja um corpo e o* ***Algoritmo da Divisão*** *válido em* $\mathbb{Z}_p[x]$*. Se* $p(x) \in \mathbb{Z}_p[x]$ *possui grau* $k$*, então os possíveis restos da divisão por* $p(x)$ *são da forma*

$$a_{k-1}x^{k-1} + \cdots + a_1x + a_0,$$

*com $a_i \in \mathbb{Z}_p$. Logo, exitem p possibilidades para cada um dos k coeficiente $a_0, \ldots, a_{k-1}$, e, consequentemente, há $p^k$ diferentes polinômios dessa forma. Portanto, pelo* ***Corolário 10****, existe exatamente $p^k$ distintas classes de congruência módulo $p(x)$ em $\mathbb{Z}_p[x]/\langle p(x)\rangle$.*

*Ilustração: considere o módulo de congruência $x^2+x+1$ em $\mathbb{Z}_2[x]$. Os possíveis restos da divisão por $x^2+x+1$ são os polinômios da forma $ax+b$ com $a, b \in \mathbb{Z}_2$. Então, existe apenas quatro possibilidades de restos: 0, 1, $x$ e $x+1$. Portanto,*

$$\mathbb{Z}_2[x]/\langle x^2+x+1\rangle = \{[0], [1], [x], [x+1]\}.$$

O conjunto de todas as classes de congruência módulo $p(x)$ será denotado por

$$F[x]/\langle p(x)\rangle$$

e terá papel fundamental à resposta da questão a ser respondida nessa seção, ou seja, se há, para um polinômio sobre um corpo $F$, um corpo maior que contenha todas as suas raízes, sem ser obrigatoriamente $\mathbb{C}$.

Todavia, antes disto, faz-se necessário apresentar os dois seguintes teoremas, sendo assegurado por um que $F[x]/\langle p(x)\rangle$ é um anel comutativo com identidade contendo o corpo $F$ (na verdade, uma cópia isomórfica de $F$) e o outro que identifica as unidades desses conjunto.

**Teorema 49** [[5], Theorem 5.8] *Sejam $F$ um corpo e $p(x)$ um polinômio não constante em $F[x]$. Então, $F[x]/\langle p(x)\rangle$ é um anel comutativo com identidade que contém $F$ (cópia isomórfica de $F$).*

**Teorema 50** [[5], Theorem 5.9] *Sejam $F$ um corpo e $p(x)$ um polinômio não constante em $F[x]$. Se $f(x) \in F[x]$ e $f(x)$ é relativamente primo com $p(x)$ ($mdc(f(x), p(x)) = 1_F$), então $[f(x)]$ é uma unidade em $F[x]/\langle p(x)\rangle$.*

**Exemplo 44**

1. *Como $x^2-5$ é irredutível em $\mathbb{Q}[x]$ e o $mdc(x^2-5, 3x+2) = 1_{\mathbb{Q}}$, com $3x+2 \in \mathbb{Q}[x]$, temos que $x^2-5$ e $3x+2$ são relativamente primos. Logo, pelo* ***Teorema 50****, $[3x+2]$ é uma unidade no anel $\mathbb{Q}[x]/\langle x^2-5\rangle$.*

## A Estrutura de F[x]/⟨p(x)⟩ quando p(x) é Irredutível

Observamos anteriormente que para um dado corpo $F$ e um polinômio não nulo $p(x)$ em $F[x]$, o conjunto de classes de congruência módulo $p(x)$, $F[x]/\langle p(x)\rangle$, é um anel comutativo com identidade. Todavia, quando $p(x)$ é irredutível tal anel é, na verdade, um corpo.

**Teorema 51** [[5], Theorem 5.10] *Sejam $F$ um corpo e $p(x)$ um polinômio não constante em $F[x]$. Então, as sentenças abaixo são equivalentes:*

*1) $p(x)$ é irredutível em $F[x]$.*

*2) $F[x]/\langle p(x)\rangle$ é um corpo.*

*3) $F[x]/\langle p(x)\rangle$ é um domínio de integridade.*

Outrossim, no contexto em que $F$ é um corpo e $p(x)$ é um polinômio irredutível em $F[x]$, pelos **Teoremas 49** e **50** podemos considerar $F$ como um subcorpo de $F[x]/\langle p(x)\rangle$, ou dizer que $F[x]/\langle p(x)\rangle$ é um ***Corpo de Extensão*** de $F$. Diante disso, os polinômios em $F[x]$ podem ser considerados como tendo coeficientes no corpo maior $F[x]/\langle p(x)\rangle$. Logo, naturalmente pergunta-se sobre as raízes desse polinômios em $F[x]/\langle p(x)\rangle$, de modo particular, se o polinômio irredutível $p(x)$ em $F[x]$ tem raízes no corpo de extensão $F[x]/\langle p(x)\rangle$.

**Exemplo 45**

1. *O polinômio $p(x) = x^3 - 3x + 5$ não possui raízes em $\mathbb{Z}_5$ (basta calcular o valor de $p(x)$ para cada elemento de $\mathbb{Z}_5$) e, como elucida o **Teorema 42**, ele será irredutível em $\mathbb{Z}_5[x]$. Assim, $K = \mathbb{Z}_5[x]/\langle x^3 - 3x + 5\rangle$ é, pelo **Teorema 51**, um corpo de extensão de $\mathbb{Z}_5$. Note que*

   $$x^3 - 3x + 5 \equiv 0 \ (mod\ x^3 - 3x + 5) \quad \Rightarrow \quad [x^3 - 3x + 5] = [0] \text{ em } K \ (\textbf{Teorema 48}).$$

   *Portanto, $\lambda = [x]$ é uma raiz de $p(x) = x^3 - 3x + 5$ em $K$, pois, utilizando a aritmética de classes de congruência, temos que*

   $$\begin{aligned} p(\lambda) &= \lambda^3 - 3\lambda + 5 \\ &= [x]^3 - 3[x] + 5 \\ &= [x^3 - 3x + 5] = [0]. \end{aligned}$$

O exemplo acima é um caso específico do teorema seguinte.

**Teorema 52** [[4], Theorem 5.11] *Sejam $F$ um corpo e $p(x)$ um polinômio irredutível em $F[x]$. Então, $F[x]/\langle p(x)\rangle$ é um corpo de extensão de $F$ que contém uma raiz de $p(x)$.*

*Demonstração:* Considere $K = F[x]/\langle p(x)\rangle$ e $p(x) = a_n x^n + \cdots + a_1 x + a_0$, com $a_i \in F$, $0 \leq i \leq n$. Pelos **Teoremas 49** e **51**, $K$ é um corpo de extensão de $F$. Como cada $a_i$, $0 \leq i \leq n$, está em $F$, então $a_i \in K$.

Vamos mostrar que $\lambda = [x] \in K$ é uma raiz de $p(x)$. Pela soma e produto de classes de congruência em $K$, temos que

$$\begin{aligned} p([x]) &= a_n[x]^n + \cdots + a_1[x] + a_0 \\ &= [a_n x^n + \cdots + a_1 x + a_0] \\ &= [p(x)] = [0_F] \qquad (\text{pois } p(x) \equiv 0_F \ (mod\ p(x))). \end{aligned}$$

Portanto, $\lambda \in K$ é uma raiz de $p(x)$.

□

**Exemplo 46**

1. *O corpo $K = \mathbb{Q}[x]/\langle x^2 - 5\rangle$ é um corpo de extensão de $\mathbb{Q}$ que contém a raiz $\lambda = [x]$ do polinômio $x^2 - 5$. Em $K$, $\lambda$ é o elemento no qual seu quadrado é 5.*

É instrutivo considerar os números complexos deste ponto de vista. Em vez de perguntar sobre um número cujo quadrado é -1, perguntamos: "Existe um corpo contendo $\mathbb{R}$ no qual o polinômio $x^2 + 1$ tem raiz?" Como $x^2 + 1$ é irredutível em $\mathbb{R}[x]$, o **Teorema 52** nos diz que a resposta é sim: $K = \mathbb{R}[x]/\langle x^2 + 1\rangle$ é um corpo de extensão de $\mathbb{R}$ que contém uma raiz de $x^2 + 1$, a saber uma $\lambda = [x]$. No corpo $K$, $\lambda$ é o elemento cujo quadrado é $-1$.

Por fim, segue o último resultado deste capítulo que responderá a questão suscitada ao término da seção anterior (verifique que o **Teorema 52** já norteou a conclusão).

**Teorema 53 (Teorema de Kronecker)** [[4], Theorem 19.1] *Sejam $F$ um corpo e $f(x)$ um polinômio não constante em $F[x]$. Então, existe um corpo de extensão $K$ de $F$ tal que $f(x)$ tem um zero.*

*Demonstração:* Pelo **Teorema 39**, $f(x)$ tem um fator irredutível $p(x)$ em $F[x]$. Ademais, como vimos no **Teorema 52**, $K = F[x]/\langle p(x)\rangle$ é um corpo de extensão de $F$ que contém uma raiz de $p(x)$. Portanto, em virtude de toda raiz de $p(x)$ ser uma raiz de $f(x)$, $K$ contém uma raiz de $f(x)$.

□

Do exposto, a indagação da existência ou não de um corpo contendo $F$ um corpo no qual um polinômio em $F[x]$ tem suas raiz, foi claramente respondida pelo **Teorema 53**, isto é, existe de fato tal corpo. Logo, o eixo basilar das ponderações sobre as raízes de um polinômio passam a ser direcionados as extensões de corpos que as contêm. Nesse sentido, abordaremos no próximo capítulo as especificidades desse conceito, essencial a temática de polinômios.

# Capítulo 3

# Extensão de Corpos

Na generalização da Teoria de Galois para corpos arbitrários, originalmente desenvolvida em termos de polinômios no corpo dos complexos, o polinômio deixa de ser o foco central de estudo e uma extensão de corpo relacionada a ele torna-se o objetivo principal das análises tendo, desse ponto de vista, importantes vantagens conceituais. Logo, no atual capítulo definiremos precisamente as extensões de corpos (conceito previamente introduzido ao término do Capítulo 2) e desenvolveremos conjunturas fundamentais sobre corpos necessárias aos resultados do Capítulo 4, sendo [3] e [5] as referências bibliográficas empregadas.

## 3.1 Aplicações de conceitos de Espaços Vetoriais para Extensões de Corpos

Diante do entendimento das características de um espaços vetoriais abordados na Seção 1.4 do Capítulo 1, observamos que, para qualquer corpo $F$, o anel de polinômios $F[x]$ pode ser visto como um espaço vetorial sobre $F$ sendo que a adição de vetores é a adição ordinária de polinômios em $F[x]$ e a multiplicação por escalar $av$ de um elemento de $F[x]$ por um elemento de $F$ é a multiplicação ordinária em $F[x]$. Os itens $i$) e $ii$) da definição de espaço vetorial seguem imediatamente do fato de $F[x]$ ser um anel com unidade.

Outrossim, podemos considerar $\mathbb{R}$ como um espaço vetorial sobre $\mathbb{Q}$, com adição de números reais (vetores) definida como habitual e com multiplicação por escalar sendo a multiplicação ordinária (o produto de um número racional por um real é um número real).

De modo similar, temos que $\mathbb{C}$ pode ser visto como espaço vetorial sobre $\mathbb{R}$. Para esses tipos de casos podemos, de forma geral, usar uma terminologia própria que será definida abaixo.

**Definição 29** [[3], Definition 29.1] *Se $F$ e $K$ são corpos com $F \subseteq K$, diremos que $K$ é um* ***Corpo de Extensão*** *de $F$, ou ainda, que $K$ é uma* ***Extensão*** *de $F$.*

Desta forma, podemos ver $\mathbb{R}$ como um corpo de extensão de $\mathbb{Q}$, e $\mathbb{C}$ como um corpo de extensão de $\mathbb{R}$ e $\mathbb{Q}$. Ressaltamos, ainda, que para auxiliar no entendimento das extensões de corpos, as representaremos por meio de diagramas, como o ao lado, estando o corpo maior no topo.


Vemos, pois, que $\mathbb{R}$ é um corpo de extensão do corpo $\mathbb{Q}$ e tem a propriedade de ser considerado como um espaço vetorial sobre $\mathbb{Q}$. Tal ocorrência se nota de maneira generalizada: *se $K$ é um corpo de extensão do corpo $F$, então $K$ é um espaço vetorial sobre $F$, com a adição de vetores e a multiplicação por escalar sendo, respectivamente, a adição e multiplicação ordinária em $K$.* Lembrando que o produto de um elemento do subcorpo $F$ e um elemento de $K$ está em $K$.

Os dois teoremas a serem apresentados a seguir são relevantes para o decorrer deste capítulo, bem como para o próximo, justamente por estarem relacionados a ideia de *extensão de dimensão finita* de um corpo. Porém, antes de elucidá-los, precisamos compreender a noção de *extensão de dimensão finita*.

**Definição 30** [[5], page 372] *Se $K$ um corpo de extensão de um corpo $F$, enunciaremos que $K$ é uma* ***Extensão de Dimensão Finita (ou Infinita)*** *sobre $F$ se $K$, visto como espaço vetorial sobre $F$, tem dimensão finita (ou infinita) sobre $F$. Denotaremos a dimensão de $K$ sobre $F$ por $[K : F]$.*

**Observação 2** *Considere $K$ um corpo de extensão de um corpo $F$. Então, $[K : F] = 1$ se, e somente se, $K = F$.*

*De fato,*

*($\Longrightarrow$) Pela definição de extensão de corpo, $F \subseteq K$. Ademais, se $[K : F] = 1$ e $\{u\}$ é uma base para a extensão, então, pela definição de base, todo elemento de $K$ é da forma*

*$\alpha u$ para algum $\alpha \in F$. Em particular, $1_F = \alpha u$, ou seja, $u = \alpha^{-1}$ está em $F$. Em outras palavras, $K \subseteq F$. Desse modo, $K = F$.*

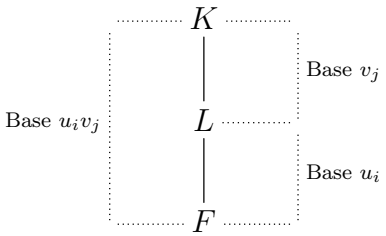
*($\Longleftarrow$) Agora, se $K = F$, para todo $\alpha \in F$, temos que $\alpha = 1_F \cdot \alpha$ e a combinação linear $\alpha \cdot 1_F = 0_F$ implica que $\alpha = 0$ ($1_F \neq 0_F$). Assim, $\{1_F\}$ é uma base para $K$ sobre $F$, daí $[K : F] = 1$.*

Sendo análogo ao **Teorema de Lagrange** na teoria de grupos, o próximo teorema, na teoria de corpos, nos monstra como as dimensões de subcorpos estão relacionadas. Aliás, se $F$, $L$ e $K$ são corpos tais que $F \subseteq L \subseteq K$, então tanto $K$ quanto $L$ podem ser olhados como espaços vetoriais sobre $F$, assim como $K$ pode ser tido como um espaço vetorial sobre $L$.

**Teorema 54** [[5], Theorem 11.4] *Sejam $F$, $L$ e $K$ corpos tais que $F \subseteq L \subseteq K$. Se $[L : F]$ e $[K : L]$ são finitos, então $K$ é uma extensão de dimensão finita sobre $F$ e*

$$[K : F] = [K : L][L : F].$$

*Demonstração:* Por hipótese, podemos assumir que $[L : F] = m$ e $[K : L] = n$, com $m, n \in \mathbb{Z}_+^*$, ou seja, existe uma base $\{u_i \mid 1 \leq i \leq m\}$ de $L$ sobre $F$ e uma base $\{v_j \mid 1 \leq j \leq n\}$ de $K$ sobre $L$.




Para verificar o teorema, basta mostrar que o conjunto $B = \{u_iv_j \mid 1 \leq i \leq m, 1 \leq j \leq n\}$ é uma base para $K$ sobre $F$ (ilustração ao lado), pois daí teremos $[K : L][L : F] = nm = [K : F]$.

Observe, inicialmente, que o conjunto $\{u_iv_j \mid 1 \leq i \leq m, 1 \leq j \leq n\}$ possui exatamente $mn$ elementos distintos, pois, caso contrário, se teria

$$u_iv_j = u_lv_t \quad \Rightarrow \quad u_iv_j - u_lv_t = 0_L,$$

com $u_i, u_l \in L$, contradizendo a independência linear dos $v's$ sobre $L$. Esclarecido isso, vamos mostrar que $B = \{u_iv_j \mid 1 \leq i \leq m, 1 \leq j \leq n\}$ é uma base para $K$ sobre $F$.

• <u>*B gera K:*</u> Seja $w$ um elemento qualquer de $K$. Como o conjunto $\{v_j \mid 1 \leq j \leq n\}$ forma uma base para $K$ sobre $L$, temos

$$w = \sum_{j=1}^{n} \beta_j v_j$$

para $\beta_j \in L$. Ademais, como o conjunto $\{u_i \mid 1 \leq i \leq m\}$ é uma base para $L$ sobre $F$ e cada $\beta_j \in L$ , segue que

$$\beta_j = \sum_{i=1}^{m} a_{ij} u_i$$

para $a_{ij} \in F$. Logo,

$$w = \sum_{j=1}^{n} \left( \sum_{i=1}^{m} a_{ij} u_i \right) v_j = \sum_{i,j} a_{ij} (u_i v_j).$$

Dessa forma, os $nm$ vetores $u_i v_j$ geram $K$ sobre $F$.

- *B é linearmente independente:* Suponha que $c_{ij} \in F$ e

$$\sum_{i,j} c_{ij} (u_i v_j) = 0.$$

Assim,

$$\sum_{j=1}^{n} \left( \sum_{i=1}^{m} c_{ij} u_i \right) v_j = 0,$$

com $\left( \sum_{i=1}^{m} c_{ij} u_i \right) \in L$. Pelo fato dos $v_j$ serem linearmente independentes sobre $L$, devemos ter

$$\sum_{i=1}^{m} c_{ij} u_i = 0, \ \forall \ j.$$

No entanto, os $u_i$ são linearmente independentes sobre $F$, daí

$$\sum_{i=1}^{m} c_{ij} u_i = 0 \quad \Rightarrow \quad c_{ij} = 0, \ \forall \ i, j.$$

Portanto, o conjunto $B = \{u_i v_j \mid 1 \leq i \leq m, 1 \leq j \leq n\}$ é uma base para $K$ sobre $F$, consequentemente $[K : L][L : F] = nm = [K : F]$.

□

Caso haja uma cadeia de extensões finitas, teremos o seguinte resultado cuja demonstração é uma ampliação direta do **Teorema 54**, por indução.

**Corolário 11** [[3], Corollary 31.6] *Sejam $F_i$, com $1 \leq i \leq r$, corpos de modo que $F_1 \subseteq F_2 \subseteq \cdots \subseteq F_r$, ou seja, $F_{i+1}$ é uma extensão de $F_i$. Se cada $[F_i : F_{i-1}]$ é finito para $1 \leq i \leq r$, então $F_r$ é uma extensão de dimensão finita sobre $F_1$ e*

$$[F_r : F_1] = [F_r : F_{r-1}][F_{r-1} : F_{r-2}] \cdots [F_2 : F_1].$$

Outra propriedade interessante a ser mencionada é a de que, para um dado isomorfismo entre dois corpos de extensão de dimensão finita de um terceiro corpo temos que seus índices são iguais. Essa característica abordada no teorema seguinte terá importante utilidade ao Corolário 14 no Capítulo 4 deste trabalho:

**Teorema 55** [[5], Theorem 11.5] *Sejam $K$ e $L$ corpos de extensão de dimensão finita sobre o corpo $F$ e $f : K \longrightarrow L$ um isomorfismo tal que $f(c) = c$, para todo $c \in F$. Então, $[K : F] = [L : F]$.*

*Demonstração:* Inicialmente, nota-se que pelo fato do isomorfismo $f : K \longrightarrow L$ ser dado por $f(c) = c$, para todo $c \in F$, torna $f$ uma transformação linear entres os espaços vetoriais $K$ e $L$, ambos sobre $F$, isto é, como elucida [1], uma função que satisfaz:

*i)* $f(k_1 + k_2) = f(k_1) + f(k_2)$, para todos $k_1, k_2 \in K$;

*ii)* $f(ck) = cf(k)$, para todo $c \in F$ e todo $k \in K$.

Logo, tem-se de imediato, como são isomorfos, que $K$ e $L$ possuem a mesma dimensão, ou seja, $[K : F] = [L : F]$.

□

## 3.2 Extensões Simples

Consideremos os corpos $F$ e $K$ tais que $F \subseteq K$. Podemos nos perguntar, naturalmente, dentre todos os subcorpos de $K$ qual as propriedades do menor entre eles que contêm algum $u \in K$ e $F$, ou ainda, quando $u$ for uma raiz de um polinômio irredutível $p(x) \in F[x]$, se existe alguma relação entre esse menor subcorpo com o corpo de extensão $F[x]/\langle p(x)\rangle$, **Teorema 52**, que também possui uma raiz de $p(x)$. Nesta seção, buscamos elucidar tais questões e abordar, de maneira nítida, esse menor subcorpo de $K$ que contém $u \in K$ e $F$.

Para tanto, considere $K$ como corpo de extensão de $F$, $u \in K$ e $F(u)$ a interseção de todos os subcorpos de $K$ contendo $F$ e $u$. Observe que $F(u) \neq \emptyset$, pois ao menos $K$ está nessa família de subcorpos, e $F(u)$ é um corpo em razão de uma interseção de qualquer família de subcorpos de $K$ ser um corpo. Logo, conforme sua própria definição, $F(u)$ é o

menor subcorpo de $K$ contendo $F$ e $u$ (devido estar contido em todo subcorpo de $K$ que contém $F$ e $u$). Nesse sentido, definimos $F(u)$ como ***Extensão Simples*** de F.

Além disso, a estrutura de $F(u)$ está intimamente vinculada ao fato de $u$ ser ou não raiz de algum polinômio em $F[x]$. Por esse motivo, a seguinte definição é necessária.

