



UNIVERSIDADE ESTADUAL PAULISTA “JÚLIO DE MESQUITA FILHO”

Instituto de Geociências e Ciências Exatas

Câmpus de Rio Claro-SP

Juliana Débora da Silva

Resoluções de equações polinomiais e a insolubilidade da quintica

Rio Claro-SP

2023



UNIVERSIDADE ESTADUAL PAULISTA “JÚLIO DE MESQUITA FILHO”

Instituto de Geociências e Ciências Exatas

Câmpus de Rio Claro-SP

Resoluções de equações polinomiais e a insolubilidade da quártica

Juliana Débora da Silva

Dissertação apresentada como parte dos requisitos para obtenção do título de Mestre em Matemática, junto ao Programa de Pós-Graduação em Matemática, mestrado profissional, do Instituto de Geociências e Ciências Exatas da Universidade Estadual Paulista “Júlio de Mesquita Filho”, Câmpus de Rio Claro-SP.

Orientadora

Profa. Dra. Elíris Cristina Rizziolli

Rio Claro-SP

2023

S586r Silva, Juliana Débora da
Resoluções de equações polinomiais e a insolubilidade da quártica /
Juliana Débora da Silva. -- Rio Claro, 2023
119 p.

Dissertação (mestrado profissional) - Universidade Estadual
Paulista (Unesp), Instituto de Geociências e Ciências Exatas, Rio
Claro
Orientadora: Elíris Cristina Rizzioli

1. Álgebra. 2. Teoria de Galois. I. Título.

Sistema de geração automática de fichas catalográficas da Unesp. Biblioteca do Instituto de
Geociências e Ciências Exatas, Rio Claro. Dados fornecidos pelo autor(a).

Essa ficha não pode ser modificada.

TERMO DE APROVAÇÃO

Juliana Débora da Silva

RESOLUÇÕES DE EQUAÇÕES POLINOMIAIS E A INSOLUBILIDADE DA QUÍNTICA

Dissertação APROVADA como requisito parcial para a obtenção do grau de Mestre no Curso de Pós-Graduação em Matemática, mestrado profissional, do Instituto de Geociências e Ciências Exatas da Universidade Estadual Paulista “Júlio de Mesquita Filho”, pela seguinte banca examinadora:

Profa. Dra. Elíris Cristina Rizziolli
Orientadora

Profa. Dra. Iara Andrea Alvares Fernandes
Faculdade de Matemática - PUC - Campinas (SP)

Prof. Dr. Lucas Antônio Caritá
IFSP - São José dos Campos (SP)

Rio Claro, 25 de outubro de 2023

Ao meu pai (in memoriam).

Agradecimentos

Essa parte do trabalho, apesar de estar no começo, foi a última a ser escrita. Aqui escrevo em primeira pessoa e exponho, de fato, o quanto esse trabalho foi realizado a muitas mãos.

Início agradecendo ao meu Deus, minhas irmãs, Tatiane e Cibele, minha mãe, meus sobrinhos Carol, Vini e Sophia, vocês que mesmo muitas vezes longe fisicamente se fizeram presentes de várias formas e me apoiaram nessa caminhada.

Nesse percurso, que teve cerca de três anos e meio, teve amiga que se tornou amor, minha leitora, corretora e incentivadora maior Janaina Mayra. Obrigada por cada abraço, palavra de acolhimento e motivação. Você é luz por onde passa, e que sorte a minha ter você ao meu lado iluminando os meus dias. Tiveram amigas que se reuniram para ouvir a apresentação online e outras que me acompanharam até de madrugada, para me dar sugestões e força quando tudo parecia tão nebuloso. Obrigada Raquel Lais, Priolinha, Alê, Jana Jana, Vivi, Fer Freitas, Maria Eugênia, Giovanna Bertonha e Melicia Geromini.

Pela paciência em esperar pelos passeios e por estar sempre ao meu lado, obrigada, Chico.

Agradeço aos meus alunos, são por e para vocês todas essas conquistas.

À minha orientadora Elíris, por toda a paciência, aprendizado, disponibilidade e generosidade. A realização desse sonho não seria possível sem o seu apoio.

Aos professores da banca da qualificação e da defesa, Lucas, Iara e Alexandrina pelos ensinamentos e apontamentos valiosos.

Após mais de 20 anos, agradeço a Tânia Vilela, minha professora da então sétima série que me mostrou as belezas da matemática e me inspirou e incentivou como docente durante todos esses anos.

Que sorte a minha ter vocês em minha vida. Meu muito obrigada hoje e sempre!

*“Lutar por um lugar
No mundo e conseguir
Libertar...”*

Sandy e Júnior

Resumo

Esta dissertação tem como objetivo explorar a história e os métodos de resoluções possíveis para equações de grau igual ou menor que cinco e tratar da impossibilidade de resolução por meio de radicais de equações gerais de grau igual a cinco. Para isso, serão explorados conceitos algébricos pertencentes à Teoria de Galois.

Palavras-chave: Álgebra, Equação, História da Matemática, Resolução por Radicais, Teoria de Galois.

Abstract

This dissertation aims to explore the history and potential methods of solving equations of a degree equal to or less than five. It also addresses the impossibility of solving these equations using general radical expressions with a degree of five. To achieve these objectives, the dissertation will delve into algebraic concepts within the Galois Theory.

Keywords: Algebra, Equation, Mathematics History, Radical Resolution, Galois Theory.

Sumário

1	Introdução	10
2	O estudo das equações algébricas	12
2.1	Equações do primeiro grau	12
2.2	Equações quadráticas	15
2.3	Equações do terceiro grau	20
2.4	Equações do quarto grau	23
3	Noções básicas de estruturas algébricas	27
3.1	Grupos	28
3.2	Anéis e Corpos	40
3.3	Anéis de Polinômios	56
4	Elementos da Teoria de Galois	67
4.1	Sobre Extensões de Corpos	70
4.2	Corpo de Galois	82
4.3	O grupo de automorfismos $G(E/F)$	85
4.4	<i>Splitting</i> corpo, extensão separável e o grupo de Galois $G(K/F)$	92
4.5	O Teorema Principal de Galois	100
5	A insolubilidade da quintica	107
5.1	Extensões por radicais	107
5.2	Funções simétricas	110
5.3	A insolubilidade da quintica	113
6	Considerações finais	115

Referências**116**

1 Introdução

Esta dissertação propõe-se a aprofundar e a estabelecer as devidas relações entre a história da matemática e a resolução de equações polinomiais de grau menor ou igual a cinco. Para tanto, será utilizado como referência principal o livro de Fraleigh [6]. Estamos interessados, principalmente, em explorar a não resolução de uma equação de quinto grau por meio de radicais utilizando da Teoria de Galois, a qual tem se mostrado imprescindível para comprovação decisiva da não solubilidade de equações polinomiais de grau igual a cinco. Podemos destacar que a importância desse tema está na beleza da sua conexão natural com a História da Matemática, os seus principais resultados e o aprofundamento que gerou os conteúdos trabalhados atualmente em Álgebra, justificando, desse modo, a presente escolha do tema para esta proposta de dissertação de Mestrado do Programa de Pós-Graduação.

A divisão dos capítulos dessa dissertação foi realizada de modo a se construir o pensamento algébrico em torno das equações algébricas de grau menor ou igual a cinco, veja que, no primeiro capítulo, referente ao desenvolvimento do nosso projeto, buscamos entender a história e a resolução de equações algébricas até o quarto grau, perceba que utilizamos a letra x em minúscula, pois a abordagem dos polinômios naquela ocasião teve um viés mais informal, fazendo a identificação implícita de cada polinômio com a função polinomial determinada por ele. No segundo capítulo, apresentamos noções básicas e primordiais para o entendimento dessa dissertação no campo das estruturas algébricas, são esses: grupos, anéis, corpos e anéis de polinômios; observe que a partir deste capítulo, para denotar os elementos polinomiais, usamos a letra X em maiúscula, com um rigor formalizado pela definição 3.88. As noções básicas de estruturas algébricas como: grupos, anéis e corpos e anéis de polinômios foram apresentadas no terceiro capítulo. Já no quarto capítulo, o foco foi a construção dos elementos sobre a teoria de Galois, no qual apresentamos as extensões

de corpos, corpo de Galois, grupo de automorfismos, *splitting* corpo, extensão separável, grupo de Galois e encerramos esse capítulo com o teorema principal de Galois. Com uma base sólida fundamentada, iniciamos então o capítulo cinco intitulado: “A insolubilidade da quártica”, no qual apresentamos as extensões por radicais e o nosso objetivo final que é a insolubilidade da quártica. Observamos ainda que utilizamos o símbolo “ $\leq$ ” para a indicação de uma subestrutura de uma determinada estrutura algébrica, ou seja, se H é um subgrupo de um grupo G , indicamos este fato por $H \leq G$, ou ainda, se F é um subcorpo de um corpo E , denotamos por $F \leq E$.

Encerramos essa dissertação com a conclusão que pudemos fomentar ao longo dos temas estudados.

2 O estudo das equações algébricas

Ao longo da história da matemática, a resolução de equações algébricas sempre foi um tema de destaque, visto que o objetivo era exibir as soluções de uma equação dada por meio de radicais (isto é, encontrar as soluções algébricas), o que significa encontrar estas soluções por meio da manipulação de seus coeficientes através das quatro operações aritméticas e extração de raízes. Essas equações apareciam na maioria das vezes advindas de problemas de fora da área da matemática.

Neste trabalho, pretende-se apresentar a história e demonstrar a evolução dos métodos de resolução das equações polinomiais, também conhecidas como equações algébricas. Veja que, equação é toda sentença matemática aberta que exprime uma relação de igualdade. Segundo Carvalho e Roque (2019) [11], Diofanto é geralmente citado como o pai da álgebra, mas, para falar da história de uma disciplina matemática como a álgebra, precisamos, antes de mais nada, definir o que entendemos por “álgebra”. O momento decisivo para a constituição da álgebra como disciplina está associado à organização em torno da classificação e da resolução de equações, que iniciou-se no século *IX*.

Nosso intuito é evidenciar que o desenvolvimento algébrico do período não é a herança de um único autor, mas sim o produto de práticas compartilhadas ao longo da história do desenvolvimento do pensamento matemático.

2.1 Equações do primeiro grau

As situações-problemas que se reduzem à resolução de uma equação de primeiro grau apareceram naturalmente ao longo das civilizações, confundindo-se, muitas vezes, com a operação de divisão. Isso fez com que quase todos que estudaram matemática, dos escribas egípcios aos servidores públicos chineses, desenvolvessem técnicas específicas para

as resoluções desses problemas.

Iniciaremos o estudo das equações do primeiro grau por meio do papiro Rhind (ou papiro Ahmes), uma das principais fontes para o estudo da matemática egípcia antiga. Este papiro foi copiado pelo escriba Ahmes por volta do ano 1650 a.C e comprado pelo antiquário escocês Alexander Henry Rhind, entre os anos de 1856 – 1857. Atualmente, o papiro faz parte do acervo do Museu Britânico (Londres) desde 1865, juntamente com toda a coleção egípcia que pertencera a Rhind.

O papiro de Rhind contém uma coleção de 87 problemas de ordem prática, que provavelmente foram utilizados para treinar jovens escribas no Egito Antigo. Alguns deles são simples e diretos, outros, mais complexos. Vejamos o problema 31:

“Uma quantidade, e $\frac{2}{3}$ dela, e $\frac{1}{2}$ dela, e $\frac{1}{7}$ dela, adicionados, torna-se 33. Qual é a quantidade?”

No simbolismo que usamos atualmente, poderíamos descrever a situação acima como:

$$x + \frac{2}{3}x + \frac{1}{2}x + \frac{1}{7}x = 33.$$

Os problemas no papiro de Rhind eram resolvidos por um método muito diferente. Vejamos:

Uma quantidade; seu quarto é somado a ela. Ela se torna 15.

Ao invés de dividir 15 por $1\frac{1}{4}$, o escriba prossegue como a seguir. Ele supõe que a quantidade é 4. Se você tomar 4 e somar seu quarto a ele, obtém $4 + 1 = 5$. Então, queríamos 15, e obtivemos 5; então precisamos multiplicar o que obtivemos por 3 para chegarmos no resultado que gostaríamos. Assim, tomamos nossa tentativa e multiplicamos por 3. A nossa tentativa inicial foi 4, de modo que a resposta é $3 \times 4 = 12$.

Esse método é conhecido como *falsa posição*, pois propomos uma resposta que não esperamos realmente que seja a correta, mas que torna os cálculos fáceis. Com isso, usamos o resultado incorreto para descobrir o número pelo qual precisamos multiplicar a nossa tentativa para obter a resposta correta.

Podemos afirmar, que equação é uma sentença matemática com sinal de igualdade (=) em que números desconhecidos são representados por letras, denominadas **incógnitas**.

A equação geral do primeiro grau $a \cdot x + b = 0$, em que a e b são números conhecidos e $a \neq 0$, pode ser resolvida isolando-se o “ x ”, ou seja, subtraindo-se b de ambos os lados da equação, obtendo, desse modo $a \cdot x = -b$, e posteriormente fazemos a divisão por a dos dois lados e obtemos $x = -\frac{b}{a}$. Esse modo de resolução nada mais é do que aplicar os princípios de equivalências das igualdades (aditivo/multiplicativo) em ambos os membros da equação.

Em uma equação algébrica, todos os valores que uma variável pode eventualmente assumir é denominado de conjunto universo e representado pela letra U . O conjunto verdade é o conjunto dos valores de U que tornam verdadeira a equação, sendo este um subconjunto do conjunto universo, ou seja, $S \subset U$. Veja que de nada adianta encontrarmos um valor de “ x ” que obedeça à equação dada se este valor não pertencer ao conjunto universo ao qual a nossa equação estiver definida.

Os elementos do conjunto verdade de uma equação são chamados raízes da equação. Para verificar se um número é raiz de uma equação, devemos obedecer à seguinte sequência:

- Substituir a incógnita por esse número;
- Determinar o valor de cada membro da equação;
- Verificar a igualdade, sendo uma sentença verdadeira, o número considerado é raiz da equação.

Resolver uma equação consiste em realizar uma sucessão de operações que nos conduzem a equações equivalentes cada vez mais simples e que nos permitem, finalmente, determinar os elementos do conjunto verdade ou, de modo equivalente, as raízes da equação. Ou seja, resolver uma equação significa determinar o seu conjunto verdade, dentro do conjunto universo considerado. Veja,

Exemplo 2.1. Qual o valor da incógnita x , considerando $U = \mathbb{R}$, que torna a igualdade $8x + 3 = -13$ verdadeira?

Notação: O conjunto verdade são os valores de U que são raízes da equação, ou seja, são os valores que ao substituírem as incógnitas tornam a equação verdadeira. Indicaremos por S .

Temos que:

$$8x + 3 = -13$$

$$8x = -13 - 3$$

$$8x = -16$$

$$x = -\frac{16}{8}$$

$$x = -2.$$

Ou seja, $S = \{-2\}$.

2.2 Equações quadráticas

Segundo Berlinghoff e Gouvêa (2010) [2], a palavra “álgebra” veio do título de um livro escrito em árabe em torno do ano 825, no século IX. O autor, Muhammad Ibn Musa Al-Khwarizmi (780 – 850), nasceu provavelmente no que é agora o Uzbequistão. Ele viveu, entretanto, em Bagdá, onde o califa tinha estabelecido uma espécie de academia de ciências chamada “A Casa da Sabedoria”. Entre todos os livros que escreveu, seu livro sobre álgebra é o mais famoso. O livro de Al-Khwarizmi inicia a discussão sobre a resolução de equações quadráticas. Vejamos um dos problemas por ele discutido:

Um quadrado e dez raízes dele são iguais a trinta e nove dirhems. Quer dizer, quanto deve ser o quadrado, o qual, quando aumentado por dez de suas próprias raízes, é igual a trinta e nove?

Na simbologia atual, podemos reescrever como sendo:

$$x^2 + 10x = 39.$$

No entanto, como a simbologia atual não tinha sido inventada, Al-Khwarizmi resolvia esse tipo de problema seguindo um passo a passo, que pode ser descrito como:

“A solução é a seguinte: você divide o número de raízes por dois, o que, no caso presente, fornece cinco. Isso você multiplica por si mesmo; o produto é vinte e cinco. Some isso a trinta e nove; a soma é sessenta e quatro. Agora, tome a raiz disso, que é oito, e subtraia disso metade do número de raízes, que é cinco; o resto é três. Essa é a raiz do quadrado que você procurava; o próprio quadrado é nove”.

É possível perceber que essa descrição é basicamente a fórmula quadrática como a conhecemos atualmente, a diferença está no fato de que a fórmula moderna considera as raízes quadradas positivas e negativas, algo que naquela época os matemáticos não faziam.

A fórmula que resolve a equação do segundo grau, como estudamos atualmente, segundo Hefez e Villela (2018) [7], é devida ao matemático hindu Sridhara, do século X , e leva o nome de *fórmula de Bháskara*.

De acordo com Carvalho [11], Bháskara enunciava os problemas que hoje chamamos de equação somente com palavras, um modo poético de descrever problemas matemáticos, vejamos um exemplo tradicional desta época, publicado em seu principal livro intitulado *Siddhanta Siromani*:

Verso 77: “De um enxame de abelhas, tome metade, depois a raiz. Este grupo extrai o pólen de um campo de jasmims. Oito nonos do todo flutuam pelo céu. Uma abelha solitária escuta seu macho zumbir sobre uma flor de lótus. Atraído pela fragrância, ele tinha se deixado aprisionar na noite anterior. Quantas abelhas havia no enxame?”

O método de resolução utilizado por Bháskara consistia em reduzir o problema a uma equação linear. Este modo era denominado pelo indiano como “eliminação do termo médio”, o que hoje se assemelha ao que denominamos de completar quadrados. Assim, podemos expressar de modo simbólico o que antes era descrito apenas com palavras, uma equação expressa por $ax^2 + bx = c$. O procedimento descreve que para resolvermos devemos primeiramente multiplicar ambos os lados por $4a$, obtendo $4a^2x^2 + 4abx = 4ac$. Depois, adicionamos b^2 a ambos os lados, obtendo $4a^2x^2 + 4abx + b^2 = 4ac + b^2$. O primeiro membro tem uma raiz e tomamos essa raiz para obter:

$$2ax + b = \sqrt{4ac + b^2}$$

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

De maneira simplificada, podemos afirmar que o método de resolução utilizado por Bháskara consiste em:

- Completar o quadrado no primeiro membro para transformar o termo que contém a quantidade desconhecida e seu quadrado em um quadrado perfeito;

- Diminuir o grau da equação extraindo a raiz quadrada dos dois membros;
- Resolver a equação de primeiro grau que daí resulta.

Mesmo com os métodos de resolução propostos por Al-Khwarizmi e Bháskara, não podemos atribuir-lhes a invenção da fórmula que usamos atualmente, visto que ambos apresentaram um método geral para a resolução de equações do segundo grau, ainda que expresso somente por palavras. A fórmula para a resolução desse tipo de equação com o simbolismo que nos é comum atualmente só foi feita por François Viète, matemático francês que viveu de 1540 a 1603.

Entretanto, vale ressaltar que de acordo com Sérgio Roberto Nobre (2014)[8], o nome Bháskara é muito conhecido entre os brasileiros por conta de uma atribuição errônea do seu nome à fórmula de resolução de uma equação do 2º grau. Poucos sabem que, na História da Matemática da Índia, houve dois personagens de nome Bháskara. Bháskara *I*, que viveu entre os anos 600 e 680, aproximadamente, e Bháskara *II*, que viveu cerca de 500 anos após o primeiro, ou seja, entre 1114 e 1185. E a nenhum dos dois pode-se atribuir a fórmula que dá as raízes de uma equação do 2º grau. Sobre o primeiro há poucas informações, porém o segundo é mais presente na bibliografia histórica, inclusive com documentos que comprovam sua produção matemática.

A fórmula que resolve a equação do segundo grau, como a conhecemos hoje, pode ser descrita como: considere a equação $ax^2 + bx + c = 0$, com os coeficientes pertencentes ao conjunto dos números complexos ($\mathbb{C}$) e $a \neq 0$, para encontrarmos as raízes dessa equação em função dos seus coeficientes, pode ser demonstrado, completando os quadrados, que:

$$ax^2 + bx + c = 0$$

$$ax^2 + bx = -c$$

$$4a(ax^2 + bx) = 4a(-c)$$

$$4a^2x^2 + 4abx = -4ac$$

$$4a^2x^2 + 4abx + b^2 = b^2 - 4ac$$

$$(2ax + b)^2 = b^2 - 4ac$$

$$\sqrt{(2ax + b)^2} = \sqrt{b^2 - 4ac}$$

$$|(2ax + b)| = \sqrt{b^2 - 4ac}$$

$$2ax + b = \pm\sqrt{b^2 - 4ac}$$

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

em que, podemos afirmar que $\sqrt{b^2 - 4ac}$ é uma das raízes quadradas do número complexo definido por $\Delta = b^2 - 4ac$, chamado comumente de discriminante da equação.

O anulamento de Δ nos fornece a condição necessária e suficiente para que a equação do segundo grau tenha uma raiz dupla igual a $-\frac{b}{2a}$.

Se os coeficientes, a, b e c da equação $ax^2 + bx + c = 0$ são reais, com $a \neq 0$, então, temos que:

- $\Delta > 0$, se e somente se, a equação tem duas raízes reais distintas;
- $\Delta = 0$, se e somente se, a equação tem duas raízes reais iguais;
- $\Delta < 0$, se e somente se, a equação tem duas raízes complexas conjugadas.

Vejamos os exemplos dos casos listados acima:

Exemplo 2.2. $\Delta > 0$:

Dada a equação quadrática $x^2 - x - 12 = 0$, teremos que:

$$\Delta = (-1)^2 - 4.1.(-12) = 1 + 48 = 49$$
$$x = \frac{-(-1) \pm \sqrt{49}}{2.1} = \frac{1 \pm 7}{2}$$
$$x' = \frac{1+7}{2} = \frac{8}{2} = 4$$
$$x'' = \frac{1-7}{2} = -\frac{6}{2} = -3.$$

Logo, as duas raízes distintas obtidas são 4 e -3.

Exemplo 2.3. $\Delta = 0$:

Dada a equação quadrática $4x^2 - 4x + 1 = 0$, teremos que:

$$\Delta = (-4)^2 - 4.4.1 = 16 - 16 = 0$$
$$x = \frac{-(-4) \pm \sqrt{0}}{2.4} = \frac{4 \pm 0}{8}$$
$$x' = \frac{4+0}{8} = \frac{4}{8} = \frac{1}{2}$$
$$x'' = \frac{4-0}{8} = -\frac{4}{8} = -\frac{1}{2}.$$

Logo, a equação possui duas raízes reais iguais, e o seu valor é $\frac{1}{2}$.

Exemplo 2.4. $\Delta < 0$:

Dada a equação quadrática $x^2 - 4x + 5 = 0$, teremos que:

$$\begin{aligned}\Delta &= (-4)^2 - 4 \cdot 1 \cdot 5 = 16 - 20 = -4 \\ x &= \frac{-(-4) \pm \sqrt{-4}}{2 \cdot 1} = \frac{4 \pm \sqrt{4 \cdot i^2}}{2} = \frac{4 \pm 2i}{2} \\ x' &= \frac{4 + 2i}{2} = 2 + i \\ x'' &= \frac{4 - 2i}{2} = 2 - i.\end{aligned}$$

Logo, a equação possui duas raízes complexas conjugadas, que são $2 + i$ e $2 - i$.

Há casos em que a equação do 2º grau é nomeada como incompleta, pois apresenta $b = 0$ ou $c = 0$. Nesses casos, não é necessário utilizar a fórmula de Bháskara, mesmo sendo possível a sua utilização, percebe-se que somente utilizando as manipulações algébricas conhecidas é possível encontrar o conjunto verdade dessas equações. Vejamos:

Exemplo 2.5. Um exemplo onde $b = 0$ é:

$$\begin{aligned}x^2 &= 16 \\ \sqrt{x^2} &= \sqrt{16} \\ |x| &= \sqrt{16} \\ x &= \pm 4.\end{aligned}$$

Podemos afirmar que a equação possui duas raízes reais, que são 4 e -4 .

Exemplo 2.6. Um exemplo onde $c = 0$ é:

$$\begin{aligned}x^2 + 10x &= 0 \\ x(x + 10) &= 0 \\ x &= 0\end{aligned}$$

ou

$$x + 10 = 0$$

$$x = -10.$$

Portanto, as raízes dessa equação são 0 e -10 .

Como pudemos perceber até esse momento, problemas matemáticos raramente aparecem de forma abstrata ao longo de sua história. O problema de resolver equações cúbicas (equações do terceiro grau) apareceu de problemas geométricos, considerados primeiro pelos matemáticos gregos. Os primeiros problemas desse tipo datam de 400 a.C., entretanto a sua resolução completa apareceu apenas dois mil anos depois, o que veremos na seção a seguir.

2.3 Equações do terceiro grau

No início do século XVI, Scipione Del Ferro obteve uma fórmula usando radicais para a solução de um certo tipo de equação cúbica, o que foi uma novidade em relação aos trabalhos árabes. Por costume da época, essa fórmula foi mantida em segredo, pois muitas vezes os matemáticos desafiavam-se para mostrar perante a sociedade o seu conhecimento. Alguns anos mais tarde, por volta de 1535, o matemático italiano Niccolo Fontana, conhecido por Tartaglia, resolveu diversas equações cúbicas, em particular as do tipo $x^3 + mx^2 = n$.

Os relatos históricos narram que um terceiro matemático italiano, Girolamo Cardano, convenceu Tartaglia a ir até Milão contar a sua resolução com a promessa de obter um patrono para ele e de jamais divulgar a sua resolução. Segundo Berlinghoff e Gouvêa (2010) [2], Cardano afirmou a Tartaglia que: “juro a você, por Deus, e como um verdadeiro homem de honra, não apenas nunca publicar suas descobertas, se você me ensiná-las, mas eu também prometo a você, e empenho minha fé como verdadeiro cristão, anotá-las em código, de modo que depois de minha morte ninguém seja capaz de entendê-las”, visto que Tartaglia pretendia publicar a sua solução da cúbica como coroação de seu tratado sobre álgebra.

Entretanto, quebrando a sua promessa e enfurecendo Tartaglia, Cardano publicou o livro intitulado *Ars Magna*, que significa “A Grande Arte”. Nele, continha uma descrição

completa de como resolver qualquer equação cúbica, com justificativas geométricas de por que os métodos funcionam. Em seu livro, mesmo atribuindo a Tartaglia a resolução, o método tornou-se conhecido por Método de Cardano.

Vejamos então que a equação $x^3 + px + q = 0$, com p, q e $u \in \mathbb{R}$ e $u \neq 0$, se transforma em uma equação solúvel por radicais quando se faz a substituição $x = u - \frac{p}{3u}$ (ou, $x = u + v$, onde $v = -\frac{p}{3u}$).

Substituindo x pela expressão dada, temos que:

$$\begin{aligned} \left(u - \frac{p}{3u}\right)^3 + p\left(u - \frac{p}{3u}\right) + q &= 0 \\ u^3 - pu + \frac{p^2}{3u} - \frac{p^3}{27u^3} + pu - \frac{p^2}{3u} + q &= 0 \\ u^3 - \frac{p^3}{27u^3} + q &= 0 \end{aligned} \tag{2.1}$$

$$u^6 + qu^3 - \frac{p^3}{27} = 0.$$

Observemos que o resultado obtido acima é uma equação do segundo grau em u^3 . Vejamos, ao assumir o valor de $a = 1$, $b = q$ e $c = -\frac{p^3}{27}$, teremos que

$$\begin{aligned} \Delta &= q^2 - 4.1. \left(-\frac{p^3}{27}\right) \\ \Delta &= q^2 + \frac{4p^3}{27}. \end{aligned}$$

Então,

$$u^3 = \frac{-q \pm \sqrt{q^2 + \frac{4p^3}{27}}}{2}$$

$$u^3 = -\frac{q}{2} \pm \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}.$$

Sendo assim, temos as possibilidades:

$$u_1 = \sqrt[3]{-\frac{q}{2} + \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}}$$

ou

$$u_2 = \sqrt[3]{-\frac{q}{2} - \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}}.$$

Pela equação (2.1), denotando $v^3 = -\frac{p^3}{27u^3}$, temos:

$$u^3 - \frac{p^3}{27u^3} + q = 0 \Rightarrow u^3 + v^3 = -q \Rightarrow v^3 = -(u^3 + q).$$

Assim, para u_1 e u_2 :

$$\begin{aligned} \bullet \quad v_1^3 &= -\left(-\frac{q}{2} + \sqrt{\frac{q^2}{4} + \frac{p^3}{27}} + q\right) = -\frac{q}{2} - \sqrt{\frac{q^2}{4} + \frac{p^3}{27}} \Rightarrow v_1 = \sqrt[3]{-\frac{q}{2} - \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}} = u_2. \\ \bullet \quad v_2^3 &= -\left(-\frac{q}{2} - \sqrt{\frac{q^2}{4} + \frac{p^3}{27}} + q\right) = -\frac{q}{2} + \sqrt{\frac{q^2}{4} + \frac{p^3}{27}} \Rightarrow v_2 = \sqrt[3]{-\frac{q}{2} + \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}} = u_1. \end{aligned}$$

Como $x = u + v$, temos $x = u_1 + v_1 = u_1 + u_2$ ou $x = u_2 + v_2 = u_2 + u_1$.

De todo modo:

$$x = \sqrt[3]{-\frac{q}{2} + \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}} + \sqrt[3]{-\frac{q}{2} - \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}}.$$

Então, as três raízes da equação

$$x^3 + px + q = 0$$

são obtidas somando cada uma das raízes cúbicas u_1, u_2, u_3 representadas pelo primeiro radical com uma das raízes cúbicas dadas pelo segundo radical, ou seja, $-\frac{p}{3u_1}, -\frac{p}{3u_2}$ e $-\frac{p}{3u_3}$.

Exemplo 2.7. Tomemos como exemplo a equação cúbica definida por $x^3 - 15x - 4 = 0$.

Pela fórmula de Cardano temos que:

$$x = \sqrt[3]{2 + \sqrt{-121}} + \sqrt[3]{2 - \sqrt{-121}} = \sqrt[3]{2 + 11i} + \sqrt[3]{2 - 11i},$$

onde $i = \sqrt{-1}$.

Podemos verificar que $2 + i$ é uma das raízes cúbicas de $2 + 11i$ e que $2 - i$ é uma das raízes cúbicas de $2 - 11i$. As demais raízes cúbicas são produto dessas primeiras raízes por $w = e^{\frac{2\pi}{3}i} = -\frac{1}{2} + \frac{\sqrt{3}}{2}i$ e por $w^2 = e^{\frac{4\pi}{3}i} = -\frac{1}{2} - \frac{\sqrt{3}}{2}i$.

Dessa forma, as raízes cúbicas de $2 + 11i$ são:

$$z_1 = 2 + i, z'_1 = -1 - \frac{\sqrt{3}}{2} + \left(\sqrt{3} - \frac{1}{2}\right)i \text{ e } z''_1 = -1 + \frac{\sqrt{3}}{2} + \left(-\sqrt{3} - \frac{1}{2}\right)i.$$

E as raízes cúbicas de $2 - 11i$ são:

$$z_2 = 2 - i, z'_2 = -1 - \frac{\sqrt{3}}{2} + \left(\frac{1}{2} - \sqrt{3}\right)i \text{ e } z''_2 = -1 + \frac{\sqrt{3}}{2} + \left(\frac{1}{2} + \sqrt{3}\right)i.$$

As possibilidades para x são: $x = z_1 + z_2, x = z_1 + z'_2, x = z_1 + z''_2, x = z'_1 + z_2, x = z'_1 + z'_2, x = z'_1 + z''_2, x = z''_1 + z_2, x = z''_1 + z'_2$ ou $x = z''_1 + z''_2$.

Sendo que as únicas possibilidades que solucionam de fato a equação são:

- $x_1 = z_1 + z_2 = 2 + i + 2 - i \Rightarrow x_1 = 4.$
- $x_2 = z'_1 + z'_2 = \left(-1 - \frac{\sqrt{3}}{2} + \left(\sqrt{3} - \frac{1}{2}\right)i\right) + \left(-1 - \frac{\sqrt{3}}{2} + \left(\frac{1}{2} - \sqrt{3}\right)i\right)$
 $\Rightarrow x_2 = -2 - \sqrt{3}.$
- $x_3 = z''_1 + z''_2 = \left(-1 + \frac{\sqrt{3}}{2} + \left(-\sqrt{3} - \frac{1}{2}\right)i\right) + \left(-1 + \frac{\sqrt{3}}{2} + \left(\frac{1}{2} + \sqrt{3}\right)i\right)$
 $\Rightarrow x_3 = -2 + \sqrt{3}.$

Portanto,

$$S = \{4, -2 - \sqrt{3}, -2 + \sqrt{3}\}.$$

Exemplo 2.8. Resolvamos a equação, $x^3 + 6x^2 + 21x + 14 = 0$, pelo mesmo método. Efetuando a substituição $x = y - 2$, para eliminar o termo do segundo grau, obtemos a equação $y^3 + 9y - 12 = 0$, esta que apresenta as seguintes raízes:

$$\begin{aligned} y_1 &= \sqrt[3]{6 + \sqrt{63}} + \sqrt[3]{6 - \sqrt{63}}, \\ y_2 &= w\sqrt[3]{6 + \sqrt{63}} + w^2\sqrt[3]{6 - \sqrt{63}}, \quad \text{e} \\ y_3 &= w^2\sqrt[3]{6 + \sqrt{63}} + w\sqrt[3]{6 - \sqrt{63}}. \end{aligned}$$

Logo, as raízes da equação procuradas são: $x_1 = y_1 - 2, x_2 = y_2 - 2 \quad \text{e} \quad x_3 = y_3 - 2.$

2.4 Equações do quarto grau

Na seção 2.3, vimos que a divulgação da resolução das equações do terceiro grau deu-se de uma forma antecipada por conta da quebra de juramento de Cardano ao Tartaglia.

De acordo com Rezende (2002) [10], Cardano e seu brilhante discípulo, Ludovico Ferrari (1522 – 1557), demonstraram a regra de Tartaglia para solução de $x^3 + px = q$. Eles propuseram a mudança de $x = y - \frac{a}{3}$ em $x^3 + ax^2 + bx + c$, além de resolver 13 tipos de equações do terceiro grau, que hoje em dia são uma só. Pouco tempo depois disso, Ferrari resolve a equação do quarto grau.

Percebemos então que, do estabelecimento das relações e manipulações algébricas, resultou a obtenção de fórmulas resolutivas para equações de grau menor que cinco, ou seja, $n \leq 4$. Desse modo, temos maneiras de exibir tais soluções, caracterizando os “métodos de resolução”, ocorridas entre os séculos *XVI* e *XIX*, em que Ferrari destacou-se por ser o primeiro a apresentar esse método resolutivo de uma equação do quarto grau a partir do método de resolução de equações do terceiro grau. Com isso, o método que apresentaremos a seguir para a resolução da equação do quarto grau leva o seu nome, ou seja, método de Ferrari. De acordo com Brandemberg (2017) [4], em seu processo, inicialmente, Ferrari trabalhou a resolução de uma equação particular, $x^4 + 6x^2 + 36 = 60x$, a partir da qual encontrou um método geral de resolução o qual mostraremos a seguir.

Consideremos a seguinte equação, onde $a_0, a_1, a_2, a_3 \in \mathbb{R}$:

$$x^4 + a_3x^3 + a_2x^2 + a_1x + a_0 = 0. \quad (2.2)$$

Temos que $x^4 + a_3x^3 = -(a_2x^2 + a_1x + a_0)$. Completando o quadrado no primeiro membro desta equação e organizando o segundo membro, temos que

$$\left(x^2 + \frac{1}{2}a_3x\right)^2 = \left(\frac{1}{4}a_3^2 - a_2\right)x^2 - a_1x - a_0. \quad (2.3)$$

Agora, manipularemos o segundo membro da equação de modo a obtermos um quadrado perfeito, para que assim ambos os membros da equação sejam duas expressões do segundo grau. Somando-se a expressão $y^2 + 2y\left(x^2 + \frac{1}{2}a_3x\right)$ a ambos os membros de (2.3), obtemos

$$\left[\left(x^2 + \frac{1}{2}a_3x\right) + y\right]^2 = \left(2y + \frac{1}{4}a_3^2 - a_2\right)x^2 + (ya_3 - a_1)x + (y^2 - a_0). \quad (2.4)$$

Determinando os valores de y que transformarão o segundo membro de (2.4) em um quadrado perfeito, devemos ter o discriminante do segundo membro de (2.4) como trinômio do segundo grau em x , nulo. Ou seja,

$$(ya_3 - a_1)^2 - 4 \cdot \left(2y + \frac{1}{4}a_3^2 - a_2\right) \cdot (y^2 - a_0) = 0.$$

Segue-se que

$$8y^3 - 4a_2y^2 + (2a_1a_3 - 8a_0)y + (4a_0a_2 - a_0a_3^2 - a_1^2) = 0. \quad (2.5)$$

Determinando y como uma das raízes da equação (2.5), da equação (2.4) obtemos

$$\left[\left(x^2 + \frac{1}{2}a_3x\right) + y\right]^2 = (\alpha x + \beta)^2, \quad (2.6)$$

com α e β adequados. Desse modo, a resolução dessa equação é feita mediante a resolução das duas seguintes equações do segundo grau

$$\left(x^2 + \frac{1}{2}a_3x\right) + y = (\alpha x + \beta) \quad \text{e} \quad \left(x^2 + \frac{1}{2}a_3x\right) + y = -(\alpha x + \beta). \quad (2.7)$$

Veja que a equação (2.2) é equivalente à equação (2.6), então, podemos afirmar que a resolução de uma equação do quarto grau pode ser reduzida à resolução de equações de graus dois e três conforme demonstrado.

Exemplo 2.9. Resolvamos a equação $x^4 - 2x^3 - x^2 - 2x - 2 = 0$ pelo método de Ferrari.

Veja que, obtendo y que satisfaça a equação (2.5), torna-se $2y^3 + y^2 + 6y + 3 = 0$. Verifica-se que $y = -\frac{1}{2}$ é solução desta equação. Com este valor de y , a equação (2.4) torna-se

$$\left(x^2 - x - \frac{1}{2}\right)^2 = x^2 + 3x + \frac{9}{4} = \left(x + \frac{3}{2}\right)^2. \quad (2.8)$$

Com isso, obtemos as seguintes equações do segundo grau

$$x^2 - x - \frac{1}{2} = x + \frac{3}{2} \quad \text{e} \quad x^2 - x - \frac{1}{2} = -\left(x + \frac{3}{2}\right), \quad (2.9)$$

cujas raízes são as raízes da equação proposta. Logo, as raízes desejadas da equação são:

$$x_1 = 1 + \sqrt{3}, x_2 = 1 - \sqrt{3}, x_3 = i \quad \text{e} \quad x_4 = -i.$$

Mesmo com o sucesso na resolução de equações do quarto grau, Leonhard Euler (1707–1783) foi um dos primeiros a perceber a complexidade envolvendo a resolução de equações de grau $n \geq 5$. Segundo Euler, no artigo de Brandenberg (2017) [4], *Elements of Algebra*:

“Isto é o mais longe que chegamos na resolução de equações algébricas. Todos os esforços realizados para resolver equações de grau maior ou igual a cinco, desta mesma forma, ou ao menos reduzi-las a equações de grau menor, não tiveram êxito: de tal forma que não podemos dar nenhuma regra geral para encontrar raízes de equações de grau superior a quatro.” (EULER apud BRANDEMBERG, 1972, p. 286.)

Podemos perceber ao longo deste capítulo que a história das equações algébricas pode ser descrita como a história da busca de métodos de resolução para uma equação polinomial geral de grau $n \geq 1$.

Feito a resolução das equações cúbicas e quárticas, o próximo passo seria as equações de grau 5. Isso se mostrou um problema mais difícil. Demonstrar que não existe uma fórmula para resolver a equação geral de grau 5, exigiu dos matemáticos da época uma mudança completa de ponto de vista, o que consequentemente levou ao desenvolvimento da álgebra abstrata.

Segundo Boyer [3], “uma das lições que a história da matemática ensina claramente é que a busca de soluções para problemas não resolvidos, sejam eles resolúveis ou não, leva invariavelmente a descobertas importantes pelo caminho”. Ainda nesse pensamento, Boyer [3] afirma que a matemática tem sido frequentemente comparada a uma árvore, pois cresce em uma estrutura acima da terra que se espalha e ramifica sempre mais, ao passo que suas raízes cada vez mais se aprofundam e alargam, em busca de fundamentos sólidos.

Com isso em mente, devemos nos fortalecer no estudo das estruturas algébricas presentes no próximo capítulo, para que possamos trilhar o caminho até a nossa demonstração desejada para a prova da insolubilidade da quártica.

3 Noções básicas de estruturas algébricas

Segundo a nota história do Fraleigh (2002) [6], a primeira publicação de uma fórmula para resolver equações cúbicas em termos dos radicais foi em 1545 no livro *Ars Magna* de Girolamo Cardano, embora a descoberta inicial do método seja em parte graças também a Scipione del Ferro e Niccolo Tartaglia. Aluno de Cardano, Lodovico Ferrari descobriu um método para solucionar equações quárticas por radicais, o que também apareceu no trabalho de Cardano.

Após muitos matemáticos tentarem resolver quárticas por métodos semelhantes, foi Joseph-Louis Lagrange em 1770 quem primeiro tentou uma análise detalhada dos princípios gerais por trás das soluções de polinômios de grau três e quatro, mostrando porque esses métodos falham para aqueles polinômios de grau maior. A ideia básica era que nos casos anteriores havia funções racionais das raízes que aceitavam dois ou três valores, respectivamente, sob todas as permutações possíveis de raízes de forma que as funções racionais poderiam ser escritas como raízes de equações de grau menor que aquele do original, para essas funções serem evidentes equações de graus maiores.

O primeiro matemático que afirmou ter uma prova da insolubilidade das equações quárticas foi Paolo Ruffini (1765–1822) no seu texto de álgebra de 1799. A sua prova seguia na mesma linha sugerida por Lagrange, no sentido que ele determinava efetivamente todos os subgrupos de S_5 , ou seja, o grupo de permutações de 5 elementos, e mostrava como esses subgrupos agiam sobre as funções racionais das raízes da equação. Infelizmente, houve muitas falhas em várias das versões publicadas da prova. Foi Niels Henrik Abel quem, em 1824 e 1826, publicou uma prova completa consertando todas as falhas de Ruffini e finalmente resolvendo essa questão de muitos séculos anteriores.

Estamos familiarizados com o fato de que um polinômio quadrático $f(X) = aX^2 + bX + c$, com $a \neq 0$, com coeficientes reais, possui zeros em $\mathbb{C}$. Na realidade, isto é verdade para $f(X) \in F[X]$, em que F é qualquer corpo com característica diferente de 2 e os zeros estão no fecho algébrico de F , $\bar{F}$, cuja definição será abordada posteriormente. Podemos nos questionar se os zeros de um polinômio cúbico sobre $\mathbb{Q}$ também podem ser sempre expressos em termos de radicais. A resposta é sim, de fato, até mesmo os zeros do polinômio de grau 4 sobre $\mathbb{Q}$ podem ser expressos em termos de radicais. Depois que os matemáticos tentaram por vários anos encontrar a “fórmula do radical” para zeros de um polinômio de 5º grau, foi um triunfo quando Abel provou que a quártica não pode ser resolvida por radicais. Nosso trabalho será descrever precisamente o que isso significa.

No que segue, abordamos definições e resultados sobre as estruturas algébricas presentes nas discussões dos próximos capítulos, dentre estas, destacamos a definição de Corpo e Domínio de Ideais Principais (PID). Todas as demonstrações aqui descritas podem ser encontradas, em detalhes, em Fraleigh [6] e Hygino [5].

3.1 Grupos

Ao longo da história, segundo Fraleigh (2002) [6], aprendemos a dominar os problemas computacionais de adição e multiplicação de números, logo, estávamos prontos para aplicar essas operações binárias à solução de problemas. Frequentemente, os problemas levam à equações envolvendo algum número desconhecido x , que deve ser determinado. As equações mais simples são as lineares da forma $a + x = b$ para a operação de adição, e $a \cdot x = b$ para a multiplicação. Na verdade, a necessidade de soluções de equações lineares aditivas, tais que $5 + x = 2$ é uma motivação muito boa para os números negativos. Da mesma forma, a necessidade de números racionais é mostrada por equações como $2 \cdot x = 3$.

É desejável que possamos resolver equações lineares envolvendo nossas operações binárias. No entanto, isso não é possível para todas as operações binárias. Por exemplo, para a operação binária, dada pela tabela

*	a	b	c
a	b	c	b
b	a	c	b
c	c	b	a

$a * x = a$ não tem solução em $S = \{a, b, c\}$ para a operação $*$. Vamos abstrair da álgebra

familiar as propriedades de adição que nos permitem resolver a equação $5 + x = 2$ em $\mathbb{Z}$. Não devemos nos referir à subtração, pois estamos preocupados com a solução formulada em termos de uma única operação binária, neste caso, adição.

Agora podemos ver quais propriedades um conjunto S e uma operação binária $*$ em S permitiriam a imitação deste procedimento para uma equação $a * x = b$ para $a, b \in S$. Basicamente, o procedimento é a existência de um elemento e em S com a propriedade $e * x = x$ para quaisquer $x \in S$. Para nosso exemplo aditivo, 0 desempenhou o papel de e e 1 desempenhou o papel de nosso exemplo multiplicativo. Também, precisamos de um elemento a' em S que tem a propriedade que $a' * a = e$. Finalmente, é necessária a operação associativa. Uma análise semelhante mostra que, a fim de resolver a equação $x * a = b$, gostaríamos de ter um elemento e em S tal que $x * e = x$ para quaisquer x em S e um a' em S tal que $a * a' = e$ além da associatividade. Com todas essas propriedades de $*$ em S , podemos ter certeza de que seremos capazes de resolver equações lineares. Assim, precisamos de uma estrutura binária associativa $(S, *)$ com um elemento neutro e tal que para cada a em S exista a' em S tal que $a * a' = a' * a = e$. Essa é precisamente a noção de *grupo*, que agora definiremos. As demonstrações desse capítulo não apresentadas, podem ser encontradas em [6].

Definição 3.1. O conceito de grupo: Seja G um conjunto não vazio, uma função de $G \times G$ em G é chamada de operação ou lei de composição interna em G . Dizemos que G é um *grupo* em relação a essa operação, se, e somente se,

- $a * (b * c) = (a * b) * c$ ($a, b, c \in G$, isto é, *vale a propriedade associativa*);
- existe $e \in G$ de maneira que $a * e = a = e * a$, $\forall a \in G$, ou seja, *existe elemento neutro*;
- *Qualquer elemento de G é simetrizável* em relação à operação considerada: $\forall a \in G$, $\exists a' \in G \mid a * a' = e = a' * a$ (o elemento a' é chamado de simétrico de a).

Notação: $(G, *)$, mas, por simplificação de linguagem, diz-se apenas “ G é um grupo” ou “grupo G ”, o que pressupõe uma operação em G (com as propriedades citadas) sobre a qual não há nenhuma dúvida.

Definição 3.2. Grupo abeliano: Dizemos que um grupo $(G, *)$ é *abeliano* ou *comutativo* se, e somente se, a operação $(x, y) \mapsto x * y$ é comutativa, isto é,

$$a * b = b * a, \forall a, b \in G.$$

Proposição 3.3. *No contexto da definição 3.1, $(G, *)$ sendo um grupo:*

- i) $e \in G$ é único e é chamado de elemento neutro;*
- ii) Para cada $a \in G$, o elemento $a' \in G$ tal que: $a * a' = a' * a$ é único e é chamado de elemento simétrico de a ;*
- iii) $\forall a, b \in G : (a * b)' = b' * a'$;*
- iv) $\forall a \in G : (a')' = a$;*

Observação 3.4. Por vezes adotamos as seguintes nomenclaturas e notações:

- $(G, +)$ grupo aditivo e denotamos $e := 0$ (neutro) e $a' := -a$ (oposto), ou usamos:
- $(G, \cdot)$ grupo multiplicativo e denotamos $e := 1$ (identidade) e $a' := a^{-1}$ (inverso).

A proposição a seguir é conhecida como a Lei do Cancelamento e será usada inúmeras vezes neste capítulo, de modo natural, mesmo sem ser citada.

Proposição 3.5. *Seja $(G, *)$ um grupo. Dados $a, x, y \in G$ são válidas as afirmações:*

- i) Se $a * x = a * y$ então $x = y$;*
- ii) Se $x * a = y * a$ então $x = y$.*

De acordo com Fraleigh (2002) [6], os grupos comutativos são chamados de abelianos em homenagem ao matemático norueguês Niels Henrik Abel (1802 – 1829). Abel estava interessado na questão da solubilidade de equações polinomiais. Em um artigo escrito em 1828, ele provou que se todas as raízes de uma equação podem ser expressas como funções racionais $f, g, \dots, h$ de um, digamos x , e se por quaisquer duas dessas raízes, $f(x)$ e $g(x)$, a relação $f(g(x)) = g(f(x))$ sempre é válida, a equação pode ser resolvida por radicais. Portanto, essas funções são elementos do grupo de permutações das raízes. Foi essa propriedade da comutatividade nesses grupos de permutação associada às equações solúveis que levou Camille Jordan em seu tratado de álgebra de 1870 a nomear tais grupos como *abelianos*; o nome desde então tem sido aplicado a grupos comutativos em geral.

Abel foi atraído pela matemática quando adolescente e logo ultrapassou todos os seus professores na Noruega. Ele finalmente recebeu uma bolsa do governo para estudar em 1825 e seguiu para Berlim, onde fez amizade com August Crelle, o fundador da mais influente revista matemática alemã, chamada *Crelle's Journal*. Abel contribuiu com vários artigos para a revista durante os próximos anos, incluindo muitos no campo das funções elípticas, cuja teoria ele criou praticamente sozinho. Abel voltou para a Noruega em 1827 sem posição e uma abundância de dívidas. Mesmo assim, ele continuou a escrever artigos brilhantes, mas morreu de tuberculose aos 26 anos, dois dias antes de Crelle conseguir encontrar um emprego para ele na universidade em Berlim.

Definição 3.6. Subgrupos: Seja $(G, *)$ um grupo. Dizemos que um subconjunto não vazio $H \subset G$ é um *subgrupo* de G se, e somente se,

1. $\forall a, b \in H \Rightarrow a * b \in H$, isto é, H é fechado para a operação de G ;
2. $(H, *)$ também é um grupo. Neste caso, a operação é a mesma de G , só que restrita a H .

Notação: Devemos considerar $H \leq G$ em que H é um subgrupo de G , e $H < G$ deve significar $H \leq G$, mas $H \neq G$.

Proposição 3.7. *Seja $(G, *)$ um grupo. Para que um subconjunto não vazio $H \subset G$ seja um subgrupo de G é necessário e suficiente que*

$$a * b' \in H, \forall a, b \in H$$

em que b' é o simétrico de b .

Há um grande número de exemplos interessantes de grupos e subgrupos, entretanto, exploraremos o principal grupo de nosso interesse, a saber, o grupo das permutações de n elementos, S_n

Exemplo 3.8. Dado um conjunto A , não vazio, uma permutação de A é uma função $\sigma : A \rightarrow A$ que é bijeção.

É possível mostrar que a coleção de todas as permutações de A , S_A , com a operação ‘composição de funções’, é um grupo, denominado grupo das permutações de A . Tal grupo tem um papel importante em Teoria dos Grupos pois, pelo Teorema de Cayley

(veja página 82 de [6]) existe uma correspondência biunívoca entre um grupo G e seu grupo de permutação S_G .

Em particular, quando $A = \{1, 2, \dots, n\}$, denotamos S_A por S_n . Neste caso, veja que existem $n!$ bijeções de $A \rightarrow A$, ou seja, S_n tem $n!$ elementos. Além disso, denotamos cada elemento $\sigma \in S_n$ da seguinte maneira:

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & \dots & n \\ \sigma(1) & \sigma(2) & \sigma(3) & \dots & \sigma(n) \end{pmatrix}$$

Com isso, é possível visualizar, de imediato, a imagem de cada elemento em $A = \{1, 2, \dots, n\}$, já que

$$1 \mapsto \sigma(1), \quad 2 \mapsto \sigma(2), \quad 3 \mapsto \sigma(3), \quad \dots, \quad n \mapsto \sigma(n)$$

Por exemplo, em S_3 , temos $3! = 6$ elementos, a saber:

$$\begin{aligned} \sigma_1 &= \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \quad \sigma_2 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \quad \sigma_3 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}, \quad \sigma_4 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \\ \sigma_5 &= \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}, \quad \sigma_6 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}. \end{aligned}$$

Neste trabalho, o subgrupo de S_n , formado pelas permutações pares, denotado por A_n , é essencial. Para o entendimento de ‘paridade’ de uma permutação é necessário primeiramente estabelecer a seguinte relação de equivalência sobre um conjunto, não vazio, A , para cada $\sigma \in S_A$: $\forall a, b \in A$,

$$a \sim b \iff b = \sigma^n(a), \text{ para algum } n \in \mathbb{Z}.$$

Neste contexto, cada classe de equivalência em A é chamada de órbita de σ .

Por exemplo, em S_8 , dado a permutação

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 3 & 8 & 6 & 7 & 4 & 1 & 5 & 2 \end{pmatrix},$$

procuremos a órbita que contém o elemento 1, para tanto veja que:

$$1 \xrightarrow{\sigma} 3 \xrightarrow{\sigma} 6 \xrightarrow{\sigma} 1 \xrightarrow{\sigma} 3 \xrightarrow{\sigma} 6 \xrightarrow{\sigma} 1 \dots$$

Assim, a órbita contendo 1 é $\{1, 3, 6\}$.

Escolhemos agora um elemento diferente de 1, digamos 2, e fazemos a mesma análise:

$$2 \xrightarrow{\sigma} 8 \xrightarrow{\sigma} 2 \xrightarrow{\sigma} 8 \dots$$

Com isso a órbita contendo 2 é $\{2, 8\}$.

Procuremos a órbita que contém o 4, para tanto veja que:

$$4 \xrightarrow{\sigma} 7 \xrightarrow{\sigma} 5 \xrightarrow{\sigma} 4 \xrightarrow{\sigma} 7 \xrightarrow{\sigma} 5 \xrightarrow{\sigma} 4 \dots$$

Portanto a órbita contendo 4 é dada por $\{4, 5, 7\}$.

Ou seja, a partição de $\{1, 2, 3, 4, 5, 6, 7, 8\}$ pelas órbitas de σ , são: $\{1, 3, 6\}$, $\{2, 8\}$ e $\{4, 5, 7\}$.

Agora, fazendo a mesma análise para a permutação

$$\mu = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 3 & 2 & 6 & 4 & 5 & 1 & 7 & 8 \end{pmatrix},$$

temos as seguintes órbitas de μ : $\{1, 3, 6\}$, $\{2\}$, $\{4\}$, $\{5\}$, $\{7\}$ e $\{8\}$.

Veja que μ tem apenas uma órbita com mais de um elemento, este fato faz de μ um ‘ciclo’, como veremos a seguir.

Dizemos que uma permutação é um ciclo quando tal permutação tem apenas uma órbita contendo mais de um elemento, neste caso, o comprimento de um ciclo é o número de elementos de sua maior órbita. Denotamos cada ciclo através dos elementos de tal maior órbita delimitados por parênteses (, , ..., ,). Por exemplo, a permutação μ acima é um ciclo de comprimento três: $\mu = (1, 3, 6)$.

É possível mostrar (veja Teorema 9.8, página 89 de [6]) que toda permutação de um conjunto finito é um produto de ciclos disjuntos, em que este produto trata-se da operação de composição entre tais permutações chamadas de ciclos. Neste sentido, a permutação σ , dada anteriormente, se decompõe em ciclos da seguinte maneira:

$$\sigma = (1, 3, 6)(2, 8)(4, 7, 5).$$

Em particular, um ciclo de comprimento dois é chamado de ‘transposição’ e pode-se mostrar que (veja Corolário 9.12 página 90 de [6]): qualquer permutação de um conjunto

finito de no mínimo dois elementos é um produto de transposições, mas ainda, permutação alguma em S_n pode ser expressa como produto de um número par de transposições e, simultaneamente, como o produto de um número ímpar de transposições. Com isso, faz sentido definir que uma determinada permutação de um conjunto finito é ‘par’ quando pode ser escrita como produto de um número par de transposições e é ‘ímpar’ quando pode ser escrita como produto de um número ímpar de transposições. Por exemplo, em S_n , $n \geq 2$, a permutação identidade ι é par, pois é o produto $(1, 2)(1, 2)$ de transposições.

Pode-se mostrar que, se $n \geq 2$, então a coleção de todas as permutações pares de $\{1, 2, 3, \dots, n\}$ forma um subgrupo de ordem $\frac{n!}{2}$ do grupo S_n , tal subgrupo é notado por A_n . Mais ainda, A_n é o único subgrupo de S_n .

Definição 3.9. Homomorfismo: Dados dois grupos $(G, *)$ e (J, Δ) , dizemos que uma aplicação $f : G \longrightarrow J$ é um *homomorfismo* de G em J se, e somente se,

$$(\forall a, b \in G)(f(a * b) = f(a) \Delta f(b)).$$

Um homomorfismo do grupo G nele próprio é chamado *endomorfismo* de G . Se $f : G \longrightarrow J$ é um homomorfismo de grupos e se f é injetora, então f recebe o nome de *monomorfismo* de G em J . Já, se $f : G \longrightarrow J$ é um homomorfismo de grupos e se f é sobrejetora, então f recebe o nome de *epimorfismo* de G em J .

Definição 3.10. Isomorfismo: Sejam $(G, *)$ e (J, Δ) grupos quaisquer. Dizemos que uma aplicação $f : G \rightarrow J$ é um *isomorfismo* do grupo G no grupo J se, e somente se,

1. f é bijetora;
2. f é um homomorfismo de grupos.

Se $G = J$, um isomorfismo $f : G \rightarrow G$ chama-se *automorfismo* de G .

Além disso, dizemos que o grupo G é isomorfo ao grupo J quando existe um isomorfismo $f : G \rightarrow J$ entre eles. Denotamos $G \simeq J$.

No que segue, ao abordar propriedades de um homomorfismo de grupos, $f : G \rightarrow J$, usaremos a notação multiplicativa tanto para o grupo G quanto para o grupo J . Além disso, denotaremos por e o elemento neutro de G e por u é o elemento neutro de J .

Proposição 3.11. *Seja $f : G \rightarrow J$ um homomorfismo de grupos. Então:*

- (i) $f(e) = u$;
- (ii) $\forall a \in G, f(a^{-1}) = f(a)^{-1}$;
- (iii) $\forall a, b \in G, f(ab^{-1}) = f(a)f(b)^{-1}$.

Demonstração. (i) $f(e) = u$ pois:

$$f(e)f(e) = f(ee) = f(e) = uf(e) \Rightarrow f(e)f(e) = uf(e) \Rightarrow f(e) = u, \text{ pela Lei do Cancelamento.}$$

(ii) $f(a^{-1}) = f(a)^{-1}$, de fato:

$$f(a)f(a^{-1}) = f(aa^{-1}) = f(e) = u = f(a)f(a)^{-1} \Rightarrow f(a)f(a^{-1}) = f(a)f(a)^{-1} \Rightarrow f(a^{-1}) = f(a)^{-1}, \text{ pela Lei do Cancelamento.}$$

(iii) $f(ab^{-1}) = f(a)f(b)^{-1}$, pois:

$$f(ab^{-1}) = f(a)f(b^{-1}) = f(a)f(b)^{-1}.$$

□

Proposição 3.12. *Seja $f : G \rightarrow J$ um homomorfismo de grupos. Então:*

- (i) $N(f)$ é um subgrupo de G ;
- (ii) f é um homomorfismo injetor se, e somente se, $N(f) = \{e\}$.

Demonstração. No que segue, usaremos diversas vezes os itens da proposição 3.11.

- (i) Como $f(e) = u$, então $e \in N(f)$ e, portanto, $N(f) \neq \emptyset$. Por outro lado, se $a, b \in N(f)$, então $f(a) = u = f(b)$ e, portanto:

$$f(ab^{-1}) = f(a)f(b^{-1}) = f(a)[f(b)]^{-1} = uu^{-1} = u.$$

Isso mostra que $ab^{-1} \in N(f)$ e portanto, pela proposição 3.7, $N(f)$ é um subgrupo de G .

- (ii) ($\Rightarrow$) Por hipótese, f é injetor e temos de mostrar que o único elemento de $N(f)$ é e .

Para isso, vamos tomar $a \in N(f)$ e demonstrar que necessariamente $a = e$.

De fato, como $a \in N(f)$, então $f(a) = u$, mas, $f(e) = u$, portanto, $f(a) = f(e)$.

Como, porém, f é injetor, por hipótese, então $a = e$. Ou seja, $N(f) = \{e\}$.

($\Leftarrow$) Sejam $X_1, X_2 \in G$ elementos tais que $f(X_1) = f(X_2)$. Multiplicando-se cada membro dessa igualdade por $[f(X_2)]^{-1}$, obtém-se $f(X_1)[f(X_2)]^{-1} = u$. Mas, pelo item (iii) da proposição 3.11, $f(X_1)[f(X_2)]^{-1} = f(X_1X_2^{-1})$. Portanto, $f(X_1X_2^{-1}) = u$, o que mostra que $X_1X_2^{-1} \in N(f) = \{e\}$. Então $X_1X_2^{-1} = e$, e portanto, $X_1 = X_2$. De onde, f é injetor, como queríamos provar.

□

Definição 3.13. Classes laterais: Seja H um subgrupo de um grupo $(G, *)$. Dado $a \in G$ indicaremos por aH (respectivamente por Ha) e chamaremos de *classe lateral* à esquerda (respectivamente à direita), módulo H , definida por a , o seguinte subconjunto de G :

$$aH = \{a * x \mid x \in H\}$$

(respectivamente, $Ha = \{x * a \mid x \in H\}$). Se G é um grupo comutativo então $aH = Ha, \forall a \in G$.

Definição 3.14. Subgrupos normais: Um subgrupo N de um grupo G se diz *normal* de G se, e somente se, $xN = Nx, \forall x \in G$.

Notação: $N \triangleleft G$.

Proposição 3.15. *Um subgrupo N de um grupo G é normal de G se, e somente se, tem-se a seguinte propriedade, para cada $x \in G$: $xyx^{-1} \in N, \forall y \in N$.*

Demonstração. Por definição, um subgrupo N de um grupo G se diz *normal* de G se, e somente se, $xN = Nx, \forall x \in G$, logo devemos mostrar que: $\forall x \in G$,

$$xN = Nx \iff xyx^{-1} \in N, \forall y \in N.$$

Façamos isso.

Seja $x \in G$, qualquer. Suponha que $xN = Nx$. Dado $y \in N$ arbitrário, defina $b := xyx^{-1}$. Sendo $b = xyx^{-1}$ tem-se $bx = xy$ com $xy \in xN$, logo $bx \in xN$, mas por hipótese, $xN = Nx$, logo $bx \in Nx$. Com isso, temos que $bx = zx$, para algum $z \in N$, consequentemente, $b = z \in N$, ou seja, $xyx^{-1} \in N$.

Reciprocamente, suponha que, dado $x \in G$ arbitrário, tem-se $xyx^{-1} \in N$, para qualquer $y \in N$, e mostremos a igualdade de conjunto $xN = Nx$.

- (i) $xN \subset Nx$, pois: seja $c \in xN$, qualquer, logo $c = xz$, para algum $z \in N$, assim: sendo e o elemento neutro de G ,

$$c = xz = xze = xz(x^{-1}x) = (xxz^{-1})x \Rightarrow c = (xxz^{-1})x \in Nx, \text{ já que, por hipótese, } xzx^{-1} \in N. \text{ Logo, } c \in Nx.$$

- (ii) $Nx \subset xN$, de fato: seja $d \in Nx$, qualquer, logo $d = zx$, para algum $z \in N$, assim: sendo e o elemento neutro de G ,

$$d = zx = ezx = (xx^{-1})zx = x(x^{-1}zx) = x(x^{-1}z(x^{-1})^{-1}) \Rightarrow d = x(x^{-1}z(x^{-1})^{-1}) \in xN, \text{ já que, por hipótese, } x^{-1}z(x^{-1})^{-1} \in N. \text{ Logo, } d \in xN.$$

□

Proposição 3.16. *Se $f : G \rightarrow J$ é um homomorfismo de grupos, então o núcleo $N(f)$ é um subgrupo normal.*

Demonstração. Já sabemos pela proposição 3.12 que $N(f)$ é um subgrupo. Para provar que $N(f)$ é subgrupo normal, faremos uso da proposição 3.15 e provaremos que, para cada $x \in G$, $xyx^{-1} \in N(f)$, para qualquer $y \in N(f)$.

Considere $b := xyx^{-1}$ e analisemos $f(b)$: $f(b) = f(xyx^{-1}) = f(x)f(y)f(x^{-1}) = f(x)uf(x^{-1}) = f(x)f(x^{-1})$, pois como $y \in N(f)$ tem-se $f(y) = u$, em que u é o elemento neutro de J .

Consequentemente, $f(b) = f(x)f(x^{-1}) = f(x)(f(x))^{-1} = u$, ou seja, $f(b) = u$ e, portanto, $b \in N(f)$.

□

Definição 3.17. Grupos quocientes: O grupo G/N obtido por meio das condições anteriores é chamado *grupo quociente* de G por N . A existência de G/N pressupõe que N seja subgrupo normal do grupo G .

Seja N um subgrupo normal de G . Observemos que

- a) $(aN) \cdot (bN) = (ab)N, \forall a, b \in G$;
- b) $[(aN) \cdot (bN)] \cdot (cN) = (aN) \cdot [(bN) \cdot (cN)], \forall a, b, c \in G$;
- c) $(aN) \cdot (eN) = (eN) \cdot (aN) = aN, \forall a \in G$;
- d) $(aN) \cdot (a^{-1}N) = (a^{-1}N) \cdot (aN) = eN = N, \forall a \in G$.

A operação $\cdot$ é chamada de produto de subconjuntos, onde: $(aN) \cdot (bN) = \{x * y \mid x \in aN \text{ e } y \in bN\}$.

No caso de N ser subgrupo normal de G indicaremos por G/N o conjunto das classes laterais à esquerda (que é o mesmo das classes laterais à direita), módulo N , em G .

Essas condições nos mostram que $(G/N, \cdot)$ é um grupo.

A partir de agora, denotamos grupos $(G, *)$ e (J, Δ) simplesmente por G e J .

Na sequência são enunciados três resultados clássicos envolvendo grupos quocientes.