**Definição 31** [[5], page 376] *Seja $K$ um corpo de extensão do corpo $F$. Um elemento $u \in K$ é dito* ***Algébrico*** *sobre $F$ se $u$ é a raiz de algum polinômio não nulo em $F[x]$. Por outro lado, se um elemento de $K$ não for raiz de qualquer polinômio em $F[x]$, então ele será* ***Transcendente*** *sobre $F$.*

Desta definição, note que todo elemento $c \in F$ é algébrico sobre $F$, uma vez que $c$ é a raiz do polinômio $f(x) = x - c$ que pertence a $F[x]$.

**Proposição 3** [[5], Exercises 7 Section 11.2] *Se $K$ é um corpo tal que $F \subseteq E \subseteq K$ e $u \in K$ é algébrico sobre $F$, então $u$ é algébrico sobre $E$.*

*Demonstração:* Pela **Definição 31**, seja $f(x) = \sum_{i=0}^{n} a_i x^n$ um polinômio em $F[x]$ que tenha $u \in K$ como raiz. Em virtude de $F \subseteq E$ por hipótese, tem-se que todo coeficiente $a_i \in F$ está em $E$, em outras palavras, $f(x) \in E[x]$. Portanto, como $u \in K$ é raiz de $f(x) \in E[x]$ e $E \subseteq K$, $u$ é algébrico sobre $E$.

□

O teorema seguinte nos fornecerá um único polinômio em $F[x]$ que propiciará descrever satisfatoriamente o corpo de extensão simples $F(u)$, pois ele será divisor de todos os demais polinômios de $F[x]$ que possuem $u$ como raiz, sendo $u$ um elemento algébrico do corpo de extensão $K$ sobre $F$.

**Teorema 56** [[5], Theorem 11.6] *Sejam $K$ um corpo de extensão do corpo $F$ e $u \in K$ um elemento algébrico sobre $F$. Então, existe um único polinômio mônico irredutível $p(x) \in F[x]$ que tenha $u$ como uma raiz. Ademais, se $u$ é uma raiz de $f(x) \in F[x]$, então $p(x)$ divide $f(x)$.*

Sob as condições do **Teorema 56**, o polinômio mônico irredutível $p(x)$ mencionado é denominado ***Polinômio Minimal*** de $u$ sobre $F$. Notamos, também, que a unicidade alegada

nesse mesmo resultado denota que ao determinar qualquer polinômio mônico irredutível em $F[x]$ tendo $u$ como raiz, ele deverá ser o polinômio minimal de $u$ sobre $F$.

**Exemplo 47**

1. *O polinômio $x^2 - 2$ em $\mathbb{Q}[x]$ é mônico, irredutível e possui $\sqrt{2} \in \mathbb{R}$ como uma raiz. Logo, $x^2 - 2$ é o polinômio minimal de $\sqrt{2}$ sobre $\mathbb{Q}$. Veja, ainda, que $x^2 - 2$ é redutível sobre $\mathbb{R}$ tendo como fatores $(x - \sqrt{2})(x + \sqrt{2})$ em $\mathbb{R}[x]$. Assim, o polinômio minimal de $\sqrt{2}$ sobre $\mathbb{R}$ é $x - \sqrt{2}$ (que é mônico e irredutível sobre $\mathbb{R}$).*

O próximo teorema certifica-nos de que quando $u \in K$, $K$ um corpo de extensão sobre um corpo $F$, é um elemento algébrico sobre $F$, então a extensão simples $F(u)$ não dependerá de $K$, mas estará inteiramente determinada por $F[x]$ e pelo polinômio minimal $p(x)$. Aliás, por vezes dizemos que $F(u)$ é o *corpo obtido ao adjuntar $u$* a $F$.

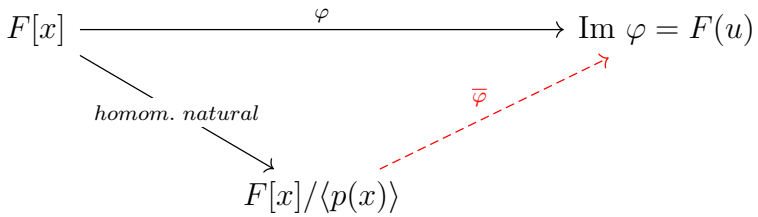
**Teorema 57** [[5], Theorem 11.7] *Considere $K$ um corpo de extensão de um corpo $F$ e $u \in K$ um elemento algébrico sobre $F$ com polinômio minimal $p(x)$ de grau $n$. Então:*

*i)* $F(u) \cong F[x]/\langle p(x) \rangle$;

*ii)* $\{1_F, u, u^2, \ldots, u^{n-1}\}$ *é uma base para o espaço vetorial $F(u)$ sobre $F$;*

*iii)* $[F(u) : F] = n$.

*Demonstração: i)* O diagrama a baixo ilustra, resumidamente, como procederemos para demonstrar este item.




Sabemos que $F(u)$ é um corpo contendo $u$ e $F$, por esse motivo todas as potências positivas de $u$ estão em $F(u)$, bem como todos os elementos da forma

$$b_0 + b_1 u + b_2 u^2 + \cdots + b_s u^s,$$

com $b_s \in F$. Em outras palavras, para qualquer polinômio $f(x) \in F[x]$, todo elemento $f(u)$ está em $F(u)$. Agora, o mapa $\varphi : F[x] \longrightarrow F(u)$ tal que $\varphi(f(x)) = f(u)$ é um homomorfismo de anéis.

De fato, para cada polinômio $f(x) = \sum_{i=0}^{n} a_i x^i$ e $g(x) = \sum_{i=0}^{n} b_i x^i$ em $F[x]$, temos

- $$\begin{aligned} \varphi(f(x)+g(x)) &= \varphi\left(\sum_{i=0}^{n} a_i x^i + \sum_{i=0}^{n} b_i x^i\right) \\ &= \varphi\left(\sum_{i=0}^{n} (a_i + b_i) x^i\right) && \text{(soma de polinômios)} \\ &= \sum_{i=0}^{n} (a_i + b_i) u^i && \text{(definição de } \varphi) \\ &= \sum_{i=0}^{n} a_i u^i + \sum_{i=0}^{n} b_i u^i \\ &= f(u) + g(u). && \text{(definição de } \varphi) \end{aligned}$$

- $$\begin{aligned} \varphi(f(x)g(x)) &= \varphi\left(\left(\sum_{i=0}^{n} a_i u^i\right)\left(\sum_{i=0}^{n} b_i u^n i\right)\right) \\ &= \varphi\left(\sum_{i=0}^{n} d_i x^i\right) && \left(\text{multip. de polinômios com } d_i = \textstyle\sum_{i=0}^{n} a_i b_{n-i}\right) \\ &= \sum_{i=0}^{n} d_i u^i && \text{(definição de } \varphi) \\ &= \left(\sum_{i=0}^{n} a_i u^i\right)\left(\sum_{i=0}^{n} b_i u^i\right) \\ &= f(u)g(u). && \text{(definição de } \varphi) \end{aligned}$$

Perceba que o kernel de $\varphi$ são todos os polinômios em $F[x]$ que tenham exatamente $u$ com uma de suas raízes. Sendo assim, pelo **Teorema 56**, o $\ker(\varphi)$ é o ideal principal $\langle p(x) \rangle$. Ademais, o **1º Teorema de Isomorfismo para Anéis** mostra que o mapa $\overline{\varphi} : F[x]/\langle p(x) \rangle \longrightarrow \text{Im } \varphi$, que associa a classe de congruência (lateral) $[f(x)]$ em $f(u)$, é um isomorfismo.

Além do mais, a irredutibilidade de $p(x)$, pelo **Teorema 51**, implica que o anel quociente $F[x]/\langle p(x) \rangle$ é um corpo, consequentemente $\text{Im}\varphi$ também será um corpo. Observe que $\varphi$ mapeia todo polinômio constante em si mesmo e $\varphi(x) = u$, ou seja, a $\text{Im}\varphi$ é um subcorpo de $F(u)$ que contém $F$ e $u$. Entretanto, $F(u)$ é o menor subcorpo de $K$ contendo $F$ e $u$, portanto devemos ter $F(u) = \text{Im}\varphi \cong F[x]/\langle p(x) \rangle$.

*ii)* Devemos mostrar que o conjunto $\{1_F, u, u^2, \ldots, u^{n-1}\}$ é uma base para o espaço vetorial $F(u)$ sobre $F$. Nesse sentido, pelo item anterior *i)*, vimos que $F(u) = \text{Im}\,\varphi$, isto é, todo elemento de $F(u)$ é da forma $f(u)$, para algum polinômio $f(x) \in F[x]$. Agora, se $\partial p(x) = n$, teremos, através do **Algoritmo da Divisão**, $f(x) = p(x)q(x) + r(x)$, com $q(x), r(x) \in F[x]$ e $r(x) = b_{n-1}x^{n-1} + \cdots + b_1x + b_0$. Logo,

$$\begin{aligned} f(u) &= p(u)q(u) + r(u) \\ &= 0_F \cdot q(u) + r(u) \\ &= r(u) = b_{n-1}u^{n-1} + \cdots + b_1u + b_0 \end{aligned}$$

Em outras palavras, o conjunto $\{1_F, u, u^2, \ldots, u^{n-1}\}$ gera $F(u)$. Além disso, almejando mostrar que esse conjunto é linearmente independente, considere a combinação linear

$$c_0 + c_1u + \cdots + c_{n-1}u^{n-1} = 0_F, \ \ \forall \ c_i \in F.$$

Em vista disso, $u$ é uma raiz do polinômio, em $F[x]$, $c_0 + c_1x + \cdots + c_{n-1}x^{n-1}$ de grau menor ou igual a $n-1$ que, pelo **Teorema 56**, deve ser divisível por $p(x)$ de grau $n$. Mas isso só ocorre quando $c_0 + c_1x + \cdots + c_{n-1}x^{n-1}$ é o polinômio nulo, isto é, cada $c_i = 0$. Portanto, o conjunto $\{1_F, u, u^2, \ldots, u^{n-1}\}$ é uma base para o espaço vetorial $F(u)$ sobre $F$.

*iii)* No item *ii)* acima concluímos que o conjunto $\{1_F, u, u^2, \ldots, u^{n-1}\}$ é uma base para o espaço vetorial $F(u)$ sobre $F$. Portanto, de imediato, $[F(u) : F] = n$.

□

Vimos no **Exemplo 47.1.** que o polinômio minimal de $\sqrt{2}$ sobre $\mathbb{Q}$ é $x^2 - 2$. Empregando o **Teorema 57** com $n = 2$ temos que $\{1, \sqrt{2}\}$ é uma base para $\mathbb{Q}(\sqrt{2})$ sobre $\mathbb{Q}$. Logo, $[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2$.

Vale evidenciar, por intermédio do **Teorema 57**, que: *se $u$ e $v$ possuem o mesmo polinômio minimal $p(x)$ em $F[x]$, então $F(u)$ é isomorfo a $F(v)$*. Tal consequência é justificada devido ao fato de $F(u)$ e $F(v)$ serem isomorfos a $F[x]/\langle p(x)\rangle$. Aliás, isso é válido mesmo quando $u$ e $v$ não estão na mesma extensão do corpo $F$ e o **Teorema 58** abaixo irá generalizar essa ideia ao considerar extensões simples de corpos distintos (não apenas do mesmo corpo), mas isomorfos. Contudo, antes de apresentá-lo, faz-se a seguinte observação útil à demonstração desse resultado.

**Observação 3** *Considere $F$ e $E$ corpos e suponha que $\sigma : F \longrightarrow E$ é um isomorfismo. O mapeamento*

$$\sigma' : F[x] \longrightarrow E[x]$$
$$f(x) = \sum_{i=0}^{n} a_i x^i \longmapsto \sum_{i=0}^{n} \sigma(a_i) x^i$$

*é um isomorfismo de anéis. Para examinar tal afirmação, sejam $f(x) = \sum_{i=0}^{n} a_i x^i$ e $g(x) = \sum_{i=0}^{n} b_i x^i$ polinômios quaisquer em $F[x]$. Então:*

- $$\begin{aligned} \sigma'(f(x)+g(x)) &= \sigma'\left(\sum_{i=0}^{n}(a_i+b_i)x^i\right) && (\textit{pela soma de polinômios}) \\ &= \sum_{i=0}^{n}\sigma(a_i+b_i)x^i && (\textit{definição de } \sigma') \\ &= \sum_{i=0}^{n}(\sigma(a_i)+\sigma(b_i))x^i && (\sigma \textit{ é um isomorfismo}) \\ &= \sum_{i=0}^{n}\sigma(a_i)x^i + \sum_{i=0}^{n}\sigma(b_i)x^i \\ &= \sigma'(f(x)) + \sigma'(g(x)). && (\textit{definição de } \sigma') \end{aligned}$$

- $$\begin{aligned} \sigma'(f(x)g(x)) &= \sigma'\left(\sum_{i=0}^{n} d_i x^i\right) && \left(\textit{multip. de polinômios, com } d_i = \sum_{i=0}^{n} a_i b_{n-i}\right) \\ &= \sum_{i=0}^{n}\sigma'(d_i)x^i && (\textit{definição de } \sigma') \\ &= \left(\sum_{i=0}^{n}\sigma(a_i)x^i\right)\left(\sum_{i=0}^{n}\sigma(b_i)x^i\right) \\ &= \sigma'(f(x))\sigma'(g(x)). && (\textit{definição de } \sigma') \end{aligned}$$

*Ademais, note que todo polinômio constante $f(x) = c$ em $F[x]$ (elemento de $F$) é mapeado pelo isomorfismo $\sigma'$ em $\sigma(c) \in E$.*

$$\begin{array}{ccc} F[x] & \xrightarrow{\sigma'} & E[x] \\ \Big| & & \Big| \\ F & \xrightarrow{\sigma} & E \end{array}$$

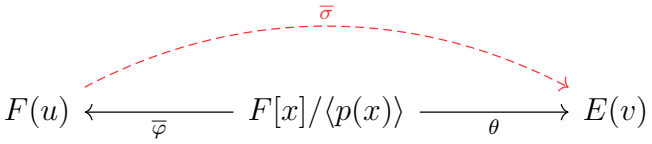
*Por conseguinte, dizemos que o isomorfismo $\sigma' : F[x] \longrightarrow E[x]$ **Estende** o isomorfismo $\sigma : F \longrightarrow E$, como representado ao lado.*

**Teorema 58** [[5], Corollary 11.8] *Sejam $\sigma : F \longrightarrow E$ um isomorfismo de corpos, $u$ um elemento algébrico em algum corpo de extensão de $F$ com polinômio minimal $p(x) \in F[x]$ e $v$ um elemento algébrico sobre algum corpo de extensão de $E$ com polinômio minimal*

$\sigma'(p(x)) \in E[x]$. *Então,* $\sigma$ *se estende a um isomorfismo de corpos* $\overline{\sigma} : F(u) \longrightarrow E(v)$ *tal que* $\overline{\sigma}(c) = \sigma(c)$ *para todo* $c \in F$.

*Demonstração:*

O diagrama ao lado elucida como iremos proceder para construir o isomorfismo $\overline{\sigma}$, ou seja, ele será o composição $\theta \circ \overline{\varphi}^{-1} : F(u) \longrightarrow F(v)$, sendo $\overline{\varphi}$ o isomorfismo do **Teorema 57**. Assim, devemos identificar o isomorfismo $\theta$.




Pela **Observação 3** acima, o isomorfismo $\sigma$ pode ser estendido à um isomorfismo $\sigma' : F[x] \longrightarrow E[x]$, e a demonstração do **Teorema 57** mostra que existe um isomorfismo

$$\begin{aligned} \overline{\tau} : E[x]/\langle \sigma'(p(x))\rangle &\longrightarrow E(v) \\ [g(x)] &\longmapsto g(v) \end{aligned} .$$

Além disso, seja $\gamma$ um homomorfismo sobrejetor

$$\begin{aligned} \gamma : E[x] &\longrightarrow E[x]/\langle \sigma'(p(x)\rangle \\ g(x) &\longmapsto [g(x)] \end{aligned}$$

e considere a composição $\overline{\tau} \circ \gamma \circ \sigma'$, isto é,

$$\begin{aligned} F[x] \xrightarrow{\sigma'} E[x] \xrightarrow{\gamma} E[x]/\langle \sigma'(p(x)\rangle \xrightarrow{\overline{\tau}} E(v) \\ f(x) \longmapsto \sigma'(f(x)) \longmapsto [\sigma'(f(x))] \longmapsto \sigma'(f(v)) \end{aligned} .$$

Logo, a composição $\overline{\tau} \circ \gamma \circ \sigma'$ é sobrejetiva, pois cada um dos três mapas é sobrejetor. Observe ainda, que o kernel dessa função composição consiste de todo polinômio $h(x) \in F[x]$ tal que $\sigma'(h(v)) = 0_E$. Mas pelo fato de $\overline{\tau}$ ser um isomorfismo,

$$\begin{aligned} \sigma'(h(v)) = 0_E &\iff [\sigma'(h(x))] \text{ é o zero (classe) em } E[x]/\langle \sigma'(p(x)\rangle \\ &\iff \sigma'(h(x)) \text{ é múltiplo de } \sigma'(p(x)). \end{aligned}$$

Entretanto, se $\sigma'(h(x)) = s(x) \cdot \sigma'(p(x))$, com $s(x) \in E[x]$ então, aplicando a inversa do isomorfismo $\sigma'$ nessa igualdade, obtemos $h(x) = \sigma'^{-1}(s(x)) \cdot p(x)$. Consequentemente, o kernel da composição $\overline{\tau} \circ \gamma \circ \sigma'$ é o ideal principal $\langle p(x)\rangle$ em $F[x]$. Desse modo, pelo **1º**

**Teorema de Isomorfismo para Anéis** (bem como pela sua demonstração) o mapa

$$\begin{aligned} \theta : F[x]/\langle p(x)\rangle &\longrightarrow E(v) \\ [f(x)] &\longmapsto \sigma'(f(v)) \end{aligned}$$

é um isomorfismo. Note, também, que $\theta([x]) = v$ e, para cada $c \in F$, $\theta([c]) = \sigma(c)$. Ademais, pelo item **iii)** da **Observação 1**, $\overline{\varphi}^{-1}$ é um isomorfismo, tal como a composição $\theta \circ \overline{\varphi}^{-1}$ pelo item **ii)** dessa mesma observação. Portanto, $\overline{\sigma} = \theta \circ \overline{\varphi}^{-1} : F(u) \longrightarrow F(v)$ é um isomorfismo que estende $\sigma$ e mapeia $u$ em $v$.

□

Veja que quando $\sigma$ é o mapa identidade $F \longrightarrow F$, o **Teorema 58** nos afirma que se dois elementos quaisquer $u$ e $v$, em algum corpo de extensão de $F$, possuem o mesmo polinômio minimal, então $F(u) \cong F(v)$ sob uma função que mapeia $u$ em $v$ e todo elemento de $F$ em si.

## 3.3 Extensões Algébricas

Nas Extensões Simples, vistas na última seção, focamos em um único elemento algébrico. Contudo, para o estudo dos zeros de polinômios temos o interesse em extensões contendo apenas elementos algébricos.

**Definição 32** [[5], page 382] *Um corpo de extensão $K$ de um corpo $F$ é uma* ***Extensão Algébrica*** *de $F$ se todo elemento de $K$ é algébrico sobre $F$.*

Observe que o polinômio $f(x) = x^2 - 2ax + (a^2 + b^2)$ em $\mathbb{R}[x]$ possui $a + bi \in \mathbb{C}$ como raiz. Dessa forma, o elemento $a + bi$ é algébrico sobre $\mathbb{R}$ e, assim, $\mathbb{C}$ é uma extensão algébrica sobre $\mathbb{R}$.

O próximo teorema nos mostra que quando consideramos uma extensão de dimensão finita de um corpo ela será, na verdade, uma extensão algébrica.

**Teorema 59** [[3], Theorem 31.3] *Se $K$ é um corpo de extensão de dimensão finita do corpo $F$, então $K$ é uma extensão algébrica sobre $F$.*

*Demonstração:* Devemos mostrar que todo $u \in K$ é algébrico sobre $F$. Se $[K : F] = n$, pela **Proposição 2**, então o conjunto $\{1, u, \ldots, u^n\}$ não pode ser linearmente independente. Dessa maneira, existem elementos $a_i \in F$, não todos nulos, tais que

$$a_n u^n + \cdots + a_1 u + a_0 = 0_F.$$

Logo, o polinômio $f(x) = a_n x^n + \cdots + a_1 x + a_0 = 0$ é um polinômio não nulo em $F[x]$, com $f(u) = 0_F$. Portanto, $u \in K$ é algébrico sobre $F$.

□

Observe que caso $K$ seja um corpo de extensão do corpo $F$ contendo um elemento transcendental $u$, então $K$ deve ser de dimensão infinita sobre $F$, pois, do contrário, $u$ seria algébrico pelo **Teorema 59**. Outrossim, a recíproca do **Teorema 59** não é válido justamente por existirem extensões algébricas de dimensão infinita, por exemplo, $\mathbb{C}$ sobre $\mathbb{R}$.

Além disto, um questionamento que pode ocorrer é se há a possibilidade de determinar o caráter algébrico de um corpo ao analisar um número finito de elementos, **Teorema 60** abaixo. Tal pensamento decorre naturalmente da generalização de uma propriedade das extensões simples, isto é, da noção de que basta verificar se o único elemento $u$ é algébrico sobre $F$ para concluir que o corpo $F(u)$ é uma extensão algébrica, pois, por meio do **Teorema 57**, $F(u)$ tem dimensão finita e, assim, algébrico, pelo **Teorema 59**.

Nesse sentido, antes de apresentar e verificar este fato, note que se $u_1, \ldots, u_n$ são elementos de um corpo de extensão $K$ de $F$ iremos tomar $F(u_1, \ldots, u_n)$ como sendo a interseção de todos os subcorpos de $K$ que contenham $F$ e cada $u_i$, $1 \leq i \leq n$. Ademais, tal qual o caso da extensão simples, $F(u_1 \ldots, u_n)$ é o menor subcorpo de $K$ que contém $F$ e todos os $u_i$, sendo denominado de ***Extensão Finitamente Gerada*** gerada por $u_1, \ldots, u_n$.