Teorema 3.18. Primeiro Teorema do isomorfismo: *Sejam G e J grupos quaisquer. Se $f : G \rightarrow J$ é um homomorfismo de grupos então o grupo quociente $\frac{G}{N}$, em que N é o núcleo de f , é isomorfo a imagem de f , $\text{Im} f$, ou seja,*

$$\frac{G}{N} \simeq \text{Im} f.$$

Demonstração. Vide resultado 34.2, página 307, da referência [6]. □

Corolário 3.19. *$f : A \rightarrow B$ é um homomorfismo sobrejetivo, então $\frac{A}{N} \simeq B$.*

Teorema 3.20. Segundo Teorema do isomorfismo: *Sejam H e N subgrupos do grupo G com $N \triangleleft G$, então: $\frac{HN}{N} \simeq \frac{H}{H \cap N}$, onde $HN = \{hn \mid h \in H \text{ e } n \in N\}$.*

Demonstração. Vide resultado 34.5, página 308, da referência [6]. □

Teorema 3.21. Terceiro Teorema do isomorfismo: *Sejam H e K subgrupos normais do grupo G com $K \subset H$, então: $\frac{G}{H} \simeq \frac{\frac{G}{K}}{\frac{H}{K}}$.*

Demonstração. Vide resultado 34.7, página 309, da referência [6]. □

Abordamos agora, de maneira bem pontual a definição de grupo cíclico, para tanto precisamos do seguinte resultado:

Teorema 3.22. *Se $(G, \cdot)$ é um grupo e $a \in G$, então o conjunto*

$$H := \{a^n : n \in \mathbb{Z}\}$$

é um subgrupo de G , mas ainda, é o menor subgrupo de G que contém o elemento a , ou seja, qualquer subgrupo contendo a contém H . Tal subgrupo é chamado de subgrupo cíclico de G gerado por a e denotado por $\langle a \rangle$.

Demonstração. Vide resultado 5.17, página 54, [6].

□

Observação 3.23. Destacamos que, em notação de grupo multiplicativo, $(G, \cdot)$, tem-se:

$$\langle a \rangle = \left\{ a^n = \underbrace{aa \dots a}_{n\text{-fatores}} : n \in \mathbb{Z} \right\}.$$

Enquanto que, em notação de grupo aditivo, $(G, +)$, tem-se:

$$\langle a \rangle = \left\{ na = \underbrace{a + a + \dots + a}_{n\text{-parcelas}} : n \in \mathbb{Z} \right\}.$$

Definição 3.24. Dizemos que um elemento a de um grupo G gera G e é um gerador para G quando $G = \langle a \rangle$.

Além disso, dizemos que um grupo é cíclico se existe alguma elemento $a \in G$ tal que gera G .

Tem-se diversos resultados e exemplos interessantes envolvendo a definição de grupo cíclico, entretanto, não faremos esta abordagem completa. Dentre todos os resultados destacamos que: todo grupo cíclico é abeliano (vide resultado 6.1, página 59, [6]).

Exemplo 3.25. O grupo aditivo $(\mathbb{Z}, +)$ é cíclico, gerado tanto por 1, quando por -1.

A partir de agora estamos interessados em definir grupo solúvel. Para tanto, é necessário explorar diversas definições e resultados, que podem ser encontrados com mais detalhes na Parte VII, a partir da página 307, da referência [6].

Definição 3.26. Série subnormal (ou subvariante) é uma sequência finita $H_0, H_1, \dots, H_n$ de subgrupos de G tais que $H_i \triangleleft H_{i+1}, \forall i \in \{0, \dots, n-1\}$.

Definição 3.27. Série normal (ou invariante) é uma sequência finita $H_0, H_1, \dots, H_n$ de subgrupos normais à G , tais que $H_i < H_{i+1}, \forall i \in \{0, \dots, n-1\}$.

Para ambos os casos: $H_0 = \{e\}$ e $H_n = G$.

Exemplo 3.28. São séries normais do grupo $\mathbb{Z}$:

$$\{0\} < 8\mathbb{Z} < 4\mathbb{Z} < \mathbb{Z}$$

e

$$\{0\} < 9\mathbb{Z} < \mathbb{Z}.$$

Definição 3.29. Uma série subnormal (normal) $\{K_j\}$ é um **refinamento de uma série subnormal (normal)** $\{H_i\}$ de um grupo G , quando $\{H_i\} \subseteq \{K_j\}$, isto é, se cada H_i for algum K_j .

Exemplo 3.30. A série $\{0\} < 72\mathbb{Z} < 24\mathbb{Z} < 8\mathbb{Z} < 4\mathbb{Z} < \mathbb{Z}$ é um refinamento da série: $\{0\} < 72\mathbb{Z} < 8\mathbb{Z} < \mathbb{Z}$.

Definição 3.31. Série de composição é uma série subnormal $H_0, \dots, H_n$ tal que $\frac{H_i}{H_{i+1}}$ é grupo simples para todo $i \in \{0, \dots, n-1\}$.

Teorema 3.32. Teorema de Jordan-Hölder *Quaisquer duas séries de composição (ou principal) de um grupo G são isomorfas.*

Demonstração. Vide resultado 35.15, página 316 da referência [6]. □

A próxima definição será essencial para o entendimento do capítulo “A insolubilidade da quártica”, particularmente, ao lema 5.3.

Definição 3.33. Um grupo G é **solúvel** se ele possui uma série de composição $\{H_i\}$, tal que todos os grupos quocientes $\frac{H_{i+1}}{H_i}$ sejam abelianos. Quando um grupo não é solúvel, dizemos que este é insolúvel.

De acordo com o Teorema de Jordan-Hölder (3.32), temos que para um grupo solúvel, *todas* as séries de composição têm os grupos quocientes $\frac{H_{i+1}}{H_i}$ abelianos.

Exemplo 3.34. O exemplo clássico de um grupo que não é solúvel, e, portanto, insolúvel, é S_5 (vide exemplo 3.8) não é um grupo solúvel já que existe uma série de composição de S_5 , a saber, $\{I_{S_5}\} < A_5 < S_5$, com A_5 não abeliano.

3.2 Anéis e Corpos

Segundo Fraleigh (2002) [6], foi David Hilbert (1826 – 1943) quem primeiro introduziu o termo *anel*, mas foi somente na segunda década do século XX que uma definição totalmente abstrata apareceu. A teoria dos anéis comutativos recebeu uma base axiomática sólida por Emmy Noether (1882 – 1935) em seu artigo monumental “Ideal Theory in Rings”, escrito em 1921. Um dos principais conceitos deste artigo é a condição da cadeia ascendente para os ideais. Noether provou que em qualquer anel em que toda cadeia ascendente de ideais tenha um elemento máximo, todo ideal é finitamente gerado.

Emmy Noether recebeu seu doutorado pela Universidade de Erlangen, Alemanha, em 1907. Hilbert a convidou para Göttingen em 1915, mas seus esforços para garantir a ela uma posição paga foram bloqueados por causa de seu gênero. Hilbert reclamou: “Não vejo que o sexo da candidata seja um argumento contra sua admissão [ao corpo docente]. Afinal, somos uma universidade, não um estabelecimento balnear”. Noether foi, no entanto, capaz de dar palestras sob o nome de Hilbert. Em última análise, após as mudanças políticas que acompanharam o fim da Primeira Guerra Mundial alcançarem Göttingen, ela recebeu em 1923 um cargo remunerado na universidade. Na década seguinte, ela foi muito influente no desenvolvimento dos conceitos básicos da álgebra moderna. Junto com outros professores judeus, no entanto, foi forçada a deixar Göttingen em 1933. Passou os últimos dois anos de sua vida no Bryn Mawr College, perto da Filadélfia.

Definição 3.35. Seja A um conjunto não vazio, $+$ e $\cdot$ duas operações binárias em A . Dizemos que a terna $(A, +, \cdot)$ é um anel quando:

- i) $(A, +)$ é um grupo abeliano;
- ii) $a(bc) = (ab)c, \forall a, b, c \in A$;
- iii) Dados, $a, b, c \in A$:
 - $a(b + c) = ab + ac$;
 - $(a + b)c = ac + bc$.

Além disso, se o anel $(A, +, \cdot)$ satisfaz

$$ab = ba, \forall a, b \in A,$$

o chamamos de anel comutativo.

Ainda, se o anel $(A, +, \cdot)$ tem um elemento $1 \in A$, tal que

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

dizemos que A é um anel com unidade.

Exemplo 3.36. Vejamos alguns anéis comuns:

- $(\mathbb{Z}, +, \cdot)$ anel comutativo com unidade.

- $(\mathbb{Q}, +, \cdot)$ anel comutativo com unidade.
- $(\mathbb{R}, +, \cdot)$ anel comutativo com unidade.
- $(\mathbb{C}, +, \cdot)$ anel comutativo com unidade.

Exemplo 3.37. Considere o conjunto, das matrizes $M_n(A) = \{(a_{ij}) : a_{ij} \in A \text{ e } i, j \in \{1, \dots, n\}\}$ em que $A \in \{\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}\}$. A terna, $(M_n(A), +, \cdot)$, em que $+$ e $\cdot$ são as operações usuais entre matrizes quadradas de ordem n , é um anel com unidade, em que a unidade é dada por:

$$\begin{pmatrix} 1 & 0 & \dots & 0 \\ 0 & 1 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & 1 \end{pmatrix}$$

Porém, não é comutativo.

Exemplo 3.38. Sejam $m > 1$, natural e o conjunto $\mathbb{Z}_m = \{\bar{0}, \bar{1}, \dots, \bar{m}\}$ dos inteiros módulo m . Então $(\mathbb{Z}_m, +_m, \cdot_m)$ é anel comutativo com unidade, onde para $\bar{a}, \bar{b} \in \mathbb{Z}_m$, $\bar{a} +_m \bar{b} = \overline{a + b}$ e $\bar{a} \cdot_m \bar{b} = \overline{a \cdot b}$.

Exemplo 3.39. Sejam $m > 1$ natural e o conjunto $m\mathbb{Z} = \{mk, k \in \mathbb{Z}\}$. Então $(m\mathbb{Z}, +, \cdot)$ é anel comutativo sem unidade.

Exemplo 3.40. Sejam $(A, +_A, \cdot_A)$ e $(B, +_B, \cdot_B)$ anéis. É possível definir $A \times B$ uma estrutura de anel, a saber:

Para todos $(a_1, b_1), (a_2, b_2) \in A \times B$, definimos as operações:

- $(a_1, b_1) + (a_2, b_2) := (a_1 +_A a_2, b_1 +_B b_2);$
- $(a_1, b_1) \cdot (a_2, b_2) := (a_1 \cdot_A a_2, b_1 \cdot_B b_2).$

com as quais a terna $(A \times B, +, \cdot)$ é um anel chamado Produto Direto de A com B .

Veja que,

- Se A e B são comutativos então o produto direto também será;
- Se A e B são anéis com unidade 1_A e 1_B , respectivamente, então o produto também tem, a saber, o par ordenado $(1_A, 1_B)$.

Proposição 3.41. *Seja A um anel. São válidas as seguintes afirmações:*

- a) $a \cdot 0 = 0 = 0 \cdot a, \forall a \in A$;
- b) $a(-b) = -ab = (-a)(b), \forall a, b \in A$;
- c) $(-a)(-b) = ab, \forall a, b \in A$;
- d) $a(b - c) = ab - ac, \forall a, b, c \in A$, em que notação $x - y$ significa $x + (-y)$;
- e) Dados $a \in A$, e $m, n \in \mathbb{N}^*$:

- $a^m \cdot a^n = a^{m+n}$
- $(a^m)^n = a^{mn}$

em que $a^1 = a$ e $a^n = a^{n-1} \cdot a, n > 1$.

Definição 3.42. Sejam A um anel e $L \subset A, L \neq \emptyset$. Dizemos que L é um subanel de A , quando:

- i) $a + b \in L$ e $a \cdot b \in L, \forall a, b \in L$;
- ii) $(L, +, \cdot)$ é um anel.

Proposição 3.43. *Sejam A um anel e $L \subset A, L \neq \emptyset$.*

L é subanel de $A \Leftrightarrow a - b \in L$ e $a \cdot b \in L, \forall a, b \in L$.

Observação 3.44. Veja que se A é anel comutativo, então, todo subanel L de A também o será.

Entretanto, se A é anel com unidade 1_A e L é um subanel de A , podem acontecer 3 situações:

- 1º) L ter unidade 1_L e $1_L = 1_A$, como, por exemplo, quando $L = \mathbb{Z}$ e $A = \mathbb{Q}$.
- 2º) L ter unidade 1_L e $1_L \neq 1_A$, como, por exemplo, quando $A = A_1 \times A_2$ e $L = \{0_{A_1}\} \times A_2$, onde A_1 e A_2 são anéis com unidade.
- 3º) L não ter unidade, como, por exemplo, quando $m > 1, L = m\mathbb{Z}$ e $A = \mathbb{Z}, m > 1$.

Definição 3.45. Seja A um anel comutativo e com unidade. Se $a, b \in A$ são tais que $a \neq 0_A, b \neq 0_A$ e $ab = 0_A$, os chamamos de divisores de zero em A .

Exemplo 3.46. Em $\mathbb{Z}_6$, temos que $\bar{2} \neq \bar{0}$ e $\bar{3} \neq \bar{0}$, mas $\bar{2} \cdot \bar{3} = \overline{2 \cdot 3} = \bar{6} = \bar{0}$.

Ou seja, $\bar{2}$ e $\bar{3}$ são divisores de zero em $\mathbb{Z}_6$.

Exemplo 3.47. Em $M_2(\mathbb{R})$, temos que:

$$A = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} \neq \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} \text{ e } B = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \neq \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}.$$

porém $A \cdot B = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$, isto é, A e B são divisores de zero em $M_2(\mathbb{R})$.

Definição 3.48. Se A é um anel comutativo com unidade e sem divisores próprios de zero em A , então dizemos que A é um anel de integridade (ou domínio de integridade).

Exemplo 3.49. a) Temos que $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$ e $\mathbb{C}$ são anéis de integridade.

b) $\mathbb{Z}_6$ não é anel de integridade.

c) $\mathbb{Z} \times \mathbb{Z}$ não é anel de integridade embora $\mathbb{Z}$ seja, pois os elementos não nulos $(1, 0)$ e $(0, 1)$ são divisores de zero em $\mathbb{Z} \times \mathbb{Z}$, já que

$$(1, 0) \cdot (0, 1) = (1 \cdot 0, 0 \cdot 1) = (0, 0).$$

Proposição 3.50. $\mathbb{Z}_m$ é anel de integridade se, e somente se, m é primo.

Demonstração. Já sabemos que $\mathbb{Z}_m$ é anel comutativo e com unidade, para qualquer $m > 1$.

Logo, provemos que:

$$\mathbb{Z}_m \text{ não tem divisores de zero} \Leftrightarrow m \text{ é primo.}$$

($\Rightarrow$) Por hipótese, temos que $\mathbb{Z}_m$ não tem divisores próprios de zero. Suponha, por absurdo, que $m > 1$ não seja primo, logo, existem $a, b \in \mathbb{Z}$, em que $1 < a, b < m$, tais que: $m = a \cdot b$. Daí,

$$a \cdot b = m \Rightarrow \overline{a \cdot b} = \bar{m} = \bar{0} \Rightarrow \overline{a \cdot b} = \bar{0} \Rightarrow \bar{a} \cdot \bar{b} = \bar{0}$$

em que $\bar{a} \neq \bar{0}$ e $\bar{b} \neq \bar{0}$. Ou seja, $\bar{a}$ e $\bar{b}$ são divisores de zero, o que é absurdo pois, por hipótese, $\mathbb{Z}_m$ não tem divisores de zero.

($\Leftarrow$) Por hipótese, temos que m é primo. Provemos que $\mathbb{Z}_m$ não tem divisor de zero. Sejam $\bar{a}, \bar{b} \in \mathbb{Z}_m$, tais que $\bar{a} \cdot \bar{b} = \bar{0}$. Daí,

$$\bar{a} \cdot \bar{b} = \bar{0} \Rightarrow \overline{a \cdot b} = \bar{0} \Rightarrow m \mid a \cdot b \Rightarrow m \mid a \text{ ou } m \mid b \Rightarrow \bar{a} = \bar{0} \text{ ou } \bar{b} = \bar{0}.$$

□

Teorema 3.51. *Seja A um anel comutativo com unidade. Então A é anel de integridade se, e somente se, $a \cdot b = a \cdot c$ implica $b = c$, onde $a, b, c \in A$ com $a \neq 0_A$.*

Demonstração. ($\Rightarrow$) Suponha que A é anel de integridade. Sejam $a, b, c \in A, a \neq 0_A$, arbitrários, tais que $a \cdot b = a \cdot c$.

Assim,

$$a \cdot b = a \cdot c \Rightarrow a \cdot b + (-a \cdot c) = 0_A \Rightarrow a \cdot b - a \cdot c = 0_A \Rightarrow a \cdot (b - c) = 0_A \Rightarrow b - c = 0_A \Rightarrow b = c.$$

Como A já é anel comutativo com unidade, resta mostrar que A não tem divisores de zero. Para tanto, sejam $a, b \in A$, tais que $a \neq 0$ e $a \cdot b = 0$. Veja que, da hipótese e de $0 = a \cdot 0$, temos:

$$a \neq 0 \text{ e } a \cdot b = a \cdot 0 \Rightarrow b = 0.$$

□

Observação 3.52. Seja A um anel com unidade, denotamos por $\mathcal{U}(A)$ o conjunto dos elementos invertíveis de A , ou seja,

$$\mathcal{U}(A) = \{a \in A : \exists \ a^{-1} \in A \text{ com } a \cdot a^{-1} = 1 = a^{-1} \cdot a\}$$

Por exemplo, $\mathcal{U}(\mathbb{Z}) = \{-1, 1\}$, $\mathcal{U}(\mathbb{Q}) = \mathbb{Q}^*$, $\mathcal{U}(\mathbb{R}) = \mathbb{R}^*$ e $\mathcal{U}(\mathbb{C}) = \mathbb{C}^*$.

Definição 3.53. Um corpo $(F, +, \cdot)$ é um anel comutativo com unidade e tal que $\mathcal{U}(F) = F - \{0\}$.

Exemplo 3.54. Por exemplo, $\mathbb{Q}, \mathbb{R}$ e $\mathbb{C}$ são corpos.

Proposição 3.55. *Todo corpo é um anel de integridade.*

Demonstração. Seja F um corpo. Como F é corpo, temos que F é comutativo e com unidade. Provemos que F cumpre: 3.48.

Para tanto, sejam: $a, b, c \in F, a \neq 0$, tais que $ab = ac$. Como $a \in \mathcal{U}(F)$, temos que: $ab = ac \Rightarrow a^{-1}(ab) = a^{-1}(ac) \Rightarrow (a^{-1}a)b = (a^{-1}a)c \Rightarrow 1b = 1c \Rightarrow b = c$.

Observação 3.56. A recíproca da proposição 3.55 não é verdadeira, pois $\mathbb{Z}$ é anel de integridade, porém, como $\mathcal{U}(\mathbb{Z}) = \{-1, 1\}$, temos que $\mathbb{Z}$ não é um corpo.

□

Teorema 3.57. *Todo anel de integridade finito é um corpo.*

Demonstração. Seja $K = \{a_1, a_2, \dots, a_n\}$ um anel de integridade finito com n elementos. Como K é um anel de integridade temos que K é comutativo com unidade. Assim, para K ser corpo basta mostrar que $\mathcal{U}(K) = K - \{0\} = K^*$.

Façamos isto. Seja $a \in K^*$ qualquer. Defina a seguinte aplicação:

$$\begin{aligned} f_a : K &\longrightarrow K \\ a_i &\longmapsto f_a(a_i) := a \cdot a_i \end{aligned}$$

Veja que f_a é injetora, pois

$$f_a(a_i) = f_a(a_j) \Rightarrow a \cdot a_i = a \cdot a_j \Rightarrow a_i = a_j.$$

Logo, como K é finito e f_a é injetora, segue que f_a também é sobrejetora, ou seja, $Im f_a = K$, isto é,

$$\{a \cdot a_1, a \cdot a_2, \dots, a \cdot a_n\} = K.$$

Observe que $1 \in K = \{a \cdot a_1, \dots, a \cdot a_n\}$. Assim, existe $a_{j_0} \in K$, tal que $1 = a \cdot a_{j_0}$. Consequentemente, a_{j_0} é o elemento inverso de a . Assim, todo elemento $a \neq 0$ de K é inversível e, portanto,

$$\therefore \mathcal{U}(K) = K^*.$$

□

Exemplo 3.58. $\mathbb{Z}_p$, com p primo, é corpo pois é um anel de integridade finito.

Definição 3.59. Se para um anel A existe um número inteiro positivo n tal que $n \cdot a = 0$, em que $n \cdot a$ significa $a + a + \dots + a$ para n parcelas, então o menor inteiro positivo com esta propriedade é denominado a característica do anel A . Ainda, se tal número inteiro não existe, então dizemos que A tem característica 0 (zero).

Exemplo 3.60. O anel $\mathbb{Z}_n$ tem característica n enquanto que, os anéis $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ e $\mathbb{C}$ tem característica 0.

Observação 3.61. É possível mostrar que: “um corpo F ou tem característica p , em que p é um número primo, e neste caso contém um subcorpo isomorfo ao corpo $\mathbb{Z}_p$, ou tem característica 0 e neste caso contém um subcorpo isomorfo ao corpo $\mathbb{Q}$ ”. Para mais detalhes consulte [6] [teorema 27.19, p. 249]. Neste contexto, os corpos $\mathbb{Z}_p$ e $\mathbb{Q}$ são chamados de **corpos primos**.

A seguir, veremos um exemplo interessante de corpo que é construído a partir de um anel de integridade A , a este corpo denominamos corpo de frações de A .

Seja A um anel de integridade e denote $A^* = A - \{0_A\}$, definimos em $A \times A^*$ a seguinte relação:

$$\forall (a, b), (c, d) \in A \times A^* : (a, b) \sim (c, d) \Leftrightarrow ad = bc.$$

Veja que esta relação é de equivalência.

Dado $(a, b) \in A \times A^*$, a classe $(\overline{a, b})$ é denotada por $\frac{a}{b}$, com isso o conjunto quociente $\frac{A \times A^*}{\sim}$ é dado por $\left\{ \frac{a}{b} : a, b \in A, b \neq 0_A \right\}$ tal conjunto, denotamos por $F(A)$.

Além disso, definindo as operações $+$ e $\cdot$ em $F(A)$, por

$$\forall \frac{a}{b}, \frac{c}{d} \in F(A) : \frac{a}{b} + \frac{c}{d} = \frac{ad + bc}{bd} \text{ e } \frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd},$$

temos que $(F(A), +, \cdot)$ é um corpo chamado Corpo das Frações de A .

Exemplo 3.62. Se $A = \mathbb{Z}$ então seu corpo de frações é dado por $F(\mathbb{Z}) = \mathbb{Q}$.

Observe ainda que $L = \left\{ \frac{a}{1} : a \in A \right\}$ é um subanel de $F(A)$.

A próxima definição estabelece um tipo especial de aplicação entre anéis de forma que mantém uma consistência entre as estruturas algébricas dos anéis envolvidos.

Definição 3.63. Sejam A e B anéis. Uma aplicação $f : A \rightarrow B$ é um homomorfismo de anéis quando dados $x, y \in A$:

- i) $f(x +_A y) = f(x) +_B f(y)$;
- ii) $f(x \cdot_A y) = f(x) \cdot_B f(y)$.

Proposição 3.64. *Seja $f : A \rightarrow B$ um homomorfismo de anéis. São válidas:*

$$(i) \ f(0_A) = 0_B;$$

$$(ii) \quad f(-a) = -f(a), \forall a \in A;$$

$$(iii) \quad f(a - b) = f(a) - f(b), \forall a, b \in A;$$

$$(iv) \quad L \text{ é subanel de } A \Rightarrow f(L) \text{ é subanel de } B;$$

$$v) \quad \text{Se } A \text{ tem unidade } 1_A \text{ e } f \text{ sobrejetora, então } f(1_A) \text{ é a unidade de } B, \text{ isto é, } 1_B = f(1_A);$$

$$vi) \quad \text{Se } A \text{ tem unidade, } f \text{ sobrejetora e } a \in \mathcal{U}(A) \text{ então } f(a) \in \mathcal{U}(B) \text{ e } (f(a))^{-1} = f(a^{-1});$$

Demonstração. As respectivas demonstrações dos itens (i), (ii) e (iii) seguem exatamente os mesmos passos das demonstrações dos itens (i), (ii) e (iii) da proposição 3.12 da seção sobre Grupos, porém usando a notação aditiva para grupos, já que A e B sendo anéis são, em particular, grupos aditivos abelianos e então f pode ser visto também como um homomorfismo entre grupos aditivos. Para os demais itens, veja que:

(iv) L é subanel de $A \Rightarrow f(L)$ é subanel de B , pois: sejam A um anel e $L \subset A, L \neq \emptyset$, sabemos, pela proposição 3.43, que L é subanel de $A \Leftrightarrow a - b \in L$ e $a \cdot b \in L, \forall a, b \in L$. Para provar que $f(L)$ é subanel de B sejam $x, y \in f(L)$, quaisquer, logo existem $a, b \in L$ tais que $f(a) = x$ e $f(b) = y$, com isso: $x - y = f(a) - f(b) = f(a - b) \in f(L)$, pois $a - b \in L$. Além disso, $x \cdot y = f(a) \cdot f(b) = f(a \cdot b) \in f(L)$, pois $a \cdot b \in L$. Portanto, pela proposição 3.43, $f(L)$ é subanel de B .

v) Se A tem unidade 1_A e f sobrejetora, então $f(1_A)$ é a unidade de B , isto é, $1_B = f(1_A)$, pois: como f é sobrejetora, então $b = f(a)$, para algum $a \in A$. Portanto, $b f(1_A) = f(a) f(1_A) = f(a 1_A) = f(a) = b$. Analogamente: $f(1_A) b = b$. Logo, $f(1_A)$ é a unidade de B , 1_B .

vi) Se A tem unidade, f sobrejetora e $a \in \mathcal{U}(A)$ então $f(a) \in \mathcal{U}(B)$ e $(f(a))^{-1} = f(a^{-1})$, de fato: veja que $f(a) f(a^{-1}) = f(a a^{-1}) = f(1_A) = 1_B$.

$$\text{De modo análogo, } f(a^{-1}) f(a) = f(a^{-1} a) = f(1_A) = 1_B.$$

$$\text{Portanto, } (f(a))^{-1} = f(a^{-1}).$$

□

Definição 3.65. Isomorfismo de anéis é um homomorfismo que é bijetor.

Exemplo 3.66. Seja A anel de integridade, então

$$\begin{aligned} f : A &\longrightarrow L \\ a &\longmapsto f(a) := \frac{a}{1} \end{aligned}$$

é um isomorfismo, em que $L = \left\{ \frac{a}{1}, a \in A \right\}$ é subanel de $F(A)$.

Como $A \simeq L$ e $L \subset F(A)$ admitimos na sequência que $A \subset F(A)$.

A seguir, definimos a subestrutura mais importante de um anel comutativo.

Definição 3.67. Seja A um anel comutativo. Dizemos que $I \subset A, I \neq \emptyset$, é um ideal de A quando satisfaz:

- i) $x - y \in I, \forall x, y \in I$;
- ii) $a \cdot x \in I, \forall x \in I, \forall a \in A$

Exemplo 3.68. (a) $n\mathbb{Z}$ é ideal de $\mathbb{Z}$.

b) Os conjuntos $I = A$ ou $I = \{0\}$ são ideais e são chamados de ideais triviais.

Observação 3.69. Todo ideal I de um anel comutativo A é um subanel. Porém, nem todo subanel é um ideal, por exemplo: $\mathbb{Z}$ é subanel de $\mathbb{Q}$, porém $\mathbb{Z}$ não é ideal de $\mathbb{Q}$. Se $\frac{1}{2} \in \mathbb{Q}$ e $1 \in \mathbb{Z} : \frac{1}{2} \cdot 1 = \frac{1}{2} \notin \mathbb{Z}$.

Proposição 3.70. Seja $f : A \mapsto B$ um homomorfismo de anéis. O conjunto $N(f) = \{a \in A : f(a) = 0_B\}$ é um ideal de A chamado núcleo de f .

Demonstração. $\forall x, y \in N(f), \forall a \in A :$

- i) $x - y \in N(f)$, pois:

$$f(x - y) = f(x) - f(y) = 0_B - 0_B = 0_B.$$
- ii) $a \cdot x \in N(f)$, pois:

$$f(a \cdot x) = f(a) \cdot f(x) = f(a) \cdot 0_B = 0_B.$$

□

Proposição 3.71. Seja $f : A \rightarrow B$ um homomorfismo de anéis. Então

f é injetivo se, e somente se, $N(f) = \{0_A\}$.

Demonstração. Esta demonstração segue exatamente os mesmos passos da demonstração do item (ii) da proposição 3.12 da seção sobre Grupos, porém usando a notação aditiva para grupos e, conseqüentemente, os três primeiros itens da proposição 3.64, já que A e B sendo anéis são, em particular, grupos aditivos abelianos e então f pode ser visto também como um homomorfismo entre grupos aditivos. $\square$

Proposição 3.72. *Sejam A um anel comutativo e I ideal de A , são válidas:*

$$i) \ 0_A \in I;$$

$$ii) \ -x \in I, \forall x \in I;$$

$$iii) \ x + y \in I, \forall x, y \in I;$$

$$iv) \ \text{Se } A \text{ tem unidade e se existe } u \in \mathcal{U}(A) \text{ tal que } u \in I, \text{ então } I = A.$$

Proposição 3.73. *Sejam A um anel comutativo e $a_1, a_2, \dots, a_n \in A$. O conjunto*

$$\langle a_1, a_2, \dots, a_n \rangle = \left\{ \sum_{i=1}^n \alpha_i \cdot a_i : \alpha_i \in A, 1 \leq i \leq n \right\} \subseteq A$$

é um ideal de A , chamado de ideal gerado por $a_1, \dots, a_n$. Em particular, quando $n = 1$,

$$\langle a \rangle = \{ \alpha \cdot a, \alpha \in A \}$$

é chamado de ideal principal gerado por a .

Demonstração. Veja que

$$0_A \in \langle a_1, \dots, a_n \rangle$$

pois

$$0_A = 0_A \cdot a_1 + 0_A \cdot a_2 + \dots + 0_A \cdot a_n \in \langle a_1, \dots, a_n \rangle \text{ com isso } \langle a_1, \dots, a_n \rangle \neq \emptyset.$$

Observe que sendo $x, y \in \langle a_1, \dots, a_n \rangle$, segue que existem $\alpha_i, \beta_i \in A, 1 \leq i \leq n$, tais que

$$x = \sum_{i=1}^n \alpha_i \cdot a_i \text{ e } y = \sum_{i=1}^n \beta_i \cdot a_i.$$

$$\bullet \ x - y \in \langle a_1, \dots, a_n \rangle, \text{ pois } x - y = \sum_{i=1}^n \alpha_i \cdot a_i - \sum_{i=1}^n \beta_i \cdot a_i = \sum_{i=1}^n (\alpha_i - \beta_i) \cdot a_i = \sum_{i=1}^n \gamma_i \cdot a_i, \\ \text{com } \gamma_i = \alpha_i - \beta_i \in A, 1 \leq i \leq n.$$

$$\text{Logo, } x - y = \sum_{i=1}^n \gamma_i \cdot a_i \in \langle a_1, \dots, a_n \rangle.$$

- Para $c \in A$, $c \cdot x \in \langle a_1, \dots, a_n \rangle$, pois $c \cdot x = c \sum_{i=1}^n \alpha_i \cdot a_i = \sum_{i=1}^n (c \cdot \alpha_i) \cdot a_i \in \langle a_1, \dots, a_n \rangle$.

Portanto, $\langle a_1, \dots, a_n \rangle$ é ideal.

□

Definição 3.74. Dizemos que um anel de integridade A é um anel principal quando todo ideal de A é principal, isto é, A é anel principal quando é anel de integridade e para todo I ideal de A , existe $a \in A$ tal que:

$$I = \langle a \rangle.$$

Um anel principal também é chamado de Domínio de Ideais Principais (P. I. D. [Principal Ideals Domain]).

Proposição 3.75. $\mathbb{Z}$ é um anel principal.

Demonstração. Seja I um ideal qualquer de $\mathbb{Z}$. Queremos mostrar que existe $b \in \mathbb{Z}$ tal que $I = \langle b \rangle$.

Veja que;

- Se $I = \{0\}$ então $I = \langle 0 \rangle$.
- Se $I \neq \langle 0 \rangle$, existe $a \in I$, $a \neq 0$, tal que $a > 0$ ou $-a > 0$.

Agora considere o seguinte conjunto $S = \{c \in I : c > 0\}$. Veja que $S \neq \emptyset$, pois $a \in S$ ou $-a \in S$, além disso, $S \subset \mathbb{N}$ e S é limitado inferiormente, nestas condições pelo Princípio da Boa Ordem (PBO), S tem um menor elemento $b \in S$.

Afirmção: $I = \langle b \rangle$. Com efeito,

- $\langle b \rangle \subset I$: pois, seja $x \in \langle b \rangle$ qualquer. Daí existe $\alpha \in \mathbb{Z}$ tal que $x = \alpha \cdot b \in I$.
- $I \subset \langle b \rangle$: pois dado $y \in I$, pelo algoritmo da divisão (de y por b), existem únicos inteiros q e r , com $0 \leq r < b$, tais que:

$$y = q \cdot b + r$$

Assim, $r = y - q \cdot b \in I$. Ou seja, $r \in I$ e $0 \leq r < b$, com isso, necessariamente $r = 0$, pois do contrário $r \in S$ e $r < b$, o que é absurdo, pois b é o menor elemento de S .

Portanto, $y = q \cdot b \in \langle b \rangle$.

□

A seguir apresentamos algumas operações com ideais.

Definição 3.76. Sejam I e J ideais do anel comutativo A . Definimos:

$$I \cap J = \{a \in A : a \in I \text{ e } a \in J\} \text{ e } I + J = \{x + y : x \in I \text{ e } y \in J\}.$$

Observação 3.77. No contexto da definição 3.76, observamos que $I \cap J$ é um ideal e é o “maior” ideal de A que está contido em I e em J e $I + J$ é um ideal e é o “menor” ideal de A que contém I e J .

Definição 3.78. Seja A um anel comutativo e I um ideal de A tal que $I \neq A$. Dizemos que:

i) I é primo, quando cumpre:

$$\forall x, y \in A : x \cdot y \in I \Rightarrow x \in I \text{ ou } y \in I.$$

ii) I é maximal quando cumpre:

$$\forall J \text{ ideal de } A, \text{ tal que } I \subsetneq J \subset A \text{ então } J = A.$$

Proposição 3.79. Se A é anel comutativo com unidade, então todo ideal maximal é ideal primo.

Demonstração. Seja M ideal de A . Vamos mostrar que M é primo, para tanto suponha que $a \cdot b \in M$ e que $a \notin M$.

Defina o seguinte ideal.

$$J = \langle a \rangle + M$$

Veja que $M \subset J$ e $M \neq J$, pois $a \in J$, porém $a \notin M$. Logo, $M \subsetneq J \subset A$.

Como M é maximal, da definição 3.78, segue que

$$J = A$$

Assim, como $1 \in A = J$, segue que $1 \in J$, mas $J = \langle a \rangle + M$, com isso existem $x_0 \in A, m_0 \in M$, tais que:

$$1 = x_0 \cdot a + m_0$$

Daí,

$$b = b \cdot 1 = b \cdot (x_0 \cdot a + m_0) = b \cdot (x_0 \cdot a) + b \cdot m_0 = x_0 \cdot (a \cdot b) + b \cdot m_0 \in M. \text{ Portanto,}$$

$$b \in M. \text{ Assim, } M \text{ é ideal primo de } A.$$

□

Proposição 3.80. *Seja A um anel comutativo com unidade. Então A é um corpo se, e somente se, os únicos ideais de A são os triviais (isto é, $\{0_A\}$ e A).*

A seguir, apresentamos o anel quociente, com efeito, sejam A um anel comutativo e I um ideal de A . A relação em A dada por

$$\forall a, b \in I : a \sim b \Leftrightarrow a - b \in I$$

é uma relação de equivalência, cuja classe de equivalência para cada $a \in A$, é dada por

$$\begin{aligned} \bar{a} = \{x \in A : x \sim a\} &= \{x \in A : x - a \in I\} = \{x \in A : x - a = i, i \in I\} = \\ &= \{a + i : i \in I\} = a + I. \end{aligned}$$

Observe que: $a + I = b + I \Leftrightarrow a \sim b \Leftrightarrow a - b \in I$.

No que segue, denominamos $a + I$ por classe lateral módulo ideal I e o conjunto quociente $\frac{A}{\sim_I}$, será denotado por $\frac{A}{I}$, ou seja, $\frac{A}{I} = \{a + I, a \in A\}$.

Além disso, podemos munir $\frac{A}{I}$ pelas seguintes operações: $\forall a + I, b + I \in \frac{A}{I}$,

- $(a + I) + (b + I) = (a + b) + I$;
- $(a + I) \cdot (b + I) = (a \cdot b) + I$.

A terna $\left(\frac{A}{I}, +, \cdot\right)$ é um anel comutativo denominada de anel quociente de A pelo ideal I .

Teorema 3.81. Teorema do isomorfismo para anéis: *Seja $f : A \rightarrow B$ um homomorfismo de anéis comutativos. Então $\frac{A}{N} \simeq \text{Im} f$, em que N é o núcleo de f .*

Demonstração. Defina a seguinte aplicação:

$$\begin{aligned} \delta : \quad \frac{A}{N} &\rightarrow \text{Im} f \\ a + N &\mapsto \delta(a + N) := f(a) \end{aligned}$$

Afirmção: δ é um isomorfismo.

1. δ é homomorfismo de anéis. Dados $a + N, b + N \in \frac{A}{I}$:

- $\delta((a + N) + (b + N)) = \delta((a + b) + N) = f(a + b) = f(a) + f(b) = \delta(a + N) + \delta(b + N)$.
- $\delta((a + N)(b + N)) = \delta(ab + N) = f(ab) = f(a)f(b) = (a + N)(b + N)$.

2. δ é injetora.

Usando a proposição 3.71, mostremos que $N(\delta) = \{0_A + N\}$.

Já sabemos que $\{0_A + N\} \subset N(\delta)$.

Mostremos que $N(\delta) \subset \{0_A + N\}$, ou seja, que para qualquer $a + N \in N(\delta)$ tem-se $a + N = 0_A + N$, ou ainda, $a \in N$.

De fato,

$$a + N \in N(\delta) \Rightarrow \delta(a + N) = 0_B \Rightarrow f(a) = 0_B \Rightarrow a \in N \Rightarrow a + N = 0_A + N \Rightarrow a + N \in \{0_A + N\}.$$

Portanto $N(\delta) = \{0_A + N\}$.

3. δ é sobrejetora

Seja $b \in \text{Im} f$, qualquer. Logo, existe $a_0 \in A$ tal que $f(a_0) = b$. Tomando a classe

$a_0 + N \in \frac{A}{N}$ temos:

$$\delta(a_0 + N) = f(a_0) = b.$$

Portanto, δ é sobrejetora.

□

Corolário 3.82. $f : A \rightarrow B$ é um homomorfismo sobrejetivo, então $\frac{A}{N(f)} \simeq B$.

Proposição 3.83. Sejam A um anel comutativo com unidade e I um ideal de A . Então,

i) $\frac{A}{I}$ é anel de integridade $\Leftrightarrow I$ é ideal primo.

ii) $\frac{A}{I}$ é um corpo $\Leftrightarrow I$ é ideal maximal.

Demonstração. Primeiramente, abordaremos o item i):

($\Rightarrow$) Seja $\frac{A}{I}$ anel de integridade. Para provar que I é um ideal primo, suponha que:

$$a \cdot b \in I.$$

Como $a \cdot b \in I$, segue que:

$$a \cdot b + I = 0 + I = I = \mathbb{O}_{\frac{A}{I}} \Rightarrow (a + I) \cdot (b + I) = \mathbb{O}_{\frac{A}{I}} \Rightarrow a + I = \mathbb{O}_{\frac{A}{I}} \text{ ou } b + I = \mathbb{O}_{\frac{A}{I}}, \text{ ou}$$

$$\text{seja, } a + I = I \text{ ou } b + I = I \Rightarrow a \in I \text{ ou } b \in I.$$

$\therefore I$ é primo.

($\Leftarrow$) Seja I ideal primo. Veja que sendo A comutativo e com unidade segue que $\frac{A}{I}$ é anel comutativo com unidade. Provemos que $\frac{A}{I}$ não tem divisores de zero, para tanto, suponha que:

$$(a + I) \cdot (b + I) = \mathbb{O}_{\frac{A}{I}}. \text{ Daí,}$$

$$(a + I) \cdot (b + I) = \mathbb{O}_{\frac{A}{I}} \Rightarrow a \cdot b + I = I \Rightarrow a \cdot b \in I \Rightarrow a \in I \text{ ou } b \in I \Rightarrow a + I = I \text{ ou } b + I = I \Rightarrow a + I = \mathbb{O}_{\frac{A}{I}} \text{ ou } b + I = \mathbb{O}_{\frac{A}{I}}.$$

Agora, demonstraremos a bicondicional referente ao item ii):

($\Rightarrow$) Suponha que $\frac{A}{I}$ é corpo e seja J ideal de A , tal que $I \subsetneq J \subset A$.

Como $I \subsetneq J$ segue que existe $x \in J$ tal que $x \notin I$.

Assim:

$$x \notin I \Rightarrow x + I \neq I = \mathbb{O}_{\frac{A}{I}} \Rightarrow x + I \neq \mathbb{O}_{\frac{A}{I}}.$$

Logo, como $\frac{A}{I}$ é corpo e $x + I \neq \mathbb{O}_{\frac{A}{I}}$ segue que existe $y + I \in \frac{A}{I}$ tal que:

$$(x + I) \cdot (y + I) = 1 + I.$$

Daí,

$$(I) \cdot (y + I) = 1 + I \Rightarrow x \cdot y + I = 1 + I \Rightarrow 1 - x \cdot y \in I \subsetneq J \Rightarrow 1 - x \cdot y \in J \Rightarrow$$

$$1 - x \cdot y = j, j \in J \Rightarrow 1 = j + x \cdot y \in J \Rightarrow 1 \in J \Rightarrow J = A.$$

$\therefore I$ é maximal.

($\Leftarrow$) Suponha que I é ideal maximal. Mostremos que $\frac{A}{I}$ é corpo.

Como A é comutativo com unidade, segue que $\frac{A}{I}$ é comutativo com unidade, restando mostrar apenas que $\mathcal{U}\left(\frac{A}{I}\right) = \frac{A}{I} - \{\mathbb{O}_{\frac{A}{I}}\}$.

Para tanto, seja $a + I \in \frac{A}{I}$ tal que $a + I \neq \mathbb{O}_{\frac{A}{I}}$.

Assim,

$$a + I \neq I \Rightarrow a \notin I$$

Com isso, o ideal $J = \langle a \rangle + I$ é tal que $I \subsetneq J \subset A$, mas I é maximal, logo

$$J = A.$$

Em particular,

$$\begin{aligned} 1 \in A = J = \langle a \rangle + I &\Rightarrow 1 \in \langle a \rangle + I \Rightarrow 1 = b \cdot a + i, \text{ com } b \in A \text{ e} \\ i \in I &\Rightarrow 1 - b \cdot a = i \in I \Rightarrow 1 - b \cdot a \in I \Rightarrow 1 + I = b \cdot a + I \Rightarrow 1 + I = (b + I) \cdot (a + I). \end{aligned}$$

Logo, $b + I$ é o elemento inverso de $a + I$. $\square$

A seguir, exploraremos o anel mais importante para essa dissertação, a saber, $F[X]$, em que F é um corpo, pois neste caso $F[X]$ é um *P.I.D.*

3.3 Anéis de Polinômios

Definição 3.84. Seja A um anel comutativo com unidade. Uma sequência em A é uma função, f , cujo domínio é o conjunto dos números naturais $\mathbb{N}$, ou seja:

$$\begin{aligned} f : \mathbb{N} &\longrightarrow A \\ n &\longmapsto f(n) := a_n \end{aligned}$$

neste caso denotamos f por $(a_n)_{n \in \mathbb{N}}$, deste modo é possível identificar qual é a lei de correspondência para cada $n \in \mathbb{N}$, a_n , denominado termo geral da sequência.

Em particular, dizemos que uma sequência $(a_n)_{n \in \mathbb{N}}$ é quase-nula quando existe $r \in \mathbb{N}$ tal que:

$$a_m = 0_A, \forall m > r.$$

Exemplo 3.85. São exemplos de sequências quase-nulas:

- 1) $(0, 0, 0, \dots, 0, \dots)$ é quase nula denotada por $\mathbb{0}$.
- 2) $(1, 2, 3, 4, 0, \dots, 0, \dots)$.
- 3) $(1, 0, 0, \dots, 0, \dots)$, denotada por 1 .

4) $(7, 8, 9, 0, \dots, 0, \dots)$.

No conjunto $\mathcal{P}_A$ das seqüências quase-nulas em A , temos duas operações binárias: $+$ e $\cdot$, definidas para todos $f, g \in \mathcal{P}_A$, digamos $f = (a_n)_n$ em que $a_m = 0$ para $m > r_0$, em que $r_0 \in \mathbb{N}$; $g = (b_n)_n$, em que $b_m = 0$, $m > r_1$, em que $r_1 \in \mathbb{N}$:

$+$: $f + g = (a_n)_n + (b_n)_n = (a_n + b_n)_n \in \mathcal{P}_A$, pois existe $r = \max\{r_0, r_1\}$ tal que $a_m = b_m = 0, m > r$.

$\cdot$: $f \cdot g = (a_n)_n \cdot (b_n)_n = (C_k)_{k \in \mathbb{N}}$, em que $C_k := \sum_{i=0}^k a_i \cdot b_{k-i}$.

Isto é, $C_0 = a_0 \cdot b_0, C_1 = a_0 \cdot b_1 + a_1 \cdot b_0, C_2 = a_0 \cdot b_2 + a_1 \cdot b_1 + a_2 \cdot b_0, \dots$

Veja que $(C_k)_{k \in \mathbb{N}} \in \mathcal{P}_A$, pois existe $r = r_0 + r_1 \in \mathbb{N}$ tal que:

$C_m = 0, \forall m > r$.

Afirmção: $(\mathcal{P}_A, +, \cdot)$ é anel comutativo com unidade, denominado anel de polinômios em A . Observe que:

$\mathbb{O} = (0, 0, 0, \dots, 0, \dots)$

$1 = (1_A, 0, 0, \dots, 0, \dots)$

$-f = (-a_n)_n$

Se A é anel de integridade então $\mathcal{P}_A$ também é anel de integridade, pois $\mathcal{P}_A$ já é comutativo com unidade e se $f \neq \mathbb{O}$ e $g \neq \mathbb{O}$ então $f \cdot g \neq \mathbb{O}$. De fato:

$f = (a_n)_n$, em que $a_{j_0} \neq 0_A$, para algum $j_0 \in \mathbb{N}$ e $a_m = 0, m > j_0$.

$g = (b_n)_n$, em que $b_{i_0} \neq 0_A, i_0 \in \mathbb{N}, b_m = 0, \forall m > i_0$.

Considere $f \cdot g = (C_n)$, onde $n \in \mathbb{N}$, note que $C_{i_0+j_0} \neq 0$, pois $c_{i_0+j_0} = a_{j_0} + b_{i_0}$ onde A é anel de integridade e $a_{j_0} \neq 0$ e $b_{i_0} \neq 0$.

Definição 3.86. Seja A anel comutativo com unidade. Se $f \in \mathcal{P}_A$ e $f \neq \mathbb{O}$, definimos grau de f , denotado por ∂f , como sendo $r \in \mathbb{N}$ tal que $a_r \neq 0$ e $a_m = 0, \forall m > r$, sendo que $f = (a_n)_n$.

Exemplo 3.87. 1) Se $f = (0, 1, 2, 3, 0, 0, \dots, 0, \dots)$, então $\partial f = 3$.

2) Se $g = (2, 0, \dots, 0, \dots)$, então $\partial g = 0$.

3) Se $a \in A, a \neq 0_A$, o polinômio $f = (a, 0, 0, \dots, 0, \dots)$ tem grau 0 e é chamado de polinômio constante não-nulo.

Definição 3.88. Representação de um polinômio em $\mathcal{P}_A$. Usamos a notação:

- $1 = (1, 0, 0, 0, \dots, 0, \dots)$;
- $X = (0, 1, 0, \dots, 0, \dots)$;
- $X^2 = X \cdot X = (0, 0, 1, 0, \dots, 0, \dots)$;
- $X^3 = X^2 \cdot X = (0, 0, 0, 1, 0, \dots)$;
- $\vdots$
- $X^n = X^{n-1} \cdot X = (0, \dots, 1, 0, \dots, 0, \dots)$.

Além disso, para sequências em A temos a “multiplicação por escalar.”

$$\begin{aligned} A \times \mathcal{P}_A &\rightarrow A \\ (\lambda, f) &\mapsto \lambda \cdot f \end{aligned}$$

em que

$$\forall \lambda \in A, \forall f = (a_n)_n \in \mathcal{P}_A : \lambda \cdot f = \lambda \cdot (a_n)_n = (\lambda \cdot a_n)_{n \in \mathbb{N}}$$

Com tudo isso, se $f \in \mathcal{P}_A$ com $f = (a_0, a_1, a_2, \dots, a_n, \dots)$ temos:

$$\begin{aligned} f &= (a_0, a_1, a_2, \dots, a_n, \dots) = (a_0, 0, \dots, 0, \dots) + (0, a_1, 0, \dots, 0, \dots) + (0, 0, a_2, 0, \dots, 0, \dots) + \\ &\dots + (0, 0, \dots, a_n, 0, \dots) + \dots = a_0(1, 0, \dots, 0, \dots) + a_1(0, 1, 0, \dots, 0, \dots) + a_2(0, 0, 1, 0, \dots, 0, \dots) + \\ &\dots + a_n(0, \dots, 0, 1, 0, \dots) = a_0 \cdot 1 + a_1 \cdot X + a_2 \cdot X^2 + \dots + a_n \cdot X^n + \dots = \sum_{i=0}^{\infty} a_i \cdot X^i \Rightarrow \\ f &= \sum_{i=0}^{\infty} a_i \cdot X^i. \end{aligned}$$

Em particular, se $f \neq \mathbb{O}$ e $\partial f = n$, temos $f = \sum_{i=0}^n a_i \cdot X^i$. Observe também que:

$$\forall f = (a_n)_n, \forall g = (b_n)_n \in \mathcal{P}_n : f = g \Leftrightarrow a_n = b_n, \forall n \in \mathbb{N}.$$

Exemplo 3.89. 1) Denotamos $f = (7, 8, 9, 0, 0, \dots, 0, \dots)$ por $f = 9X^2 + 8X + 7$.

2) Denotamos $f = (2, 0, 3, 0, 0, \dots)$ por $f = 3X^2 + 2$.

3) Denotamos $h = (1, 0, 0, \dots, 0, 4, 0, \dots)$ por $h = 4X^n + 1$.

Observação 3.90. No contexto da definição 3.88, denotamos $\mathcal{P}_A$ por $A[X]$. E se $f \in \mathcal{P}_A$, denotamos $f(X) = \sum_{i=0}^{\infty} a_i \cdot X^i \in A[X]$.

Observação 3.91. Veja que a função

$$\begin{aligned} \psi : A &\longrightarrow A[X] \\ a &\longmapsto f(X) = a \end{aligned}$$

é um homomorfismo de anéis e injetivo, tal função é chamada de imersão de A em $A[X]$, pelo seguinte fato:

Como ψ é um homomorfismo injetivo, tem-se, pela proposição 3.71, que $N(\psi) = \{0\}$. Assim pelo Teorema 3.81:

$$\frac{A}{N(\psi)} \simeq \text{Im}\psi, \text{ em que } \text{Im}\psi \subset A[X].$$

Ou seja,

$$A \simeq \text{Im}\psi, \text{ em que } \text{Im}\psi \subset A[X].$$

Portanto, podemos admitir nessa roupagem que, “ $A \subset A[X]$ ”.

Além disso, se A é um anel comutativo com unidade e $u \in A$, pode-se mostrar que a aplicação:

$$\begin{aligned} \phi_u : A[X] &\longrightarrow A \\ f(X) = \sum_{i=0}^{\infty} a_i \cdot X^i &\longmapsto \phi_u(f(X)) = \sum_{i=0}^{\infty} a_i \cdot u^i \end{aligned}$$

é um homomorfismo de anéis chamado homomorfismo de valoração, fato este que será demonstrado, em um caso análogo, no próximo capítulo, no teorema 4.3. Neste contexto, definimos

$$f(u) := \phi_u(f(X)).$$

Exemplo 3.92. Considere $A = \mathbb{Z}$ e $-1 \in \mathbb{Z}$. Sejam $f(X), g(X), h(X) \in \mathbb{Z}[X]$ dados por $f(X) = X^3 + X^2 + 1, g(X) = X^5 + X^4$ e $h(X) = X^2 - 1$. Assim,

$$f(-1) = \phi_{-1}(f(X)) = (-1)^3 + (-1)^2 + 1 = 1$$

$$g(-1) = \phi_{-1}(g(X)) = (-1)^5 + (-1)^4 = 0$$

$$h(-1) = \phi_{-1}(h(X)) = (-1)^2 - 1 = 0.$$

Definição 3.93. Sejam A anel comutativo com unidade e $f(X) \in A[X]$. Dizemos que $u \in A$ é um zero (ou raiz) de f , quando:

$$\phi_u(f(X)) = 0, \text{ isto é, } f(u) = 0.$$

Teorema 3.94. *Seja F um corpo. Se $f(X)$ e $g(X)$ são elementos de $F[X]$ onde $g(X) \neq \mathbb{O}$, então existem, e são únicos, elementos $q(X)$ e $r(X)$ em $F[X]$ tais que:*

$$f(X) = g(X) \cdot q(X) + r(X), \text{ com } r(X) = \mathbb{O} \text{ ou } 0 \leq \partial r < \partial g.$$

Demonstração. i) Existência.

Se $f(X) = \mathbb{O}$, basta tomar $q(X) = r(X) = \mathbb{O}$.

Se $\partial f < \partial g$, basta tomar $q(X) = \mathbb{O}$ e $r(X) = f(X)$.

Se $\partial f \geq \partial g$, provemos por indução sobre $n = \partial f$.

Para tanto, considere $\partial f = n \geq m = \partial g$ e denote $F(X) = a_n \cdot X^n + \dots a_1 \cdot X + a_0$, com $a_n \neq 0$ e $g(X) = b_m \cdot X^m + \dots + b_1 \cdot X + b_0$, com $b_m \neq 0$.

Segue a indução:

i) Para $n = 0$, $\partial f = 0$ implica $f(X) = a_0 \neq \mathbb{O}$. Por hipótese $\partial f \geq \partial g$, logo $\partial g = 0$, isto é, $g(X) = b_0 \neq \mathbb{O}$.

Como F é corpo, basta tomar $q(X) = a_0 \cdot b_0^{-1}$ e $r(X) = \mathbb{O}$.

ii) Suponha que para todo $h(X) \in F[X]$ com $0 < \partial h < n$, existam $q(X), r(X) \in F[X]$ tais que $h(X) = q(X) \cdot g(X) + r(X)$ onde $r(X) = \mathbb{O}$ ou $0 \leq \partial r < \partial g$.

iii) Provemos que o resultado é válido para $\partial f = n$. Defina $f_1(X) = f(X) - (a_n \cdot b_m^{-1}) \cdot X^{n-m} \cdot g(X)$. Então, $f_1(X) = a_0 + a_0 1 \cdot X + \dots + a_n \cdot X^n - (a_n \cdot b_m^{-1}) \cdot X^{n-m} \cdot (b_0 + b_1 \cdot X + \dots + b_m \cdot X^m) = a_0 + a_n \cdot X + \dots + a_n \cdot X^n - b_0 \cdot a_n \cdot b_m^{-1} \cdot X^{n-m} - b_1 \cdot a_n \cdot b_m^{-1} \cdot X^{n-m+1} - \dots - a_n \cdot X^n$.

Perceba que $\partial f_1 < n$. Pela hipótese de indução, segue que existem $q_1(X), r_1(X) \in F[X]$ tais que $f_1(X) = q_1(X) \cdot g(X) + r_1(X)$ com $r_1(X) = \mathbb{O}$ ou $0 \leq \partial r_1 < \partial g$.

Logo,

$$f(X) = f_1(X) + (a_n \cdot b_m^{-1}) \cdot X^{n-m} \cdot g(X) = \\ [q_1(X) + (a_n \cdot b_m^{-1}) \cdot X^{n-m}] \cdot g(X) + r_1(X) \text{ onde } r_1(X) = \mathbb{O} \text{ ou } 0 \leq \partial r_1 < \partial g.$$

Portanto, existem $q(X) = q_1(X) + (a_n \cdot b_m^{-1}) \cdot X^{n-m}$ e $r(X) = r_1(X)$ em $F[X]$ tais que $f(X) = g(X) \cdot q(X) + r(X)$ com $r(X) = \mathbb{O}$ ou $0 \leq \partial r < \partial g$.

ii) Unicidade.

Suponha que existam $q_1(X), q_2(X), r_1(X), r_2(X) \in F[X]$ tais que:

* $f(X) = g(X) \cdot q_1(X) + r_1(X)$ e $f(X) = g(X) \cdot q_2(X) + r_2(X)$, com $r_i(X) = \mathbb{O}$ ou $0 \leq \partial r_i < \partial g, i \in \{1, 2\}$.

Daí, de *:

$g(X) \cdot (q_1(X) - q_2(X)) = r_2(X) - r_1(X)$ em que, $r_i(X) = \mathbb{O}$ ou $0 \leq \partial r_i < \partial g, i \in \{1, 2\}$, logo

- Se $r_2(X) - r_1(X) = \mathbb{O}$ então $q_1(X) - q_2(X) = \mathbb{O}$ o que implica $q_1(X) = q_2(X)$ e $r_1(X) = r_2(X)$.
- Se $0 \leq \partial r_i < \partial g$, então $\partial(r_1 - r_2) < \partial g$, assim o grau do polinômio $g(X) \cdot (q_1(X) - q_2(X))$ deve ser nulo ou ter grau estritamente menor que ∂g , o que implica que, necessariamente, $q_1(X) - q_2(X) = \mathbb{O}$, ou seja, $q_1(X) = q_2(X)$ e $r_1(X) = r_2(X)$.

□

Corolário 3.95. *Sejam $f(X) \in F[X]$, F corpo, e $u \in F$. Então u é zero de $f(X)$ se, e somente se, $f(X) = (X - u) \cdot q(X)$, para algum $q(X) \in F[X]$.*

Demonstração. $(\Rightarrow)$ Suponha que u é um zero de $f(X)$, ou seja, $f(u) = 0_F$.

Veja que, pelo teorema 3.94, dividindo $f(X)$ por $(X - u)$ segue que existem $q(X)$ e $r(X)$ em $F[X]$ tais que

$$* \quad f(X) = (X - u) \cdot q(X) + r(X) \text{ com } r(X) = \mathbb{O} \text{ ou } 0 \leq \partial r < 1.$$

De *, segue que, $r(X) = c$ onde $c \in F$ como também ϕ_u é homomorfismo,

$$0 = f(u) = \phi_u(f(X)) = \phi_u((X - u) \cdot q(X) + c) = \phi_u(X - u) \cdot \phi_u(q(X)) + \phi_u(c) = c \Rightarrow c = 0.$$

Portanto, $r(X) = \mathbb{O}$.

$$\therefore f(X) = (X - u) \cdot q(X).$$

($\Leftarrow$) Suponha que existe $q(X) \in F[X]$ tal que

$$f(X) = (X - u) \cdot q(X)$$

Assim,

$$\begin{aligned} f(u) &= \phi_u(f(X)) = \phi_u((X - u) \cdot q(X)) = \phi_u(X - u) \cdot \phi_u(q(X)) = 0 \\ \therefore f(u) &= 0. \end{aligned}$$

□

Teorema 3.96. *Se F é um corpo então $F[X]$ é um anel principal (P.I.D.).*

Demonstração. Temos que mostrar que dado qualquer ideal $I[X]$ de $F[X]$, existe $f(X) \in F[X]$ tal que

$$I[X] = \langle f(X) \rangle$$

Veja que

- Se $I[X] = \mathbb{O}$, então $I[X] = \langle \mathbb{O} \rangle$.
- $I[X] \neq \{\mathbb{O}\}$, então existe $g(X) \in I[X], g \neq \mathbb{O}$, de menor grau.

Temos duas possibilidades:

- $\partial g = 0$:

$$g(X) = c \in F^* = \mathcal{U}(F[X]), \text{ logo pela proposição 3.72 (iv) : } I[X] = F[X] = \langle 1 \rangle$$

$$\text{Portanto, } I[X] = \langle 1 \rangle$$

- $\partial g \geq 1$:

Mostremos que $I = \langle g(X) \rangle$.

$$\text{i) } \langle g(X) \rangle \subset I, \text{ pois } g(X) \in I.$$

ii) $I \subset \langle g(X) \rangle$, pois, seja $f(X) \in I$, qualquer. Pelo teorema 3.94 existem $q(X), r(X) \in F[X]$ tais que:

$$f(X) = q(X) \cdot g(X) + r(X), \text{ com } r(X) = \mathbb{O} \text{ ou } 0 \leq \partial r < \partial g.$$

Assim,

$$r(X) = f(X) - q(X) \cdot g(X) \in I[X] \Rightarrow r(X) \in I[X].$$

Se $r(X) \neq \mathbb{O}$, então, $0 \leq \partial r < \partial g$, ou seja, $r(X)$ seria um polinômio de grau menor que ∂g em I , o que é absurdo pois g é o elemento de menor grau de I .

Logo, necessariamente, $r(X) = \mathbb{O}$.

Portanto, $f(X) = q(X) \cdot g(X) \in \langle g(X) \rangle$.

$\therefore$ Por (i) e (ii), $I = \langle g(X) \rangle$.

□

Definição 3.97. Um polinômio não constante $f(X) \in F[X]$ é **irredutível sobre F** ou é um **polinômio irredutível em $F[X]$** se $f(X)$ não pode ser expresso como um produto $g(X) \cdot h(X)$ em $F[X]$ ambos de grau menor que o grau de $f(X)$. Se $f(X) \in F[X]$ é um polinômio não constante que não é irredutível sobre F , então $f(X)$ é **redutível sobre F** .

Observação 3.98. Existem critérios importantes sobre irredutibilidade polinomial, destacamos alguns destes, em que as demonstrações podem ser encontradas nas páginas 214 à 216 de [6]:

- a) Seja $f(X) \in F[X]$, de grau 2 ou 3. Então, $f(X)$ é redutível sobre F se, e somente se, tem um zero em F .
- b) Se $f(X) \in \mathbb{Z}[X]$, então, $f(X)$ fatora em um produto de dois polinômios de graus menores r e s em $\mathbb{Q}[Z]$ se, e somente se, tiver tal fatoração com polinômios de mesmo grau r e s em $\mathbb{Z}[X]$.
- c) Se $f(X) = X^n + a_{n-1} \cdot X^{n-1} + \dots + a_0$ está em $\mathbb{Z}[X]$ com $a_0 \neq 0$, e se $F(X)$ tem um zero em $\mathbb{Q}$, então, tem um zero m em $\mathbb{Z}$ e m divide a_0 .
- d) **Critério de Eisenstein:** Seja $p \in \mathbb{Z}$ um primo. Suponha que $f(X) = a_n \cdot X^n + \dots + a_0$ está em $\mathbb{Z}[X]$, e $a_n \not\equiv 0 \pmod{p}$, mas $a_i \equiv 0 \pmod{p}$ para todo $i < n$, com $a_0 \not\equiv 0 \pmod{p^2}$. Então, $f(X)$ é irredutível sobre $\mathbb{Q}$.
- e) O polinômio

$$\phi_p(X) = \frac{X^p - 1}{X - 1} = X^{p-1} + X^{p-2} + \dots + X + 1$$

é irredutível sobre $\mathbb{Q}$ para qualquer primo p .

Exemplo 3.99. Veja que há duas formas de argumentação sobre a irredutibilidade de $X^2 - 2$ em $\mathbb{Q}$. Pelo corolário 3.95, como este polinômio é de grau 2, sua redutibilidade se constataria pelo produto de dois fatores de grau 1, o que ocorre se, e somente se, os zeros de $X^2 - 2$, a saber, $\sqrt{2}$ e $-\sqrt{2}$, estivessem em $\mathbb{Q}$, o que não é verdade. Entretanto, pelo item b), da observação 3.98, $X^2 - 2$ tem zero em $\mathbb{Q}$ se, e somente se, tem zero em $\mathbb{Z}$, e pelo item c), da mesma observação, as únicas possibilidades de zeros em $\mathbb{Z}$ são os divisores de 2, ou seja, ± 1 e ± 2 , os quais não são zeros de $X^2 - 2$.

Exemplo 3.100. Estudemos a irredutibilidade do polinômio de grau 4

$$f(X) = X^4 - 2X^2 + 8X + 1$$

sobre $\mathbb{Q}$. Para que $f(X)$ seja irredutível precisamos excluir as possibilidades de fatoração deste polinômio dos dois casos: produto de um fator linear com um fator de grau 3 e o produto de dois fatores de grau 2.

Se $f(X)$ tem um fator linear em $\mathbb{Q}[X]$, então, pelo item b) da observação 3.98, também tem um fator linear em $\mathbb{Z}[X]$, o que equivale dizer que $f(X)$ tem um zero em $\mathbb{Z}$. Entretanto, pelo item c) da mesma observação, esse zero teria que ser um divisor de 1 em $\mathbb{Z}$, isto é, ou ± 1 . Mas, $f(1) = 8$ e $f(-1) = -8$, então, tal fatoração é impossível.

Se $f(X)$ fatora em dois fatores quadráticos em $\mathbb{Q}[X]$, então, pelo item b) da observação 3.98, também se fatora em dois fatores quadráticos em $\mathbb{Z}[X]$, a saber,

$$f(X) = (X^2 + aX + b) \cdot (X^2 + cX + d)$$

em $\mathbb{Z}[X]$.

Igualando os coeficientes das potências de X , necessariamente temos:

$$b \cdot d = 1, a \cdot d + b \cdot c = 8, a \cdot c + b + d = -2, \text{ e } a + c = 0$$

para inteiros $a, b, c, d \in \mathbb{Z}$.

De $b \cdot d = 1$, vemos que $b = d = 1$ ou $b = d = -1$. Em qualquer caso, $b = d$ e de $a \cdot d + b \cdot c = 8$, deduzimos que $d \cdot (a + c) = 8$. Mas isso é impossível, pois $a + c = 0$.

Portanto, uma fatoração em dois polinômios quadráticos também é impossível e $f(X)$ é irredutível sobre $\mathbb{Q}$.

Exemplo 3.101. Tomando $p = 3$, vemos pelo item d) da observação 3.98 que

$$25X^5 - 9X^4 - 3X^2 - 12$$

é irredutível sobre $\mathbb{Q}$.

Corolário 3.102. Se $p(X)$ é irredutível em $F[X]$ e $p(X)$ divide o produto $r_1(X) \dots r_n(X)$, com $r_i(X) \in F[X], \forall i \in \{1, \dots, n\}$ então, $p(X)$ divide $r_i(X)$ para algum $i \in \{1, \dots, n\}$.