**Observação 4**

**i)** *Constate, para mais, que uma extensão finitamente gerada pode, na verdade, ser um extensão simples. Um exemplo disso é o corpo* $\mathbb{Q}(\sqrt{3})$ *que contém* $\sqrt{3}$ *e* $-\sqrt{3}$*, ou seja,* $\mathbb{Q}(\sqrt{3}, -\sqrt{3}) = \mathbb{Q}(\sqrt{3})$.

**ii)** *Perceba que toda extensão de dimensão finita é também finitamente gerada. De fato, se o conjunto* $\{u_1, \ldots, u_n\}$ *é uma base de* $K$ *sobre* $F$*, então toda combinação linear*

*dos $u_i$ ($1 \leq i \leq n$), com coeficientes em $F$, estão em $F(u_1, \ldots, u_n)$. Portanto, $K = F(u_1, \ldots, u_n)$.*

**iii)** *Salienta-se que uma forma efetiva de se lidar com as extensões finitamente geradas é reconhecer que elas podem ser obtidas a partir de uma cadeia de extensões simples. Por exemplo, se tomarmos $K$ como um corpo de extensão de $F$ e $u, v \in K$ tem-se que $F(u, v) = F(u)(v)$:*

$$F \subseteq F(u) \subseteq F(u)(v) = F(u, v).$$

*Decerto, $F(u, v)$ é um subcorpo de $K$ que deve conter $F(u)$, pois $u \in F(u, v)$ e $F \subseteq F(u, v)$. Mais ainda, como $v \in F(u, v)$ o menor subcorpo contendo $F(u)$ e $v$, isto é, $F(u)(v)$ está contido em $F(u, v)$. No entanto, $F(u)(v)$ é um corpo englobando $F$, $u$ e $v$, ou seja, $F(u, v) \subseteq F(u)(v)$. Portanto, $F(u, v) = F(u)(v)$.*

Agora, segue o resultado que elucida como podemos determinar se uma extensão é algébrica.

**Teorema 60** [[5], Theorem 11.10] *Se $K = F(u_1, \ldots, u_n)$ é um corpo de extensão finitamente gerado do corpo $F$ e cada $u_i$ ($1 \leq i \leq n$) é algébrico sobre $F$, então $K$ é uma extensão algébrica de dimensão finita de $F$.*

**Exemplo 48**

**1.** *Temos que $\sqrt{2}$ e $\sqrt{3}$ são algébricos sobre $\mathbb{Q}$, assim, pelo **Teorema 60**, $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ é um corpo de extensão algébrico de dimensão finita sobre $\mathbb{Q}$. Além disso, para calcular a dimensão de $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ sobre $\mathbb{Q}$ pode-se considerar o seguinte encadeamento de extensões simples:*

$$\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{2}) \subseteq \mathbb{Q}(\sqrt{2})(\sqrt{3}) = \mathbb{Q}(\sqrt{2}, \sqrt{3}).$$

*Sabemos que $[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2$ e, pelo **Teorema 54**,*

$$[\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}] = [\mathbb{Q}(\sqrt{2})(\sqrt{3}) : \mathbb{Q}(\sqrt{2})][\mathbb{Q}(\sqrt{2} : \mathbb{Q})].$$

*Logo, precisamos determinar $[\mathbb{Q}(\sqrt{2})(\sqrt{3}) : \mathbb{Q}(\sqrt{2})]$, isto é, encontrar o polinômio minimal de $\sqrt{3}$ sobre $\mathbb{Q}(\sqrt{2})$. O candidato mais evidente é $x^2 - 3$ que é irredutível em*

$\mathbb{Q}[x]$, *mas devemos verificar que ele é irredutível sobre* $\mathbb{Q}(\sqrt{2})$ *para concluir que, de fato, ele será o polinômio minimal. Para isso, vamos mostrar que* $\pm\sqrt{3} \notin \mathbb{Q}(\sqrt{2})$. *Suponha que* $\sqrt{3}$ *ou* $-\sqrt{3}$ *estão em* $\mathbb{Q}(\sqrt{2})$, *daí*

$$\pm\sqrt{3} = a + b\sqrt{2}, \text{ com } a, b \in \mathbb{Q}.$$

*Elevando ao quadrado ambos os lados da igualdade acima, temos*

$$3 = a^2 + 2ab\sqrt{2} + 2b^2 \Rightarrow \sqrt{2} = \frac{3 - a^2 - 2b^2}{2ab},$$

*contradizendo a irracionalidade de* $\sqrt{2}$. *Analogamente, tem-se uma contradição caso* $a = 0$ *ou* $b = 0$. *Com efeito,* $\pm\sqrt{3} \notin \mathbb{Q}(\sqrt{2})$ *e, por isso,* $x^2 - 3$ *é irredutível sobre* $\mathbb{Q}(\sqrt{2})$ *pelo* ***Teorema 42***. *Desse modo,* $x^2 - 3$ *é o polinômio minimal de* $\sqrt{3}$ *sobre* $\mathbb{Q}(\sqrt{2})$ *e, por intermédio do* ***Teorema 57***, $[\mathbb{Q}(\sqrt{2})(\sqrt{3}) : \mathbb{Q}(\sqrt{2})] = 2$. *Portanto, fazendo uso do* ***Teorema 54***,

$$[\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}] = [\mathbb{Q}(\sqrt{2})(\sqrt{3}) : \mathbb{Q}(\sqrt{2})][\mathbb{Q}(\sqrt{2} : \mathbb{Q})] = 2 \cdot 2 = 4.$$

O resultado posterior é similar ao **Teorema 54** - o corpo superior em uma sequência de extensões de dimensão finita tem dimensão finita sobre o corpo base - para extensões algébricas que podem ou não ter dimensão finita.

**Teorema 61** [[5], Corollary 11.11] *Se* $K$ *é um corpo de extensão algébrico do corpo* $L$ *e* $L$ *é uma extensão algébrica do corpo* $F$, *então* $K$ *é uma extensão algébrica sobre* $F$.

**Corolário 12** [[5], Corollary 11.12] *Considere o corpo* $K$ *como uma extensão do corpo* $F$ *e* $E$ *o conjunto de todos os elementos de* $K$ *que são algébricos sobre* $F$. *Então,* $E$ *é um subcorpo de* $K$ *e um corpo de extensão algébrico sobre* $F$.

Observamos que se $K = \mathbb{C}$ e $F = \mathbb{Q}$ no **Corolário 12**, então o corpo $E$ é chamado de *corpo dos números algébricos*.

## 3.4 Corpo de Raízes

Nas seções anteriores, analisávamos corpos de extensão que continham uma raiz de um polinômio $f(x)$ em $F[x]$. Agora, estaremos interessados em averiguar as propriedades de

uma extensão de corpo (mesmo que não seja única) contendo todas as raízes de $f(x)$, isto é, as $n$ raízes distintas de $f(x)$ se $\partial f(x) = n$, **Corolário 5**.

Aponta-se, também, a possibilidade de encontrar, quando o corpo de extensão, digamos $K$, do corpo $F$ não contenha todas as raízes de $f(x)$, um corpo de extensão de $K$ contendo as raízes adicionais de $f(x)$. Porém, caso tal extensão $K$ não exista, é admissível assumir que todas as raízes de $f(x)$ estão em $K$.

Considere $K$ um corpo de extensão do corpo $F$ e $f(x)$ um polinômio não constante de grau $n$ em $F[x]$. Se $f(x)$ fatora em $K[x]$ como

$$f(x) = c(x - u_1)(x - u_2)\cdots(x - u_n)$$

então $f(x)$ ***se Divide (splits) sobre o corpo*** $K$. Nesse contexto, os elementos $u_1, \ldots, u_n$, não necessariamente distintos, são as únicas raízes de $f(x)$ em $K$ ou em qualquer corpo de extensão de $K$. De fato, se $v$ está em alguma extensão de $K$ e $f(v) = 0_F$, então para $c$ não nulo e $f(x)$ não constante

$$\begin{aligned} c(x - u_1)(x - u_2)\cdots(x - u_n) = 0_F &\iff v - u_i = 0_F, \text{ para algum } i = 1, \ldots, n \\ &\iff v = u_i. \end{aligned}$$

Portanto, se $f(x)$ se divide sobre $K$, diremos que $K$ contém todas as raízes desse polinômio.

Agora, iremos conceituar o menor corpo de extensão que contém todas as raízes de $f(x)$, pois isso será elementar ao desenvolvimento do Capítulo 4.

**Definição 33** [[5], page 388] *Se $F$ é um corpo e $f(x) \in F[x]$, então um corpo de extensão $K$ de $F$ é dito ser um* ***Corpo de Raízes*** *de $f(x)$ sobre $F$ desde que*

*(i) $f(x)$ se divide sobre $K$, refiramos $f(x) = c(x - u_1)(x - u_2)\cdots(x - u_n)$;*

*(ii) $K = F(u_1, \ldots, u_n)$.*

**Exemplo 49**

1. *O polinômio $f(x) = x^4 - 5x^2 + 6$ em $\mathbb{Q}[x]$ se fatora como $(x^2 - 2)(x^2 - 3)$, então suas raízes em $\mathbb{R}$ são $\pm\sqrt{2}$ e $\pm\sqrt{3}$. Portanto, $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ é o corpo de raízes de $f(x)$ sobre $\mathbb{Q}$.*

**Observação 5** *Todo polinômio do primeiro grau $ax + b$ em $F[x]$ divide-se sobre $F$, pois*

$$ax + b = a(x + a^{-1}b) = a(x - (-a^{-1}b))$$

*com $-a^{-1}b \in F$. Claramente, $F = F(-a^{-1}b)$ em decorrência de $F$ ser o menor corpo contendo $F$ e $-a^{-1}b$. Portanto, $F$ é ele próprio o corpo de raízes de $ax + b$ sobre $F$.*

**Proposição 4** [[5], Exercises 5 Section 11.4] *Seja $K$ um corpo de raízes de $f(x)$ sobre o corpo $F$. Se $E$ é um corpo tal que $F \subseteq E \subseteq K$, então $K$ é um corpo de raízes de $f(x)$ sobre $E$.*

*Demonstração:* Devemos mostrar que $K = E(u_1, \ldots, u_n)$, sendo $u_1, \ldots, u_n$ as raízes de $f(x)$ em $K$. Para isso, observe, inicialmente, que o polinômio $f(x) \in F[x]$ está em $E[x]$, pois $F \subseteq E$ por hipótese. Ademais, como $E(u_1, \ldots, u_n)$ é o menor subcorpo de $K$ contendo $E$ e cada um dos $u_i$ $(1 \leq i \leq n)$ e $E \subseteq K$ (hipótese), segue que $E(u_1, \ldots, u_n) \subseteq K$.

Além do mais, como $\{u_1, \ldots, u_n\} \in K$, por $K = F(u_1, \ldots, u_n)$ (hipótese), tem-se que $K \subseteq E(u_1, \ldots, u_n)$. Portanto, $K = E(u_1, \ldots, u_n)$, em outras palavras, $K$ é um corpo de raízes de $f(x)$ sobre $E$.

□

Pondera-se, além do mais, que todo polinômio tem um corpo de raízes sobre o corpo $F$. De fato, informalmente, se $f(x) \in F[x]$ conseguimos determinar, através do **Teorema de Kronecker**, uma extensão $F(u)$ contendo uma raiz $u$ de $f(x)$. Agora, o **Teorema do Fator** nos mostra que, em $F(u)[x]$, $f(x) = (x - u)g(x)$. Logo, novamente pelo **Teorema de Kronecker**, existe uma extensão $F(u)(v)$ de $F(u)$ que contém uma raiz $v$ de $g(x)$. Procedendo dessa forma obteremos, eventualmente, um corpo de raízes de $f(x)$. O teorema adiante formaliza esse argumento e expõe algo a mais.

**Teorema 62** [[5], Theorem 11.13] *Se $F$ é um corpo e $f(x)$ é um polinômio de grau $n$ em $F[x]$, então existe um corpo de raízes $K$ de $f(x)$ sobre $F$ tal que $[K : F] \leq n!$*

Ademais, uma outra questão potencialmente importante a ser analisada sobre os corpos de raízes é compreender se há alguma relação entre os de um mesmo polinômio caso ele tenha mais de um corpo de raízes. A resposta para isso é um caso particular do resultado que segue, bastante útil ao teorema fundamental deste trabalho, o famigerado **Teorema Fundamental da Teoria de Galois**, **Teorema 75**.

**Teorema 63** [[5], Theorem 11.14] *Sejam $\sigma : F \longrightarrow E$ um isomorfismo de corpos, $f(x)$ um polinômio não constante em $F[x]$ e $\sigma'(f(x))$ o polinômio correspondente em $E[x]$ (como na Observação 3). Se $K$ é um corpo de raízes de $f(x)$ sobre $F$ e $L$ é o corpo de raízes de $\sigma'(f(x))$ sobre $E$, então $\sigma$ pode ser estendido a um isomorfismo $\tau : K \longrightarrow L$.*

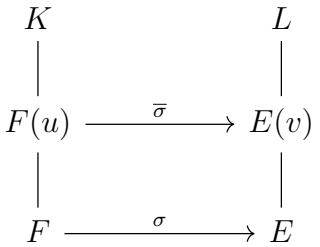
*Demonstração:* Para verificar que o isomorfismo $\sigma : F \longrightarrow E$ pode ser estendido a um isomorfismo $\tau : K \longrightarrow L$, utilizaremos indução sobre o grau de $f(x)$ ($\partial f(x)$).

• *Para $\partial f(x) = 1$:* Neste caso, pela definição de corpo de raízes, $f(x) = c(x - u)$ em $K[x]$ e $K = F(u)$. Todavia, $f(x) = cx + cu$ está em $F[x]$, ou seja, deve-se ter $c \in F$ e $cu \in F$. Logo, $u = c^{-1}uc$ pertence a $F$. Consequentemente, $K = F(u) = F$. Além do mais, mediante a **Observação 3**, o isomorfismo $\sigma' : F[x] \longrightarrow E[x]$ estende $\sigma$, assim $\sigma'(f(x))$ também é um polinômio do primeiro grau em $E[x]$ e usando um argumento análogo tem-se que $E = L$. Desse modo, o próprio $\sigma$ é o isomorfismo desejado.

• *Hipótese de Indução:* Suponha que o teorema seja válido para todo polinômio em $F[x]$ de grau menor ou igual a $n - 1$.

• *Para $\partial f(x) = n$:* Mediante o **Teorema 39**, $f(x)$ tem um fator irredutível em $F[x]$ e multiplicando esse polinômio pelo inverso de seu coeficiente líder produz um fator mônico irredutível $p(x) \in F[x]$ de $f(x)$. Devido o isomorfismo $\sigma' : F[x] \longrightarrow E[x]$ estender $\sigma$ (**Observação 3**), $\sigma'(p(x))$ é um fator mônico irredutível de $\sigma'(f(x))$ em $E[x]$. Ademais, observe que toda raiz de $p(x)$ é também uma raiz de $f(x)$, por essa razão todas as raízes de $p(x)$ estão em $K$. Similarmente, $L$ contém todas as raízes de $\sigma'(p(x))$.

Agora, seja $u \in K$ uma raiz de $p(x)$ e $v \in L$ uma raiz de $\sigma'(p(x))$. Por intermédio do **Teorema 58**, $\sigma$ se estende para um isomorfismo $\overline{\sigma} : F(u) \to E(v)$ que mapeia $u$ em $v$ (ilustração ao lado).




Podemos visualizar, através do **Teorema 41**, que $f(x) = (x - u)g(x)$ em $F(u)[x]$ e, por meio disso, em $E(v)[x]$

$$\begin{aligned} \sigma'(f(x)) &= \sigma'((x - u)) \cdot \sigma'(g(x)) \\ &= (x - \sigma(u)) \cdot \sigma'(g(x)) \\ &= (x - v) \cdot \sigma'(g(x)). \end{aligned}$$

Outrossim, $f(x)$ se divide sobre $K$, ou seja, pode ser representado da forma

$$f(x) = c(x-u)(x-u_2)\cdots(x-u_n), \text{ com } c \in F.$$

Mas, como $f(x) = (x-u)g(x)$, deve-se ter $g(x) = c(x-u_2)\cdots(x-u_n)$. Logo, pelo fato de $F(u, u_2, \ldots, u_n) = K$ ser o menor subcorpo contendo todas as raízes de $g(x)$ e o corpo $F(u)$, $K$ é um corpo de raízes de $g(x)$ sobre $F(u)$. Analogamente, $L$ é um corpo de raízes de $\sigma'(g(x))$ sobre $E(v)$. Dado que $\partial g(x) = n-1$, a hipótese de indução resulta que o isomorfismo $\overline{\sigma} : F(u) \longrightarrow E(v)$ pode ser estendido à um isomorfismo $\tau : K \longrightarrow L$, concluindo, pois, a etapa indutiva.

Portanto, por indução, o isomorfismo $\sigma : F \longrightarrow E$ pode ser estendido a um isomorfismo $\tau : K \longrightarrow L$.

□

Veja que se $F = E$ e $\sigma : F \longrightarrow F$ é o mapa identidade no **Teorema 63**, então esse resultado afirma que quaisquer dois corpos de raízes de $f(x)$ são isomorfos (respondendo, assim, qual a relação questionada anteriormente).

Outrossim, fora a peculiaridade inerente dos corpos de raízes conter todas as raízes de algum polinômio sobre $F$ (definição), esses corpos têm uma propriedade bastante importante determinada abaixo.

**Definição 34** [[5], page 391] *Seja $K$ um corpo de extensão algébrico sobre um corpo $F$, diremos que $K$ é uma **Extensão Normal** sempre que um polinômio irredutível em $F[x]$ tendo uma raiz em $K$ divide-se sobre $K$, ou seja, tem todas as suas raízes em $K$.*

Frisa-se que essa noção de extensão normal foi explicitamente reconhecida por Galois, mas em termos de polinômios sobre $\mathbb{C}$. O teorema subsequente expressará que um corpo é uma extensão de raízes se, e somente se, ele for uma extensão normal de dimensão finita.

**Teorema 64** [[5], Theorem 11.15] *O corpo $K$ é um corpo de raízes sobre o corpo $F$ de algum polinômio em $F[x]$ se, e somente se, $K$ é uma extensão normal de dimensão finita de $F$.*

*Demonstração:* ($\Longrightarrow$) Considerando $K$ como o corpo de raízes de $f(x) \in F[x]$, teremos $K = F(u_1, \ldots, u_n)$ sendo os $u_i$ $(1 \leq i \leq n)$ são todos raízes de $f(x)$. Por conseguinte, pelo

**Teorema 60**, $[K : F]$ é finito. Seja $p(x) \in F[x]$ um polinômio irredutível tendo uma raiz $v \in K$. Agora, considere $p(x)$ como polinômio em $K[x]$ e seja $L$ o corpo de raízes de $p(x)$ sobre $K$, com $F \subseteq K \subseteq L$. Vamos provar que $p(x)$ divide-se sobre $K$, ou seja, mostraremos que toda raiz de $p(x)$ em $L$ está, na realidade, em $K$. Para isso, seja $w \in L$ uma raiz qualquer de $p(x)$ diferente de $v$.

O **Teorema 58**, com $E = F$ e $\sigma$ o mapa identidade ($\iota$), assegura a existência de um isomorfismo $\overline{\sigma} : F(v) \longrightarrow F(w)$ mapeando $v$ em $w$ e todo elemento de $F$ em si mesmo. O diagrama ao lado representa a situação presente, tomando $K(w)$ um subcorpo de $L$.

$$\begin{array}{ccc} K & & K(w) \\ | & & | \\ F(v) & \xrightarrow{\overline{\sigma}} & F(w) \\ | & & | \\ F & \xrightarrow{\iota} & F \end{array}$$

Em virtude de

$$\begin{aligned} K(w) &= F(u_1, \ldots, u_n)(w) \\ &= F(u_1, \ldots, u_n, w) \\ &= F(w)(u_1, \ldots, u_n) \end{aligned}$$

temos que $K(w)$ é um corpo de raízes de $f(x)$ sobre $F(w)$. Ademais, como $v \in K$ e $K$ é um corpo de raízes de $f(x)$ sobre $F$, $K$ também sera um corpo de raízes de $f(x)$ sobre o subcorpo $F(v)$. Dessa maneira, por meio do **Teorema 63**, o isomorfismo $\overline{\sigma} : F(v) \longrightarrow F(w)$ se estende para um isomorfismo $\tau : K \longrightarrow K(w)$ que mapeia $v$ em $w$ e todo elemento de $F$ em si mesmo. Logo, através do **Teorema 55**, $[K : F] = [K(w) : F]$.

Além disso, observe que na cadeia de extensões $F \subseteq K \subseteq K(w)$, pelo **Teorema 57**, $[K(w) : K]$ é finito, bem como $[K : F]$ visto no primeiro parágrafo dessa demonstração. Desse modo, pelo **Teorema 54**

$$[K : F] = [K(w) : F] = [K(w) : K][K : F] \Rightarrow [K(w) : K] = 1.$$

Consequentemente, pela **Observação 2**, $K(w) = K$, isto é, $w \in K$. Em outras palavras, toda raiz de $p(x)$ em $L$ está em $K$ e $p(x)$ divide-se sobre $K$. Diante disso, $K$ é normal sobre $F$.

($\Longleftarrow$) Assumindo que $K$ é uma extensão normal de dimensão finita de $F$, podemos considerar a base $\{u_1, \ldots, u_n\}$. Assim, pelo item **ii)** da **Observação 4**, $F = F(u_1, \ldots, u_n)$. Veja, ainda, que, fazendo uso do **Teorema 59**, cada $u_i$ é algébrico sobre $F$ com polinômio minimal $p_i(x)$, com $1 \leq i \leq n$. Aliás, como cada um dos $p_i(x)$ dividem-se sobre $K$ pela

normalidade, tem-se que $f(x) = p_1(x) \cdots p_n(x)$ também divide-se sobre $K$. À vista disso, $K$ é o corpo de raízes de $f(x)$.

Portanto, o corpo $K$ é um corpo de raízes sobre o corpo $F$ de algum polinômio em $F[x]$ se, e somente se, $K$ é uma extensão normal de dimensão finita de $F$.

□

**Observação 6** *Viu-se que todo polinômio tem um corpo de raízes sobre o corpo $F$, ou seja, para cada polinômio em $F[x]$ podemos determinar um respectivo corpo de extensão sobre $F$ contendo suas raízes. Todavia, ressalta-se a existência de um corpo de extensão que contém todas as raízes de todos os polinômios não constantes em $F[x]$. Tal corpo se diz ser* ***Algebricamente Fechado****.*

*Destaca-se, também, que se $K$ é uma extensão algébrica de $F$ e $K$ é algebricamente fechado, então, neste caso, $K$ é chamado de* ***Fecho Algébrico*** *de $F$. A unicidade do fecho algébrico é justificada por um teorema análogo ao* ***Teorema 63*** *que diz que quaisquer dois fechos algébricos de $F$ são isomorfos (veja em Fraleigh [3], Corolário 49.5). Para mais detalhes sobre a existência do fecho algébrico consulte [3] página 288.*

## 3.5 Separabilidade

Notamos na seção anterior que todo polinômio possui um corpo de raízes que contém todas as suas raízes, podendo haver repetidas (iguais) ou todas serem distintas. Considerando o segundo caso, tem-se um propriedade complementar à normalidade, isto é, a separabilidade de um corpo de extensão que abordaremos agora.

No entanto, para defini-la precisamos elucidar as seguintes caracterizações:

• Seja um corpo $F$, um polinômio $f(x) \in F[x]$ de grau $n$ é ***Separável*** se tiver $n$ raízes distintas em algum corpo de raízes - sabendo que quaisquer dois corpos de raízes são isomorfos, pelo **Teorema 63**, segue-se que $f(x)$ tem $n$ raízes distintas em cada corpo de raízes. De forma equivalente, $f(x)$ é separável se não tiver raízes repetidas em qualquer corpo de raízes.

• Se $K$ é um corpo de extensão do corpo $F$, então um elemento $u \in K$ é ***Separável*** sobre $F$ se $u$ é algébrico sobre $F$ e seu polinômio minimal $p(x) \in F[x]$ é separável.

**Definição 35** [[5], page 394] *Seja $K$ um corpo de extensão sobre um corpo $F$. $K$ é uma* ***Extensão Separável****, ou apenas* ***Separável*** *sobre $F$, se todo elemento de $K$ é separável sobre $F$. Desse modo, necessariamente, uma extensão separável é algébrica.*

**Exemplo 50**

1. *O polinômio $f(x) = x^4 - x^3 - x + 1$ em $\mathbb{Q}[x]$ não é separável, pois ele pode ser fatorado como $(x-1)^2(x^2+x+1)$, ou seja, ele possui uma raiz repetida em um total de três raízes distintas em $\mathbb{C}$. Porém o polinômio $x^2+5$ em $\mathbb{Q}[x]$ é separável em decorrência de possuir duas raízes distintas $\sqrt{5}i$ e $-\sqrt{5}i$ em $\mathbb{C}$.*

**Proposição 5** [[5], Exercises 1 Section 11.5] *Se o corpo $K$ é uma extensão separável sobre o corpo $F$ e $E$ é um corpo tal que $F \subseteq E \subseteq K$, então $K$ é separável sobre $E$.*

*Demonstração:* Precisamos mostrar que qualquer elemento em $K$ é algébrico sobre $E$ e seu polinômio minimal em $E[x]$ é separável. Logo, seja $p(x) \in F[x]$ o polinômio minimal de algum elemento $u \in K$ que é separável, pois $K$ é uma extensão separável sobre o corpo $F$. Note que o polinômio minimal separável $p(x)$ está em $E[x]$, pois $F \subseteq E$ por hipótese. Aliás, como $u \in K$ é a raiz de polinômio não nulo $p(x)$ em $E[x]$, por definição, $u$ é algébrico sobre $E$. Portanto, pela arbitrariedade de $u \in K$, $K$ é separável sobre $E$.

□

Almejando determinar a separabilidade de um polinômio ou de um corpo, muitos testes fazem uso do conceito de *derivada* de $f(x) = a_n x^n + \cdots + a_2 x^2 + a_1 x + a_0 \in F[x]$ definida por

$$f'(x) = n a_n x^{n-1} + \cdots + 3a_3 x^2 + 2a_2 x + a_1 \in F[x].$$

Ademais, as derivadas como definida acima (forma algébrica) possuem as propriedades (familiares) abaixo que são facilmente verificáveis:

(i) $(f+g)'(x) = f'(x) + g'(x)$;

(ii) $(fg)'(x) = f(x)g'(x) + f'(x)g(x)$,

com $f(x), g(x) \in F[x]$.

Nos teoremas seguinte, encontramos caracterização para um polinômio ser separável e para uma extensão ser separável. No primeiro teorema, veremos que não há a necessidade do entendimento sobre corpos de raízes para determinar a separabilidade.

**Teorema 65** [[5], Lemma 11.16] *Considere $F$ um corpo e $f(x) \in F[x]$. Se $f(x)$ e $f'(x)$ são relativamente primos em $F[x]$, então $f(x)$ é separável.*

**Teorema 66** [[5], Theorem 11.17] *Seja $F$ um corpo de característica 0. Então, todo polinômio irredutível em $F[x]$ é separável e todo corpo de extensão algébrico $K$ de $F$ é uma extensão separável.*

Outra peculiaridade assinalada ao estudar esse tipo de extensão é que toda extensão separável finitamente gerada é uma extensão simples. Tal fato, abordado no teorema a seguir, será útil a demonstração do **Corolário 15** do próximo capítulo.

**Teorema 67** [[5], Theorem 11.18*] *Se o corpo $K$ é uma extensão separável finitamente gerada do corpo $F$, então $K = F(u)$ para algum $u \in K$.*

A demonstração (feita por indução sobre $n$ em $K = F(u_1, \ldots, u_n)$) deste resultado será omitida, mas salientamos um fato importante de se comentar para o caso em que $n = 2$, isto é, que o candidato oportuno em $K$ para ter-se $K = F(v, w) = F(u)$ é $u = v + cw$, onde $c \in F$ de modo que

$$c \neq \frac{v_i - v}{w - w_j}, \ \forall \ 1 \leq i \leq m, 1 \leq j \leq n,$$

sendo os $v_i$ e os $w_j$ as raízes dos polinômios minimais $p(x)$ e $q(x)$, respectivamente, em $L$ (corpo de raízes de $p(x)q(x)$ sobre $F$).

**Exemplo 51**

1. *Aplicando o que foi explanado acima para $\mathbb{Q}(\sqrt{2}, \sqrt{3})$, temos $v = \sqrt{2}$, $v_2 = -\sqrt{2}$, $w = \sqrt{3}$ e $w_2 = -\sqrt{3}$. Logo, podemos escolher $c = 1$ e, assim, teremos $u = \sqrt{2} + \sqrt{3}$. Portanto, $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ é a extensão simples $\mathbb{Q}(\sqrt{2} + \sqrt{3})$.*

# Capítulo 4

# Teoria de Galois

Neste capítulo, dividido em duas seções, iremos apresentar a descoberta singular de Galois da estreita conexão entre cada corpo de extensão, onde residem as soluções da equação do tipo $f(x) = 0$, e determinados grupos e subgrupos (Seção 4.1), sendo essa ligação notabilizada no Teorema Fundamental da Teoria de Galois na Seção 4.2. Ressalta-se, ainda, que a principal referência bibliográfica utilizada no presado capítulo foi [5].

## 4.1 O Grupo de Galois

Relacionar a cada extensão de corpo com um certo grupo, denominado de Grupo de Galois (composto por automorfismos), é uma estratégia ímpar à edificação desse saber matemático. Nesse sentido, na presente seção se definirá o grupo de Galois e será abordado suas propriedades básicas que proporcionarão, junto com os teoremas da teoria de grupos, designar fatos importantes sobre a extensão de corpos.

**Definição 36** [[5], page 408] *Seja $K$ um corpo de extensão de $F$. Um $F$-automorfismo de $K$ é um isomorfismo $\sigma : K \longrightarrow K$ que fixa cada elemento de $F$, isto é, $\sigma(c) = c$ para todo $c \in F$. O conjunto de todos os $F$-automorfismos de $K$ é denotado por $Gal_F K$ e nomeado de **Grupo de Galois** de $K$ sobre $F$.*

A justificativa para $Gal_F K$ ser um grupo segue abaixo:

**Teorema 68** [[5], Theorem 12.1] *Se $K$ é um corpo de extensão do corpo $F$, então $Gal_F K$ é um grupo sob a operação de composição de funções.*

*Demonstração:* A princípio, notamos que $Gal_F K$ é um conjunto não vazio, pois o mapa identidade $\iota : K \longrightarrow K$ é um automorfismo. Agora, se $\sigma, \tau \in Gal_F K$ então, pelo item ***ii)*** da **Observação 1**, $\sigma \circ \tau$ é um isomorfismo de $K$ em $K$. Nesse sentido, para cada $c \in K$ temos $(\sigma \circ \tau)(c) = \sigma(\tau(c)) = \sigma(c) = c$, isto é, $\sigma \circ \tau \in Gal_F K$ e, assim, $Gal_F K$ é fechado.

Outrossim, sabemos que a composição de funções é associativa, o mapa identidade $\iota$ é o elemento identidade de $Gal_F K$ e toda função bijetiva possui inversa (**Teorema 9**). Logo, se $\sigma \in Gal_F K$ então $\sigma^{-1}$ é um isomorfismo de $K$ em $K$ pelo item **iii)** da **Observação 1**. Veja que, para todo $c \in F$,

$$\sigma(c) = c \Rightarrow \sigma^{-1}(\sigma(c)) = \sigma^{-1}(c) \Rightarrow \sigma^{-1}(c) = \iota(c) = c.$$

Portanto, $\sigma^{-1} \in Gal_F K$ e conclui-se que $Gal_F K$ é um grupo.

□

Um aspecto interessante dos automorfismos em $Gal_F K$ é que se os avaliarmos em uma raiz em $K$ de um polinômio em $F[x]$ o resultado também será uma raiz desse polinômio, como veremos no teorema seguinte. Por exemplo, se considerarmos o automorfismo $\sigma : \mathbb{C} \longrightarrow \mathbb{C}$ dado por $\sigma(a + bi) = a - bi$ verificamos que, para qualquer número real $a$, temos

$$\sigma(a) = \sigma(a + 0i) = a - 0i = a.$$

Ou seja, $\sigma \in Gal_{\mathbb{R}}\mathbb{C}$. Observe, agora, que $i$ e $-i$ são raízes de $f(x) = x^2 + 1$ em $\mathbb{R}[x]$ e $\sigma(i) = -i$ e $\sigma(-i) = i$, isto é, $\sigma$ permuta as raízes.

**Teorema 69** [[5], Theorem 12.2] *Sejam $K$ um corpo de extensão do corpo $F$ e $f(x) \in F[x]$. Se $u \in K$ é uma raiz de $f(x)$ e $\sigma \in Gal_F K$, então $\sigma(u)$ também é uma raiz de $f(x)$.*

*Demonstração:* Seja $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_2 x^2 + a_1 x + a_0$ com $a_i \in F$, $0 \leq i \leq n$ então,

$$a_n u^n + a_{n-1}u^{n-1} + \cdots + a_2 u^2 + a_1 u + a_0 = 0_K.$$

Como $\sigma$ é um homomorfismo e $\sigma(a_i) = a_i$ para cada $a_i \in F$, segue que

$$\begin{aligned} 0_F = \sigma(0_F) &= \sigma(a_n u^n + a_{n-1}u^{n-1} + \cdots + a_2 u^2 + a_1 u + a_0) \\ &= \sigma(a_n)\sigma(u^n) + \sigma(a_{n-1})\sigma(u^{n-1}) + \cdots + \sigma(a_2)\sigma(u^2) + \sigma(a_1)\sigma(u) + \sigma(a_0) \\ &= a_n\sigma(u)^n + a_{n-1}\sigma(u)^{n-1} + \cdots + a_2\sigma(u)^2 + a_1\sigma(u) + a_0 \\ &= f(\sigma(u)). \end{aligned}$$

Portanto, $\sigma(u)$ é uma raiz de $f(x)$.

□

A partir do **Teorema 69** podemos nos questionar se para $u \in K$ algébrico sobre $F$ toda raiz de seu polinômio minimal $p(x) \in F[x]$ em $K$ é imagem de $u$ sob algum automorfismo de $Gal_F K$. O resultado seguinte mostra-nos que de fato isso ocorre.

**Teorema 70** [[5], Theorem 12.3] *Sejam $K$ o corpo de raízes de algum polinômio sobre $F$ e $u, v \in K$. Então existe um automorfismo $\sigma \in Gal_F K$ tal que $\sigma(u) = v$ se, e somente se, $u$ e $v$ têm o mesmo polinômio minimal em $F[x]$.*

*Demonstração:* ($\Longrightarrow$) Segue diretamente do **Teorema 69**.

($\Longleftarrow$) Se $u$ e $v$ possuem o mesmo polinômio minimal, então, fazendo uso do **Teorema 58**, existe um isomorfismo $\sigma : F(u) \longrightarrow F(v)$ tal que $\sigma(u) = v$ e $\sigma$ fixa cada elemento de $F$. Como $K$ é um corpo de raízes de algum polinômio sobre $F$, ele é o corpo de raízes do mesmo polinômio sobre $F(u)$ e $F(v)$.

$$\begin{array}{ccc} K & \xrightarrow{\quad\sigma\quad} & K \\ \big| & & \big| \\ F(u) & \xrightarrow{\quad\sigma\quad} & F(v) \\ \big| & & \big| \\ F & \xrightarrow{\quad\iota\quad} & F \end{array}$$

Consequentemente, por meio do **Teorema 63**, $\sigma$ pode ser estendido para um $F$-automorfismo de $K$, também denominado por $\sigma$ (como representado no diagrama ao lado). Portanto, $\sigma \in Gal_F K$ e $\sigma(u) = v$.

□

Perante estas propriedades sobre os $F$-automorfismos de $K$, cogita-se de que forma podemos definir todos os elementos de $Gal_F K$. Nesse conjuntura, o teorema abaixo nos esclarece de que forma podemos determinar completamente esse grupo.

**Teorema 71** [[5], Theorem 12.4] *Seja $K = F(u_1, \ldots, u_n)$ um corpo de extensão algébrico sobre o corpo $F$. Se $\sigma, \tau \in Gal_F K$ e $\sigma(u_i) = \tau(u_i)$ para cada $i = 1, 2, \ldots, n$, então $\sigma = \tau$,*

*isto é, um automorfismo em $Gal_F K$ está completamente determinado por sua ação em $u_1, \ldots, u_n$.*

*Demonstração:* Queremos mostrar que $\sigma = \tau$, ou ainda, $\sigma^{-1} \circ \tau$ é o mapa identidade $\iota$. Para isso, considere que $\beta = \sigma^{-1} \circ \tau \in Gal_F K$. Sabemos que $\sigma(u_i) = \tau(u_i)$ para todo $i$, assim

$$\begin{aligned} \beta(u_i) = (\sigma^{-1} \circ \tau)(u_i) &= \sigma^{-1}(\tau(u_i)) \\ &= \sigma^{-1}(\sigma(u_i)) \\ &= (\sigma^{-1} \circ \sigma)(u_i) \\ &= \iota(u_i) = u_i. \end{aligned}$$

Agora, para um $v$ qualquer em $F(u_1)$ existem, mediante o **Teorema 57**, $c_i \in F$ tais que $v = c_0 + c_1 u_1 + c_2 {u_1}^2 + \cdots + c_{m-1} {u_1}^{m-1}$, onde $m$ é o grau do polinômio minimal de $u_1$. Devido $\beta$ ser um homomorfismo que fixa todos os $u_i$, em particular $u_1$, e todos os elementos de $F$, segue que

$$\begin{aligned} \beta(v) &= \beta(c_0 + c_1 u_1 + c_2 {u_1}^2 + \cdots + c_{m-1} {u_1}^{m-1}) \\ &= \beta(c_0) + \beta(c_1)\beta(u_1) + \beta(c_2)\beta({u_1}^2) + \cdots + \beta(c_{m-1})\beta({u_1}^{m-1}) \\ &= c_0 + c_1 u_1 + c_2 {u_1}^2 + \cdots + c_{m-1} {u_1}^{m-1} = v. \end{aligned}$$

Dessa maneira, para todo $v \in F(u_1)$, $\beta(v) = v$. Analogamente, temos que $\beta(v) = v$ para todo $v \in F(u_1)(u_2) = F(u_1, u_2)$ e posteriormente para $v \in F(u_1, u_2)(u_3) = F(u_1, u_2, u_3)$. Logo, após repetir esse processo por um número finito de vezes teremos que $\beta(v) = v$ para todo $v \in F(u_1, \ldots, u_n) = K$. Portanto, $\iota = \beta = \sigma^{-1} \circ \tau$ e

$$\begin{aligned} \sigma = \sigma \circ \iota &= \sigma \circ (\sigma^{-1}\tau) \\ &= (\sigma \circ \sigma^{-1}) \circ \tau \\ &= \iota \circ \tau = \tau. \end{aligned}$$

□

**Exemplo 52**

1. *Qualquer automorfismo no grupo de Galois de $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ sobre $\mathbb{Q}$ associa, pelo **Teorema 69**, $\sqrt{2}$ a $\sqrt{2}$ ou $-\sqrt{2}$ e $\sqrt{3}$ a $\sqrt{3}$ ou $-\sqrt{3}$, as raízes de $x^2 - 2$ e $x^2 - 3$ respectivamente. Ademais, o **Teorema 71** nos garante que um elemento de $Gal_{\mathbb{Q}}\mathbb{Q}(\sqrt{2}, \sqrt{3})$*

*está completamente determinado por sua ação em $\sqrt{2}$ e $\sqrt{3}$. Logo, deve haver no máximo quatro automorfismos nesse grupo (as quatro possíveis ações em $\sqrt{2}$ e $\sqrt{3}$):*

$$\sqrt{2} \overset{\iota}{\longmapsto} \sqrt{2} \qquad \sqrt{2} \overset{\lambda}{\longmapsto} -\sqrt{2} \qquad \sqrt{2} \overset{\alpha}{\longmapsto} \sqrt{2} \qquad \sqrt{2} \overset{\beta}{\longmapsto} -\sqrt{2}$$

$$\sqrt{3} \overset{\iota}{\longmapsto} \sqrt{3} \qquad \sqrt{3} \overset{\lambda}{\longmapsto} \sqrt{3} \qquad \sqrt{3} \overset{\alpha}{\longmapsto} -\sqrt{3} \qquad \sqrt{3} \overset{\beta}{\longmapsto} -\sqrt{3}$$

*Iremos mostrar que $Gal_{\mathbb{Q}}\mathbb{Q}(\sqrt{2},\sqrt{3})$ é um grupo de ordem 4 construindo os automorfismos $\lambda$, $\alpha$, $\beta$ distintos da identidade.*

• *Construção de $\lambda$: primeiramente, observe que $x^2-2$ é o polinômio minimal de $\sqrt{2}$ e $-\sqrt{2}$ sobre $\mathbb{Q}$ (**Exemplo 47.1.**). Dessa forma, existe, pelo **Teorema 58**, um isomorfismo $\sigma : \mathbb{Q}(\sqrt{2}) \to \mathbb{Q}(-\sqrt{2})$ tal que $\sigma(\sqrt{2}) = -\sqrt{2}$. Além disso, $x^2-3$ é o polinômio minimal de $\sqrt{3}$ e $-\sqrt{3}$ sobre $\mathbb{Q}(\sqrt{2})$ (**Exemplo 48.1.**).*

*Novamente pelo **Teorema 58**, $\sigma$ pode ser estendido à um $\mathbb{Q}$-automorfismo $\lambda$ de $\mathbb{Q}(\sqrt{2})(\sqrt{3}) = \mathbb{Q}(\sqrt{2},\sqrt{3})$ tal que $\lambda(\sqrt{3}) = \sqrt{3}$. Portanto, $\lambda \in Gal_{\mathbb{Q}}\mathbb{Q}(\sqrt{2},\sqrt{3})$ com $\lambda(\sqrt{2}) = \sigma(\sqrt{2}) = -\sqrt{2}$ e $\lambda(\sqrt{3}) = \sqrt{3}$.*

$$\begin{array}{ccc} \mathbb{Q}(\sqrt{2},\sqrt{3}) & \xrightarrow{\lambda} & \mathbb{Q}(\sqrt{2},\sqrt{3}) \\ \big| & & \big| \\ \mathbb{Q}(\sqrt{2}) & \xrightarrow{\sigma} & \mathbb{Q}(-\sqrt{2}) \\ \big| & & \big| \\ \mathbb{Q} & \xrightarrow{\iota} & \mathbb{Q} \end{array}$$

• *Construção de $\alpha$: a produção de $\alpha$ é similar a anterior ao considerar $\mathbb{Q}(\sqrt{2},\sqrt{3}) = \mathbb{Q}(\sqrt{3},\sqrt{2}) = \mathbb{Q}(\sqrt{3})(\sqrt{2})$, ou seja, $\alpha$ será um $\mathbb{Q}$-automorfismo de $\mathbb{Q}(\sqrt{3},\sqrt{2})$ que estende um isomorfismo $\sigma : \mathbb{Q}(\sqrt{3}) \to \mathbb{Q}(-\sqrt{3})$.*

$$\begin{array}{ccc} \mathbb{Q}(\sqrt{3},\sqrt{2}) & \xrightarrow{\alpha} & \mathbb{Q}(\sqrt{3},\sqrt{2}) \\ \big| & & \big| \\ \mathbb{Q}(\sqrt{3}) & \xrightarrow{\sigma} & \mathbb{Q}(-\sqrt{3}) \\ \big| & & \big| \\ \mathbb{Q} & \xrightarrow{\iota} & \mathbb{Q} \end{array}$$

• *Construção de $\beta$: para esse último caso, segue-se de forma semelhante ao da produção de $\lambda$, mas o $\mathbb{Q}$-automorfismo de $\mathbb{Q}(\sqrt{2},\sqrt{3})$ que estende $\sigma$ será $\beta$ tal que $\beta(\sqrt{3}) = -\sqrt{3}$.*

*Salienta-se, ainda, que os três automorfismos $\lambda$, $\alpha$ e $\beta$ possuem ordem 2 em $Gal_{\mathbb{Q}}\mathbb{Q}(\sqrt{2},\sqrt{3})$. Em exemplificação,*

$$(\beta \circ \beta)(\sqrt{2}) = \beta(\beta(\sqrt{2})) = \beta(-\sqrt{2}) = -\beta(\sqrt{2}) = -(-\sqrt{2}) = \sqrt{2} = \iota(\sqrt{2}),$$

*e*

$$(\beta \circ \beta)(\sqrt{3}) = \beta(\beta(\sqrt{3})) = \beta(-\sqrt{3}) = -\beta(\sqrt{3}) = -(-\sqrt{3}) = \sqrt{3} = \iota(\sqrt{3}).$$

*Logo, por intermédio do* ***Teorema 71****,* $\beta \circ \beta = \iota$*. Analogamente, concluiu-se o mesmo para* $\lambda$ *e* $\alpha$*.*

O resultado que segue é um caso particular do **Teorema de Cayley** na Teoria de Grupos.