Teorema 3.103. Seja F um corpo, então todo polinômio não constante $f(X) \in F[X]$ pode ser fatorado em $F[X]$ em um produto de polinômios irredutíveis sobre F . Além disso, essa fatoração é única a menos da ordem de tais polinômios irredutíveis sobre F e por possível produto de uma constante diferente de zero.

Demonstração. Seja $f(X)$ um polinômio não-constante. Se $f(X)$ não é irredutível, então $f(X) = g(X) \cdot h(X)$, com o grau de $g(X)$ e o grau de $h(X)$ ambos menores que o grau de $f(X)$. Se $g(X)$ e $h(X)$ são ambos irredutíveis, o resultado está provado. Caso contrário, pelo menos um desses se fatora em polinômios de grau menor. Nesse raciocínio, chegamos a uma fatoração

$$f(X) = p_1(X) \cdot p_2(X) \dots p_r(X),$$

em que cada $p_i(X)$ é irredutível para $i \in \{1, 2, \dots, r\}$.

Resta-nos mostrar a unicidade a menos de ordem de produto e constantes não nulas em F .

Suponha que

$$p_1(X) \cdot p_2(X) \dots p_r(X) = f(X) = q_1(X) \cdot q_2(X) \dots q_s(X)$$

sejam duas fatorações de $f(X)$ em polinômios irredutíveis.

Pelo corolário 3.102, $p_1(X)$ divide algum $q_j(X)$, sem perda de generalidade podemos supor que $p_1(X)$ divide $q_1(X)$.

Se $q_1(X)$ é irredutível, então

$$q_1(X) = u_1 p_1(X),$$

com $u_1 \in F - \{0\}$ e, portanto, $u_1 \in \mathcal{U}(F[X])$.

Assim substituindo $q_1(X)$ por $u_1 p_1(X)$ obtemos

$$p_1(X) \cdot p_2(X) \dots p_r(X) = u_1 p_1(X) q_2(X) \dots q_s(X) \Rightarrow p_2(X) \dots p_r(X) = u_1 q_2(X) \dots q_s(X).$$

Por um argumento semelhante, se, digamos $q_2(X) = u_2 p_2(X)$, então

$$p_3(X) \dots p_r(X) = u_1 u_2 q_3(X) \dots q_s(X).$$

Continuando esse processo obtemos:

$$1 = u_1 u_2 \dots u_r q_{r+1}(X) \dots q_s(X). \quad (3.1)$$

Entretanto, isso apenas é possível se $s = r$, conseqüentemente a equação acima é igual $1 = u_1 u_2 \dots u_r$.

Assim, os fatores irredutíveis $p_i(X)$ e $q_j(X)$ são os mesmos, exceto possivelmente por ordem de fatores e produto de uma constante diferente de zero.

□

Teorema 3.104. *Um ideal $\langle p(X) \rangle \neq \mathbb{O}$ de $F[X]$ é maximal se, e somente se, $p(X)$ é irredutível sobre F .*

Demonstração. Suponha que $\langle p(X) \rangle \neq \mathbb{O}$ é um ideal maximal de $F[X]$. Então $\langle p(X) \rangle \neq F[X]$, o que implica $p(X) \notin F[X]$. Seja $p(X) = f(X) \cdot g(X)$ uma fatoração de $p(X)$ em $F[X]$. Como $\langle p(X) \rangle$ é um ideal maximal e, portanto, um ideal primo, $f(X) \cdot g(X) \in \langle p(X) \rangle$ implica que $f(X) \in \langle p(X) \rangle$ ou $g(X) \in \langle p(X) \rangle$; ou seja, $f(X)$ ou $g(X)$ tem $p(X)$ como um fator. Mas então não podemos ter os graus de $f(X)$ e $g(X)$ menores que o grau de $p(X)$. Isso mostra que $p(X)$ é irredutível sobre F .

Reciprocamente, se $p(X)$ é irredutível sobre F , suponha que $N[X]$ seja um ideal tal que $\langle p(X) \rangle \subset N[X] \subset F[X]$. Agora N é um ideal principal pelo teorema 3.96, então $N[X] = \langle g(X) \rangle$ para algum $g(X) \in N[X]$. Se $p(X) \in N[X]$ então $p(X) = g(X) \cdot q(X)$ para algum $q(X) \in F[X]$. Mas $p(X)$ é irredutível, o que implica que $g(X)$ ou $q(X)$ é de grau 0. Se $q(X)$ é de grau 0, implica que $q(X) = c \neq 0$, onde $c \in F$, e $g(X) = \left(\frac{1}{c}\right) \cdot p(X)$ está em $\langle p(X) \rangle$, portanto, $N[X] = \langle p(X) \rangle$. Absurdo! Pois $\langle p(X) \rangle \subsetneq N[X]$. Se $g(X)$ é de grau 0, ou seja, uma constante diferente de zero em F , então $g(X)$ é uma unidade em $F[X]$, logo, $\langle g(X) \rangle = N[X] = F[X]$. Portanto, $\langle p(X) \rangle$ é maximal. □

Essa seção é essencial para o desenvolvimento do próximo capítulo, que é o cerne deste trabalho, e este fato será comprovado através das inúmeras citações de resultados presente no capítulo 3.

4 Elementos da Teoria de Galois

Já estudadas as equações polinomiais com coeficientes complexos até o quarto grau e suas respectivas resoluções, uma pergunta natural que se coloca é se as equações de grau maior que quatro possuem sempre raízes complexas e, em tal caso, se há fórmulas algébricas para expressá-las em função dos coeficientes da equação.

De acordo com Hefez e Villela (2018)[7], a primeira pergunta é respondida de modo afirmativo pelo Teorema Fundamental da Álgebra, entretanto a segunda pergunta foi respondida de modo negativo pelo matemático norueguês Niels Henrik Abel (1802 – 1829), em um artigo publicado em 1824, para as equações gerais de graus maiores ou iguais a cinco.

Porém, algumas equações que abordaremos admitem fórmulas resolventes algébricas em termos dos seus coeficientes. Foi o jovem matemático francês Évariste Galois (1811 – 1832) que caracterizou tais equações, por meio de um estudo, que abordaremos nesse trabalho, conhecido hoje como Teoria de Galois.

Segundo Boyer (1974) [3], a multiplicidade de álgebras inventadas no século *XIX* poderia ter dado à matemática uma tendência centrífuga se não tivessem sido desenvolvidos certos conceitos estruturais. Um dos conceitos mais importantes desse período foi a noção de grupo. Na álgebra, o conceito de grupo foi a força mais importante para a coesão, e um fator essencial no surgimento das ideias abstratas. Não há um nome responsável pelo surgimento da ideia de grupo, mas quem mais se sobressai e que deu o nome a esse conceito foi o jovem Évariste Galois, morto em um duelo que lhe custou a vida por uma “questão de honra” pouco antes de seu vigésimo primeiro aniversário.

Galois nasceu nas proximidades de Paris, na aldeia de Boug-la-Reine, onde seu pai era o prefeito. Seus pais eram bastante cultos, entretanto, não tinham apresentado particular aptidão pela matemática, deles o jovem Galois herdou o seu ódio fervoroso pela tirania. Ao

entrar na escola aos doze anos apresentou pouco interesse pelo latim, grego ou álgebra, mas ficou apaixonado pela *Geometria* de Legendre. Um pouco mais adiante, ele leu e compreendeu obras de álgebra e análise de mestres como Lagrange e Abel, porém, mesmo assim os seus trabalhos escolares permaneciam medíocres e seus professores o consideravam como um aluno excêntrico. Com dezesseis anos, Galois sabia que seus professores não tinham percebido a sua genialidade matemática, mesmo assim, esperava entrar na escola que havia produzido diversos matemáticos célebres, a *École Polytechnique*, porém, foi recusado devido à sua falta de preparo sistemático. Esse foi o seu primeiro fracasso amargo. Aos dezessete anos, Galois expôs suas descobertas fundamentais em um artigo e pediu a Cauchy que apresentasse à *Académie*. Cauchy perdeu o artigo. Daí em diante Galois não odiava somente os examinadores como também os acadêmicos. Um segundo fracasso em uma nova tentativa de ingressar na *Polytechnique* aumentou a sua amargura na vida, todavia, o maior choque estava por vir. Atacado por causa de intrigas clericais, seu pai sentiu-se perseguido e suicidou-se.

Apesar de todos os contratempos que sofrera ao longo de sua vida, Galois entrou na *École Normale* a fim de preparar-se para lecionar; continuou sua pesquisa e em 1830 submeteu um artigo num concurso para o prêmio de matemática da *Académie*. Fourier era o secretário da *Académie*, levou o artigo para ler em sua casa e morreu logo depois, com isso, o artigo se perdeu. Enfrentando em diversas áreas da sua vida tirania e frustrações, Galois aderiu à causa da revolução em 1830. Uma carta fervorosa criticando a indecisão do diretor da *École Normale* resultou em sua expulsão. Tentou, mais uma vez, por meio de Poisson submeter um artigo à *Académie*. Este artigo continha uma série de resultados importantes que hoje fazem parte da Teoria de Galois; mas Poisson, o assessor, devolveu o artigo com a observação de que era “incompreensível”. Totalmente desiludido, Galois entrou para a Guarda Nacional. No ano de 1831, numa reunião de republicanos, fez um brinde que foi interpretado como uma ameaça à vida de Louis Philippe, com isso ele foi preso. Embora solto logo em seguida, foi preso novamente pouco tempo depois e condenado a seis meses de prisão. Saindo da prisão, em seguida envolveu-se com uma mulher e por causa dela, em nome de um código de “honra”, não pôde evitar um duelo que custou sua vida. Numa carta anterior ao duelo, escreveu para amigos, “Fui desafiado por dois patriotas - era impossível recusar”. Na noite anterior ao duelo, com pressentimento de morte, Galois passou horas escrevendo uma carta a um amigo, notas para a posterioridade

sobre suas descobertas. Solicitou que a carta fosse publicada (o que ocorreu no mesmo ano) na *Revue Encyclopedique* e exprimiu a esperança que Jacobi e Gauss pudessem dar publicamente sua opinião sobre a importância dos teoremas apresentados. Na manhã de 30 de maio de 1832, Galois foi ao encontro de seu adversário em um duelo com pistolas. Recebeu um tiro no intestino e ficou caído no local até que um camponês que passava o encontrou e levou-o para o hospital, no qual morreu de peritonite na manhã seguinte. Em seu funeral, compareceram milhares de republicanos. Tinha apenas vinte anos, o mais jovem matemático a fazer descobertas tão significativas.

Galois confiou ao destinatário de sua última carta alguns de seus manuscritos para a *Académie* e em 1846 Liouville editou alguns e publicou em seu *Journal*. Liouville considerou a tarefa como difícil, já que Galois não seguira o conselho de Descartes, “Quando se discute uma questão transcendente, deve-se ser transcendentemente claro”. No entanto, Liouville sentiu-se recompensado quando após preencher as lacunas das provas, percebeu o método pelo qual Galois provara o seguinte teorema:

Para que uma equação irredutível de grau primo possa ser resolvida por radicais é necessário e suficiente que todas as suas raízes sejam funções racionais de duas quaisquer dentre elas.

Logo, o objetivo principal das pesquisas de Galois havia sido o de determinar quando as equações polinomiais são resolúveis por radicais. O início de suas investigações foi por meio de um trabalho de Lagrange sobre as permutações de raízes de uma equação polinomial. Inspirado pela prova de Abel da irresolubilidade por radicais da equação quártica, Galois descobriu que uma equação algébrica irredutível é resolúvel por radicais se, e somente se, seu grupo, o grupo de permutações sobre suas raízes, é resolúvel. A resolução de um grupo solúvel envolve relações entre o grupo e seus subgrupos. Lagrange já tinha provado que a ordem de um subgrupo deve ser um divisor da ordem do grupo (se for finito), mas Galois foi muito além, a saber: a teoria de Galois apresenta um algoritmo para achar de fato as raízes de uma equação quando essas podem ser expressas por radicais, mas a ênfase do seu método está na teoria das equações que, geralmente, se volta mais para a estrutura algébrica ao invés dos casos específicos.

Percebe-se que Galois estava muito perto da atitude moderna e, no entanto, era tão inarticulado que não conseguiu fazer-se compreender pelos professores do seu tempo. Hoje fala-se bastante nas escolas secundárias em “Matemática Moderna”, mas ela só é conside-

rada moderna no sentido de que as ideias de Galois, finalmente, estão chegando a todos, mais de um século depois que o destino o tratou tão mal ao longo de sua curta existência.

Sobre equações do quinto grau solúveis, segundo o Teorema de Abel-Ruffini, uma equação do quinto grau completa não pode ser resolvida por radicais. De acordo com esse teorema, não existe até o presente momento uma fórmula ou técnica para resolver todas as equações do quinto grau por meio de radicais. Entretanto, equações triviais como $x^5 - 243 = 0$ são solúveis e há também casos específicos de equações do quinto grau, de acordo com Andrade (2019) [1], que utilizam-se da igualdade e da transformação de Martinelli para serem resolvidas, substituindo-se a variável x de uma equação do quinto grau, por $\frac{(-b+t)}{5a}$, para que, desse modo, seja possível eliminar o termo de quarto grau da equação. Utilizando um polinômio de décimo grau, faz-se a mudança de variável para que se obtenha um equação do quinto grau que tenha somente soluções inteiras, como é o caso da solução da equação $X^5 + 112X^4 + 4428X^3 + 76032X^2 + 551232X + 1244160 = 0$, esta resolução completa pode ser encontrada em [1]. Mostraremos no próximo capítulo, a existência de uma equação quártica que não pode ser resolvida por radicais.

Iniciamos a construção dos resultados através da definição de extensão de um corpo.

4.1 Sobre Extensões de Corpos

Definição 4.1. Um corpo E é uma **extensão de corpo do corpo F** se F é um subcorpo de E . Denotamos este fato por $F \leq E$.

Exemplo 4.2. $\mathbb{R}$ é uma extensão de $\mathbb{Q}$ e $\mathbb{C}$ é uma extensão de corpos de ambos $\mathbb{R}$ e $\mathbb{Q}$.



Figura 4.1: Diagrama da extensão de corpos

Teorema 4.3. Sejam E uma extensão de um corpo F e $\alpha \in E$. A aplicação $\phi_\alpha : F[X] \rightarrow E$ tal que para todo $f(X) = \sum_{i=0}^n a_i X^i \in F[X]$ tem-se $\phi_\alpha(f(X)) = \phi_\alpha\left(\sum_{i=0}^n a_i X^i\right) =$

$\sum_{i=0}^n a_i \alpha^i \in E$ é um homomorfismo de $F[X]$ em E tal que $\phi_\alpha(a) = a, \forall a \in F$ e $\phi_\alpha(X) = \alpha$.
Tal homomorfismo é denominado **homomorfismo de valoração de $F[X]$ em E** .

Demonstração. A demonstração do teorema é uma consequência das definições de adição e multiplicação em $F[X]$. A aplicação ϕ_α está bem definida, isto é, independente de nossa representação de $f(X) \in F[X]$ como uma soma finita

$$a_0 + a_1 \cdot X + \dots + a_n \cdot X^n,$$

uma vez que tal soma finita representando $f(X)$ pode ser alterada apenas pela inserção ou exclusão de termos da forma $0 \cdot X^i$, que não afeta o valor de $\phi_\alpha(f(X))$.

Se $f(X) = a_0 + a_1 \cdot X + \dots + a_n X^n$, $g(X) = b_0 + b_1 \cdot X + \dots + b_m \cdot X^m$, e $h(X) = f(X) + g(X) = c_0 + c_1 \cdot X + \dots + c_r \cdot X^r$, então,

$$\phi_\alpha(f(X) + g(X)) = \phi_\alpha(h(X)) = c_0 + c_1 \cdot \alpha + \dots + c_r \cdot \alpha^r,$$

enquanto

$$\phi_\alpha(f(X)) + \phi_\alpha(g(X)) = (a_0 + a_1 \cdot \alpha + \dots + a_n \cdot \alpha^n) + (b_0 + b_1 \cdot \alpha + \dots + b_m \cdot \alpha^m).$$

Como por definição de adição polinomial, temos $c_i = a_i + b_i$, vemos que

$$\phi_\alpha(f(X) + g(X)) = \phi_\alpha(f(X)) + \phi_\alpha(g(X)).$$

Voltamos a multiplicação, vemos que

$$f(X) \cdot g(X) = d_0 + d_1 \cdot X + \dots + d_s \cdot X^s,$$

então

$$\phi_\alpha(f(X) \cdot g(X)) = d_0 + d_1 \cdot \alpha + \dots + d_s \cdot \alpha^s,$$

enquanto

$$[\phi_\alpha(f(X))][\phi_\alpha(g(X))] = (a_0 + a_1 \cdot \alpha + \dots + a_n \cdot \alpha^n) \cdot (b_0 + b_1 \cdot \alpha + \dots + b_m \cdot \alpha^m).$$

Visto que pela definição da multiplicação polinomial $\alpha_j = \sum_{i=0}^j a_i \cdot b_{j-i}$, vemos que

$$\phi_\alpha(f(X) \cdot g(X)) = [\phi_\alpha(f(X))] \cdot [\phi_\alpha(g(X))].$$

Assim, ϕ_α é um homomorfismo.

A própria definição de ϕ_α aplicada a um polinômio constante $a \in F[X]$, no qual $a \in F$, nos fornece $\phi_\alpha(a) = a$, então, ϕ_α aplica F isomorficamente pela aplicação de identidade. Novamente, por definição de ϕ_α , temos que $\phi_\alpha(X) = \phi_\alpha(1 \cdot X) = 1 \cdot \alpha = \alpha$.

□

Exemplo 4.4. (a) Considere $F = \mathbb{Q}$ e $E = \mathbb{R}$ no teorema 4.3, e considere o homomorfismo de valoração $\phi_2 : \mathbb{Q}[X] \rightarrow \mathbb{R}$. Então, dado $a_0 + a_1X + \dots + a_nX^n \in \mathbb{Q}[X]$,

$$\phi_2(a_0 + a_1 \cdot X + \dots + a_n \cdot X^n) = a_0 + a_1 \cdot 2 + \dots + a_n \cdot 2^n.$$

Observe que

$$\phi_2(X^2 + X - 6) = 2^2 + 2 - 6 = 0.$$

Assim $X^2 + X - 6$ está no núcleo ϕ_2 . Então,

$$X^2 + X - 6 = (X - 2) \cdot (X + 3),$$

e a razão pela qual $\phi_2(X^2 + X - 6) = 0$ é que $\phi_2(X - 2) = 2 - 2 = 0$.

(b) Sejam $F = \mathbb{Q}$ e $E = \mathbb{C}$ pelo teorema 4.3 e considere o homomorfismo de valoração $\phi_i : \mathbb{Q}[X] \rightarrow \mathbb{C}$. Então, dado $a_0 + a_1X + \dots + a_nX^n \in \mathbb{Q}[X]$,

$$\phi_i(a_0 + a_1 \cdot X + \dots + a_n \cdot X^n) = a_0 + a_1 \cdot i + \dots + a_n \cdot i^n$$

e $\phi_i(X) = i$. Observe que

$$\phi_i(X^2 + 1) = i^2 + 1 = 0,$$

então, $X^2 + 1$ está no núcleo N de ϕ_i .

Definição 4.5. Sejam E uma extensão de um corpo F , $\alpha \in E$ e, considere o homomorfismo de valoração, ϕ_α , de $F[X]$ em E . Para qualquer $f(X) = \sum_{i=0}^n a_i X^i \in F[X]$, denotando $f(\alpha) := \phi_\alpha(f(X)) = \phi_\alpha\left(\sum_{i=0}^n a_i X^i\right) = \sum_{i=0}^n a_i \alpha^i$, tem-se que α é um **zero de** $f(X)$ quando $f(\alpha) = 0$.

Teorema 4.6. Teorema de Kronecker's: *Sejam F um corpo e $f(X)$ um polinômio não constante em $F[X]$. Então, existe uma extensão E do corpo F e $\alpha \in E$ tais que $f(\alpha) = 0$.*

Demonstração. Pelo teorema 3.103, $f(X)$ tem uma fatoração em $F[X]$ em polinômios que são irredutíveis sobre F . Seja $p(X)$ um polinômio irredutível em tal fatoração. É suficiente encontrar um corpo de extensão E de F contendo um elemento α tal que $p(\alpha) = 0$.

Pelo teorema 3.104, $\langle p(X) \rangle$ é um ideal maximal em $F[X]$, então $\frac{F[X]}{\langle p(X) \rangle}$ é um corpo, pela proposição 3.83. Afirmamos que F pode ser identificado como um subcorpo de $\frac{F[X]}{\langle p(X) \rangle}$ através da aplicação $\psi : F \rightarrow \frac{F[X]}{\langle p(X) \rangle}$ dada por

$$\psi(a) = a + \langle p(X) \rangle.$$

para $a \in F$.

Essa aplicação é injetora, pois se $\psi(a) = \psi(b)$, temos $a + \langle p(X) \rangle = b + \langle p(X) \rangle$ para algum $a, b \in F$, por conseguinte, $(a-b) \in \langle p(X) \rangle$, logo $a-b$ deve ser múltiplo do polinômio $p(X)$, que é de grau ≥ 1 . Agora $a, b \in F$ implica que $a-b$ está em F . Assim devemos ter $a-b=0$, pois $a-b = q(X) \cdot p(X)$ com $\partial p(X) \geq 1$ apenas se $q(X) = \mathbb{O}$ e $a-b=0$, então $a=b$, logo ψ é injetiva.

Consequentemente, restringindo o contradomínio de ψ para a sua imagem, que é um subcorpo de $\frac{F[X]}{\langle p(X) \rangle}$, temos uma correspondência biunívoca entre F com a imagem de ψ , com isso identificamos F com $\{a + \langle p(X) \rangle \mid a \in F\}$.

Assim, podemos visualizar que $E = \frac{F[X]}{\langle p(X) \rangle}$ como uma extensão do corpo F . Ou seja, construímos a extensão desejada E de F . Resta-nos mostrar que E contém um zero de $p(X)$.

Vamos definir

$$\alpha = X + \langle p(X) \rangle,$$

então $\alpha \in E$. Considere o homomorfismo de valoração $\phi_\alpha : F[X] \rightarrow E$, dado pelo teorema 4.3. Se $p(X) = a_0 + a_1 \cdot X + \dots + a_n \cdot X^n$, onde $a_i \in F$, então, nós temos

$$\phi_\alpha(p(X)) = a_0 + a_1(X + \langle p(X) \rangle) + \dots + a_n(X + \langle p(X) \rangle)^n$$

em $E = \frac{F[X]}{\langle p(X) \rangle}$. Mas podemos calcular em $\frac{F[X]}{\langle p(X) \rangle}$ escolhendo os representantes, e X é um representante do conjunto $\alpha = X + \langle p(X) \rangle$. Portanto,

$p(\alpha) = (a_0 + a_1 \cdot X + \dots + a_n \cdot X^n) + \langle p(X) \rangle = p(X) + \langle p(X) \rangle = \langle p(X) \rangle = 0$
 em $\frac{F[X]}{\langle p(X) \rangle}$. Encontramos um elemento α em $E = \frac{F[X]}{\langle p(X) \rangle}$ tal que $p(\alpha) = 0$, portanto,
 $f(\alpha) = 0$. $\square$

Exemplo 4.7. Seja $F = \mathbb{Q}$ e considere $f(X) = X^4 - 5X^2 + 6 \in \mathbb{Q}$. Veja que $f(X)$ em sua forma fatorada em $\mathbb{Q}$ é dada por $(X^2 - 2) \cdot (X^2 - 3)$, sendo, ambos os fatores, polinômios irredutíveis sobre $\mathbb{Q}$. Podemos começar com $X^2 - 2$ e construir um corpo de extensão de E de $\mathbb{Q}$ contendo α tal que $\alpha^2 - 2 = 0$, a saber: $E = \frac{\mathbb{Q}}{\langle X^2 - 2 \rangle}$. Outra maneira, é construir um corpo de extensão K de $\mathbb{Q}$ contendo β tal que $\beta^2 - 3 = 0$, que neste caso seria $K = \frac{\mathbb{Q}[X]}{\langle X^2 - 3 \rangle}$.

Definição 4.8. Sejam E uma extensão de um corpo F e $\alpha \in E$. Dizemos que α é **algébrico sobre F** se $f(\alpha) = 0$, para algum $f(X) \in F[X]$, diferente do polinômio nulo. Se α não é algébrico sobre F , então dizemos que α é **transcendente sobre F** .

Exemplo 4.9. Veja que $\mathbb{C}$ é uma extensão do corpo $\mathbb{Q}$. Como $\sqrt{2}$ é um zero de $X^2 - 2$, vemos que $\sqrt{2}$ é um elemento algébrico sobre $\mathbb{Q}$. Além disso, i é um elemento algébrico sobre $\mathbb{Q}$, pois é um zero do polinômio $X^2 + 1$ de $\mathbb{Q}[X]$.

Sabe-se que os números reais π e e são transcendentos sobre $\mathbb{Q}$.

Observe que, embora π seja transcendente sobre $\mathbb{Q}$, π é algébrico sobre $\mathbb{R}$, pois é um zero do polinômio $(X - \pi) \in \mathbb{R}[X]$. Ou seja, a definição de elementos algébricos e transcendentos depende fortemente do corpo F considerado.

Exemplo 4.10. Podemos ver que o número real $\sqrt{1 + \sqrt{3}}$ é algébrico sobre $\mathbb{Q}$. Para $\alpha = \sqrt{1 + \sqrt{3}}$, então, $\alpha^2 = 1 + \sqrt{3}$, ou seja, $\alpha^2 - 1 = \sqrt{3}$ e $(\alpha^2 - 1)^2 = 3$. Portanto, $\alpha^4 - 2\alpha^2 - 2 = 0$, logo, α é um zero de $X^4 - 2X^2 - 2 \in \mathbb{Q}[X]$.

Teorema 4.11. Sejam E uma extensão de um corpo F e $\alpha \in E$. Considere o homomorfismo de valoração de $F[X]$ em E , $\phi_\alpha : F[X] \rightarrow E$, tal que $\phi_\alpha(a) = a, \forall a \in F$ e $\phi_\alpha(X) = \alpha$. Neste contexto, α é transcendente sobre F se, e somente se, ϕ_α é um isomorfismo de $F[X]$ com um subconjunto de E que seja um anel de integridade.

Demonstração. O elemento α é transcendente sobre F se, e somente se, $f(\alpha) \neq 0$ para todo $f(X) \in F[X]$, polinômio não-nulo. Mas isso ocorre se, e somente se, $\phi_\alpha(f(X)) \neq 0$ para todo $f(X) \in F[X]$, polinômio não-nulo, ou seja, se, e somente se, o núcleo de ϕ_α

é $\{0\}$, isto é, se, e somente se, ϕ_α é uma aplicação injetora, pela proposição 3.71. Neste caso, pelo Teorema do Isomorfismo, 3.81:

$$\frac{F[X]}{N(\phi_\alpha)} \simeq \phi_\alpha[F[X]],$$

ou seja,

$$F[X] \simeq \phi_\alpha[F[X]],$$

em que $\phi_\alpha[F[X]]$ é um subdomínio de E .

□

Teorema 4.12. *Sejam E uma extensão do corpo F e $\alpha \in E$. Se α é algébrico sobre F , então existe um polinômio irredutível $p(X) \in F[X]$ tal que $p(\alpha) = 0$. Este polinômio irredutível $p(X)$ é unicamente determinado, a menos de fator constante, não nulo, em F e, ainda, tal polinômio é de grau mínimo ≥ 1 em $F[X]$ tendo α como zero. Além disso, se $f(\alpha) = 0$ para $f(X) \in F[X]$, com $f(X) \neq \mathbb{O}$, então $p(X)$ divide $f(X)$.*

Demonstração. Seja ϕ_α o homomorfismo de valoração de $F[X]$ em E , dado por 4.3. O núcleo de ϕ_α é um ideal e pelo teorema 3.96 deve ser um ideal principal gerado por algum $p(X) \in F[X]$. Agora $\langle p(X) \rangle$ consiste precisamente naqueles elementos de $F[X]$ que tem α como zero. Assim, se $f(\alpha) = 0$ para $f(X) \neq \mathbb{O}$, logo, $f(X) \in \langle p(X) \rangle$, por isso, $p(X)$ divide $f(X)$. Assim, $p(X)$ é um polinômio de grau mínimo ≥ 1 , tendo α como zero, e qualquer outro polinômio do mesmo grau que $p(X)$ deve ser da forma $a \cdot p(X)$, para algum $a \in F$. Resta-nos apenas mostrar que $p(X)$ é irredutível. Se $p(X) = r(X) \cdot s(X)$ fosse uma fatoração de $p(X)$ em polinômios de menor grau, então, $p(\alpha) = 0$ implicaria que $r(\alpha) \cdot s(\alpha) = 0$, então $r(\alpha) = 0$ ou $s(\alpha) = 0$, já que E é um corpo. Isso contradiria o fato de que $p(X)$ é de grau mínimo ≥ 1 tal que $p(\alpha) = 0$. Assim $p(X)$ é irredutível. □

Definição 4.13. Sejam E uma extensão de um corpo F e $\alpha \in E$ algébrico sobre F . O único polinômio mônico $p(X)$ com a propriedade descrita no teorema 4.12 é chamado de **polinômio irredutível para α sobre F** e é denotado por $\text{irr}(\alpha, F)$. O grau de $\text{irr}(\alpha, F)$ é o grau de α sobre F , denotado por $\text{deg}(\alpha, F)$.

Exemplo 4.14. Sabemos que $\text{irr}(\sqrt{2}, \mathbb{Q}) = X^2 - 2$. Vemos que para $\alpha = \sqrt{1 + \sqrt{3}}$ em $\mathbb{R}$, α é um zero de $X^4 - 2X^2 - 2 \in \mathbb{Q}[X]$. Como $X^4 - 2X^2 - 2$ é irredutível sobre $\mathbb{Q}$ (por Eisenstein com $p = 2$), vemos que

$$\text{irr}(\sqrt{1 + \sqrt{3}}, \mathbb{Q}) = X^4 - 2X^2 - 2.$$

Assim, $\sqrt{1 + \sqrt{3}}$ é algébrico de grau 4 sobre $\mathbb{Q}$.

Observação 4.15. Sejam E uma extensão de um corpo F e $\alpha \in E$. Veja que, se α é algébrico sobre F , com a definição acima e considerando o homomorfismo de valoração $\phi_\alpha : F[X] \rightarrow E$, tem-se que $N(\phi_\alpha) = \langle \text{irr}(\alpha, F) \rangle$.

Consequentemente, pelo teorema 3.104, sendo $\text{irr}(\alpha, F)$ um polinômio irredutível em $F[X]$, o ideal $\langle \text{irr}(\alpha, F) \rangle$ é um ideal maximal de $F[X]$ e, portanto, pela proposição 3.83, tem-se que:

$$\frac{F[X]}{\langle \text{irr}(\alpha, F) \rangle} \text{ é corpo.}$$

Neste contexto, estamos interessados em definir a Extensão Simples, $F(\alpha)$, de F , que é a menor extensão do corpo F que contém F e α . Para tanto, exploramos as duas possibilidades da natureza de α sob o ponto de vista da sua transcendência, ou não, sobre F . A saber:

Caso 1: se α é algébrico sobre F , então, pela Observação 4.15:

$$\frac{F[X]}{\langle \text{irr}(\alpha, F) \rangle} \text{ é corpo,}$$

e $\phi_\alpha : F[X] \rightarrow E$ é tal que $\ker(\phi_\alpha) = \langle \text{irr}(\alpha, F) \rangle$ e pelo teorema 3.81 temos que

$$\frac{F[X]}{N(\phi_\alpha)} \simeq \phi_\alpha[F[X]],$$

ou seja,

$$\frac{F[X]}{\langle \text{irr}(\alpha, F) \rangle} \simeq \phi_\alpha[F[X]] \subset E.$$

Então, $\frac{F[X]}{\text{irr}(\alpha, F)}$ é um corpo isomorfo a $\phi_\alpha[F[X]]$ e com isso, $\phi_\alpha[F[X]]$ é um subcorpo de E , mas ainda, é o menor subcorpo de E contendo F e α e é denotado por $F(\alpha)$.

Caso 2: se α é transcendente sobre F , então pelo teorema 4.11, temos que ϕ_α é um isomorfismo entre $F[X]$ e um subdomínio de E , a saber,

$$F[X] \simeq \phi_\alpha[F[X]] \subset E.$$

Denotamos $\phi_\alpha[F[x]]$ por $F[\alpha]$ e o corpo das frações de $F[\alpha]$ denotamos por $F(\alpha)$ que é corpo em E , mas ainda, é o menor subcorpo de E que contém F e α .

Definição 4.16. Um corpo de extensão E de um corpo F é uma **extensão simples** de F se $E = F(\alpha)$ para algum $\alpha \in E$.

Exemplo 4.17. Vejamos alguns exemplos para elucidação dos itens acima:

- 1) $\frac{\mathbb{Q}[X]}{\langle x^2 - 2 \rangle}$ corresponde a extensão simples, do corpo $\mathbb{Q}$, $\mathbb{Q}(\sqrt{2})$
- 2) $\frac{\mathbb{Q}[X]}{\langle x^2 - 3 \rangle}$ corresponde a extensão simples, do corpo $\mathbb{Q}$, $\mathbb{Q}(\sqrt{3})$
- 3) $\mathbb{Q}(\pi)$ é o menor subcorpo de $\mathbb{R}$ que contém $\mathbb{Q}$ e π .

Teorema 4.18. *Sejam E uma extensão simples $F(\alpha)$ de um corpo F . Se α é algébrico sobre F tal que o grau de $\text{irr}(\alpha, F)$ é n , com $n \neq 1$, então cada elemento β de $E = F(\alpha)$ pode ser expresso unicamente na forma*

$$\beta = b_0 + b_1 \cdot \alpha + \dots + b_{n-1} \cdot \alpha^{n-1},$$

em que $b_i \in F, \forall i \in \{0, \dots, n-1\}$.