**Corolário 13** [[5], Corollary 12.5] *Seja* $K$ *o corpo de raízes de um polinômio separável* $f(x)$ *de grau* $n$ *em* $F[x]$*, então* $Gal_F K$ *é isomorfo a um subgrupo de* $S_n$*.*

*Demonstração:* Como $f(x)$ é separável, sabemos que possui $n$ raízes distintas em $K$ digamos $u_1, \ldots, u_n$. Outrossim, vamos considerar $S_n$ como o grupo das permutações do conjunto $R = \{u_1, \ldots, u_n\}$. Agora, se $\sigma \in Gal_F K$, então, pelo **Teorema 69**, $\sigma(u_1), \sigma(u_2), \ldots, \sigma(u_n)$ são raízes de $f(x)$. Além disso, em virtude de $\sigma$ ser injetiva, todos os $\sigma(u_i)$ são distintos e, assim, devem ser os $u_1, u_2, \ldots, u_n$ em alguma ordem, ou seja, restringir $\sigma$ ao conjunto $R$ ($\sigma|_R$) é, na verdade, uma permutação de $R$.

Defina um mapa $\theta$ da seguinte maneira:

$$\begin{aligned} \theta : Gal_F K &\longrightarrow S_n \\ \sigma &\longmapsto \sigma|_R \end{aligned} \quad .$$

Note que $\theta$, com a operação composição de funções, é um homomorfismo de grupos, pois $\theta(\sigma \circ \tau) = (\sigma \circ \tau)|_R = \sigma|_R \circ \tau|_R$ para todo $\sigma, \tau \in Gal_F K$ (veja o comentário abaixo para exemplificação de $\theta$). Desse modo, sendo $K = F(u_1, \ldots, u_n)$ - definição de corpo de raízes - vemos que $\theta$ é injetivo, pois se $\sigma|_R = \tau|_R$ teremos $\sigma(u_i) = \tau(u_i)$ para todo $i = 1, \ldots, n$, e, pelo **Teorema 71**, $\sigma = \tau$. Por fim, sabemos, de imediato, que $\theta$ é sobrejetor com relação ao subconjunto imagem (Im $\theta$) de $S_n$.

Portanto, $Gal_F K$ é isomorfo a Im $\theta$ que é, pelo **Teorema 10**, um subgrupo de $S_n$. □

Para uma melhor compreensão de como $\theta$, definida acima, é um homomorfismo observe que para $n = 4$ tem-se $R = \{u_1, u_2, u_3, u_4\}$. Considere ainda $\sigma, \tau \in Gal_F K$ tais que

$$\tau(u_1) = u_2, \quad \tau(u_2) = u_3, \quad \tau(u_3) = u_4, \quad \tau(u_4) = u_1$$

e

$$\sigma(u_1) = u_3, \quad \sigma(u_2) = u_4, \quad \sigma(u_3) = u_1, \quad \sigma(u_4) = u_2$$

Em notação cíclica, temos (1234) para $\tau|_R$ e (13)(24) para $\sigma|_R$. Nesse sentido, para $u_1$ segue que

$$\theta(\sigma \circ \tau) = (\sigma \circ \tau)(u_1) = \sigma(\tau(u_1)) = \sigma(u_2) = u_4.$$

Por outro lado,

$$\sigma|_R \circ \tau|_R = (13)(24)(1234) = (1432),$$

em outras palavras, a permutação $\sigma|_R \circ \tau|_R$ leva $u_1$ em $u_4$. Similarmente, avaliando $(\sigma \circ \tau)$ em $u_2, u_3, u_4$ concluímos que $\theta(\sigma \circ \tau) = (\sigma \circ \tau)|_R = \sigma|_R \circ \tau|_R$. O entendimento desse homomorfismo $\theta$ configura-se como benéfico, pois uma ideia análoga será utilizada para a demonstração do último Corolário desta sessão.

Outrossim, no **Exemplo 52.1.**, vimos que $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ é o corpo de raízes do polinômio $f(x) = (x^2 - 2)(x^2 - 3)$ e todo automorfismo em $Gal_{\mathbb{Q}}\mathbb{Q}(\sqrt{2}, \sqrt{3})$ permuta as quatro raízes de $f(x)$. Então, fazendo uso do **Corolário 13**, $Gal_{\mathbb{Q}}\mathbb{Q}(\sqrt{2}, \sqrt{3}) \cong H \leq S_4$. Aliás, tem-se como importante esclarecer a seguinte questão: quando $K$ é um corpo raízes de um polinômio $f(x) \in F[x]$, então, pelo **Corolário 13**, cada elemento de $Gal_F K$ produz uma permutação das raízes de $f(x)$, mas uma permutação das raízes não precisa originar-se de um $F$-automorfismo de $K$. Em exemplificação, não existe um $\mathbb{Q}$-automorfismo de $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ que expresse a permutação das raízes

$$\sqrt{2} \longmapsto \sqrt{3}, -\sqrt{2} \longmapsto -\sqrt{3}, \sqrt{3} \longmapsto \sqrt{2}, -\sqrt{3} \longmapsto -\sqrt{2},$$

pois caso existisse, pelo **Teorema 70**, $\sqrt{2}$ e $\sqrt{3}$ teriam o mesmo polinômio minimal, mas isso não acontece em virtude de $x^2 - 2 \neq x^2 - 3$ que são os respectivos polinômios minimais de $\sqrt{2}$ e $\sqrt{3}$ em $\mathbb{Q}[x]$ (os $\mathbb{Q}$-automorfismo de $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ permutam $\sqrt{2}$ em $\sqrt{2}$ ou $-\sqrt{2}$ e $\sqrt{3}$ em $\sqrt{3}$ ou $-\sqrt{3}$).

Frisamos, também, que se $K$ é o corpo de raízes do polinômio $f(x)$, iremos identificar comumente $Gal_F K$ com seu subgrupo isomorfo em $S_n$ tipificando cada automorfismo com a permutação que induz nas raízes de $f(x)$.

Neste momento, iremos definir certos corpos fundamentais a Teoria de Galois. Para isso, seja $K$ um corpo de extensão do corpo $F$. O corpo $E$ de modo que $F \subseteq E \subseteq K$ é chamado

de ***Corpo Intermediário*** da extensão, podendo $K$, nessa situação, ser considerado com uma extensão de $E$.

Ademais, evidencia-se uma peculiaridade, neste contexto, do corpo intermediário $E$ com o seu respectivo grupo de Galois, isto é, podemos constatar que todo automorfismo em $Gal_E K$, conjunto de todos os automorfismos que fixam cada elemento de $E$, está em $Gal_F K$, pois cada automorfismo de $Gal_E K$ fixa automaticamente todos os elementos de $F$ dado que $F \subseteq E$. Desse modo, quando dispusermos de um corpo intermediário $E$ podemos afirmar que $Gal_E K$ é um subgrupo de $Gal_F K$.

**Exemplo 53**

1. *O conjunto $\mathbb{Q}(\sqrt{2})$ é um corpo intermediário da extensão $\mathbb{Q}(\sqrt{2}, \sqrt{3})$. Através do* ***Exemplo 52.1.*** *sabemos que $Gal_{\mathbb{Q}}\mathbb{Q}(\sqrt{2}, \sqrt{3}) = \{\iota, \lambda, \alpha, \beta\}$ e dentre esse grupo os automorfismos que fixam os elementos de $\mathbb{Q}(\sqrt{2})$ são, pelo* ***Teorema 71****, exatamente aqueles mapeiam $\sqrt{2}$ em si mesmo. Portanto, $Gal_{\mathbb{Q}(\sqrt{2})}\mathbb{Q}(\sqrt{2}, \sqrt{3}) = \{\iota, \alpha\}$ que é um subgrupo de $Gal_{\mathbb{Q}}\mathbb{Q}(\sqrt{2}, \sqrt{3}) = \{\iota, \lambda, \alpha, \beta\}$.*

Percebendo esta associação natural de cada corpo intermediário com um subgrupo de Galois, o teorema subsequente explicita como podemos associar um subgrupo $H$ do grupo de Galois a um corpo intermediário da extensão.

**Teorema 72** [[5], Theorem 12.6] *Seja $K$ um corpo de extensão do corpo $F$. Se $H$ é um subgrupo de $Gal_F K$, seja*

$$E_H = \{k \in K \mid \sigma(k) = k \text{ para cada } \sigma \in H\}.$$

*Então, $E_H$ é um corpo intermediário da extensão.*

*Demonstração:* Iremos verificar, primeiramente, que $E_H$ é um subcorpo de $K$ e posteriormente que ele é um corpo intermediário, ou seja, $F \subseteq E_H$.

- <u>*Subcorpo:*</u> Sejam $b, c \in E_H$ e $\sigma \in H$. Logo,

$$\begin{aligned} \sigma(b+c) &= \sigma(b) + \sigma(c) && \text{(pois } \sigma \text{ é um automorfismo)} \\ &= b + c && \text{(pela definição de } E_H\text{)} \end{aligned}$$

e

$$\begin{aligned} \sigma(bc) &= \sigma(b)\sigma(c) \quad \text{(pois } \sigma \text{ é um automorfismo)} \\ &= bc \qquad\qquad \text{(pela definição de } E_H\text{)}. \end{aligned}$$

Desse modo, $E_H$ é fechado sob as operações de adição e multiplicação. Além disso, para todo automorfismo, $\sigma(0_F) = 0_F$ e $\sigma(1_F) = 1_F$, assim, $0_F$ e $1_F$ estão em $E_H$. Agora, pelo **Teorema 23**, para todo elemento não nulo em $E_H$ e qualquer $\sigma \in H$ resulta

$$\sigma(-c) = -c \quad \text{e} \quad \sigma(c^{-1}) = \sigma(c)^{-1} = c^{-1},$$

isto é, $-c \in E_H$ e $c^{-1} \in E_H$. Dessa forma, $E_H$ é um subcorpo de $K$.

• *Corpo Intermediário:* Por $H$ ser um subgrupo de $Gal_F K$, temos $\sigma(c) = c$ para todo $c \in F$ e para todo $\sigma \in H$. Dessa maneira, $F \subseteq E_H$.

Portanto, $E_H$ é um corpo intermediário da extensão.

□

O corpo $E_H$, como definido anteriormente, é denominado de ***Corpo Fixo*** do subgrupo $H$.

**Exemplo 54**

1. *Seja o subgrupo $H = \{\iota, \alpha\}$ do grupo de Galois $Gal_{\mathbb{Q}}\mathbb{Q}(\sqrt{2}, \sqrt{3})$, como no **Exemplo 52.1.**. Pelo fato de $\alpha(\sqrt{2}) = \sqrt{2}$, o subcorpo $\mathbb{Q}(\sqrt{2})$ está contido no corpo fixo $E_H$ de $H$. De outro modo, para mostrar que $E_H = \mathbb{Q}(\sqrt{2})$ deve-se provar que os elementos de $\mathbb{Q}(\sqrt{2})$ são os únicos fixados por $\iota$ e $\alpha$. De fato, $\alpha$ não fixa $\sqrt{3}$, ou seja, $\sqrt{3} \notin E_H$, e $\sqrt{2} \in E_H$, pois tanto $\iota$ quanto $\alpha$ fixam $\sqrt{2}$. Portanto, $E_H = \mathbb{Q}(\sqrt{2})$.*

O próximo resultado é essencial para completar a demonstração do teorema principal deste Capítulo.

**Corolário 14** [[5], Lemma 12.12] *Sejam $K$ um corpo de extensão normal de dimensão finita do corpo $F$ e $E$ um corpo intermediário que é normal sobre $F$. Então, existe um homomorfismo sobrejetor de grupos $\theta : Gal_F K \longrightarrow Gal_F E$ sendo o grupo $Gal_E K$ o seu kernel.*

*Demonstração:* Seja $u \in E$ e $\sigma \in Gal_F K$. Como $E$ é uma extensão normal de $F$, $u$ é algébrico sobre $F$ e seu polinômio minimal $p(x)$ decompõe-se em $E[x]$, em outras palavras, todas as suas raízes estão em $E$. Nesse contexto, pelo **Teorema 69**, $\sigma(u)$ deve ser uma raiz de $p(x)$ e, assim, $\sigma(u) \in E$. Logo, $\sigma(E) \subseteq E$ para algum $\sigma$ em $Gal_F K$. Aliás, a restrição de $\sigma$ em $E$ ($\sigma|_E$) é um $F$-isomorfismo $E \cong \sigma(E)$ e, pelo **Teorema 55**, $[E : F] = [\sigma(E) : F]$. Para mais, devido a $F \subseteq \sigma(E) \subseteq E$ e por meio do **Teorema 54**, temos

$$[E : F] = [E : \sigma(E)][\sigma(E) : F] \quad \Rightarrow \quad [E : \sigma(E)] = 1.$$

Então, como visto na **Observação 2**, $E = \sigma(E)$ e $\sigma|_E$ é, na realidade, um automorfismo de $Gal_F E$.

Agora, definamos o mapa (semelhante ao definido no **Corolário 13**) $\theta : Gal_F K \longrightarrow Gal_F E$ dado por $\theta(\sigma) = \sigma|E$. Observe que $\theta$, como indicado e sob a operação composição de funções, é um homomorfismo de grupos, uma vez que $\theta(\sigma \circ \tau) = (\sigma \circ \tau)|_E = \sigma|_E \circ \tau|_E$ para todo $\sigma, \tau \in Gal_F K$ (comentário ilustrativo abaixo) e seu kernel consiste dos automorfismos de $K$ que restritos a $E$ são iguais ao mapa identidade, isto é, o subgrupo de $Gal_E K$.

Vamos mostrar, por fim, que $\theta$ é sobrejetivo. Observe que, por intermédio do **Teorema 64**, $K$ é um corpo de raízes sobre $F$ e, assim, $K$ é um corpo de raízes do mesmo polinômio sobre $E$ pela **Proposição 4**.

$$\begin{array}{ccc} K & \xrightarrow{\sigma} & K \\ | & & | \\ E & \xrightarrow{\tau} & E \\ | & & | \\ F & \xrightarrow{\iota} & F \end{array}$$

Logo, o **Teorema 63** nos mostra que todo automorfismo $\tau \in Gal_F E$ pode ser estendido para um $F$-automorfismo $\sigma \in Gal_F K$ (diagrama ao lado). Consequentemente, $\sigma|_E = \tau$, ou seja, $\theta(\sigma) = \tau$.

Portanto, $\theta$ é um homomorfismo sobrejetor cujo kernel é o grupo $Gal_E K$.

□

Buscando verificar o caráter homomórfico de $\theta$, considere $F = \mathbb{Q}$, o corpo intermediário $E = \mathbb{Q}(\sqrt{2})$ do **Exemplo 53.1.** e $K = \mathbb{Q}(\sqrt{2}, \sqrt{3})$. Logo,

$$\begin{array}{c} \theta : Gal_{\mathbb{Q}}\mathbb{Q}(\sqrt{2}, \sqrt{3}) \longrightarrow Gal_{\mathbb{Q}}\mathbb{Q}(\sqrt{2}) \\ \sigma \longmapsto \sigma|_{\mathbb{Q}(\sqrt{2})} \end{array}.$$

Pelo **Exemplo 52.1.**, sabemos que $Gal_{\mathbb{Q}}\mathbb{Q}(\sqrt{2}) = \{\iota, \lambda\}$. Dessa forma, $\beta|_{\mathbb{Q}(\sqrt{2})} = \lambda$ e

$\alpha|_{\mathbb{Q}(\sqrt{2})} = \iota$ e portanto, $\theta$ assim definida é um homomorfismo, pois

$$\theta(\alpha \circ \lambda) = (\alpha \circ \lambda)|_{\mathbb{Q}(\sqrt{2})} = (\alpha \circ \lambda)(\sqrt{2}) = \alpha(\lambda(\sqrt{2})) = \alpha(-\sqrt{2}) = -\sqrt{2},$$

ou simplesmente,

$$\begin{array}{c} \theta(\alpha \circ \lambda) = \sigma(\lambda) \\ \sqrt{2} \longmapsto -\sqrt{2} \end{array} .$$

Por outro lado,

$$\begin{array}{ll} \theta(\alpha) = \iota & \\ \sqrt{2} \longmapsto \sqrt{2} & \end{array} \quad \text{e} \quad \begin{array}{ll} \theta(\lambda) = \lambda & \\ \sqrt{2} \longmapsto -\sqrt{2} & \end{array} .$$

Daí,

$$\sigma(\alpha) \circ \sigma(\lambda) = (\iota \circ \lambda)(\sqrt{2}) = \iota(\lambda(\sqrt{2})) = \iota(-\sqrt{2}) = -\sqrt{2}.$$

Desse modo, $\sigma(\alpha \circ \lambda) = (\alpha \circ \lambda)|_{\mathbb{Q}(\sqrt{2})} = \alpha|_{\mathbb{Q}(\sqrt{2})} \circ \lambda|_{\mathbb{Q}(\sqrt{2})}$. Ademais, similarmente temos

$$\begin{array}{ll} \theta(\alpha \circ \lambda) = \sigma(\lambda) & \\ \sqrt{2} \longmapsto -\sqrt{2} & \end{array} , \quad \begin{array}{ll} \theta(\lambda) = \lambda & \\ \sqrt{2} \longmapsto -\sqrt{2} & \end{array} \quad \text{e} \quad \begin{array}{ll} \theta(\beta) = \lambda & \\ \sqrt{2} \longmapsto -\sqrt{2} & \end{array} .$$

Então,

$$\sigma(\lambda) \circ \sigma(\beta) = (\lambda \circ \beta)(\sqrt{2}) = \lambda(\beta(\sqrt{2})) = \lambda(-\sqrt{2}) = -(-\sqrt{2}) = \sqrt{2}.$$

Consequentemente, $\sigma(\lambda \circ \beta) = (\lambda \circ \beta)|_{\mathbb{Q}(\sqrt{2})} = \lambda|_{\mathbb{Q}(\sqrt{2})} \circ \beta|_{\mathbb{Q}(\sqrt{2})}$. Mais ainda,

$$\ker(\theta) = \{\iota, \alpha\} = Gal_{\mathbb{Q}(\sqrt{2})}\mathbb{Q}(\sqrt{2}, \sqrt{3}).$$

**Observação 7** *Para um corpo de extensão $K$ do corpo $F$ e um corpo intermediário $E$ normal sobre $F$ temos que se $\sigma \in Gal_F K$ então $\sigma|_E \in Gal_F E$. De fato, no primeiro parágrafo da demonstração do* ***Corolário 14*** *concluímos que o $F$-isomorfismo $\sigma|_E$, com $\sigma \in Gal_F K$, na verdade é um automorfismo de $Gal_F E$ sem utilizar o fato de $K$ ser normal sobre $F$.*

Em síntese, na presente seção explanou-se um caráter fundamental deste trabalho, isto é, o Grupo de Galois e as características relativas a ele. Tal arcabouço será essencial a próxima seção cujas últimas peças serão identificadas para a apresentação e verificação do resultado medular da Teoria de Galois.

## 4.2 Teorema Fundamental da Teoria de Galois

O eixo central da teoria de Galois é relacionar as propriedades da extensão de um corpo com as de seu grupo de Galois, garantindo correspondências entre os corpos intermediários e os subgrupos do grupo de Galois.

Nesse sentido, seja $S$ o conjunto de todos os corpos intermediários e $T$ o conjunto de todos os subgrupos do grupo de Galois $Gal_F K$, com $K$ sendo uma extensão de dimensão finita de $F$. Iremos definir o mapa $\phi : S \longrightarrow T$ dada por:

$$\phi(E) = Gal_E K, \text{ para cada corpo intermediário } E.$$

Nomearemos a relação $\phi$ por ***Correspondência de Galois***. Logo, é possível verificar que $K$, considerando-o subcorpo de si mesmo, corresponde ao subgrupo identidade de $Gal_F K$ e o subcorpo $F$, com relação a si próprio, corresponde a todo o grupo $Gal_F K$.

**Exemplo 55**

1. *Se considerarmos a correspondência de Galois $\phi$ para a extensão $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ de $\mathbb{Q}$ e o corpo intermediário $\mathbb{Q}(\sqrt{2})$ teremos, como observado no* ***Exemplo 53.1.****,*

$$\mathbb{Q}(\sqrt{2}, \sqrt{3}) \xmapsto{\phi} Gal_{\mathbb{Q}(\sqrt{2},\sqrt{3})}\mathbb{Q}(\sqrt{2}, \sqrt{3}) = \{\iota\}$$

$$\mathbb{Q}(\sqrt{2}) \xmapsto{\phi} Gal_{\mathbb{Q}(\sqrt{2})}\mathbb{Q}(\sqrt{2}, \sqrt{3}) = \{\iota, \alpha\}$$

$$\mathbb{Q} \xmapsto{\phi} Gal_{\mathbb{Q}}\mathbb{Q}(\sqrt{2}, \sqrt{3}) = \{\iota, \lambda, \alpha, \beta\}$$

Agora, iremos analisar e edificar as condições adequadas para que a correspondência de Galois seja um mapeamento bijetivo entre o conjunto dos corpos intermediários e o conjunto dos subgrupos de $Gal_F K$.

**Corolário 15** [[5], Lemma 12.7] *Seja $K$ um corpo de extensão de dimensão finita do corpo $F$. Se $H$ é um subgrupo do grupo de Galois $Gal_F K$ e $E$ é o corpo fixo de $H$, então $K$ é uma extensão separável, normal e simples de $E$.*

*Demonstração:* Para a verificação do presente resultado, iremos provar, inicialmente, que $K$ é uma extensão separável, em seguida que ele é simples e, por fim, normal de $E$.

• *Extensão Separável:* Inicialmente, através do **Teorema 59**, cada $u \in K$ é algébrico sobre $F$ e, assim, é algébrico sobre $E$ pela **Proposição 3**. Ademais, pelo **Teorema 69**, todo automorfismo em $H$ deve mapear $u$ em alguma raiz de seu polinômio minimal $p(x) \in E[x]$. Logo, $u$ tem um número finito de imagens distintas sob automorfismos em $H$, digamos $u = u_1, u_2, \ldots, u_t \in K$.

Nesse contexto, seja $\sigma \in H$ e $u_i = \tau(u)$, com $\tau \in H$. Como $\sigma \circ \tau \in H$, vemos que $\sigma(u_i)$ é também uma imagem de $u$, ou seja, deve estar no conjunto $\{u_1, u_2, \ldots, u_t\}$. Devido $\sigma$ ser injetiva, os elementos $\sigma(u_1), \sigma(u_2), \ldots, \sigma(u_t)$ são $t$ imagens distintas de $u$ e, dessa forma, eles têm de ser um dos elementos $u_1, u_2, \ldots, u_t$ em alguma ordem. Em outras palavras, todo automorfismo em $H$ permuta $u_2, u_2, \ldots, u_t$.

Agora, considerando $f(x) \in K[x]$ dado por

$$f(x) = (x - u_1)(x - u_2) \cdots (x - u_t),$$

temos que $f(x)$ é separável, pois todos os $u_i$ são distintos.

*Afirmação:* $f(x)$ está, na verdade, em $E[x]$. De fato, seja $\sigma \in H$ e, como descrito na **Observação 3**, $\sigma$ induz um isomorfismo $K[x] \cong K[x]$, denominado de $\sigma'$, que age sobre os coeficientes dos polinômios em $K[x]$. Então,

$$\sigma'(f(x)) = (x - \sigma(u_1))(x - \sigma(u_2)) \cdots (x - \sigma(u_t)).$$

Em virtude de $\sigma$ permutar os $u_i$, isto é, um rearranjo dos fatores de $f(x)$, segue que $\sigma'(f(x)) = f(x)$. Dessa maneira, todo automorfismo de $H$ mapeia os coeficientes do polinômio separável $f(x)$ para si mesmo. Daí, esses coeficientes estão em $E$ (o corpo fixo de $H$) o que demonstra a afirmação.

Diante disto, como $u = u_1$ é uma raiz de $f(x) \in E[x]$, $u$ é separável sobre $E$, consequentemente, pela arbitrariedade de $u$, $K$ é uma extensão separável de $E$.

• *Extensão Simples:* Por $K$ ser de dimensão finita sobre $F$, temos que $K$ é finitamente gerado sobre $F$, como analisado no item **ii)** da **Observação 4**. Logo, como $[K : F]$ é finito e $[K : F] = [K : E][E : F]$, $K$ é finitamente gerado sobre $E$, o que acarreta, pelo **Teorema 67**, em $K = E(u)$ para algum $u \in K$.

• *Extensão Normal:* Considere o polinômio $f(x)$ como descrito na prova anterior de separabilidade de $K$ sobre $F$. Nesse cenário, temos que $f(x)$ decompõe-se em $K[x]$ e, por

consequência, $K = E(u)$ é o corpo de raízes de $f(x)$ sobre $E$. Desse modo, pelo **Teorema 11.15** , $K$ é normal sobre $E$.

Portanto, $K$ é uma extensão separável, normal e simples de $E$.

□

Uma ilustração do **Corolário 15** é o **Exemplo 55.1.** quando faz-se $K = \mathbb{Q}(\sqrt{2}, \sqrt{3})$, $E = \mathbb{Q}(\sqrt{2})$ e $H = \{\iota, \alpha\}$.

**Teorema 73** [[5], Theorem 12.8] *Seja $K$ um corpo de extensão de dimensão finita do corpo $F$. Se $H$ é um subgrupo do grupo de Galois $Gal_F K$ e $E$ é o corpo fixo de $H$, então $H = Gal_E K$ e $|H| = [K : E]$. Portanto, a correspondência de Galois é sobrejetiva.*

*Demonstração:* Vimos no **Corolário 15** que $K = E(u)$ para algum $u \in K$. Considerando que o polinômio minimal $p(x)$ de $u$ sobre $E$ possui grau $n$, então $[K : E] = n$ pelo **Teorema 57**. Observa-se, pelos **Teoremas 69** e **71**, que os distintos automorfismos de $Gal_E K$ mapeiam $u$ sobre distintas raízes de $p(x)$. Consequentemente, o número de automorfismos distintos em $Gal_E K$ é no máximo $n$ (quantidade de raízes de $p(x)$).

Agora, devido $E$ ser o conjunto de todos os elementos de $K$ fixados pelos automorfismos de $H$ (definição de corpo fixo) e $Gal_E K$ conter todos os automorfismos que fixam $E$ segue que $H \subseteq Gal_E K$. Logo,

$$|H| \leq |Gal_E K| \leq n = [K : E].$$

Outrossim, seja $f(x)$ um polinômio como na prova do **Corolário 15**. Nesse sentido, $H$ contém pelo menos $t$ automorfismos, o número das distintas imagens de $u$ sob $H$. Dessa forma, como $u = u_1$ é uma raiz de $f(x)$, por meio do **Teorema 56**, $p(x)$ divide $f(x)$. À vista disso,

$$|H| \geq t = \partial f(x) \geq \partial p(x) = n = [K : E].$$

Portanto, das desigualdades anteriores, $|H| = |Gal_E K| = [K : E]$ e, por isso, $H = Gal_E K$.

□

**Observação 8** *Nota-se que a correspondência de Galois pode não ser injetiva. Por exemplo, todo automorfismo no grupo de $\mathbb{Q}(\sqrt[3]{2})$ sobre $\mathbb{Q}$ deve mapear $\sqrt[3]{2}$ para uma raiz de*

$x^3 - 2$, *pelo* ***Teorema 69****. Como todos os elementos de* $\mathbb{Q}(\sqrt[3]{2})$ *são números reais (****Teorema 57****) e* $\sqrt[3]{2}$ *é a única raiz real desse polinômio (sendo* $w\sqrt[3]{2}$ *e* $w^2\sqrt[3]{2}$ *as outras duas raízes, onde* $w = (-1+\sqrt{3}i)/2$*), tem-se que cada automorfismo em* $Gal_{\mathbb{Q}}\mathbb{Q}(\sqrt[3]{2})$ *mapeia* $\sqrt[3]{2}$ *em si mesmo. Logo, mediante o* ***Teorema 71****,* $Gal_{\mathbb{Q}}\mathbb{Q}(\sqrt[3]{2}) = \{\iota\}$*.*

*Nesse contexto, ambos os corpos intermediários* $\mathbb{Q}(\sqrt[3]{2})$ *e* $\mathbb{Q}$ *estão associados com* $\{\iota\}$ *sob a correspondência de Galois, ou seja, ela não é injetiva. Além disso, observa-se que* $\mathbb{Q}(\sqrt[3]{2})$ *não é uma extensão normal de* $\mathbb{Q}$*.*

## Extensão de Galois

A **Observação 8** anterior evidência que a correspondência de Galois, apesar de ser sobrejetiva pelo **Teorema 73**, pode não ser injetiva. Logo, para garantir a injetividade necessita-se acrescentar hipótese sobre a extensão sendo a normalidade e a separabilidade possíveis candidatos pelo que foi analisado nas provas e exemplos anteriores.

**Definição 37** [[5], page 417] *Se* $K$ *e um corpo de extensão separável, normal e de dimensão finita do corpo* $F$*, diremos que* $K$ *é uma* ***Extensão de Galois*** *de* $F$ *ou que* $K$ *é* ***Galois*** *sobre* $F$*.*

Observamos que uma extensão de Galois de característica 0 é, na realidade, um corpo de raízes, pelos **Teoremas 64** e **Teorema 66**.

**Teorema 74** [[5], Theorem 12.9] *Sejam* $K$ *uma extensão de Galois de* $F$ *e* $E$ *um corpo intermediário. Então* $E$ *é o corpo fixo do subgrupo* $Gal_E K$*.*

*Demonstração:* Seja $E_0$ o corpo fixo do subgrupo $Gal_E K$. Por definição, temos que $E \subset E_0$. Logo, resta provar que $E_0 \subset E$ e para isso vamos provar a contrapositiva: Se $u \notin E$, então $u$ é movido por algum automorfismo em $Gal_E K$, ou seja, $u \notin E_0$. Como $K$ é um uma extensão de Galois do corpo intermediário $E$ (normal de dimensão finita pelo **Teorema 64** e pela **Proposição 4**; separável pela **Proposição 5**), ele é uma extensão algébrica de $E$. Assim, $u$ é algébrico sobre $E$ com algum polinômio minimal $p(x) \in E[x]$ de grau maior ou igual a 2, pois se $\partial p(x) = 1$, então $u \in E$.

Outrossim, pela separabilidade, as raízes de $p(x)$ são todas distintas e, pela normalidade, todas estão em $K$. Desse modo, para uma raiz $v$ de $p(x)$ diferente de $u$, existe um automorfismo $\sigma \in Gal_E K$ tal que $\sigma(u) = v$, por meio do **Teorema 70**. Ou seja, $u$ não é fixado pelos automorfismos de $Gal_E K$. Portanto, $u \notin E_0$, e daí $E = E_0$.

□

Salienta-se que se $E$ e $H$ são dois corpos intermediários com $Gal_E K = Gal_H K$, então o **Teorema 74** nos ilustra que tanto $E$ quanto $H$ são os corpos fixados pelo mesmo grupo, e, assim, $E = H$. Portanto, *a correspondência de Galois é injetiva para extensões de Galois.*

**Corolário 16** [[5], Corollary 12.10] *Seja $K$ um corpo de extensão de dimensão finita sobre um corpo $F$. Então, $K$ é Galois sobre $F$ se, e somente se, $F$ e o corpo fixo do grupo de Galois $Gal_F K$.*

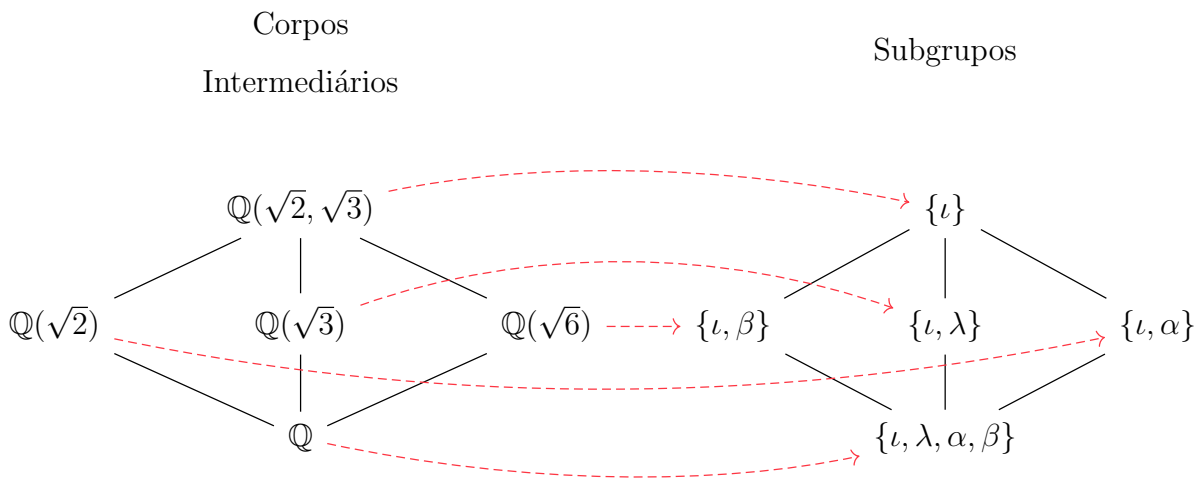
*Demonstração:* ($\Longrightarrow$) Supondo que $K$ é Galois sobre $F$, então pelo **Teorema 74** com $E = F$, mostra-se que $F$ é o corpo fixado por $Gal_F K$.

($\Longleftarrow$) Agora, se $F$ é o corpo fixo de $Gal_F K$, então, através do **Corolário 15** com $E = F$, verifica-se que $K$ é Galois sobre $F$.

Portanto, o corpo de extensão $K$ de $F$ é Galois sobre $F$ se, e somente se, $F$ e o corpo fixo do grupo de Galois $Gal_F K$.

□

Note que o corpo $\mathbb{Q}(\sqrt{2}, \sqrt{3})$, como no **Exemplo 55.1.**, é uma extensão de Galois de $\mathbb{Q}$ justamente por ele ser o corpo de raízes de $f(x) = (x^2 - 2)(x^2 - 3)$ (separável, pois $\sqrt{2} \neq \sqrt{3}$; e normal de dimensão finita pelo **Teorema 64** - $[\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}] = 4$), sendo $Gal_{\mathbb{Q}}\mathbb{Q}(\sqrt{2}, \sqrt{3}) = \{\iota, \lambda, \alpha, \beta\}$ mediante o **Exemplo 52.1.**. Desse modo, através do **Teorema 73** e pela observação feita após o **Teorema 74**, a correspondência de Galois é bijetiva para esse caso. Logo, os diagramas abaixo ilustram como os subcorpos e os subgrupos estão na mesma posição relativa sob a correspondência de Galois. Como exemplificação, o **Exemplo 53.1.** mostra-nos que $\mathbb{Q}(\sqrt{2})$ corresponde a $\{\iota, \alpha\}$.




Observe que, neste caso, todos os corpos intermediários são extensão de Galois de $\mathbb{Q}$ ($\mathbb{Q}(\sqrt{2})$ é o corpo de raízes de $x^2-2$). Ademais, os subgrupos correspondentes do grupo de Galois são normais e uma conjuntura semelhante ocorre no caso geral elucidado abaixo.

**Teorema 75 (Teorema Fundamental da Teoria de Galois)** [[5], Theorem 12.11] *Se $K$ é um corpo de extensão de Galois do corpo $F$, então:*

*1) Existe uma bijeção entre o conjunto $S$ de todos os corpos intermediários da extensão $K$ e do conjunto $T$ de todos os subgrupos do grupo de Galois $Gal_F K$. Ademais,*

$$[K:E] = |Gal_F K| \ \ e \ \ [E:F] = [Gal_F K : Gal_E K].$$

*2) Um corpo intermediário $E$ é uma extensão normal de $F$ se, e somente se, o grupo correspondente $Gal_E K$ é um subgrupo normal de $Gal_F K$ e, nesse caso, $Gal_F E \cong Gal_F K / Gal_E K$.*

*Demonstração: 1)* Temos que correspondência de Galois é sobrejetora pelo **Teorema 73** e injetora pela observação do **Teorema 74**, ou seja, ela é uma bijeção entre os conjuntos $S$ e $T$. Além disso, o **Teorema 74** nos garante que cada corpo intermediário $E$ é o corpo fixo de $Gal_E K$, consequentemente, $[K:E] = |Gal_E K|$ pelo **Teorema 73**. Em particular, se $F = E$, então $[K:F] = |Gal_F K|$. Logo, utilizando o **Teorema de Lagrange** e **Teorema 54** segue que

$$[K:E][E:F] = [K:F] = |Gal_F K| = |Gal_E K|[Gal_F K : Gal_E K].$$

Simplificando os termos iguais na equação acima, isto é, $[K : F] = |Gal_F K|$, concluímos que

$$[E : F] = [Gal_F K : Gal_E K].$$

*2)* ($\Longleftarrow$) Vamos assumir, inicialmente, que $Gal_E K$ é um subgrupo normal de $Gal_F K$. Se $f(x)$ é um polinômio irredutível em $F[x]$, com uma raiz $u \in E$, devemos mostrar que $f(x)$ decompõe-se em $E[x]$. Pela normalidade de $K$ sobre $F$, sabemos que $f(x)$ se decompõe em $K[x]$, então precisa-se verificar apenas que cada raiz $v$ de $f(x)$ em $K$ está, na verdade, em $E$. Pelo **Teorema 70**, existe um automorfismo $\sigma \in Gal_F K$ tal que $\sigma(u) = v$. Ademais, para um elemento qualquer $\tau$ de $Gal_E K$, por esse subgrupo ser normal, tem-se $\tau \circ \sigma = \sigma \circ \tau_1$ para algum $\tau_1 \in Gal_E K$. Como $u \in E$, temos

$$\tau(v) = \tau(\sigma(u)) = \sigma(\tau_1(u)) = \sigma(u) = v.$$

Desse modo, $v$ é fixado por qualquer elemento $\tau$ em $Gal_E K$ e, portanto, deve estar no corpo fixo de $Gal_E K$, ou seja, o corpo $E$ como ilustrado no **Teorema 74**.

($\Longrightarrow$) Supondo, agora, que $E$ é uma extensão normal de $F$, tem-se que $E$ tem dimensão finita sobre $F$, pois, pela prova do item (1) deste Teorema, $[K : F] = |Gal_F K|$ e $[K : E] = |Gal_E K|$ são finitos, assim $[E : F]$ é finito. Por intermédio do **Corolário 14**, existe um homomorfismo sobrejetor de grupos $\theta : Gal_F K \to Gal_F E$ cujo kernel é $Gal_E K$. Dessa foma, $Gal_E K$ é um subgrupo normal de $Gal_F K$, mediante o **Teorema 14**, e $Gal_F K / Gal_E K \cong Gal_F E$ pelo **1º Teorema de Isomorfismo para Grupos**. □

Em síntese, o **Teorema Fundamental da Teoria de Galois**, além de garantir a existência da bijetividade na correspondência de Galois para extensões de Galois, determina a normalidade de um dado corpo intermediário mediante a normalidade de um subgrupo associado. Tal relação agudamente próxima entre essas duas estruturas algébricas distintas confere à Teoria de Galois uma rica e bela profundidade teórica. Ademais, com o intuito de vivificar os conceitos trabalhados por esse teorema, no capítulo seguinte se abordará alguns exemplos.

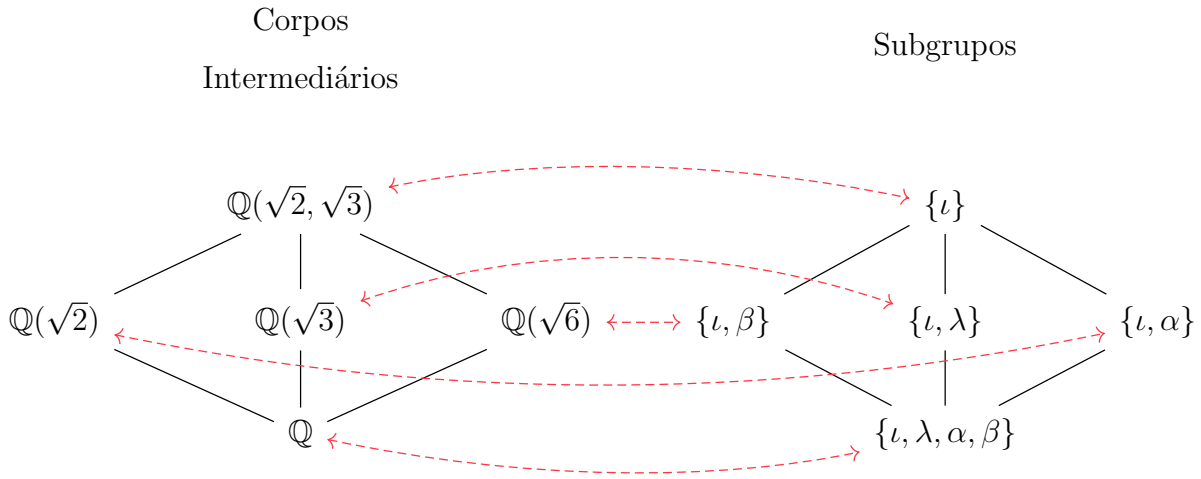
# Capítulo 5

# Exemplos da Teoria de Galois

Objetivando elucidar as ideias transmitidas pelo **Teorema Fundamental da Teoria de Galois** são exibidos abaixo alguns exemplos onde serão calculados os grupos de Galois sobre os racionais $\mathbb{Q}$. Neles perceberemos que a correspondência de Galois reverte a inclusão dos corpos, isto é, se $K$ é um corpo de extensão do corpo $F$, $F \subseteq K$, e $Gal_K K$ e $Gal_F K$ são seus respectivos grupos de Galois, então $Gal_K K \subseteq Gal_F K$, como pode ser observado no **Exemplo 55.1.**.