Demonstração. Para o homomorfismo de valoração usual ϕ_α , todo elemento de

$$F(\alpha) = \phi_\alpha[F[X]]$$

é da forma $\phi_\alpha(f(X)) = f(\alpha)$, um polinômio formal em α com coeficientes em F . Seja

$$\text{irr}(\alpha, F) = p(X) = X^n + a_{n-1} \cdot X^{n-1} + \dots + a_0.$$

Então $p(\alpha) = 0$, logo

$$\alpha^n = -a_{n-1} \cdot \alpha^{n-1} - \dots - a_0.$$

Essa equação em $F(\alpha)$ pode ser usada para expressar todo monômio α^m para $m \geq n$ em termos de potências menores que n . Por exemplo,

$$\begin{aligned} \alpha^{n+1} &= \alpha \alpha^n = -a_{n-1} \alpha^n - a_{n-2} \alpha^{n-1} - \dots - a_0 = \\ &= -a_{n-1}(-a_{n-1} \alpha^{n-1} - \dots - a_0) - a_{n-2} \alpha^{n-1} - \dots - a_0 \alpha. \end{aligned}$$

Assim, se $\beta \in F(\alpha)$, β pode ser expresso na forma requerida

$$\beta = b_0 + b_1 \alpha + \dots + b_{n-1} \alpha^{n-1}.$$

Para unicidade, se

$$b_0 + b_1\alpha + \dots + b_{n-1}\alpha^{n-1} = b'_0 + b'_1\alpha + \dots + b'_{n-1}\alpha^{n-1}$$

para $b'_i \in F$, então

$$(b_0 - b'_0) + (b_1 - b'_1)X + \dots + (b_{n-1} - b'_{n-1})X^{n-1} = g(X)$$

está em $F[X]$ e $g(\alpha) = 0$. Além disso, o grau de $g(X)$ é menor que o grau de $\text{irr}(\alpha, F)$. Como $\text{irr}(\alpha, F)$ é um polinômio diferente de zero de grau mínimo em $F[X]$ tendo α como zero, devemos ter $g(X) = 0$. Portanto, $b_i - b'_i = 0$, então

$$b_i = b'_i,$$

e a unicidade de b_i é estabelecida. □

Teorema 4.19. *Sejam E uma extensão do corpo F , e $\alpha \in E$ algébrico sobre F . Se $\deg(\alpha, F) = n$, então $F(\alpha)$ é um espaço vetorial n -dimensional sobre F com base $\{1, \alpha, \alpha^2, \dots, \alpha^{n-1}\}$. Além disso, todo elemento β de $F(\alpha)$ é algébrico sobre F , e $\deg(\beta, F) \leq \deg(\alpha, F)$.*

Demonstração. Seja $\beta \in F(\alpha)$ onde α é algébrico sobre F de grau n . Considere os elementos

$$1, \beta, \beta^2, \dots, \beta^n.$$

Estes não podem ser $n + 1$ elementos distintos de $F(\alpha)$ que são linearmente independentes sobre F , qualquer base de $F(\alpha)$ sobre F teria que conter pelo menos tantos elementos quanto há em qualquer conjunto de vetores linearmente independentes sobre F . No entanto, a base $\{1, \alpha, \dots, \alpha^{n-1}\}$ tem n elementos. Se $\beta^i = \beta^j$, então $\beta^i - \beta^j = 0$, logo, qualquer caso, existe $b_i \in F$ tal que

$$b_0 + b_1 \cdot \beta + b_2 \cdot \beta^2 + \dots + b_n \cdot \beta^n = 0,$$

onde nem todo $b_i = 0$. Então $f(X) = b_n \cdot X^n + \dots + b_1 \cdot X + b_0$ é um elemento não nulo de $F[X]$ tal que $f(\beta) = 0$. Portanto, β é algébrico sobre F e $\deg(\beta, F)$ é no máximo n . □

A próxima definição é essencial para o conceito de grau de uma extensão E de um corpo F .

Definição 4.20. Uma extensão E de um corpo F é uma **extensão algébrica** de F se cada elemento em E é algébrico sobre F .

Definição 4.21. Se uma extensão E de um corpo F é de dimensão finita n , como um espaço vetorial sobre F , então dizemos que E é uma **extensão finita de grau n sobre F** . Denotamos por $[E : F]$ o grau de E sobre F .

Teorema 4.22. *Toda extensão finita E de um corpo F é uma extensão algébrica sobre F .*

Demonstração. Devemos mostrar que para $\alpha \in E$, α é algébrico sobre F . Se $[E : F] = n$, então

$$1, \alpha, \alpha^2, \dots, \alpha^n$$

não podem ser elementos linearmente independentes, então existem $a_0, a_1, a_2, \dots, a_n \in F$ não todos nulos tais que

$$a_n \cdot \alpha^n + \dots + a_2 \cdot \alpha^2 + a_1 \cdot \alpha + a_0 = 0,$$

Logo, $f(X) = a_n \cdot X^n + \dots + a_2 \cdot X^2 + a_1 \cdot X + a_0$ é um polinômio não nulo em $F[X]$ tal que $f(\alpha) = 0$. Portanto, α é algébrico sobre F . $\square$

Teorema 4.23. (Teorema da Torre) *Se E é uma extensão finita de um corpo F e K é uma extensão finita do corpo E , então, K é uma extensão finita de F e*

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

Demonstração. Digamos que $[K : E] = m$ e $[E : F] = n$. Sejam $\{\alpha_i \mid i \in \{1, \dots, n\}\}$ uma base para E com um espaço vetorial sobre F e o conjunto $\{\beta_j \mid j \in \{1, \dots, m\}\}$ uma base para K com um espaço vetorial sobre E . Veja que é suficiente mostrarmos que os mn elementos $\alpha_i \beta'_j$ s formam uma base para K , visto como um espaço vetorial sobre F . Façamos isto:

Seja γ qualquer elemento de K . Como os β'_j s formam uma base para K sobre E , temos que

$$\gamma = \sum_{j=1}^m b_j \cdot \beta_j$$

para $b_j \in E$. Como os α'_i s formam uma base para E sobre F , temos

$$b_j = \sum_{i=1}^n a_{ij} \cdot \alpha_i$$

para $a_{ij} \in F$. Então

$$\gamma = \sum_{j=1}^m \left(\sum_{i=1}^n a_{ij} \cdot \alpha_i \right) \cdot \beta_j = \sum_{i,j} a_{ij} \cdot (\alpha_i \cdot \beta_j),$$

sendo assim, os mn vetores $\alpha_i \cdot \beta_j$'s geram K sobre F .

Resta-nos mostrar que os mn elementos $\alpha_i \cdot \beta_j$'s são linearmente independentes sobre F . Suponha que $\sum_{i,j} c_{ij} \cdot (\alpha_i \cdot \beta_j) = 0$, com $c_{ij} \in F$. Então

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

e $\left(\sum_{i=1}^n c_{ij} \cdot \alpha_i \right) \in E$. Como os elementos β_j 's são linearmente independentes sobre E , necessariamente tem-se

$$\sum_{i=1}^n c_{ij} \cdot \alpha_i = 0$$

para todo $j \in \{1, \dots, m\}$. Mas, agora, os α_i 's são linearmente independentes sobre F , então $\sum_{i=1}^n c_{ij} \cdot \alpha_i = 0$ implica que $c_{ij} = 0$ para todo $i \in \{1, \dots, n\}$ e $j \in \{1, \dots, m\}$. Assim, os $\alpha_i \cdot \beta_j$ não apenas geram K sobre F mas também são independentes sobre F . Portanto, tais elementos formam uma base para K sobre F .

Observe que provamos esse teorema exibindo uma base. Vale lembrar que se $\{\alpha_i \mid i \in \{1, \dots, n\}\}$ é uma base para E sobre F e $\{\beta_j \mid j \in \{1, \dots, m\}\}$ é uma base para K sobre E , para extensões de corpos $F \leq E \leq K$, então, o conjunto $\{\alpha_i \beta_j\}$ de mn produtos é uma base para K sobre F .

□

Aplicando o Princípio da Indução Finita, temos o seguinte resultado:

Corolário 4.24. *Se F_i é um corpo, $i \in \{1, \dots, r\}$, e F_{i+1} é uma extensão finita de F_i , então F_r é uma extensão finita de F_1 , e*

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

O próximo corolário nos garantirá que não existe elemento em $\mathbb{Q}(\sqrt{2})$ que seja um zero de $X^3 - 2$. Para tanto, bastará observar que $\deg(\sqrt{2}, \mathbb{Q}) = 2$, enquanto um zero de $X^3 - 2$ é de grau 3 sobre $\mathbb{Q}$, e 3 não divide 2.

Corolário 4.25. *Se E é uma extensão do corpo F , $\alpha \in E$ é algébrico sobre F e $\beta \in F(\alpha)$, então $\deg(\beta, F)$ divide $\deg(\alpha, F)$.*

Demonstração. Pelo teorema 4.19, $\deg(\alpha, F) = [F(\alpha) : F]$ e $\deg(\beta, F) = [F(\beta) : F]$. Temos as extensões $F \leq F(\beta) \leq F(\alpha)$, então, pelo teorema 4.23 $[F(\beta) : F]$ divide $[F(\alpha) : F]$, ou seja, $\deg(\beta, F)$ divide $\deg(\alpha, F)$. $\square$

Observação 4.26. Seja E uma extensão de um corpo F . Considere os elementos $\alpha_1, \dots, \alpha_n \in E$, não necessariamente algébricos sobre F . Por definição, $F(\alpha_1)$ é a menor extensão de corpo de F que contém α_1 . Analogamente, podemos definir $F(\alpha_1)(\alpha_2)$ como sendo a menor extensão de F contendo α_1 e α_2 , denotamos esta extensão por $F(\alpha_1, \alpha_2)$. Procedendo de modo iterado, definimos a extensão $F(\alpha_1, \dots, \alpha_n)$ de F como sendo a menor extensão de corpo de F que contém $\alpha_1, \dots, \alpha_n$.

Exemplo 4.27. O teorema 4.19 mostra que $\{1, \sqrt{2}\}$ é uma base para $\mathbb{Q}(\sqrt{2})$ sobre $\mathbb{Q}$. Usando a técnica mostrada no exemplo 4.10, podemos ver que $\sqrt{2} + \sqrt{3}$ é um zero de $X^4 - 10X^2 + 1$. Também podemos mostrar que este polinômio é irredutível em $\mathbb{Q}[X]$. Assim, $\text{irr}(\sqrt{2} + \sqrt{3}, \mathbb{Q}) = X^4 - 10X^2 + 1$ e então $[\mathbb{Q}(\sqrt{2} + \sqrt{3}) : \mathbb{Q}] = 4$. Assim $(\sqrt{2} + \sqrt{3}) \notin \mathbb{Q}(\sqrt{2})$, então $\sqrt{3} \notin \mathbb{Q}(\sqrt{2})$. Consequentemente, $\{1, \sqrt{3}\}$ é uma base para $\mathbb{Q}(\sqrt{2}, \sqrt{3}) = (\mathbb{Q}(\sqrt{2}))(\sqrt{3})$ sobre $\mathbb{Q}(\sqrt{2})$. A prova do teorema 4.23 mostra que $\{1, \sqrt{2}, \sqrt{3}, \sqrt{6}\}$ é uma base para $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ sobre $\mathbb{Q}$.

Teorema 4.28. Se E é uma extensão algébrica de um corpo F . Então existe um número finito de elementos $\alpha_1, \dots, \alpha_n$ em E tal que $E = F(\alpha_1, \dots, \alpha_n)$ se, e somente se, E é um espaço vetorial de dimensão finita sobre F , isto é, se, e somente se, E é uma extensão finita de F .

Demonstração. Suponha que $E = F(\alpha_1, \dots, \alpha_n)$. Como E é uma extensão algébrica de F , cada $\alpha_i \in \{1, \dots, n\}$ é algébrico sobre F , então cada α_i é algébrico sobre todo corpo de extensão de F em E . Assim $F(\alpha_1)$ é algébrica sobre F e, em geral, $F(\alpha_1, \dots, \alpha_j)$ é algébrica sobre $F(\alpha_i, \dots, \alpha_{j-1})$ para $j \in \{2, \dots, n\}$. Pelo corolário 4.24 aplicado à sequência de extensões finitas

$$F, F(\alpha_1), F(\alpha_1, \alpha_2), \dots, F(\alpha_1, \dots, \alpha_n) = E$$

segue que E é uma extensão finita de F .

Reciprocamente, suponha que E seja uma extensão algébrica finita de F . Se $[E : F] = 1$, então $E = F(1) = F$, e terminamos. Se $E \neq F$, seja $\alpha_1 \in E$, onde $\alpha_1 \notin F$. Então, $[F(\alpha_1) : F] > 1$. Se $F(\alpha_1) = E$, terminamos; se não, seja $\alpha_2 \in E$, onde $\alpha_2 \notin F(\alpha_1)$.

Continuando esse processo, vemos pelo teorema 4.23 que, como $[E : F]$ é finito, devemos chegar a α_n tal que

$$F(\alpha_1, \dots, \alpha_n) = E.$$

□

Definição 4.29. Um corpo F é **algebricamente fechado** se todo polinômio não constante em $F[X]$ tem um zero em F .

Definição 4.30. Considere E é uma extensão do corpo F . Então

$$\overline{F}_E = \{\alpha \in E \mid \alpha \text{ é algébrico sobre } F\}$$

é um subcorpo de E , chamado **fecho algébrico de F sobre E** . Veja que todo corpo F tem um **fecho algébrico**, ou seja, uma extensão algébrica $\overline{F}$ que é algebricamente fechado.

Proposição 4.31. *Um corpo F é algebricamente fechado se, e somente se, todo polinômio não constante em $F[X]$ fatora em $F[X]$ em fatores lineares.*

Demonstração. Seja F algebricamente fechado e considere $f(X)$ um polinômio não constante em $F[X]$. Então, $f(X)$ tem um zero $a \in F$. Pelo corolário 3.95, $X - a$ é um fator de $f(X)$, assim, $f(X) = (X - a) \cdot g(X)$. Logo, se $g(X)$ não é constante, tem um zero $b \in F$, e temos $f(X) = (X - a) \cdot (X - b) \cdot h(X)$. Continuando, obtemos uma fatoração de $f(X)$ em $F[X]$ em fatores lineares.

Por outro lado, suponha que todo polinômio não constante de $F[X]$ tenha uma fatoração em fatores lineares. Se $a \cdot X - b$ é um fator linear de $f(X)$, então b/a é um zero de $f(X)$. Por isso, F é algebricamente fechado. □

4.2 Corpo de Galois

Nesta seção apresentamos um importante corpo finito denotado por $GF(p^n)$, em que p é um número primo. Este corpo é conhecido como Corpo de Galois de ordem p^n . Para apresentá-lo, primeiramente, precisamos de resultados envolvendo a característica de um corpo e da definição da n -ésima raiz da unidade.

Teorema 4.32. *Seja E uma extensão finita de grau n sobre um corpo finito F . Se F tem q elementos, então E tem q^n elementos.*

Demonstração. Seja $\{\alpha_1, \dots, \alpha_n\}$ uma base para E com o espaço vetorial sobre F . Todo $\beta \in E$ pode ser escrito *unicamente* na forma

$$\beta = b_1 \cdot \alpha_1 + \dots + b_n \cdot \alpha_n$$

para $b_i \in F$. Visto que cada b_i pode ser qualquer um dos elementos de F , o número total de tais combinações lineares distintas de α_i é q^n $\square$

Corolário 4.33. *Se E é um corpo finito de característica p , então E contém exatamente p^n elementos para algum inteiro positivo n .*

Demonstração. Todo corpo finito E é uma extensão finita de um corpo primo isomorfo ao corpo $\mathbb{Z}_p$, onde p é a característica de E (veja observação 3.61). O corolário segue do teorema 4.32. $\square$

Teorema 4.34. *Seja E um corpo de p^n elementos contidos em um fecho algébrico $\overline{\mathbb{Z}_p}$ de $\mathbb{Z}_p$. Os elementos de E são precisamente os zeros em $\overline{\mathbb{Z}_p}$ do polinômio $X^{p^n} - X$ em $\mathbb{Z}_p[X]$.*

Demonstração. O conjunto E^* dos elementos não nulos de E formam um grupo multiplicativo de ordem $p^n - 1$ sob a multiplicação de corpos. Para $\alpha \in E^*$, a ordem de α neste grupo divide a ordem $p^n - 1$ do grupo. Assim, para $\alpha \in E^*$, temos $\alpha^{p^n - 1} = 1$, então $\alpha^{p^n} = \alpha$. Portanto, todo elemento em E é um zero de $X^{p^n} - X$. Como $X^{p^n} - X$ pode ter no máximo p^n zeros, observamos que E contém precisamente os zeros de $X^{p^n} - X$ em $\overline{\mathbb{Z}_p}$. $\square$

Definição 4.35. Um elemento α de um corpo é uma n -ésima raiz da unidade se $\alpha^n = 1$. Dizemos que α é uma n -ésima raiz primitiva da unidade se $\alpha^n = 1$ e $\alpha^m \neq 1$ para $0 < m < n$.

Observação 4.36. Consequentemente, os elementos não nulos de um corpo finito de p^n elementos são todas as $(p^n - 1)$ -ésimas raízes da unidade.

Além disso, é importante observar que o grupo multiplicativo $(F^*, \cdot)$ de elementos não nulos de um corpo finito F é cíclico. (para mais detalhes consultar Corolário 23.6, página 213, de [6]). Fato esse que será usado na demonstração do próximo resultado.

Proposição 4.37. *Uma extensão finita E de um corpo finito F é uma extensão simples de F .*

Demonstração. Seja α um gerador para o grupo cíclico E^* de elementos diferentes de zero de E . Então $E = F(\alpha)$. $\square$

É possível mostrar que se F é um corpo de característica prima p com fecho algébrico $\overline{F}$, então $X^{p^n} - X$ tem p^n zeros distintos em $\overline{F}$.

Se F é um corpo de característica prima p , então $(\alpha + \beta)^{p^n} = \alpha^{p^n} + \beta^{p^n}$ para todo $\alpha, \beta \in F$ e todos os inteiros positivos n .

Teorema 4.38. *Um corpo finito com p^n elementos sempre existe para toda potência de primo p^n . Denotamos tal corpo por $GF(p^n)$.*

Demonstração. Sejam $\overline{\mathbb{Z}}_p$ um fecho algébrico de $\mathbb{Z}_p$ e K um subconjunto de $\overline{\mathbb{Z}}_p$ consistindo de todos os zeros de $X^{p^n} - X$ em $\overline{\mathbb{Z}}_p$. Para quaisquer $\alpha, \beta \in K$, vimos que $(\alpha + \beta) \in K$, e a equação $(\alpha\beta)^{p^n} = \alpha^{p^n} \cdot \beta^{p^n} = \alpha \cdot \beta$ mostra que $\alpha \cdot \beta \in K$. De $\alpha^{p^n} = \alpha$ obtemos que $(-\alpha)^{p^n} = (-1)^{p^n} \cdot \alpha^{p^n} = (-1)^{p^n} \cdot \alpha$. Se p é um primo ímpar, então $(-1)^{p^n} = -1$ e se $p = 2$, então $-1 = 1$. Portanto $(-\alpha)^{p^n} = -\alpha$, então $-\alpha \in K$. Agora 0 e 1 são zeros de $X^{p^n} - X$. Para $\alpha \neq 0$, $\alpha^{p^n} = \alpha$ implica que $\left(\frac{1}{\alpha}\right)^{p^n} = \frac{1}{\alpha}$. Assim, K é um subcorpo de $\overline{\mathbb{Z}}_p$ contendo $\mathbb{Z}_p$. Portanto, K é o corpo desejado de p^n elementos, pois vimos que $X^{p^n} - X$ tem p^n zeros distintos em $\overline{\mathbb{Z}}_p$. $\square$

Corolário 4.39. *Se F é qualquer corpo finito, então, para todo inteiro positivo n , existe um polinômio irredutível em $F[X]$ de grau n .*

Demonstração. Seja F com $q = p^r$ elementos, onde p é a característica de F . Pelo teorema 4.38, existe um corpo $K \subset \overline{F}$ contendo $\overline{\mathbb{Z}}_p$ (a menos de isomorfismo) e consistindo precisamente dos zeros de $X^{p^{rn}} - X$. Queremos mostrar que $F \subset K$. Todo elemento de F é um zero de $X^{p^r} - X$, pelo teorema 4.34. Agora $p^{rs} = p^r \cdot p^{r(s-1)}$. Aplicando esta equação repetidamente aos expoentes e usando o fato de que para $\alpha \in F$ temos $\alpha^{p^r} = \alpha$, vemos que para $\alpha \in F$,

$$\alpha^{p^{rn}} = \alpha^{p^{r(n-1)}} = \alpha^{p^{r(n-2)}} = \dots = \alpha^{p^r} = \alpha.$$

Assim $F \subset K$. Então, o teorema 4.32 mostra que devemos ter $[K : F] = n$. Vimos que a extensão K é simples sobre F no corolário 4.37, então, $K = F(\beta)$ para algum $\beta \in K$. Portanto, $\text{irr}(\beta, F)$ necessariamente tem grau n . $\square$

Por fim, o próximo resultado garante que, para cada número primo p , existe um único corpo de Galois, de ordem p^n , a menos de isomorfismo.

Teorema 4.40. *Sejam p um primo e $n \in \mathbb{Z}^+$. Se E e E' são corpos de ordem p^n , então $E \simeq E'$.*

Demonstração. Vide resultado 33.12, página 304, da referência [6]. □

4.3 O grupo de automorfismos $G(E/F)$

Definição 4.41. Seja E uma extensão algébrica de um corpo F . Dois elementos $\alpha, \beta \in E$ são **conjugados sobre F** se $\text{irr}(\alpha, F) = \text{irr}(\beta, F)$, isto é, se α e β são zeros do mesmo polinômio irredutível sobre F .

O conceito de elementos conjugados que acabamos de definir está de acordo com a ideia clássica dos *números complexos conjugados*, pois se entendermos que por números complexos conjugados entendemos números que são *conjugados sobre $\mathbb{R}$* . Se $a, b \in \mathbb{R}$ e $b \neq 0$, os números complexos conjugados $a+bi$ e $a-bi$ são ambos zeros de $X^2 - 2aX + a^2 + b^2$, que é irredutível sobre $\mathbb{R}$.

O próximo teorema estabelece uma relação interessante sobre a definição de elementos conjugados e um isomorfismo, que é chamado de isomorfismo de conjugação.

Teorema 4.42. *Sejam F um corpo, α e β elementos algébricos sobre F em que $\deg(\alpha, F) = n$. A aplicação $\psi_{\alpha, \beta} : F(\alpha) \rightarrow F(\beta)$ definida por*

$$\psi_{\alpha, \beta}(c_0 + c_1 \cdot \alpha + \dots + c_{n-1} \cdot \alpha^{n-1}) = c_0 + c_1 \cdot \beta + \dots + c_{n-1} \cdot \beta^{n-1}$$

para $c_i \in F, i \in \{0, \dots, n-1\}$, é um isomorfismo de $F(\alpha)$ sobre $F(\beta)$ se, e somente se, α e β são conjugados sobre F .

Demonstração. Suponha que $\psi_{\alpha, \beta} : F(\alpha) \rightarrow F(\beta)$ conforme definido no enunciado do teorema é um isomorfismo. Seja $\text{irr}(\alpha, F) = a_0 + a_1 \cdot X + \dots + a_n \cdot X^n$. Então $a_0 + a_1 \cdot \alpha + \dots + a_n \cdot \alpha^n = 0$, assim

$$\psi_{\alpha, \beta}(a_0 + a_1 \cdot \alpha + \dots + a_n \cdot \alpha^n) = a_0 + a_1 \cdot \beta + \dots + a_n \cdot \beta^n = 0.$$

Pela afirmação do teorema 4.12, isso implica que $\text{irr}(\beta, F)$ divide $\text{irr}(\alpha, F)$. Um argumento semelhante usando o isomorfismo $(\psi_{\alpha, \beta})^{-1} = \psi_{\beta, \alpha}$ mostra que $\text{irr}(\alpha, F)$ divide $\text{irr}(\beta, F)$. Portanto, como ambos os polinômios são mônicos, $\text{irr}(\alpha, F) = \text{irr}(\beta, F)$, então α e β são conjugados sobre F .

Reciprocamente, suponha que $\text{irr}(\alpha, F) = \text{irr}(\beta, F) = p(X)$. Então os homomorfismos de valoração $\phi_\alpha : F[X] \rightarrow F(\alpha)$ e $\psi_\beta : F[X] \rightarrow F(\beta)$ têm ambos o mesmo núcleo $\langle p(X) \rangle$. Já vimos que para $\phi_\alpha : F[X] \rightarrow F(\alpha)$, existe um homomorfismo natural ψ_α aplicando $\frac{F[X]}{\langle p(X) \rangle}$ em $\phi_\alpha[F[X]] = F(\alpha)$. Da mesma forma, ϕ_β dá origem a um isomorfismo ψ_β aplicando $\frac{F[X]}{\langle p(X) \rangle}$ em $F(\beta)$. Seja $\psi_{\alpha, \beta} = \psi_\beta(\psi_\alpha)^{-1}$. A composição de dois isomorfismos, $\psi_{\alpha, \beta}$ é novamente um isomorfismo da aplicação $F(\alpha)$ em $F(\beta)$. Para $(c_0 + c_1 \cdot \alpha + \dots + c_{n-1} \cdot \alpha^{n-1}) \in F(\alpha)$, temos que

$$\begin{aligned} \psi_{\alpha, \beta}(c_0 + c_1 \cdot \alpha + \dots + c_{n-1} \cdot \alpha^{n-1}) &= (\psi_\beta \cdot \psi_\alpha)^{-1} \cdot (c_0 + c_1 \cdot \alpha + \dots + c_{n-1} \cdot \alpha^{n-1}) = \\ &= \psi_\beta((c_0 + c_1 \cdot x + \dots + c_{n-1} \cdot x^{n-1}) + \langle p(X) \rangle) = c_0 + c_1 \cdot \beta + \dots + c_{n-1} \cdot \beta^{n-1}. \end{aligned}$$

Assim, $\psi_{\alpha, \beta}$ é a aplicação definida no enunciado do teorema. $\square$

Corolário 4.43. *Seja α algébrico sobre um corpo F . Todo isomorfismo ψ de $F(\alpha)$ em um subcorpo de $\overline{F}$ tal que $\psi(a) = a$ para $a \in F$ aplica α em um conjugado β de α sobre F . Reciprocamente, para cada conjugado β de α sobre F , existe exatamente um isomorfismo $\psi_{\alpha, \beta}$ de $F(\alpha)$ sobre um subcorpo de $\overline{F}$ aplicando em α em β e aplicando cada $a \in F$ sobre si mesmo.*

Exemplo 4.44. Considere $\mathbb{Q}(\sqrt{2})$ sobre $\mathbb{Q}$. Os zeros de $\text{irr}(\sqrt{2}, \mathbb{Q}) = X^2 - 2$ são $\sqrt{2}$ e $-\sqrt{2}$, então $\sqrt{2}$ e $-\sqrt{2}$ são conjugados sobre $\mathbb{Q}$. De acordo com o teorema 4.42 a aplicação $\psi_{\sqrt{2}, -\sqrt{2}} : \mathbb{Q}(\sqrt{2}) \rightarrow \mathbb{Q}(\sqrt{2})$ definida por

$$\psi_{\sqrt{2}, -\sqrt{2}}(a + b\sqrt{2}) = a - b\sqrt{2}$$

é um isomorfismo de $\mathbb{Q}(\sqrt{2})$ sobre si mesmo.

Definição 4.45. Dizemos que um isomorfismo de um corpo sobre si mesmo é um **automorfismo do corpo**.

Definição 4.46. Se σ é um isomorfismo de um corpo E sobre algum corpo, então um elemento a de E é **fixo por** σ se $\sigma(a) = a$. Uma coleção S de isomorfismos de E **deixa um subcorpo** F de E **fixo** se cada $a \in F$ é fixo para todo $\sigma \in S$. Se $\{\sigma\}$ fixa F , então dizemos que σ **deixa** F **fixo**.

Exemplo 4.47. Seja $E = \mathbb{Q}(\sqrt{2}, \sqrt{3})$. A aplicação $\sigma : E \rightarrow E$ definida por

$$\sigma(a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6}) = a + b\sqrt{2} - c\sqrt{3} - d\sqrt{6}$$

para $a, b, c, d \in \mathbb{Q}$ é um automorfismo de E e é o isomorfismo do conjugado de $\psi_{\sqrt{3}, -\sqrt{3}}$ de E sobre si mesmo se vemos E como $(\mathbb{Q}(\sqrt{2}))(\sqrt{3})$. Vemos que σ deixa $\mathbb{Q}(\sqrt{2})$ fixo.

Teorema 4.48. *Seja $\{\sigma_i \mid i \in I\}$ uma coleção de automorfismos de um corpo E , em que I é um conjunto de índices qualquer. Então o conjunto $E_{\{\sigma_i\}}$ de todos os $a \in E$ deixados fixos para todos σ_i para $i \in I$ formam um subcorpo de E .*

Demonstração. Se $\sigma_i(a) = a$ e $\sigma_i(b)$ para todo $i \in I$, então

$$\sigma_i(a \pm b) = \sigma_i(a) \pm \sigma_i(b) = a \pm b$$

e

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

para todo $i \in I$. Também, se $b \neq 0$, então

$$\sigma_i\left(\frac{a}{b}\right) = \frac{\sigma_i(a)}{\sigma_i(b)} = \frac{a}{b}$$

para todo $i \in I$. Como os σ_i são automorfismos, temos

$$\sigma_i(0) = 0 \text{ e } \sigma_i(1) = 1$$

para todo $i \in I$. Por isso, $0, 1 \in E_{\{\sigma_i\}}$. Assim, $E_{\{\sigma_i\}}$ é um subcorpo de E . □

Definição 4.49. O corpo $E_{\{\sigma_i\}}$ do teorema 4.48 é chamado **o corpo fixo de $\{\sigma_i \mid i \in I\}$** . Para um único automorfismo σ , nos referimos a ele como $E_{\{\sigma\}}$ o **corpo fixo de σ** .

Considere o automorfismo $\psi_{\sqrt{2}, -\sqrt{2}}$ de $\mathbb{Q}(\sqrt{2})$ assim como citado anteriormente. Para $a, b \in \mathbb{Q}$, temos

$$\psi_{\sqrt{2}, -\sqrt{2}}(a + b\sqrt{2}) = a - b\sqrt{2},$$

e $a - b\sqrt{2} = a + b\sqrt{2}$ se, e somente se $b = 0$. Assim, o corpo fixo $\psi_{\sqrt{2}, -\sqrt{2}}$ é $\mathbb{Q}$.

Teorema 4.50. *O conjunto de todos os automorfismos de um corpo E é um grupo sob composição de funções.*

Demonstração. A multiplicação de automorfismos de E é definida pela composição de função e, portanto, é associativa (é uma *multiplicação de permutação*). A permutação de identidade $i : E \rightarrow E$ dada por $i(\alpha) = \alpha$ para $\alpha \in E$ é um automorfismo de E . Se σ é um automorfismo, então a permutação σ^{-1} também é um automorfismo. Assim, todos os automorfismos de E formam um subgrupo de S_E , do grupo de permutações de E . $\square$

Teorema 4.51. *Sejam E um corpo e F um subcorpo de E . Então, o conjunto $G(E/F)$ de todos os automorfismos de E deixando F fixo, com a operação de composição, forma um subgrupo do grupo de todos os automorfismos de E . Além disso, $F \subset E_{G(E/F)}$.*

Demonstração. Para $\sigma, \tau \in G(E/F)$ e $a \in F$, temos

$$(\sigma\tau)(a) = \sigma(\tau(a)) = \sigma(a) = a,$$

então $\sigma\tau \in G(E/F)$. Assim, o automorfismo de identidade i está em $G(E/F)$. Além disso, se $\sigma(a) = a$ para $a \in F$, então $a = \sigma^{-1}(a)$ para $\sigma \in G(E/F)$ implica que $\sigma^{-1} \in G(E/F)$. Logo, $G(E/F)$ é um subgrupo do grupo de todos os automorfismos de E .

Como todo elemento de F é fixo por todo elemento de $G(E/F)$, segue-se que o corpo $E_{G(E/F)}$ para *todo* elemento de E deixado fixo por $G(E/F)$ contém F . $\square$

Definição 4.52. O grupo $G(E/F)$ do teorema 4.51 é o **grupo de automorfismos de E deixando F fixo**, ou, mais brevemente, o **grupo de E sobre F** .