## Exemplo 1

Vimos, no capítulo anterior, que o corpo $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ é uma extensão de Galois de $\mathbb{Q}$ sendo $Gal_{\mathbb{Q}}\mathbb{Q}(\sqrt{2}, \sqrt{3}) = \{\iota, \lambda, \alpha, \beta\}$, e obteve-se o seguinte diagrama cujo elementos estão posicionados relativamente sob a correspondência de Galois




Todavia, isto ocorre de maneira geral para polinômios que possuem fatores $(x^2 - t)(x^2 - q)$

com $t$ e $q$ primos entre si. De fato, como $t$ e $q$ são primos entre si segue que $\pm\sqrt{t}$ e $\pm\sqrt{q}$, as raízes, respectivamente, de $(x^2-t)$ e $(x^2-q)$, são irracionais pelo Teorema de Fundamental da Aritmética. Ademais, por meio do **Critério de Eisenstein**, com $p = t$, $x^2 - t$ é irredutível sobre $\mathbb{Q}$, consequentemente $x^2 - t$ é irredutível sobre $\mathbb{Q}$. Aliás, tem-se que $\pm\sqrt{q} \notin \mathbb{Q}(\sqrt{t})$, pois caso contrário teria-se

$$\pm\sqrt{q} = a + b\sqrt{t}, \text{ com } a, b \in \mathbb{Q}.$$

Elevando ao quadrado ambos os lados da igualdade acima, temos

$$q = a^2 + 2ab\sqrt{t} + tb^2 \Rightarrow \sqrt{t} = \frac{q - a^2 - tb^2}{2ab},$$

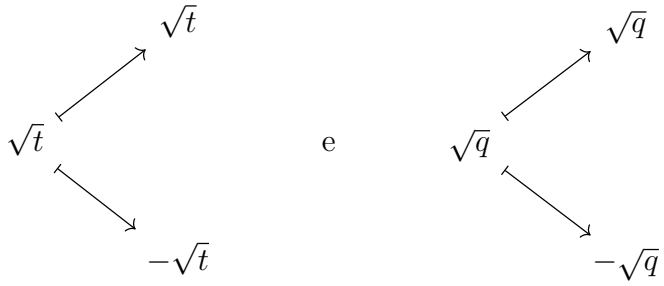
contradizendo a irracionalidade de $\sqrt{t}$. Analogamente, tem-se uma contradição caso $a = 0$ ou $b = 0$. Logo, $\pm\sqrt{q} \notin \mathbb{Q}(\sqrt{t})$ com $x^2 - q$ sendo o seu polinômio minimal. Assim, pode-se considerar o seguinte encadeamento de extensões simples:

$$\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{t}) \subseteq \mathbb{Q}(\sqrt{t})(\sqrt{q}) = \mathbb{Q}(\sqrt{t}, \sqrt{q}).$$

Outrossim, como $\{1, \sqrt{t}\}$ é uma base para $\mathbb{Q}(\sqrt{t})$ e $\{1, \sqrt{q}\}$ é uma base para $\mathbb{Q}(\sqrt{t}, \sqrt{q})$ sobre $\mathbb{Q}(\sqrt{t})$, segue-se que

$$\{1, \sqrt{t}, \sqrt{q}, \sqrt{t}\sqrt{q}\}$$

é uma base para $\mathbb{Q}(\sqrt{t}, \sqrt{q})$. Logo, pelo fato de $[\mathbb{Q}(\sqrt{t}, \sqrt{q}) : \mathbb{Q}] = 4$ devemos ter que $|Gal_{\mathbb{Q}}\mathbb{Q}(\sqrt{t}, \sqrt{q})| = 4$. Tendo em vista que cada um dos quatro automorfismo de $\sigma$ em $Gal_{\mathbb{Q}}\mathbb{Q}(\sqrt{t}, \sqrt{q})$ é completamente determinado por sua ação nos elementos da base $\{1, \sqrt{t}, \sqrt{q}, \sqrt{t}\sqrt{q}\}$ (**Teorema 71**), e esses valores são, por sua vez, determinados por $\sigma(\sqrt{t})$ e $\sigma(\sqrt{q})$, as possíveis opções são




Como $\sigma(\sqrt{t})$ deve ser sempre uma das duas raízes de $x^2 - t$ sobre $\mathbb{Q}$ e $\sigma(\sqrt{q})$ é uma das raízes de $x^2 - q$ pelo **Teorema 69**, tem-se que as duas possibilidades para $\sigma(\sqrt{t})$

combinadas com as duas possibilidades para $\sigma(\sqrt{q})$, devem fornecer os quatro automorfismos de $Gal_{\mathbb{Q}}\mathbb{Q}(\sqrt{t},\sqrt{q})$, como descrito a seguir

| | $\iota$ | $\tau_1$ | $\tau_2$ | $\tau_3$ |
|---|---|---|---|---|
| $\sqrt{t}\to$ | $\sqrt{t}$ | $-\sqrt{t}$ | $\sqrt{t}$ | $-\sqrt{t}$ |
| $\sqrt{q}\to$ | $\sqrt{q}$ | $\sqrt{q}$ | $-\sqrt{q}$ | $-\sqrt{q}$ |

Por exemplo, $\tau_1(\sqrt{t}) = -\sqrt{t}$ e $\tau_1(\sqrt{q}) = \sqrt{q}$. Agora, veja que:

- $(\tau_2 \circ \tau_3)(\sqrt{t}) = \tau_2(\tau_3(\sqrt{t})) = \tau_2(-\sqrt{t}) = -\sqrt{t}$,
- $(\tau_2 \circ \tau_3)(\sqrt{q}) = \tau_2(\tau_3(\sqrt{q})) = \tau_2(-\sqrt{q}) = \sqrt{q}$.

Nesse sentido, $\tau_2 \circ \tau_3 = \tau_1$. Por outro lado,

- $(\tau_3 \circ \tau_2)(\sqrt{t}) = \tau_3(\tau_2(\sqrt{t})) = \tau_3(\sqrt{t}) = -\sqrt{t}$,
- $(\tau_3 \circ \tau_2)(\sqrt{q}) = \tau_3(\tau_2(\sqrt{q})) = \tau_3(-\sqrt{q}) = \sqrt{q}$.

Então, $\tau_3 \circ \tau_2 = \tau_1$. Logo, notamos que $\tau_2 \circ \tau_3 = \tau_3 \circ \tau_2$, em outras palavras, $Gal_{\mathbb{Q}}\mathbb{Q}(\sqrt{t},\sqrt{q})$ é abeliano. Outrossim, verificando a tabela tem-se que

- $\tau_1, \tau_2$ e $\tau_3$ possuem ordem 2, isto é, $\tau_i^2 = \iota$.

Objetivando determinar os subgrupos de $Gal_{\mathbb{Q}}\mathbb{Q}(\sqrt{t},\sqrt{q})$, verificamos, pelo **Corolário 13**, que $Gal_{\mathbb{Q}}\mathbb{Q}(\sqrt{t},\sqrt{q})$ é isomorfo a um subgrupo de $S_4$, mas a ordem dos elementos de $Gal_{\mathbb{Q}}\mathbb{Q}(\sqrt{t},\sqrt{q})$ é a mesma dos elementos de $S_4$ e eles se comportam de maneira similar, ou seja, $Gal_{\mathbb{Q}}\mathbb{Q}(\sqrt{t},\sqrt{q}) \cong S_4$. Dessa maneira, analisando os automorfismos obtidos, tem-se que os subgrupos de $Gal_{\mathbb{Q}}\mathbb{Q}(\sqrt{t},\sqrt{q})$ são:

| Ordem 1 | Ordem 2 | Ordem 4 |
|---|---|---|
| $H_1 = \{\iota\} = \langle\iota\rangle$ | $H_2 = \{\iota, \tau_1\} = \langle\tau_1\rangle$ | $H_5 = Gal_{\mathbb{Q}}\mathbb{Q}(\sqrt{t},\sqrt{q}) \cong S_4$ |
| | $H_3 = \{\iota, \tau_2\} = \langle\tau_2\rangle$ | |
| | $H_4 = \{\iota, \tau_3\} = \langle\tau_3\rangle$ | |

A determinação do corpo fixo $E_{H_i}$ de cada $H_i$ $(1 \leq i \leq 5)$ é feita utilizando ativamente o aspecto bijetor da correspondência de Galois, são eles:

- $\underline{E_{H_1} \text{ e } E_{H_5}}$: o subcorpo $E_{H_1}$ será a extensão de $\mathbb{Q}$ fixada por $\{\iota\}$, ou seja, $\mathbb{Q}(\sqrt{t},\sqrt{q})$, já $E_{H_5}$ é o subcorpo cujo todos os elementos são fixados por cada automorfismo de $Gal_{\mathbb{Q}}\mathbb{Q}(\sqrt{t},\sqrt{q}) = \{\iota, \tau_1, \tau_2, \tau_3\}$ e o único que se encaixa nessa condição é o próprio $\mathbb{Q}$.

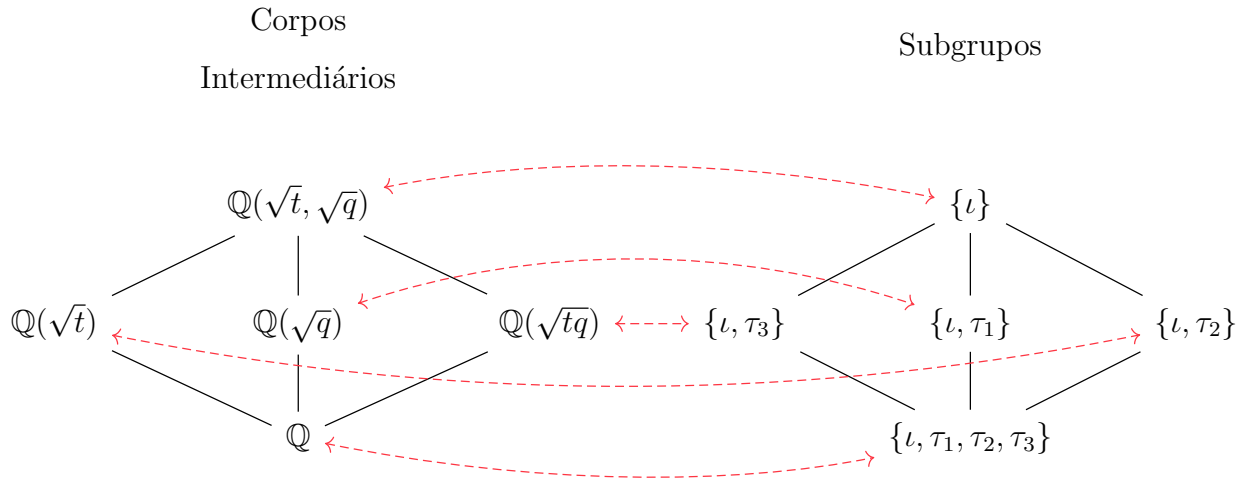
- $\underline{E_{H_2}}$: para encontrar $E_{H_2}$ basta determinar uma extensão de $\mathbb{Q}$ deixada fixa por $\{\iota, \tau_1\}$. Como $\iota$ e $\tau_1$ deixam $\sqrt{q}$ fixo, $\mathbb{Q}(\sqrt{q})$ é o corpo que procuramos;

- $\underline{E_{H_3}}$: de forma similar para $E_{H_3}$ é o bastante mostrar uma extensão de $\mathbb{Q}$ deixada fixada por $\{\iota, \tau_2\}$. Como $\iota$ e $\tau_2$ deixam $\sqrt{t}$ fixo, o corpo desejado é $\mathbb{Q}(\sqrt{t})$;

- $\underline{E_{H_4}}$: analogamente, é suficiente mostrar uma extensão de $\mathbb{Q}$ deixada fixada por $\{\iota, \tau_3\}$. Observe que

  - $\iota(\sqrt{t}\sqrt{q}) = \sqrt{t}\sqrt{q}$;
  - $\tau_3(\sqrt{t}\sqrt{q}) = \tau_3(\sqrt{t})\tau_3(\sqrt{q}) = (-\sqrt{t})(-\sqrt{q}) = \sqrt{t}\sqrt{q}$;
  - $\tau_1(\sqrt{t}\sqrt{q}) = \tau_1(\sqrt{t})\tau_1(\sqrt{q}) = (-\sqrt{t})(\sqrt{q}) = -\sqrt{t}\sqrt{q} = \tau_2$.

Logo, corpo de extensão de $\mathbb{Q}$ procurado é $\mathbb{Q}(\sqrt{t}\sqrt{q}) = \mathbb{Q}(\sqrt{tq})$. Portanto, os diagramas abaixo retratam os corpos intermediários com seus respectivos grupos de Galois associados




## Exemplo 2

Seja o polinômio $f(x) = x^3 - 2$ sobre $\mathbb{Q}$. Pelo **Critério de Eisenstein**, com $p = 2$, $f(x)$ é irredutível sobre $\mathbb{Q}$. Ademais, claramente o valor $u = \sqrt[3]{2}$ é uma raiz de $f(x)$ e $u \notin \mathbb{Q}$. Logo, tome $\mathbb{Q}(u)$ como um corpo de extensão de $\mathbb{Q}$ que contém a raiz $u$. Como $x^3 - 2$ é o polinômio minimal de $u$, pelo **Teorema 57**, $[\mathbb{Q}(u) : \mathbb{Q}] = 3$. Vimos no **Exemplo 39.1.** que as outras duas raízes de $f(x)$ são os números complexos $u\omega$ e $u\omega^2$, onde

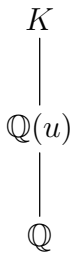
$$\omega = \cos\frac{2\pi}{3} + i\sin\frac{2\pi}{3} = -\frac{1}{2} + \frac{\sqrt{3}}{2}i,$$

ou seja, não estão em $\mathbb{Q}(u)$.

Logo, seja $K$ um corpo de extensão de $\mathbb{Q}(u)$, como ao lado, que contenha $i\sqrt{3}$, isto é,

$$K = \mathbb{Q}(u)(i\sqrt{3}) = \mathbb{Q}(u, i\sqrt{3}).$$

Pelo fato de $K$ conter todas as raízes de $f(x)$ ele é o corpo de raízes de $f(x)$ sobre $\mathbb{Q}$.

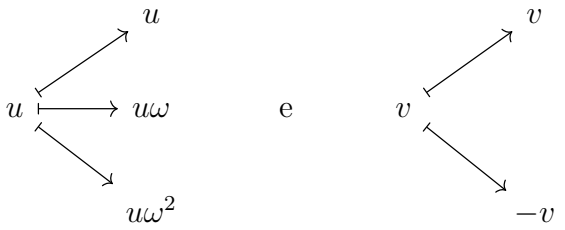



Note que $\{1, u, u^2\}$ é uma base para $\mathbb{Q}(u)$ sobre $\mathbb{Q}$ e $\{1, i\sqrt{3}\}$ é uma base para $K$ sobre $\mathbb{Q}(u)$ (o polinômio minimal de $i\sqrt{3}$ em $K$ sobre $\mathbb{Q}$ é $x^2 + 3$). Então,

$$\{1, u, u^2, v, uv, u^2v\}$$

é uma base para $K$ sobre $\mathbb{Q}$, onde $u = \sqrt[3]{2}$ e $v = i\sqrt{3}$. Logo, como $[K : \mathbb{Q}] = 6$ devemos ter que $|Gal_{\mathbb{Q}}K)| = 6$.

Agora, vamos terminar os seis automorfismos de $Gal_{\mathbb{Q}}K$. Sabemos, pelo **Teorema 71**, que cada automorfismo $\sigma$ em $Gal_{\mathbb{Q}}K$ é completamente determinado por sua ação nos elementos da base $\{1, u, u^2, v, uv, u^2v\}$, e esses valores são, por sua vez, determinados por $\sigma(u)$ e $\sigma(v)$, ou seja, as possíveis opções são




Todavia, pelo **Teorema 69**, $\sigma(u)$ deve ser sempre uma das três raízes de $f(x) = x^3 - 2$ sobre $\mathbb{Q}$. Da mesma forma, $\sigma(v)$ deve ser uma raiz de seu polinômio minimal $x^2 + 3$. Assim, as três possibilidades para $\sigma(u)$ combinadas com as duas possibilidades para $\sigma(v)$, devem fornecer os seis automorfismos, como descrito abaixo

| | $\iota$ | $\tau_1$ | $\tau_2$ | $\varphi_1$ | $\varphi_2$ | $\varphi_3$ |
|---|---|---|---|---|---|---|
| $u \to$ | $u$ | $u\omega$ | $u\omega^2$ | $u$ | $u\omega$ | $u\omega^2$ |
| $v \to$ | $v$ | $v$ | $v$ | $-v$ | $-v$ | $-v$ |

Logo, por exemplo, $\tau_1(u) = u\omega$ e $\tau_1(v) = v$. Ademais, note que:

- $(\varphi_1 \circ \tau_2)(u) = \varphi_1(\tau_2(u)) = \varphi_1(u\omega^2) = \varphi_1(u)\varphi_1(u) = uw^3 = u$,
  pois $\omega^3 = 1$, neste caso;
- $(\varphi_1 \circ \tau_2)(v) = \varphi_1(\tau_2(v)) = \varphi_1(v) = -v$.

Nesse sentido, $\varphi_1 \circ \tau_2 = \varphi_1$. Por outro lado,

- $(\tau_2 \circ \varphi_1)(u) = \tau_2(\varphi_1(u)) = \tau_2(u) = uw^2$,
- $(\tau_2 \circ \varphi_1)(v) = \tau_2(\varphi_1(v)) = \tau_2(-v) = -v$.

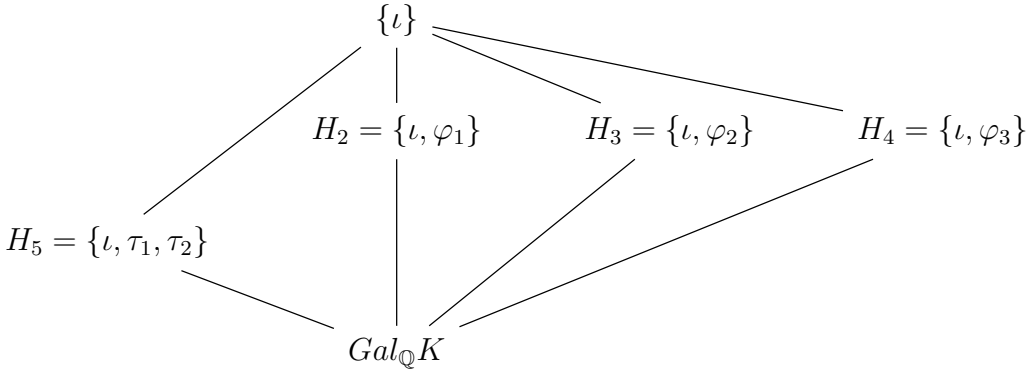
Então, $\tau_2 \circ \varphi_1 = \varphi_3$. Desse modo, vemos que $\varphi_1 \circ \tau_2 \neq \tau_2 \circ \varphi_1$, em outras palavras, $Gal_{\mathbb{Q}}K$ não é abeliano. Outrossim, analisando a tabela tem-se que

- $\tau_1$ e $\tau_2$ possuem ordem 3, isto é, $\tau_i^3 = \iota$;
- $\varphi_1, \varphi_2$ e $\varphi_3$ têm ordem 2.

Com o intuito de determinar os subgrupos de $Gal_{\mathbb{Q}}K$, temos, pelo **Corolário 13**, que $Gal_{\mathbb{Q}}K$ é isomorfo a um subgrupo de $S_3$, porém a ordem dos elementos de $Gal_{\mathbb{Q}}K$ é a mesma dos elementos de $S_3$ e eles se comportam de maneira similar, isto é, $Gal_{\mathbb{Q}}K \cong S_3$. Assim sendo, analisando os automorfismos obtidos e notando que $\tau_1^2 = \tau_2$, segue que os subgrupos de $Gal_{\mathbb{Q}}K$ são:

| Ordem 1 | Ordem 2 | Ordem 3 | Ordem 6 |
|---|---|---|---|
| $H_1 = \{\iota\} = \langle\iota\rangle$ | $H_2 = \{\iota, \varphi_1\} = \langle\varphi_1\rangle$ | $H_5 = \{\iota, \tau_1, \tau_2\} = \langle\tau_1\rangle$ | $H_6 = Gal_{\mathbb{Q}}K \cong S_3$ |
| | $H_3 = \{\iota, \varphi_2\} = \langle\varphi_2\rangle$ | | |
| | $H_4 = \{\iota, \varphi_3\} = \langle\varphi_3\rangle$ | | |

Logo, temos o seguinte diagrama dos subgrupos de $Gal_{\mathbb{Q}}K$




Para estabelecer cada corpo fixo $E_{H_i}$ de cada subgrupo $H_i$ $(1 \leq i \leq 6)$ de $Gal_{\mathbb{Q}}K$ iremos utilizar fortemente o caráter bijetor da correspondência de Galois, lembrando que:

$$\omega = -\frac{1}{2} + \frac{v}{2} \quad \text{e} \quad \omega^2 = -\frac{1}{2} - \frac{v}{2}.$$

- $\underline{E_{H_1} \text{ e } E_{H_6}}$: o subcorpo $E_{H_1}$ será a extensão de $\mathbb{Q}$ fixada por $\{\iota\}$, isto é, $\mathbb{Q}(u, \omega)$, enquanto $E_{H_6}$ é o subcorpo cujo todos os elementos são fixados por cada automorfismo de $Gal_{\mathbb{Q}}K = \{\iota, \tau_1, \tau_2, \varphi_1, \varphi_2, \varphi_3\}$ e o único que se encaixa nessa condição é $\mathbb{Q}$.

- $\underline{E_{H_2}}$: para encontrar $E_{H_2}$ basta determinar uma extensão de $\mathbb{Q}$ deixada fixada por $\{\iota, \varphi_1\}$. Como $\iota$ e $\varphi_1$ deixam $u$ fixo, $E_{H_2} = \mathbb{Q}(u)$;

- $\underline{E_{H_5}}$: similarmente, é suficiente mostrar uma extensão de $\mathbb{Q}$ deixada fixada por $\{\iota, \tau_1, \tau_2\}$. Como $\iota$, $\tau_1$ e $\tau_2$ deixam $v$ fixo, nota-se que $\mathbb{Q}(\omega)$ é o corpo desejado, pois

  - $\iota(\omega) = \omega$;
  - $\tau_1(\omega) = \tau_2\left(-\frac{1}{2} + \frac{v}{2}\right) = -\frac{1}{2} + \frac{v}{2} = \omega$;
  - $\tau_2(\omega) = \tau_2\left(-\frac{1}{2} + \frac{v}{2}\right) = -\frac{1}{2} + \frac{v}{2} = \omega$.