Exemplo 4.53. Considere o corpo $\mathbb{Q}(\sqrt{2}, \sqrt{3})$. No exemplo 4.27, mostramos que $[\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}] = 4$. Se visualizarmos $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ como $(\mathbb{Q}(\sqrt{3}))(\sqrt{2})$, o isomorfismo de conjugação $\psi_{\sqrt{2}, -\sqrt{2}}$ do teorema 4.42 definido por

$$\psi_{\sqrt{2}, -\sqrt{2}}(a + b\sqrt{2}) = a - b\sqrt{2}$$

para $a, b \in \mathbb{Q}(\sqrt{3})$ é um automorfismo de $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ tendo $\mathbb{Q}(\sqrt{3})$ como corpo fixo. Similarmente, temos o automorfismo $\psi_{\sqrt{3}, -\sqrt{3}}$ de $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ tendo $\mathbb{Q}(\sqrt{2})$ como corpo fixo. Como o produto de dois automorfismos é um automorfismo, podemos considerar $\psi_{\sqrt{2}, -\sqrt{2}}\psi_{\sqrt{3}, -\sqrt{3}}$ que move tanto $\sqrt{2}$ e $\sqrt{3}$, ou seja, não deixa nenhum número fixo. Consideremos:

i = automorfismo identidade,

$$\sigma_1 = \psi_{\sqrt{2}, -\sqrt{2}},$$

$$\sigma_2 = \psi_{\sqrt{3}, -\sqrt{3}}, \text{ e}$$

$$\sigma_3 = \psi_{\sqrt{2}, -\sqrt{2}}\psi_{\sqrt{3}, -\sqrt{3}}.$$

O grupo de todos os automorfismos de $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ tem um corpo fixo pelo teorema 4.48. Este corpo fixo deve conter $\mathbb{Q}$, já que todo automorfismo de um corpo deixa 1 e, portanto, o subcorpo principal fixo. Uma base para $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ sobre $\mathbb{Q}$ é $\{1, \sqrt{2}, \sqrt{3}, \sqrt{6}\}$. Como $\sigma_1(\sqrt{2}) = -\sqrt{2}$, $\sigma_1(\sqrt{6}) = -\sqrt{6}$ e $\sigma_2(\sqrt{3}) = -\sqrt{3}$, vemos que $\mathbb{Q}$ é exatamente o corpo fixo de $\{i, \sigma_1, \sigma_2, \sigma_3\}$. É possível verificar que $G = \{i, \sigma_1, \sigma_2, \sigma_3\}$ é um grupo sob multiplicação de automorfismo (composição de funções). A tabela para o grupo G é fornecida abaixo.

	i	σ_1	σ_2	σ_3
i	i	σ_1	σ_2	σ_3
σ_1	σ_1	i	σ_3	σ_2
σ_2	σ_2	σ_3	i	σ_1
σ_3	σ_3	σ_2	σ_1	i

Por exemplo,

$$\sigma_1\sigma_3 = \psi_{\sqrt{2}, -\sqrt{2}}(\psi_{\sqrt{2}, -\sqrt{2}}\psi_{\sqrt{3}, -\sqrt{3}}) = \psi_{\sqrt{2}, -\sqrt{3}} = \sigma_2.$$

Podemos mostrar que G é na verdade é o grupo $G(\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q})$, porque todo automorfismo τ de $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ implica $\sqrt{2}$ em qualquer um dos $\pm\sqrt{2}$, pelo corolário 4.43. Da mesma forma, τ implica $\sqrt{3}$ em $\pm\sqrt{3}$. Mas, como $\{1, \sqrt{2}, \sqrt{3}, \sqrt{2}\sqrt{3}\}$ é uma base para $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ sobre $\mathbb{Q}$, um automorfismo de $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ deixando $\mathbb{Q}$ fixo é determinado por seus valores em $\sqrt{2}$ e $\sqrt{3}$. Agora, i, σ_1, σ_2 , e σ_3 fornecem todas as combinações possíveis de valores em $\sqrt{2}$ e $\sqrt{3}$ e, portanto, são todos os automorfismos possíveis de $\mathbb{Q}(\sqrt{2}, \sqrt{3})$.

Corolário 4.54. *Sejam $\overline{F}$ e $\overline{F'}$ dois fechos algébricos de F . Então $\overline{F}$ é isomorfo a $\overline{F'}$ sob um isomorfismo deixando cada elemento de F fixo.*

Demonstração. Pelo teorema 4.55, o isomorfismo de identidade de F sobre F pode ser estendido para um isomorfismo τ que aplica $\overline{F}$ em um subcorpo de $\overline{F'}$ que deixa F fixo. Precisamos mostrar que τ está em $\overline{F'}$. Mas pelo teorema 4.55, a aplicação $\tau^{-1} : \tau[F] \rightarrow \overline{F}$ pode ser estendida para um isomorfismo de $\overline{F'}$ sobre um subcorpo de $\overline{F}$. Como τ^{-1} já está em $\overline{F}$, devemos ter $\tau[\overline{F}] = \overline{F'}$. $\square$

Teorema 4.55. (Teorema da Extensão do Isomorfismo) *Seja E uma extensão algébrica de um corpo F . Seja σ um isomorfismo de F sobre um corpo F' . Seja $\overline{F'}$ um fecho algébrico de F' . Então, σ pode ser estendido a um isomorfismo τ de E em um subcorpo de $\overline{F'}$ tal que $\tau(a) = \sigma(a)$ para todo $a \in F$.*

Demonstração. Considere todos os pares (L, λ) , onde L é um corpo tal que $F \leq L \leq E$ e λ é um isomorfismo de L sobre o subcorpo de $\overline{F'}$ tal que $\lambda(a) = \sigma(a)$ para $a \in F$. O conjunto S tal que os pares (L, λ) não são vazios, pois (F, σ) é tal par. Defina uma ordenação parcial em S por $(L_1, \lambda_1) \leq (L_2, \lambda_2)$, se $L_1 \leq L_2$ e $\lambda_1(a) = \lambda_2(a)$ para $a \in L_1$. É possível verificar que a relação $\leq$ fornece uma ordenação parcial de S .

Seja $T = \{(H_i, \lambda_i) \mid i \in I\}$ uma cadeia de S . Afirmamos que $H = \cup_{i \in I} H_i$ é um subcorpo de E . Seja $a, b \in H$, onde $a \in H_1$ e $b \in H_2$; então ou $H_1 \leq H_2$ ou $H_2 \leq H_1$, uma vez que T é uma cadeia. Se, digamos, $H_1 \leq H_2$, então $a, b \in H_2$, então $a \pm b, ab$, e a/b para $b \neq 0$ estão todos em H_2 , e portanto, em H . Como para cada $i \in I, F \subseteq H_i \subseteq E$, temos que $F \subseteq H \subseteq E$. Assim, H é um subcorpo de E .

Defina $\lambda : H \rightarrow \overline{F'}$ como segue. Seja $c \in H_i$ para algum $i \in I$, e seja

$$\lambda(c) = \lambda_i(c).$$

A aplicação λ está bem definida porque se $c \in H_1$ e $c \in H_2$, então $(H_1, \lambda_1) \leq (H_2, \lambda_2)$ ou $(H_2, \lambda_2) \leq (H_1, \lambda_1)$, já que T é uma cadeia. Em ambos os casos, $\lambda_1(c) = \lambda_2(c)$. Afirmamos que λ é um isomorfismo de H em um subcorpo de $\overline{F'}$. Se $a, b \in H$ então existe um H_i tal que $a, b \in H_i$, e

$$\lambda(a + b) = \lambda_i(a + b) = \lambda_i(a) + \lambda_i(b) = \lambda(a) + \lambda(b).$$

Similarmente,

$$\lambda(ab) = \lambda_i(ab) = \lambda_i(a)\lambda_i(b) = \lambda(a)\lambda(b).$$

Se $\lambda(a) = 0$, então $a \in H_i$ para algum i , implica que $\lambda_i(a) = 0$, então $a = 0$. Portanto, λ é um isomorfismo. Assim $(H, \lambda) \in S$, e fica perceptível de nossas definições de H e λ que (H, λ) é um limite superior para T .

Mostramos que toda cadeia de S tem um limite superior em S , portanto as hipóteses do lema de Zorn's são satisfeitas. Logo, existe um elemento máximo (K, τ) de S . Seja $\tau(K) = K'$, onde $K' \leq \overline{F'}$. Agora, se $K \neq E$, seja $\alpha \in E$ mas $\alpha \notin K$. Agora α é algébrico

sobre F , então α é algébrico sobre K . Além disso, seja $p(X) = irr(\alpha, K)$. Seja ψ_α o isomorfismo canônico

$$\psi_\alpha : K[X]/\langle p(X) \rangle \rightarrow K(\alpha),$$

correspondendo ao homomorfismo de valoração $\phi_\alpha : K[X] \rightarrow K(\alpha)$. Se

$$p(X) = a_0 + a_1X + \dots + a_nX^n,$$

considerando

$$q(X) = \tau(a_0) + \tau(a_1)X + \dots + \tau(a_n)X^n$$

em $K'[X]$. Como τ é um isomorfismo, $q(X)$ é irredutível em $K'[X]$. Seja $K' \leq F'$, existe um zero α' de $q(X)$ em $\overline{F'}$. Então

$$\psi'_\alpha : K'[X]/\langle q(X) \rangle \rightarrow K'(\alpha')$$

um isomorfismo análogo à ψ_α . Vejamos que

$$\bar{\tau} : K[X]/\langle p(X) \rangle \rightarrow K'[X]/\langle q(X) \rangle$$

seja o isomorfismo estendendo τ em K e aplicando $X + \langle p(X) \rangle$ em $X + \langle q(X) \rangle$. Vejamos

$$\begin{array}{ccccccc}
 & & K[x] & \xrightarrow{\tau_x} & K'[x] & & \\
 & \nearrow \gamma \text{ canônico} & \downarrow & & \downarrow & \nwarrow \gamma' \text{ canônico} & \\
 & & K & \xrightarrow{\tau} & K' & & \\
 K(\alpha) & \xleftarrow{\psi_\alpha} & K[x]/\langle p(x) \rangle & \xrightarrow[\bar{\tau} = \gamma' \tau_x \gamma^{-1}]{\bar{\tau}} & K'[x]/\langle p(x) \rangle & \xrightarrow{\psi_{\alpha'}} & K'(\alpha')
 \end{array} \tag{4.1}$$

Em seguida, a composição das aplicações

$$\psi_{\alpha'} \tau \psi_\alpha^{-1} : K(\alpha) \rightarrow K'(\alpha')$$

é um isomorfismo de $K(\alpha)$ em um subcorpo de $\overline{F'}$.

Podemos perceber que $(K, \tau) < (K(\alpha), \psi_{\alpha'} \tau \psi_\alpha^{-1})$, o que contradiz que (K, τ) é máximo. Portanto temos que $K = E$.

□

Corolário 4.56. *Seja $E \subset \overline{F}$ uma extensão algébrica de F e $\alpha, \beta \in E$ são conjugados sobre F , então o isomorfismo de conjugação $\psi_{\alpha, \beta} : F(\alpha) \rightarrow F(\beta)$, dado pelo teorema 4.42, pode ser estendido a um isomorfismo de E sobre um subcorpo de $\overline{F}$.*

Demonstração. A prova deste corolário vem do teorema 4.55, se nas hipóteses do teorema substituímos F por $F(\alpha)$, F' por $F(\beta)$ e $\overline{F'}$ por $\overline{F}$. $\square$

Teorema 4.57. *Seja E uma extensão finita de um corpo F . Se σ é um isomorfismo de F sobre um corpo F' e se $\overline{F'}$ é o fecho algébrico de F' . Então, o número de extensões de σ para um isomorfismo τ de E em um subcorpo de $\overline{F'}$ é finito e independente de F' , $\overline{F'}$, e σ . Ou seja, o número de extensões é totalmente determinado pelos dois corpos E e F ; é intrínseco a eles.*

Demonstração. Para ver a demonstração desse teorema, consultar Fraleigh [6], p. 427, teorema 49.7. $\square$

Definição 4.58. *Seja E uma extensão finita de um corpo F . O número de isomorfismos de E sobre um subcorpo de $\overline{F'}$, que deixa F fixo, é chamado o **índice** $\{E : F\}$ de E sobre F .*

Corolário 4.59. *Se $F \leq E \leq K$, onde K é uma extensão finita do corpo F , então $\{K : F\} = \{K : E\}\{E : F\}$.*

Demonstração. Segue do teorema 4.57 que cada um dos $\{E : F\}$ isomorfismos τ_i de E sobre um subcorpo de $\overline{F}$ deixando F fixo tem $\{K : E\}$ extensões para um isomorfismo de K em um subcorpo de $\overline{F}$. $\square$

Exemplo 4.60. Considere $E = \mathbb{Q}(\sqrt{2}, \sqrt{3})$ sobre $\mathbb{Q}$. Veja que podemos mostrar que $\{E : \mathbb{Q}\} = [E : \mathbb{Q}] = 4$. Além disso, $\{E : \mathbb{Q}(\sqrt{2})\} = 2$ e $\{\mathbb{Q}(\sqrt{2}) : \mathbb{Q}\} = 2$ então

$$4 = \{E : \mathbb{Q}\} = \{E : \mathbb{Q}(\sqrt{2})\}\{\mathbb{Q}(\sqrt{2}) : \mathbb{Q}\} = (2)(2).$$

Isso ilustra o corolário 4.59.

4.4 *Splitting* corpo, extensão separável e o grupo de Galois $G(K/F)$

Um dos objetivos deste capítulo é determinar em quais condições tem-se:

$$|G(E/F)| = \{E : F\} = [E : F],$$

em que E é um extensão finita de um corpo F .

Para tanto, faz-se necessário a abordagem sobre *splitting* corpo e extensão separável.

Definição 4.61. Seja F um corpo com fecho algébrico $\overline{F}$. Seja $\{f_i(X) \mid i \in I\}$ uma coleção de polinômios em $F[X]$. Um corpo $E \subset \overline{F}$ é o ***splitting* corpo de $\{f_i(X) \mid i \in I\}$ sobre F** se E é o menor subcorpo de $\overline{F}$ contendo F e todos os zeros em $\overline{F}$ de cada um dos $f_i(X)$ para $i \in I$. Um corpo $K \subset \overline{F}$ é um ***splitting* corpo sobre F** se for o *splitting* corpo de algum conjunto de polinômios em $F[X]$.

Exemplo 4.62. Vemos que $\mathbb{Q}[(\sqrt{2}, \sqrt{3})]$ é um *splitting* corpo de $\{X^2 - 2, X^2 - 3\}$ e também de $\{X^4 - 5X^2 + 6\}$.

Observação 4.63. No que segue, dado um polinômio $f(X) \in F[X]$, qualquer, referimos ao *splitting* corpo de $\{f(X)\}$ sobre F como, simplesmente, o *splitting* corpo de $f(X)$ sobre F .

Veja que o ***splitting* corpo de $\{f_i(X) \mid i \in I\}$ sobre F** em $\overline{F}$ é a interseção de todos os subcorpos de $\overline{F}$ contendo F e todos os zeros em $\overline{F}$ de cada $f_i(X), i \in I$, portanto, podemos afirmar que tal *splitting* corpo sempre existe.

Teorema 4.64. Dado F um corpo intermediário E , onde $F \subset E \subset \overline{F}$. Então E é um *splitting* corpo sobre F se, e somente se, todo automorfismo de $\overline{F}$ deixando F fixo, aplica E sobre si mesmo e, portanto, induz um automorfismo de E deixando F fixo.

Demonstração. Seja E um *splitting* corpo sobre F em $\overline{F}$ de $\{f_i(X) \mid i \in I\}$, e seja σ um automorfismo de $\overline{F}$ que deixa F fixo. Seja $\{\alpha_j \mid j \in J\}$ o conjunto de todos os zeros em $\overline{F}$ de todos os $f_i(X)$ para $i \in I$. Vejamos que para um α_j fixo, o corpo $F(\alpha_j)$ tem como elementos todas as expressões da forma

$$g(\alpha_j) = a_0 + a_1\alpha_j + \dots + a_{n_j-1}\alpha_j^{n_j-1},$$

onde n_j é o grau de $\text{irr}(\alpha_j, F)$ e $a_k \in F$. Considere o conjunto de todas as somas *finitas* de produtos *finitos* de elementos da forma $g(\alpha_j)$ para todo $j \in J$. O conjunto S é um subconjunto de E fechado para a adição e a multiplicação e contendo 0, 1, e o inverso aditivo de cada elemento. Cada elemento de S está em algum $F(\alpha_{j_1}, \dots, \alpha_{j_n}) \subseteq S$,

podemos ver que S também contém o inverso multiplicativo de cada elemento diferente de zero. Assim S é um subcorpo de E contendo todos os α_j para $j \in J$. Pela definição de *splitting* corpo de E de $\{f_i(X) \mid i \in I\}$, vemos que $S = E$. Com isso, mostramos que $\{\alpha_j \mid j \in J\}$ gera E sobre F , no sentido de tomar somas *finitas* e produtos *finitos*. Sabendo disso, podemos ver que o valor de σ em qualquer elemento de E é completamente determinado pelos valores $\sigma(\alpha_j)$. Pelo corolário 4.43, $\sigma(\alpha_j)$ também deve ser um zero de $\text{irr}(\alpha_j, F)$. Pelo teorema 4.12, $\text{irr}(\alpha_j, F)$ divide $f_i(X)$ para qual $f_i(\alpha_j) = 0$, então $\sigma(\alpha_j) \in E$ também. Assim, σ aplica E em um subcorpo de E isomorficamente. No entanto, o mesmo é verdade para um automorfismo σ^{-1} de $\overline{F}$. Como $B \in E$,

$$\beta = \sigma(\sigma^{-1}(\beta)),$$

podemos ver que σ aplica E em E e, portanto, induz um automorfismo de E .

Suponha, inversamente, que todo automorfismo de $\overline{F}$ deixando F fixo induz um automorfismo de E . Seja $g(X)$ um polinômio irreduzível em $F[X]$ tendo α zero em E . Se β é qualquer zero de $g(X)$ em $\overline{F}$, então pelo teorema 4.42, existe um isomorfismo de conjugação $\psi_{\alpha, \beta}$ de $F(\alpha)$ sobre $F(\beta)$ deixando F fixo. Pelo teorema 4.55, $\psi_{\alpha, \beta}$ pode ser estendido para um isomorfismo τ de $\overline{F}$ sobre um subcorpo de $\overline{F}$. Mas então

$$\tau^{-1} : \tau[\overline{F}] \rightarrow \overline{F}$$

pode ser estendido a um isomorfismo que aplica $\overline{F}$ sobre um subcorpo de $\overline{F}$. Como a imagem de τ^{-1} já é toda em $\overline{F}$, temos que τ está em $\overline{F}$, então τ é um automorfismo de $\overline{F}$ que deixa F fixo. Então, por suposição, τ induz um automorfismo de E , então $\tau(\alpha) = \beta$ está em E . Mostramos que se $g(X)$ é um polinômio irreduzível em $F[X]$ tendo um zero em E , então todos os zeros de $g(X)$ em $\overline{F}$ estão em E . Portanto, se $\{g_k(X)\}$ é o conjunto de todos os polinômios irreduzíveis em $F[X]$ tendo um zero em E , então E é um *splitting* corpo de $\{g_k(X)\}$.

□

Definição 4.65. Seja E uma extensão de um corpo F . Um polinômio $f(X) \in F[X]$ **divide em E** se $f(X)$ pode ser fatorado em um produto de fatores lineares em $E[X]$.

Exemplo 4.66. O polinômio $X^4 - 5X^2 + 6$ em $\mathbb{Q}[X]$ se divide no corpo $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ em $(X - \sqrt{2})(X + \sqrt{2})(X - \sqrt{3})(X + \sqrt{3})$.

Corolário 4.67. *Dado F um corpo, se $E \subset \overline{F}$ é um *splitting* corpo sobre F , então, todo polinômio irredutível em $F[X]$ tendo um zero em E se divide em E .*

Demonstração. Se E é um *splitting* corpo sobre F em $\overline{F}$, então todo automorfismo de $\overline{F}$ induz um automorfismo de E . A segunda metade da prova do teorema 4.64 mostra que E também é o *splitting* corpo sobre F do conjunto $\{g_k(X)\}$ de todos os polinômios irredutíveis em $F[X]$ tendo um zero em E . Assim, um polinômio irredutível $f(X)$ de $F[X]$ tendo um zero em E tem todos os seus zeros em $\overline{F}$ em E . Portanto, sua fatoração em fatores lineares em $\overline{F}[X]$, dados pela proposição 4.31, na verdade ocorrem em $E[X]$, então $f(X)$ divide em E . $\square$

Corolário 4.68. *Dado F um corpo, se $E \subset \overline{F}$ é um *splitting* corpo sobre F , então toda aplicação isomorfa de E em um subcorpo de $\overline{F}$ e deixando F fixo é na verdade um automorfismo de E . Em particular, se E é um *splitting* corpo de grau finito sobre F , então*

$$\{E : F\} = |G(E/F)|.$$

Demonstração. Todo isomorfismo σ que aplica E sobre um subcorpo de $\overline{F}$ deixando F fixo, pode ser estendido a um automorfismo τ de $\overline{F}$, pelo teorema 4.55, juntamente com o argumento para a segunda metade da prova do teorema 4.64. Se E é um *splitting* corpo sobre F , então, pelo teorema 4.64, τ restrito a E , isto é σ , é um automorfismo de E . Assim, para um *splitting* corpo de E sobre F , toda aplicação isomorfa de E sobre um subcorpo de $\overline{F}$ deixando F fixo é um automorfismo de E .

A equação $\{E : F\} = |G(E/F)|$ segue para um *splitting* corpo de E de grau finito sobre F , uma vez que $\{E : F\}$ foi definido como o número de diferentes aplicações isomorfas de E sobre um subcorpo de $\overline{F}$ deixando F fixo. $\square$

Exemplo 4.69. Observe que $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ é um *splitting* corpo de

$$\{X^2 - 2, X^2 - 3\}$$

sobre $\mathbb{Q}$. Vimos que as aplicações i, σ_1, σ_2 , e σ_3 são todos os automorfismos de $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ deixando $\mathbb{Q}$ fixo. (Na verdade, como todo automorfismo de um corpo deve deixar o subcorpo primo fixo, vemos que esses são os únicos automorfismos de $\mathbb{Q}(\sqrt{2}, \sqrt{3})$.) Então

$$\{\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}\} = 4 = |G(\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q})|.$$

ilustrando o corolário 4.68.

Agora daremos início ao conceito de extensão separável, para tanto faz-se necessário a definição de multiplicidade.

Definição 4.70. Seja $f(X) \in F[X]$. Um elemento α de $\overline{F}$ tal que $f(\alpha) = 0$ é um **zero de $f(X)$ de multiplicidade ν** se ν é o maior inteiro tal que $(X - \alpha)^\nu$ é um fator de $f(X)$ em $\overline{F}[X]$.

Teorema 4.71. *Seja $f(X)$ irredutível sobre $F[X]$. Então todos os zeros de $f(X)$ em $\overline{F}$ têm a mesma multiplicidade.*

Demonstração. Sejam α e β zeros de $f(X)$ em $\overline{F}$. Então, pelo teorema 4.42, existe um isomorfismo de conjugação $\psi_{\alpha,\beta} : F(\alpha) \rightarrow F(\beta)$. Pelo corolário 4.56, $\psi_{\alpha,\beta}$ pode ser estendido a um isomorfismo $\tau : \overline{F} \rightarrow \overline{F}$. Logo, τ induz um isomorfismo natural $\tau_X : \overline{F}[X] \rightarrow \overline{F}[X]$, com $\tau_X(X) = X$. Agora τ_X deixa $f(X)$ fixo, já que $f(X) \in F[X]$ e $\psi_{\alpha,\beta}$ deixa F fixo. No entanto,

$$\tau_X((X - \alpha)^\nu) = (X - \beta)^\nu,$$

o que mostra que a multiplicidade de β em $f(X)$ é maior ou igual à multiplicidade de α . Um argumento simétrico fornece a desigualdade inversa, então a multiplicidade de α é igual a de β . $\square$

Corolário 4.72. *Se $f(X)$ é irredutível em $F[X]$, então $f(x)$ tem uma fatoração em $F[X]$ da forma*

$$a \prod_{i \in I} (X - \alpha_i)^\nu,$$

onde os α_i são os zeros distintos de $f(X)$ em $\overline{F}$, $a \in F$ e I é um conjunto de índices.

Teorema 4.73. *Se E é uma extensão finita de F , então $\{E : F\}$ divide $[E : F]$.*

Demonstração. Pelo teorema 4.28, se E é espaço vetorial finito sobre F , então $E = F(\alpha_1, \dots, \alpha_n)$, onde $\alpha_i \in \overline{F}$. Digamos que $\text{irr}(\alpha_i, F(\alpha_1, \dots, \alpha_{i-1}))$ têm α_i como um dos n_i zeros distintos, os quais têm multiplicidade comum v_i , pelo teorema 4.71. Então

$$[F(\alpha_1, \dots, \alpha_i) : F(\alpha_1, \dots, \alpha_{i-1})] = n_i v_i = \{F(\alpha_1, \dots, \alpha_i) : F(\alpha_1, \dots, \alpha_{i-1})\} v_i.$$

Pelo teorema 4.23 e o corolário 4.59,

$$[E : F] = \prod_i n_i v_i,$$

e

$$\{E : F\} = \prod_i n_i.$$

Portanto, $\{E : F\}$ divide $[E : F]$. □

Definição 4.74. Uma extensão finita E de F é uma **extensão separável de F** se $\{E : F\} = [E : F]$. Um elemento α de $\overline{F}$ é **separável sobre F** se $F(\alpha)$ é uma extensão separável sobre F . Um polinômio irreduzível $f(X) \in F[X]$ é **separável sobre F** se todo zero de $f(X)$ em $\overline{F}$ é separável sobre F .

Exemplo 4.75. O corpo $E = \mathbb{Q}[(\sqrt{2}, \sqrt{3})]$ é separável sobre $\mathbb{Q}$, pois já vimos que:

$$\{E : \mathbb{Q}\} = 4 = [E : \mathbb{Q}].$$

Teorema 4.76. Se K é uma extensão finita de E e E é uma extensão finita de F , isto é, $F \leq E \leq K$, então K é separável sobre F se, e somente se, K é separável sobre E e E é separável sobre F .

Demonstração. Já temos que:

$$[K : F] = [K : E][E : F],$$

e

$$\{K : F\} = \{K : E\}\{E : F\}.$$

Então se K é separável sobre F , de modo que $[K : F] = \{K : F\}$, devemos ter $[K : E] = \{K : E\}$ e $[E : F] = \{E : F\}$, já que em cada caso o índice divide o grau, pelo teorema 4.73. Assim, se K é separável sobre F , então K é separável sobre E e E é separável sobre F .

Por outro lado, observe que $[K : E] = \{K : E\}$ e $[E : F] = \{E : F\}$ implica que

$$[K : F] = [K : E][E : F] = \{K : E\}\{E : F\} = \{K : F\}.$$

□

Corolário 4.77. Se E é uma extensão finita de F , então E é separável sobre F se, e somente se, cada α em E é separável sobre F .

Demonstração. Suponha que E seja separável sobre F , e seja $\alpha \in E$. Considere as extensões

$$F \leq F(\alpha) \leq E,$$

O teorema 4.76 mostra que $F(\alpha)$ é separável sobre F .

Suponha, por outro lado, que todo $\alpha \in E$ seja separável sobre F . Como E é uma extensão finita de F , existem $\alpha_1, \dots, \alpha_n$, tais que

$$F \subset F(\alpha_1) \subset F(\alpha_1, \alpha_2) \subset \dots \subset E = F(\alpha_1, \dots, \alpha_n).$$

Agora, como α_i é separável sobre F , α_i é separável sobre $F(\alpha_1, \dots, \alpha_{i-1})$, porque

$$q(X) = \text{irr}(\alpha_i, F(\alpha_1, \dots, \alpha_{i-1}))$$

divide $\text{irr}(\alpha_i, F)$, de modo que α_i é um zero de $q(X)$ de multiplicidade 1. Assim $(\alpha_1, \dots, \alpha_i)$ é separável sobre $F(\alpha_1, \dots, \alpha_{i-1})$, então E é separável sobre F pelo teorema 4.76, estendido por indução. $\square$

Definição 4.78. Um corpo é **perfeito** se toda extensão finita é uma extensão separável.

Exemplo 4.79. É possível mostrar que todo corpo de característica zero é perfeito e que todo corpo finito é perfeito, veja mais informações na página 440 de [6].

O próximo teorema é clássico da teoria de Galois e será crucial na demonstração do Teorema Principal de Galois, 4.84

Teorema 4.80. (Teorema do Elemento Primitivo) *Seja E uma extensão finita separável de um corpo F . Então, existe $\alpha \in E$ tal que $F = F(\alpha)$. (Tal elemento α é chamado de **elemento primitivo**). Ou seja, uma extensão finita separável de um corpo é uma extensão simples.*

Demonstração. Se F é um corpo finito, então E também é finito. Seja α um gerador para o grupo cíclico E^* de elementos diferentes de zero de E sob a multiplicação. Temos então que $E = F(\alpha)$, então α é um elemento primitivo neste caso.

Suponhamos que F é infinito, e provaremos o teorema no caso de $E = F(\beta, \gamma)$. O argumento de indução deste para o caso geral é direto. Seja $\text{irr}(\beta, F)$ com zeros distintos $\beta = \beta_1, \dots, \beta_n$, e seja $\text{irr}(\gamma, F)$ com zeros distintos $\gamma = \gamma_1, \dots, \gamma_m$ em $\overline{F}$, onde todos os zeros são de multiplicidade 1, já que E é uma extensão separável de F . Como F é infinito, podemos encontrar um $a \in F$ tal que

$$a \neq (\beta_i - \beta)/(\gamma - \gamma_j)$$

para todos i e j , com $j \neq 1$. Ou seja, $a(\gamma - \gamma_j) \neq \beta_i - \beta$. Deixando $\alpha = \beta + a\gamma$, temos que $\alpha = \beta + a\gamma \neq \beta_i + a\gamma_j$, então

$$\alpha - a\gamma_j \neq \beta_i$$

para todo i e todo $j \neq 1$. Seja $f(X) = \text{irr}(\beta, F)$, e considere

$$h(X) = f(\alpha - aX) \in (F(\alpha))[X].$$

Agora, $h(\gamma) = f(\beta) = 0$. Porém, $h(\gamma_j) \neq 0$ para $j \neq 1$ por construção, já que β_i eram os únicos zeros de $f(X)$. Portanto, $h(X)$ e $g(X) = \text{irr}(\gamma, F)$ têm um fator comum em $(F(\alpha))[X]$, ou seja, $\text{irr}(\gamma, F(\alpha))$, que deve ser linear, já que γ é o único zero comum de $g(X)$ e $h(X)$. Assim, $\gamma \in F(\alpha)$ e, portanto, $\beta = \alpha - a\gamma$ está em $F(\alpha)$. Portanto, $F(\beta, \gamma) = F(\alpha)$.

□

Definição 4.81. Uma extensão finita K de um corpo F é uma *extensão normal finita* de F se K é um corpo *splitting* e uma *extensão separável* de F .

Teorema 4.82. Seja K uma extensão normal finita de F e E uma extensão de F . Considere a cadeia de extensões $F \leq E \leq K \leq \overline{F}$. Então K é uma extensão normal finita de E e $G(K/E)$ é exatamente o subgrupo de $G(K/F)$ consistindo de todos aqueles automorfismos que deixam E fixo. Além disso, quaisquer dois automorfismos σ e τ em $G(K/F)$ induzem o mesmo isomorfismo de E sobre um subcorpo de $\overline{F}$ se, e somente se, σ e τ pertencem a mesma classe lateral à esquerda de $G(K/E)$ em $G(K/F)$.

Demonstração. Se K é um *splitting* corpo de um conjunto $\{f_i(X) \mid i \in I\}$ de polinômios em $F[X]$, então K é um *splitting* corpo sobre E desse mesmo conjunto de polinômios vistos como elementos de $E[X]$. O teorema 4.76 mostra que K é separável sobre E , já que K é separável sobre F . Assim K é uma extensão normal de E . Isso estabelece nossa primeira afirmação.

Agora todo elemento de $G(K/E)$ é um automorfismo de K deixando F fixo, já que deixa até mesmo o corpo possivelmente maior E fixo. Assim $G(K/E)$ pode ser visto como um subconjunto de $G(K/F)$. Como $G(K/E)$ também é um grupo sob composição de funções, vemos que $G(K/E) \leq G(K/F)$.

Finalmente, para σ e τ em $G(K/F)$, σ e τ estão na mesma classe lateral à esquerda de $G(K/E)$ se, e somente se, $\tau^{-1}\sigma \in G(K/E)$ ou se, e somente se, $\sigma = \tau\mu$ para $\mu \in G(K/E)$. Mas se $\sigma = \tau\mu$ para $\mu \in G(K/E)$, então para $\alpha \in E$, temos

$$\sigma(\alpha) = (\tau\mu)(\alpha) = \tau(\mu(\alpha)) = \tau(\alpha),$$

desde que $\mu(\alpha) = \alpha$ para $\alpha \in E$. Reciprocamente, se $\sigma(\alpha) = \tau(\alpha)$ para todo $\alpha \in E$, então

$$(\tau^{-1}\sigma)(\alpha) = \alpha$$

para todo $\alpha \in E$, então $\tau^{-1}\sigma$ deixa E fixo, e $\mu = \tau^{-1}\sigma$ está em $G(K/E)$. $\square$

Definição 4.83. Se K é uma extensão normal finita de um corpo F , então $G(K/F)$ é chamado o *grupo de Galois de K sobre F* .

4.5 O Teorema Principal de Galois

O teorema fundamental da teoria de Galois mostra que determinada correspondência é biunívoca quando a extensão é finita, normal e separável. Uma extensão reunindo estas três propriedades é chamada extensão de Galois. Vejamos o teorema principal.