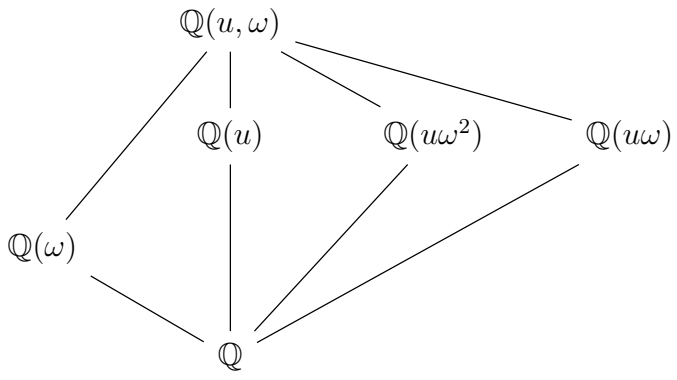
- $\underline{E_{H_3}}$: para determinar o subcorpo $E_{H_3}$ notamos que a extensão $\mathbb{Q}(u\omega^2)$ de $\mathbb{Q}$ é a fixada por $\{\iota, \varphi_2\}$, pois

  - $\iota(u\omega^2) = u\omega^2$,
  - $\varphi_2(u\omega^2) = \varphi_2\left(-\frac{u}{2} - \frac{uv}{2}\right) = -\frac{u\omega}{2} + \frac{u\omega v}{2} = u\omega\left(-\frac{1}{2} + \frac{v}{2}\right) = u\omega^2$.

- $\underline{E_{H_4}}$: a determinação de $E_{H_4}$, segue análoga a de $E_{H_3}$, observando que a extensão $\mathbb{Q}(u\omega)$ de $\mathbb{Q}$ é a fixada por $\{\iota, \varphi_3\}$, justamente por

  - $\iota(u\omega) = u\omega$,
  - $\varphi_3(u\omega) = \varphi_3\left(-\frac{u}{2} + \frac{uv}{2}\right) = -\frac{u\omega^2}{2} - \frac{u\omega^2 v}{2} = u\omega^2\left(-\frac{1}{2} - \frac{v}{2}\right) = u\omega^2\omega^2 = u\omega$.

Portanto, a rede dos respectivos corpos intermediários dos subgrupos de Galois quando $f(x) = x^3 - 2$ é



## Exemplo 3

Faremos uma análise similar aos exemplos anteriores, porém com o polinômio $f(x) = x^4 - 2$ sobre $\mathbb{Q}$.

Pelo **Critério de Eisenstein**, com $p = 2$, $f(x)$ é irredutível sobre $\mathbb{Q}$. Ademais, claramente o valor $u = \sqrt[4]{2}$ é uma raiz real de $f(x)$. Como $u \notin \mathbb{Q}$, tome $\mathbb{Q}(u)$ como um corpo de extensão de $\mathbb{Q}$ que contém a raiz $u$. Outrossim, como comentado após a definição das raiz n-ésima primitiva da unidade (**Definição 26**) as raízes de $f(x)$ são os valores complexos

$$u, -u, iu, -iu,$$

pois, neste caso,

$$\omega = \cos\frac{2\pi}{4} + i\sin\frac{2\pi}{4} = \cos\frac{\pi}{2} + i\sin\frac{\pi}{2} = i.$$

Observa-se, ainda, que o corpo de raízes $K$ de $x^4 - 2$ sobre $\mathbb{Q}$ deve conter $i$ e como $i \notin \mathbb{Q}(u) \subseteq \mathbb{R}$, tem-se que $\mathbb{Q}(u) \neq K$. Todavia, se adjuntarmos $i$ a $\mathbb{Q}(u)$, notamos que $\mathbb{Q}(u, i)$ contém todas as raízes de $f(x)$, consequentemente $K = \mathbb{Q}(u, i)$ (diagrama ao lado).

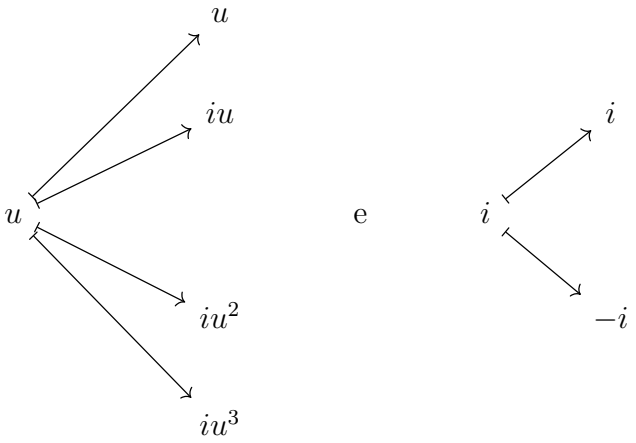
$$\begin{array}{c} K = \mathbb{Q}(u,i) \\ | \\ \mathbb{Q}(u) \\ | \\ \mathbb{Q} \end{array}$$

Aliás, é fácil ver que o polinômio minimal de $i$ sobre $\mathbb{Q}(u)$ é $x^2 + 1$, cujas raízes são $\pm i$. Agora, como $\{1, u, u^2, u^3\}$ é uma base para $\mathbb{Q}(u)$ sobre $\mathbb{Q}$ e $\{1, i\}$ é uma base para $K$ sobre $\mathbb{Q}(u)$, tem-se que

$$\{1, u, u^2, u^3, i, iu, iu^2, iu^3\}$$

é uma base para $K$ sobre $\mathbb{Q}$. Logo, pelo fato de $[K : \mathbb{Q}] = 8$ devemos ter que $|Gal_{\mathbb{Q}}K| = 8$.

Vamos terminar, nesse momento, os oito automorfismos de $Gal_{\mathbb{Q}}K$. Sabemos, pelo **Teorema 71**, que cada automorfismo $\sigma$ em $Gal_{\mathbb{Q}}K$ é completamente determinado por sua ação nos elementos da base $\{1, u, u^2, u^3, i, iu, iu^2, iu^3\}$, e esses valores são, por sua vez, determinados por $\sigma(u)$ e $\sigma(i)$, ou seja, as possíveis opções são




No entanto, pelo **Teorema 69**, $\sigma(u)$ deve ser sempre uma das quatro raízes de $f(x) = x^4 - 2$ sobre $\mathbb{Q}$. Similarmente, $\sigma(i)$ deve ser uma das duas raiz de seu polinômio minimal $x^2 + 1$. Assim, as quatro possibilidades para $\sigma(u)$ combinadas com as duas possibilidades para $\sigma(i)$, devem fornecer os oito automorfismos, como descrito abaixo

| | $\iota$ | $\tau$ | $\tau^2$ | $\tau^3$ | $\varphi$ | $\tau \circ \varphi$ | $\tau^2 \circ \varphi$ | $\tau^3 \circ \varphi$ |
|---|---|---|---|---|---|---|---|---|
| $u \to$ | $u$ | $iu$ | $-u$ | $-iu$ | $u$ | $iu$ | $-u$ | $-iu$ |
| $i \to$ | $i$ | $i$ | $i$ | $i$ | $-i$ | $-i$ | $-i$ | $-i$ |

Por exemplo, $\tau^2(u) = -u$ e $\tau^2(i) = i$. Ademais, veja que:

- $(\varphi \circ \tau)(u) = \varphi(\tau(u)) = \varphi(iu) = \varphi(i)\varphi(u) = -iu$,
- $(\varphi \circ \tau)(i) = \varphi(\tau(i)) = \varphi(i) = -i$.

Por outro lado,

- $(\tau \circ \varphi)(u) = iu$,
- $(\tau \circ \varphi)(i) = -i$.

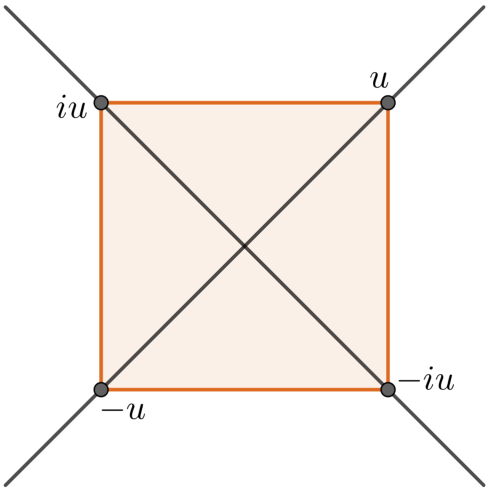
Então, vemos que $\varphi \circ \tau \neq \tau \circ \varphi$, em outras palavras, $Gal_{\mathbb{Q}}K$ não é abeliano. Outrossim, analisando a tabela tem-se que

- $\tau$ e $\tau^3$ possuem ordem 4, isto é, $(\tau^3)^4 = \iota$;
- $\tau^2, \varphi, \tau \circ \varphi, \tau^2 \circ \varphi, \tau^3 \circ \varphi$ têm ordem 2.

Para determinar os subgrupos de $Gal_{\mathbb{Q}}K$, notamos que, pelo fato de $Gal_{\mathbb{Q}}K$ possuir ordem 8 e ser não abeliano, através do **Teorema 12**, ele será isomorfo a $D_4$ ou $Q_8$. No

entanto, como $Gal_{\mathbb{Q}}K$ possui geradores de ordem 4 e 2 e isso caracteriza o grupo $D_4$. Nesse sentido, $Gal_{\mathbb{Q}}K \cong D_4$. Recorde que $D_4$ é definido como o grupo de todas as simetrias do quadrado. Logo, classificando os quatro vértices desse polígono regular como as raízes de $f(x) = x^4 - 2$ (figura abaixo) de modo que as simetrias sejam as permutações de $Gal_{\mathbb{Q}}K$.

Figura 5.1: Simetrias do quadrado cujos vértices são as raízes de $f(x) = x^4 - 2$.

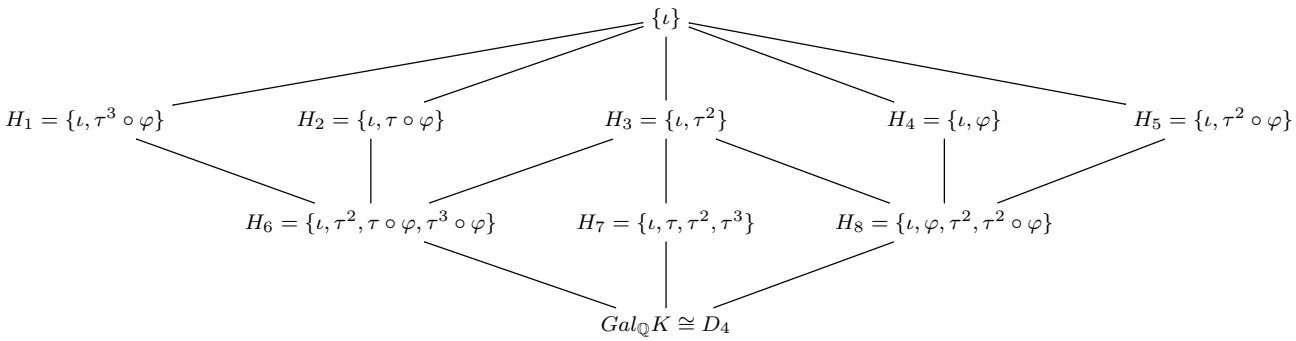



Fonte: De autoria própria.

Assim sendo, os subgrupos de $Gal_{\mathbb{Q}}K$ são:

| Ordem 1 | Ordem 2 | Ordem 4 | Ordem 8 |
|---|---|---|---|
| $H_0 = \{\iota\}$ | $H_1 = \{\iota, \tau^3 \circ \varphi\}$ | $H_6 = \{\iota, \tau^2, \tau \circ \varphi, \tau^3 \circ \varphi\}$ | $Gal_{\mathbb{Q}}K \cong D_4$ |
| | $H_2 = \{\iota, \tau \circ \varphi\}$ | $H_7 = \{\iota, \tau, \tau^2, \tau^3\}$ | |
| | $H_3 = \{\iota, \tau^2\}$ | $H_8 = \{\iota, \varphi, \tau^2, \tau^2 \circ \varphi\}$ | |
| | $H_4 = \{\iota, \varphi\}$ | | |
| | $H_5 = \{\iota, \tau^2 \circ \varphi\}$ | | |

Dessa maneira, tem-se o diagrama abaixo dos subcorpos de $Gal_{\mathbb{Q}}K$:




Para determinar cada corpo fixo $E_{H_i}$ de cada subgrupo $H_i$ $(0 \leq i \leq 8)$ de $Gal_{\mathbb{Q}}K$ iremos utilizar fortemente o caráter bijetor da correspondência de Galois:

- $\underline{E_{H_0} \text{ e } E_{Gal_{\mathbb{Q}}K}}$: o subcorpo $E_{H_0}$ será a extensão de $\mathbb{Q}$ fixada por $\{\iota\}$, isto é, $\mathbb{Q}(u, i)$, enquanto $E_{Gal_{\mathbb{Q}}K}$ é o subcorpo cujo todos os elementos são fixados por cada automorfismo de $Gal_{\mathbb{Q}}K = \{\iota, \tau, \tau^2, \tau^3, \varphi, \tau \circ \varphi, \tau^2 \circ \varphi, \tau^3 \circ \varphi\}$ e o único que se encaixa nessa condição é $\mathbb{Q}$.

- $\underline{E_{H_7}}$: o subcorpo $E_{H_7}$ será a extensão de $\mathbb{Q}$ de grau 2 fixada por $\{\iota, \tau, \tau^2, \tau^3\}$. Vendo que cada um desses automorfismos deixa $i$ fixo, $\mathbb{Q}(i)$ é o corpo procurado.

- $\underline{E_{H_6}}$: buscando encontrar $E_{H_6}$ deve-se determinar uma extensão de $\mathbb{Q}$ de grau 2 deixada fixa por $\{\iota, \tau^2, \tau \circ \varphi, \tau^3 \circ \varphi\}$. Como $\iota$, $\tau^2$, $\tau \circ \varphi$ e $\tau^3 \circ \varphi$ deixam $iu^2$ fixo, pois

  - $\iota(iu^2) = iu^2$;
  - $\tau^2(iu^2) = \tau^2(i)\tau^2(u^2) = i\tau^2(u \cdot u) = i\tau^2(u)\tau^2(u) = iu$;
  - $(\tau \circ \varphi)(iu^2) = \tau(\varphi(iu^2)) = \tau(-iu^2) = \tau(-i)\tau(u)\tau(u) = (-i)(iu)(iu) = iu^2$;
  - $(\tau^3 \circ \varphi)(iu^2) = \tau^3(\varphi(iu^2)) = \tau^3(-iu^2) = \tau^3(-i)\tau^3(u)\tau^3(u) = (-i)(-iu)(-iu) = iu^2$.

Logo, $\mathbb{Q}(iu^2)$ é a extensão desejada. Observe que $u^2 = (\sqrt[4]{2})^2 = \sqrt{2}$, ou seja, $E_{H_6} = \mathbb{Q}(i\sqrt{2})$.

- $\underline{E_{H_8}}$: similarmente ao caso anterior, é suficiente mostrar uma extensão de $\mathbb{Q}$ de grau 2 fixada por $\{\iota, \varphi, \tau^2, \tau^2 \circ \varphi\}$. Observe que cada um desses automorfismos deixam $u^2$ fixo:

  - $\iota(u^2) = u^2$;
  - $\varphi(u^2) = \varphi(u)\varphi(u) = (u)(u) = u^2$;
  - $\tau^2(u^2) = \tau^2(u)\tau^2(u) = (-u)(-u) = u^2$;
  - $(\tau^2 \circ \varphi)(u^2) = \tau^2(\varphi(u^2)) = \tau^2(u^2) = \tau^2(u)\tau^2(u) = u^2$.

Nesse sentido, $E_{H_8} = \mathbb{Q}(u^2)$, mas como $u^2 = (\sqrt[4]{2})^2 = \sqrt{2}$ temos que $E_{H_8} = \mathbb{Q}(\sqrt{2})$.

- $\underline{E_{H_4}}$: ao analisar a tabela dos oito automorfismos, verificamos que $u$ é o único elemento fixado por $H_4 = \{\iota, \varphi\}$. Logo, extensão $\mathbb{Q}(u)$ de $\mathbb{Q}$ é a fixada por $H_4$.

- $\underline{E_{H_5}}$: a determinação de $E_{H_5}$, segue análoga a de $E_{H_4}$, observando que a extensão $\mathbb{Q}(iu)$ de $\mathbb{Q}$ é a fixada por $\{\iota, \tau^2\varphi\}$, justamente por

  - $\iota(iu) = iu$
  - $\tau^2\varphi(iu) = \tau^2(\varphi(iu)) = \tau^2(-iu) = (-i)(-u) = iu.$

Desse modo, $E_{H_5} = \mathbb{Q}(iu)$

- $\underline{E_{H_3}}$: analisamos que a extensão $\mathbb{Q}(u^2, i)$ de $\mathbb{Q}$ é a fixada por $\{\iota, \tau^2\}$, pois

  - $\iota(u^2) = u^2$
  - $\tau^2(u^2) = \tau^2(u)\tau^2(u) = (-u)(-u) = u^2$

e

  - $\iota(i) = i$
  - $\tau^2(i) = i.$

Logo, $E_{H_3} = \mathbb{Q}(u^2, i)$, ou ainda, como $u^2 = \sqrt{2}$, $E_{H_3} = \mathbb{Q}(\sqrt{2}, i)$.

- $\underline{E_{H_2}}$: para determinar $E_{H_2}$, observamos que para qualquer $k \in K$ o elemento $\iota(k) + (\tau \circ \varphi)(k)$ fica fixo por $\iota$ e $\tau \circ \varphi$. Fazendo $k = u$, vemos que

$$\iota(u) + (\tau \circ \varphi)(u) = u + iu$$

é fixado por $H_2 = \{\iota, \tau \circ \varphi\}$, pois

  - $\iota(u + iu) = u + iu$
  - $(\tau \circ \varphi)(u + iu) = \tau(\varphi(u + iu)) = \tau(u - iu) = iu - (i)(iu) = u + iu.$

Assim, $E_{H_2} = \mathbb{Q}(u + iu)$.

- $\underline{E_{H_1}}$: nota-se que para qualquer $k \in K$ o elemento $\iota(k) - (\tau^3 \circ \varphi)(k)$ é deixado fixo por $\iota$ e $\tau^3 \circ \varphi$. Tomando $k = u$, vemos que

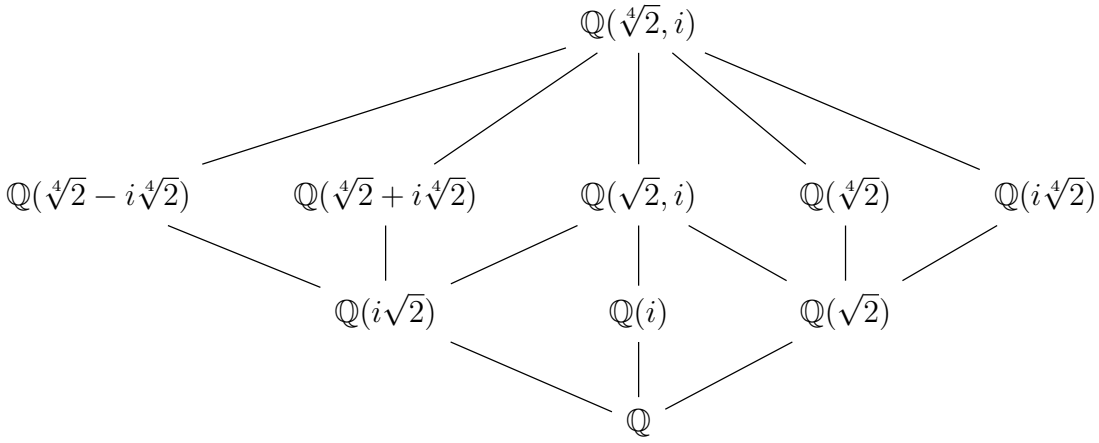
$$\iota(u) - (\tau^3 \circ \varphi)(u) = u - iu$$

é fixado por $H_1 = \{\iota, \tau^3 \circ \varphi\}$, pois

- $\iota(u - iu) = u - iu$
- $(\tau^3 \circ \varphi)(u - iu) = \tau^3(\varphi(u - iu)) = \tau^3(u + iu) = -iu + (i)(-iu) = u - iu.$

Nesse sentido, $E_{H_1} = \mathbb{Q}(u - iu)$.

Portanto, a reticulado dos respectivos corpos intermediários dos subgrupos de Galois quando $f(x) = x^4 - 2$ é



# Considerações Finais

Em síntese, além de compreender aspectos elementares da Álgebra Abstrata, o presente trabalho viabilizou o entendimento das propriedades dos corpos de extensão (simples, algébricos, separáveis, normais) sob a ótica de adjunção de raízes de polinômios. Ademais, a partir desse arcabouço inicial, pode-se assimilar os principais saberes envoltos a Teoria de Galois como, por exemplo, as peculiaridades dos grupos de Galois e a correspondência entre os corpos intermediários com esses grupos. Diante disso, mesmo havendo atualmente métodos numéricos/algébricos atrelados ao uso softwares matemáticos auxiliando na determinação de raízes polinomiais, a beleza e profundidade teórica da Teoria de Galois permanecem vigorosas e instigantes.

# Referências Bibliográficas


[1] COELHO, Flávio Ulhoa; LOURENÇO, Mary Lilian. **Um Curso de Álgebra Linear**. 2001.

[2] DOMINGUES, Hygino H.; IEZZI, Gelson. **Álgebra Moderna**. Saraiva Educação SA, 1970.

[3] FRALEIGH, John B. **A First Course in Abstract Algebra**. 2008.

[4] GALLIAN, Joseph. **Contemporary Abstract Algebra**. Chapman and Hall/CRC. 2021.

[5] HUNGERFORD, Thomas W. **Abstract Algebra: An Introduction**. 2013.

[6] SILVA, Marco Antônio. **Grupos Finitos**. 2002.

[7] STEWART, Ian. **Galois Theory**. CRC press, 2022.