Teorema 4.84. *Seja K uma extensão normal finita de um corpo F , com o grupo Galois $G(K/F)$. Para um corpo intermediário E , em que $F \subset E \subset K$, seja $\lambda(E)$ o subgrupo de $G(K/F)$ que deixa E fixo. Então, λ é uma correspondência biunívoca entre o conjunto de todos os corpos intermediários E e o conjunto de todos os subgrupos de $G(K/F)$. Além disso, as seguintes propriedades valem para λ :*

1. $\lambda(E) = G(K/E)$;
2. $E = K_{G(K/E)} = K_{\lambda(E)}$;
3. Se $H \leq G(K/F)$, então $\lambda(K_H) = H$;
4. $[K : E] = |\lambda(E)|$ e $[E : F] = (G(K/F) : \lambda(E))$, em que $(G(K/F) : \lambda(E))$ é o número de classes laterais à esquerda de $\lambda(E)$ em $G(K/F)$;
5. E é uma extensão normal de F se, e somente se, $\lambda(E)$ é um subgrupo normal de $G(K/F)$. Em particular, quando $\lambda(E)$ é um subgrupo normal de $G(K/F)$, tem-se

$$G(E/F) \simeq \frac{G(K/F)}{G(K/E)};$$

Antes de demonstrarmos este teorema façamos um exemplo de sua utilização:

Exemplo 4.85. Seja $K = \mathbb{Q}(\sqrt{2}, \sqrt{3})$. Agora K , é uma extensão normal de $\mathbb{Q}$, e o exemplo 4.53 mostrou que existem quatro automorfismos de K deixando $\mathbb{Q}$ fixo. Lembremos os valores se sua base são $\{1, \sqrt{2}, \sqrt{3}, \sqrt{6}\}$ para K sobre $\mathbb{Q}$.

$$\begin{array}{ccccc} & & \{i, \sigma_1, \sigma_2, \sigma_3\} & & \\ & \swarrow & | & \searrow & \\ \{i, \sigma_1\} & & \{i, \sigma_2\} & & \{i, \sigma_3\} \\ & \swarrow & | & \searrow & \\ & & \{i\} & & \end{array} \quad (4.2)$$

Equation 4.2: Diagrama de grupo.

$$\begin{array}{ccccc} & & \mathbb{Q}(\sqrt{2}, \sqrt{3}) = K_{\{i\}} & & \\ & \swarrow & | & \searrow & \\ K_{\{i, \sigma_1\}} = \mathbb{Q}(\sqrt{3}) & & \mathbb{Q}(\sqrt{2}) = K_{\{i, \sigma_2\}} & & \mathbb{Q}(\sqrt{6}) = K_{\{i, \sigma_3\}} \\ & \swarrow & | & \searrow & \\ & & \mathbb{Q} = K_{\{i, \sigma_1, \sigma_2, \sigma_3\}} & & \end{array} \quad (4.3)$$

Equation 4.3: Diagrama de corpo.

Vejamos que:

i : Aplicação identidade.

σ_1 : Aplica $\sqrt{2}$ em $-\sqrt{2}$, $\sqrt{6}$ em $-\sqrt{6}$, e deixa os outros fixos.

σ_2 : Aplica $\sqrt{3}$ em $-\sqrt{3}$, $\sqrt{6}$ em $-\sqrt{6}$, e deixa os outros fixos.

σ_3 : Aplica $\sqrt{2}$ em $-\sqrt{2}$, $\sqrt{3}$ em $-\sqrt{3}$, e deixa os outros fixos.

A lista completa de subgrupos, com cada subgrupo emparelhado com o corpo intermediário correspondente que deixa fixo, é a seguinte:

$$\begin{array}{ll} \{i, \sigma_1, \sigma_2, \sigma_3\} & \longleftrightarrow \mathbb{Q} \\ \{i, \sigma_1\} & \longleftrightarrow \mathbb{Q}(\sqrt{3}) \\ \{i, \sigma_2\} & \longleftrightarrow \mathbb{Q}(\sqrt{2}) \\ \{i, \sigma_3\} & \longleftrightarrow \mathbb{Q}(\sqrt{6}) \\ \{i\} & \longleftrightarrow \mathbb{Q}(\sqrt{2}, \sqrt{3}). \end{array}$$

Todos os subgrupos abelianos $\{i, \sigma_1, \sigma_2, \sigma_3\}$ são subgrupos normais e todos os corpos intermediários são extensões normais de $\mathbb{Q}$.

Observe que se um subgrupo estiver contido em outro, então o maior dos dois subgrupos corresponde ao menor dos dois corpos fixos correspondentes. Quanto maior o subgrupo, ou seja, quanto mais automorfismos, menor será o corpo fixo, ou seja, menos elementos permanecerão fixos. Na figura 4.2 damos os diagramas correspondentes para os subgrupos e corpos intermediários. Observe que os grupos próximos ao topo correspondem aos corpos próximos à parte inferior. Ou seja, um diagrama parece o outro invertido ou virado de cabeça para baixo.

Agora seguimos com a demonstração o teorema 4.84, ou seja, encerramos este capítulo com a demonstração do principal resultado desta dissertação, por ser a conexão entre a Teoria de Grupos e a Teoria de Corpos.

Demonstração. Primeiramente, observamos que a bijeção de λ segue das propriedades 1, 2 e 3. De fato:

- i) Injetividade: Se E_1 e E_2 são corpos intermediários tais que $\lambda(E_1) = \lambda(E_2)$, por 1, isto implica que $G(K/E_1) = G(K/E_2)$. Assim, de 2, temos:

$$E_1 = K_{G(K/E_1)} = K_{\lambda(E_1)} = K_{\lambda(E_2)} = K_{G(K/E_2)} = E_2.$$

Portanto, $E_1 = E_2$.

- ii) Sobrejetividade: Seja H subgrupo de $G(K/F)$, qualquer. Da proposição 3, segue que o corpo intermediário K_H é tal que $\lambda(K_H) = H$, logo $H \in \text{Im } \lambda$. Por (i) e (ii), λ é bijeção.

Provemos agora as propriedades de 1 à 5.

Veja que a propriedade (1), $\lambda(E) = G(K/E)$, é válida, pois o subgrupo de $G(K/F)$ que deixa E fixo, é exatamente o grupo $G(K/E)$, em que

$$G(K/E) = \{\sigma : K \longrightarrow K, \text{ automorfismo, tal que } \sigma(a) = a, \forall a \in E\},$$

já que se $\sigma(a) = a, \forall a \in E$, sendo $F \leq E$, tem-se também, $\sigma(b) = b, \forall b \in F$.

Com relação à propriedade (2), veja que neste contexto, segue, pelo teorema 4.51, que

$$E \leq K_{G(K/E)}.$$

Por outro lado, se $\alpha \in K$ tal que $\alpha \notin E$, então como K é uma extensão normal de E , usando o isomorfismo de conjugação e o teorema 4.55, podemos encontrar um automorfismo de K que deixa E fixo e que aplica α em um zero $\beta, \alpha \neq \beta$, de $\text{irr}(\alpha, F)$.

Ou seja, se $\alpha \in K$ e $\alpha \notin E$ então existe $\sigma \in G(K/F)$ tal que $\sigma(\alpha) \neq \alpha$, logo $\alpha \notin K_{G(K/F)}$, pela argumentação contrapositiva,

$$K_{G(K/E)} \leq E.$$

Portanto, segue a igualdade

$$E = K_{G(K/E)}.$$

Provemos agora a propriedade 3, a saber: se $H \leq G(K/F)$ então

$$\lambda(K_H) = H.$$

Suponha por absurdo que $\lambda(K_H) \neq H$, ou seja, que H seja um subgrupo próprio de $\lambda(K_H)$.

Veja que como K é uma extensão normal finita, em particular, K é uma extensão separável finita, logo, pelo teorema 4.80,

$$K = K_H(\alpha), \text{ para algum } \alpha \in K.$$

Digamos que $[K : K_H] = n$, e então como K é extensão normal finita, temos:

$$n = [K : K_H] = |\{K : K_H\}| = |G(K/K_H)|.$$

Assim, H subgrupo próprio de $G(K/K_H)$ implica que $|H| < |G(K/K_H)| = n$, e assim, segue também que

$$|H| < [K : K_H] = n.$$

Agora suponha que $H = \{\sigma_1, \sigma_2, \dots, \sigma_{|H|}\}$ e considere o polinômio:

$$f(X) = \prod_{i=1}^{|H|} (X - \sigma_i(\alpha)).$$

Veja que o grau de $f(X)$ é $|H|$ que é tal que $|H| < n$.

Agora, os coeficientes de cada potência de X em $f(X)$ são expressões simétricas em $\sigma_i(\alpha)$, por exemplo, o coeficiente de

$$X^{|H|-1} \text{ é } -\sigma_1(\alpha) - \sigma_2(\alpha) - \dots - \sigma_{|H|}(\alpha),$$

portanto, esses coeficientes são invariantes sobre cada isomorfismo $\sigma_i \in H$, pois se $\sigma \in H$, então

$$\sigma\sigma_1, \dots, \sigma\sigma_{|H|}$$

é ainda a sequência

$$\sigma_1, \dots, \sigma_{|H|},$$

exceto pela ordem, pois H é um grupo.

Consequentemente, $f(X)$ tem os coeficientes em K_H , ou seja,

$$f(X) \in K_H[X].$$

Além disso, como algum dos σ_i é a identidade i , segue que algum dos $\sigma_i(\alpha)$ é α , e então $f(X) = 0$.

Portanto, temos que

$$\deg(\alpha, K_H) \leq |H| < n = [K : K_H] = [K_H(\alpha) : K_H],$$

o que é impossível, pois

$$\deg(\alpha, K_H) = [K_H(\alpha) : K_H]$$

por definição.

Logo, necessariamente,

$$H = \lambda(K_H)$$

e segue a propriedade 3.

A propriedade 4, segue do fato que $[K : E] = \{K : E\}$, $[E : F] = \{E : F\}$, e da última definição do teorema 4.82.

Com relação a propriedade 5, veja primeiramente que, pelo teorema 4.76, que toda extensão E de F , tal que $F \subset E \subset K$, em que K é separável sobre F , também é separável sobre F . Portanto, E é normal sobre F se, e somente se, E é um *splitting* corpo sobre F .

Pelo teorema 4.55, todo isomorfismo de E , sobre um subcorpo de $\overline{F}$ que deixa F fixo pode ser estendido para um automorfismo de K , pois K é uma extensão normal sobre F . Portanto, os automorfismos de $G(K/F)$ induzem todos os possíveis isomorfismos de E sobre um subcorpo de $\overline{F}$ que deixa F fixo. Pelo teorema 4.64, isso mostra que E é um *splitting* corpo sobre F e, conseqüentemente, é normal sobre F , se, e somente se, para todo $\sigma \in G(K/F)$ e $\alpha \in E$, $\sigma(\alpha) \in E$.

Pela propriedade 2, E é o corpo fixo de $G(K/E)$, logo $\sigma(\alpha) \in E$ se, e somente se, para todo $\tau \in G(K/E)$:

$$\tau(\sigma(\alpha)) = \sigma(\alpha)$$

e essa igualdade é válida, se e somente se,

$$(\sigma^{-1}\tau\sigma)(\alpha) = \alpha, \forall \alpha \in E, \forall \sigma \in G(K/F), \forall \tau \in G(K/E).$$

Mas isto significa que para quaisquer $\sigma \in G(K/F)$ e $\tau \in G(K/E)$, $\sigma^{-1}\tau\sigma$ deixa todo elemento de E fixo, ou seja,

$$\sigma^{-1}\tau\sigma \in G(K/E),$$

e, pela proposição 3.15, sabendo que $\sigma^{-1}\tau\sigma = \sigma^{-1}\tau(\sigma^{-1})^{-1}$, essa é exatamente a condição para que $G(K/E)$ seja um subgrupo normal de $G(K/F)$.

Resta mostrar que quando E é extensão normal de F , então: $G(E/F) \simeq \frac{G(K/F)}{G(K/E)}$.

Para tanto, dado $\sigma \in G(K/F)$, seja σ_E o automorfismo de E induzido por σ (que existe pois estamos assumindo que E é uma extensão normal de F).

Portanto, $\sigma_E \in G(E/F)$.

A aplicação

$$\begin{aligned} \Phi : G(K/F) &\longrightarrow G(E/F) \\ \sigma &\longmapsto \Phi(\sigma) := \sigma_E \end{aligned}$$

é um homomorfismo de grupos pois:

$$\forall \sigma, \psi \in G(K/F) : \Phi(\sigma\psi) = (\sigma\psi)_E = \sigma_E\psi_E = \Phi(\sigma)\Phi(\psi),$$

agora, sabemos que pelo teorema 4.64, todo automorfismo μ de E que deixa F fixo pode ser estendido para algum automorfismo de K , ou seja, tal automorfismo é $\mu = \tau_E$ para algum $\tau \in G(K/F)$. Portanto, a aplicação Φ é sobrejetora. Além disso, note que o núcleo de Φ é $G(K/E)$.

Portanto, pelo 1º Teorema do Isomorfismo 3.18 para grupo:

$$\frac{G(K/F)}{G(K/E)} \simeq G(E/F).$$

□

O próximo capítulo, finalmente exibimos um polinômio de grau 5 insolúvel por radicais e para a argumentação deste fato este último resultado é crucial.

5 A insolubilidade da quintica

Neste capítulo, mostraremos que nem todos os zeros de um polinômio quántico (grau 5) $f(X)$ podem ser expressos em termos de radicais. Estamos familiarizados com o fato de que um polinômio quádrático $f(X) = aX^2 + bX + c, a \neq 0$, com coeficientes reais, tem $\frac{-b \pm \sqrt{b^2 - 4ac}}{2a}$ como zeros em $\mathbb{C}$. Mas ainda, ao longo dos capítulos anteriores, mostramos que todo polinômio de grau 3 ou 4 também tem a propriedade de que cada zero pode ser expresso em termos de radicais, entretanto, este fato nem sempre ocorre para um polinômio de grau 5. Depois que matemáticos tentaram durante anos encontrar a “fórmula do radical” para zeros de um polinômio de 5º grau, foi um triunfo quando Abel provou que uma determinada quántica não pode ser solúvel por radicais. Finalizamos este capítulo com a apresentação de um polinômio de quinto grau, em $\mathbb{Q}[X]$, não solúvel por radicais, a saber, o teorema 5.8. No que segue, iniciamos a jornada para a demonstração desse resultado.

5.1 Extensões por radicais

Definição 5.1. Uma extensão K de um corpo F é uma **extensão de F por radicais** se houver elementos $\alpha_1, \dots, \alpha_r \in K$ e inteiros positivos $n_1, \dots, n_r$ de tal modo que $K = F(\alpha_1, \dots, \alpha_r), \alpha_1^{n_1} \in F$ e $\alpha_i^{n_i} \in F(\alpha_1, \dots, \alpha_{i-1})$ para $1 < i \leq r$. Um polinômio $f(X) \in F[X]$ é **solúvel por radicais** F se o *splitting* corpo E de $f(X)$ sobre F está contido em uma extensão de F por radicais.

Um polinômio $f(X) \in F[X]$ é, portanto, solúvel por radicais sobre F se pudermos obter cada zero de $f(X)$ usando uma sequência finita das operações de adição, subtração, multiplicação, divisão e tomando raízes n_i -ésimas, começando com elementos de F .

Embora nosso objetivo final seja demonstrar que existe uma quántica não solúvel na

característica 0, não quer dizer que nenhuma quártica seja solúvel, como mostra o exemplo a seguir.

Exemplo 5.2. O polinômio $X^5 - 1$ é solúvel por radicais sobre $\mathbb{Q}$. O *splitting* corpo K de $X^5 - 1$ é gerado sobre $\mathbb{Q}$ por uma raiz quinta primitiva ζ de unidade. Então $\zeta^5 = 1$, e $K = \mathbb{Q}(\zeta)$. Analogamente, $X^5 - 2$ é solúvel por radicais sobre $\mathbb{Q}$, para o seu *splitting* corpo sobre $\mathbb{Q}$ é gerado por $\sqrt[5]{2}$ e ζ , em que $\sqrt[5]{2}$ é o zero de $X^5 - 2$.

Assumimos a partir de agora que todos os corpos mencionados têm característica 0.

O seguinte lema faz a conexão entre a solubilidade de um polinômio com o grupo de Galois.

Lema 5.3. *Sejam F um corpo de característica 0 e $a \in F$. Se K é um *splitting* corpo de $X^n - a$ sobre F , então $G(K/F)$ é um grupo solúvel.*

Demonstração. Suponha primeiro que F contém todas as raízes n -ésimas da unidade. Pela observação 4.36, as raízes n -ésimas da unidade formam um subgrupo cíclico de $(F^*, \cdot)$. Seja ζ um gerador do subgrupo. (Na verdade, os geradores são exatamente as raízes n -ésimas primitivas da unidade). Então, as raízes n -ésimas da unidade são

$$1, \zeta, \zeta^2, \dots, \zeta^{n-1}.$$

Se $\beta \in \bar{F}$ é um zero de $(X^n - a) \in F[X]$, então todos os zeros de $X^n - a$ são

$$\beta, \zeta\beta, \zeta^2\beta, \dots, \zeta^{n-1}\beta.$$

Desde que $K = F(\beta)$, um automorfismo σ em $G(K/F)$ é determinado pelo valor $\sigma(\beta)$ do automorfismo σ em β . Agora se $\sigma(\beta) = \zeta^i\beta$ e $\tau(\beta) = \zeta^j\beta$, onde $\tau \in G(K/F)$, então

$$(\tau\sigma)(\beta) = \tau(\sigma(\beta)) = \tau(\zeta^i\beta) = \zeta^i\tau(\beta) = \zeta^i\zeta^j\beta,$$

desde que $\zeta^i \in F$. Analogamente,

$$(\sigma\tau)(\beta) = \zeta^j\zeta^i\beta.$$

Por isso $\sigma\tau = \tau\sigma$, e $G(K/F)$ é abeliano e, portanto, solúvel.

Agora suponha que F não contém uma raiz n -ésima primitiva da unidade. Seja ζ um gerador do grupo cíclico de raízes n -ésimas da unidade sob multiplicação em $\bar{F}$. Seja β novamente um zero de $X^n - a$. Como β e $\zeta\beta$ estão ambos no *splitting* corpo K de

$X^n - a, \zeta = (\zeta\beta)/\beta$ está em K . Seja $F' = F(\zeta)$, então teremos as extensões $F < F' \leq K$. Agora F' é uma extensão normal de F , desde que F' é um *splitting* corpo de $X^n - 1$. Como, $F' = F(\zeta)$, um automorfismo η em $G(F'/F)$ é determinado por $\eta(\zeta)$, e devemos ter $\eta(\zeta) = \zeta^i$ para algum i , já que todos os zeros de $X^n - 1$ são potências de ζ . Se $\mu(\zeta) = \zeta^j$ para $\mu \in G(F'/F)$, então

$$(\mu\eta)(\zeta) = \mu(\eta(\zeta)) = \mu(\zeta^i) = \mu(\zeta)^i = (\zeta^j)^i = \zeta^{ij},$$

e, analogamente,

$$(\eta\mu)(\zeta) = \zeta^{ij}.$$

Por isso, $G(F'/F)$ é abeliano. Pelo Teorema Principal da Teoria de Galois 4.84,

$$\{i\} \leq G(K/F') \leq G(K/F)$$

é, segundo as definições 3.26 e ?? uma série normal e, portanto, uma série subnormal de grupos. A primeira parte da prova mostra que $G(K/F')$ é abeliano, e a teoria de Galois nos diz que $G(K/F)/G(K/F')$ é isomorfo a $G(F'/F)$, que é abeliano. Agora, se um grupo tem uma série subnormal de subgrupos com grupos de quocientes abelianos, então qualquer refinamento desta série também tem grupos de quocientes abelianos. Assim, uma série de composição de $G(K/F)$ deve ter grupos de quociente abeliano, então $G(K/F)$ é solúvel. $\square$

O teorema a seguir faz a conexão de todos os elementos necessários para a argumentação de 5.8

Teorema 5.4. *Seja F um corpo de característica 0. Considere a cadeia de extensões de corpos $F \leq E \leq K \leq \bar{F}$, em que E é uma extensão normal de F e K é uma extensão de F por radicais, então $G(E/F)$ é um grupo solúvel.*

Demonstração. Mostraremos primeiro que K está contido em uma extensão normal finita L de F por radicais e que o grupo $G(L/F)$ é solúvel. Se K é uma extensão por radicais, então $K = F(\alpha_1, \dots, \alpha_r)$ em que $\alpha_i^{n_i} \in F(\alpha_1, \dots, \alpha_{i-1})$ para $1 < i \leq r$ e $\alpha_1^{n_1} \in F$. Para formar L , primeiro formamos o *splitting* corpo L_1 de $f_1(X) = X^{n_1} - \alpha_1^{n_1}$ sobre F . Então L_1 é uma extensão normal de F , e do lema 5.3 mostra-se que $G(L_1/F)$ é um grupo solúvel. Agora $\alpha_2^{n_2} \in L_1$ formamos o polinômio

$$f_2(X) = \prod_{\sigma \in G(L_1/F)} [X^{n_2} - \sigma(\alpha_2)^{n_2}].$$

Como este polinômio é invariante sob ação de qualquer σ em $G(L_1/F)$, vemos que $f_2(X) \in F[X]$. Seja L_2 o *splitting* corpo de $f_2(X)$ sobre L_1 . Então L_2 é um *splitting* corpo sobre F também e é uma extensão normal de F por radicais. Podemos formar L_2 a partir de L_1 por meio de passos repetidos como no lema 5.3, passando para o *splitting* corpo de $X^{n_2} - \sigma(\alpha_2)^{n_2}$ a cada passo. Pelo lema 5.3, vemos que o grupo Galois sobre F de cada nova extensão, assim formada, continua a ser solúvel. Continuamos este processo de formação do *splitting* corpo sobre F desta forma: Na fase i , formaremos o *splitting* corpo do polinômio

$$f_i(X) = \prod_{\sigma \in G(L_{i-1}/F)} [X^{n_i} - \sigma(\alpha_i)^{n_i}]$$

sobre L_{i-1} . Finalmente, obtemos um corpo $L = L_r$ que é uma extensão normal de F por radicais, e vemos que $G(L/F)$ é um grupo solúvel. Vemos pela construção que K é subcorpo de L .

Para concluir, basta notar que pelo teorema 4.84, temos que $G(E/F) \simeq G(L/F)/G(L/E)$. Por isso, $G(E/F)$ é um grupo quociente e, portanto, uma imagem homomorfa, de $G(L/F)$. Logo, $G(L/F)$ é solúvel e então $G(E/F)$ é solúvel. $\square$

Observação 5.5. Sabemos por definição, que um polinômio $f(X) \in F[X]$ é solúvel por radicais sobre F quando seu *splitting* corpo, E , está contido em uma extensão de F por radicais, K . Ou seja, se E é *splitting* corpo de $f(X)$ obedecendo a cadeia de extensões $F \leq E \leq K \leq \bar{F}$, com K sendo uma extensão de F por radicais. Se isto ocorre, segue do teorema anterior que o grupo de Galois de E sobre F , $G(E/F)$, é um grupo solúvel.

Com isso, através da argumentação contra-positiva, podemos afirmar que: sendo E o *splitting* corpo de $f(X)$ obedecendo a cadeia de extensões $F \leq E \leq K \leq \bar{F}$, com K sendo uma extensão de F , se $G(E/F)$, é um grupo não solúvel (isto é, insolúvel), então, K não é uma extensão por radicais de F e, portanto, o polinômio $f(X)$ não é solúvel por radicais sobre F .

5.2 Funções simétricas

Sejam F um corpo e $y_1, y_2, \dots, y_n$ indeterminadas. Existem determinados automorfismos naturais de $F(y_1, y_2, \dots, y_n)$ que deixam F fixo, nomeadamente, aqueles defi-

nidos por permutações de $\{y_1, \dots, y_n\}$. Para ser mais explícito, seja σ uma permutação de $\{1, \dots, n\}$, ou seja, $\sigma \in S_n$. Então σ dá origem a uma aplicação natural $\bar{\sigma} : (y_1, \dots, y_n) \rightarrow F(y_1, \dots, y_n)$ dada por

$$\bar{\sigma} \left(\frac{f(y_1, \dots, y_n)}{g(y_1, \dots, y_n)} \right) = \frac{f(y_{\sigma(1)}, \dots, y_{\sigma(n)})}{g(y_{\sigma(1)}, \dots, y_{\sigma(n)})}$$

para $f(y_1, \dots, y_n), g(y_1, \dots, y_n) \in F[y_1, \dots, y_n]$, com $g(y_1, \dots, y_n) \neq 0$. Veja que $\bar{\sigma}$ é um automorfismo de $F(y_1, \dots, y_n)$ que deixa F fixo. Os elementos de $F(y_1, \dots, y_n)$ deixados fixos por todo $\bar{\sigma}$, para todo $\sigma \in S_n$, são aquelas funções racionais que são simétricas nos indeterminados $y_1, \dots, y_n$.

Definição 5.6. Um elemento do corpo $F(y_1, \dots, y_n)$ é uma **função simétrica em $y_1, \dots, y_n$ sobre F** , se for deixada fixa por todas as permutações de $y_1, \dots, y_n$, no sentido explicado acima.

Teorema 5.7. *Sejam $s_1, \dots, s_n$ as funções simétricas elementares nos indeterminados $y_1, \dots, y_n$. Então toda função simétrica de $y_1, \dots, y_n$ sobre F é uma função racional das funções simétricas elementares. Além disso, $F(y_1, \dots, y_n)$ é uma extensão normal finita de grau $n!$ de $F(s_1, \dots, s_n)$, e o grupo de Galois desta extensão é naturalmente isomorfo a S_n .*

Demonstração. Seja $\bar{S}_n$ o grupo de todos os automorfismos $\bar{\sigma}$ para $\sigma \in S_n$. Observe que $\bar{S}_n$ é isomorfo a S_n . Seja K o subcorpo de $F(y_1, \dots, y_n)$ que é corpo fixo de $\bar{S}_n$. Considere o polinômio

$$f(X) = \prod_{i=1}^n (X - y_i);$$

este polinômio $f(X) \in (F(y_1, \dots, y_n))[X]$ é um **polinômio geral de grau n** . Seja $\bar{\sigma}_X$ a extensão de $\bar{\sigma}$, de forma natural, para $(F(y_1, \dots, y_n))[X]$, onde $\bar{\sigma}_X(X) = X$. Agora $f(X)$ é deixado fixo por cada aplicação de $\bar{\sigma}_X$ para $\sigma \in S_n$; ou seja,

$$\prod_{i=1}^n (X - y_i) = \prod_{i=1}^n (X - y_{\sigma(i)}).$$

Assim, os coeficientes de $f(X)$ estão em K ; são *funções simétricas elementares* em $y_1, \dots, y_n$. Como ilustração, observe que o termo constante de $f(X)$ é

$$(-1)^n y_1 y_2 \dots y_n,$$

o coeficiente de X^{n-1} é $-(y_1 + y_2 + \dots + y_n)$, e assim por diante. Estas são funções simétricas em $y_1, \dots, y_n$.

A primeira função simétrica elementar em $y_1, \dots, y_n$ é

$$s_1 = y_1 + y_2 + \dots + y_n,$$

a segunda é $s_2 = y_1y_2 + y_1y_3 + \dots + y_{n-1}y_n$, e assim por diante, e o enésimo é $s_n = y_1y_2 \dots y_n$.

Considere o corpo $E = F(s_1, \dots, s_n)$. Como $E \leq K$, onde K é o corpo de todas as funções simétricas em $y_1, \dots, y_n$ sobre F . Mas $F(y_1, \dots, y_n)$ é uma extensão normal finita de E , ou seja, o *splitting* corpo de

$$f(X) = \prod_{i=1}^n (X - y_i)$$

sobre E . Como o grau de $f(X)$ é n , temos que

$$[F(y_1, \dots, y_n) : E] \leq n!.$$

No entanto, como K é o corpo fixo de $\overline{S_n}$ e

$$|\overline{S_n}| = |S_n| = n!,$$

temos também que

$$n! \leq [F(y_1, \dots, y_n) : K] \leq [F(y_1, \dots, y_n) : E].$$

Portanto,

$$n! \leq [F(y_1, \dots, y_n) : K] \leq [F(y_1, \dots, y_n) : E] \leq n!,$$

então

$$K = E.$$

O grupo de Galois de $F(y_1, \dots, y_n)$ sobre E é, portanto, $\overline{S_n}$. O fato de $K = E$ mostra que toda função simétrica pode ser expressa como uma função racional das funções simétricas elementares $s_1, \dots, s_n$. $\square$

5.3 A insolubilidade da quántica

A estratégia será de mostrar que existe um subcorpo F de $\mathbb{R}$ e um polinômio $f(X) \in F[X]$ de grau 5 tal que o *splitting* corpo E de $f(X)$ sobre F tem um grupo de Galois isomorfo a S_5 , por meio do teorema 5.7, que sabemos que é um grupo insolúvel, pelo exemplo 3.34. Pois com isso, segue da observação 5.5 que $f(X)$ não é solúvel por radical sobre F .

Sejam $y_1 \in \mathbb{R}$ transcendente sobre $\mathbb{Q}$, $y_2 \in \mathbb{R}$ transcendente sobre $\mathbb{Q}(y_1)$, e assim sucessivamente, até chegarmos $y_5 \in \mathbb{R}$ transcendente sobre $\mathbb{Q}(y_1, \dots, y_4)$. Pela completude do corpo dos números reais tais números reais transcendentos existem. Os transcendentos encontrados dessa maneira são **elementos transcendentos independentes sobre $\mathbb{Q}$** . Seja $E = \mathbb{Q}(y_1, \dots, y_5)$, e seja

$$f(X) = \prod_{i=1}^5 (X - y_i).$$

Então $f(X) \in E[X]$. Agora, os coeficientes de $f(X)$ estão, a menos de sinal, entre as *funções simétricas elementares* sobre y_i , a saber,

$$s_1 = y_1 + y_2 + \dots + y_5,$$

$$s_2 = y_1y_2 + y_1y_3 + y_1y_4 + y_1y_5 + y_2y_3 + y_2y_4 + y_2y_5 + y_3y_4 + y_3y_5 + y_4y_5,$$

$$\vdots$$

$$s_5 = y_1y_2y_3y_4y_5.$$

O coeficiente de X^i em $f(X)$ é $\pm s_{5-i}$. Seja $F = \mathbb{Q}(s_1, s_2, \dots, s_5)$; então $f(X) \in F[X]$ (conforme a figura 5.1).

$$\begin{array}{c} E = \mathbb{Q}(y_1, \dots, y_5) \\ | \\ F = \mathbb{Q}(s_1, \dots, s_5) \\ | \\ \mathbb{Q} \end{array}$$

Figura 5.1: Torre de corpos.

Então, E é um *splitting* corpo sobre F de $f(X)$. Uma vez que y_i se comportam como indeterminados sobre $\mathbb{Q}$, para cada $\sigma \in S_5$, σ induz como automorfismo $\bar{\sigma}$ de E definido

por $\bar{\sigma}(a) = a$ para $a \in \mathbb{Q}$ e $\bar{\sigma}(y_i) = y_{\sigma(i)}$. Uma vez que $\prod_{i=1}^5 (X - y_i)$ é o mesmo polinômio que $\prod_{i=1}^5 (X - y_{\sigma(i)})$, temos que

$$\bar{\sigma}(s_i) = s_i$$

para cada i , assim $\bar{\sigma}$ deixa F fixo, e portanto $\bar{\sigma} \in G(E/F)$. Agora, S_5 tem ordem $5!$, então

$$|G(E/F)| \geq 5!.$$

Mas, o *splitting* corpo do polinômio de grau 5 sobre F tem grau no máximo $5!$ sobre F , podemos ver que

$$|G(E/F)| \leq 5!.$$

Então, $|G(E/F)| = 5!$ e o automorfismo $\bar{\sigma}$ compõem o grupo completo de Galois $G(E/F)$. Portanto, $G(E/F) \simeq S_5$, então $G(E/F)$ não é solúvel. Isso completa nosso esboço, e resumimos em um teorema, a saber:

Teorema 5.8. *Sejam $y_1, \dots, y_5$ números reais transcendentos independentes sobre $\mathbb{Q}$. O polinômio*

$$f(X) = \prod_{i=1}^5 (X - y_i)$$

não é solúvel por radicais sobre $F = \mathbb{Q}(s_1, \dots, s_5)$, em que s_i é o i -enésimo elemento da função simétrica em $y_1, \dots, y_5$.

Ou seja, o esboço para a compreensão do teorema 5.8 consistiu em provarmos que existe um subcorpo F dos números reais e um polinômio $f(X) \in F[X]$ de grau cinco com um *splitting* corpo E sobre F de tal modo que $G(E/F) \simeq S_5$. Entretanto, S_5 não é um grupo solúvel já que sua série de composição é dada por $\{i\} < A_5 < S_5$, com A_5 não abeliano.

6 Considerações finais

Ao longo dessa dissertação, pudemos estudar a evolução da álgebra ao longo dos séculos. Diversos estudiosos contribuíram para a sua construção, como Al-Khwarizmi, Bháskara, Tartaglia, Cardano e o gênio incompreendido Galois. Toda essa teoria desenvolvida foi primordial para resolvermos problemas abstratos na matemática.

Buscamos também estabelecer a conexão entre a história da matemática com a construção da formalização da álgebra como disciplina, com foco principal nos métodos de resolução das equações polinomiais de grau menor igual que cinco.

Com esse percurso traçado, chegamos na insolubilidade da quártica, apresentamos as noções básicas de estruturas algébricas como: grupos, anéis, corpos e anéis de polinômios, elementos da teoria de Galois, tais como: extensão de corpos, corpo de Galois, grupo de automorfismos, *splitting* corpo, extensão separável e o grupo de Galois, onde também apresentamos o seu teorema principal, até, por fim, chegarmos na insolubilidade da quártica por radicais.

Logo, podemos perceber o quanto a álgebra foi um campo de estudo bem elaborado, com fundamentos teóricos que permeiam até os dias atuais. O estudo da insolubilidade da quártica apresenta todo esse trajeto e também destaca a genialidade do jovem Galois.

Vimos também, que o critério de solubilidade desenvolvido por Galois, resolveu um problema milenar. Esse fato torna seu critério uma das soluções mais importantes da história da matemática. Porém, destacamos que a importância desse critério consiste no uso de uma estrutura abstrata (grupos) para solucionar um problema que não apresentava nenhuma conexão aparente. E isso evidenciou o potencial da álgebra para a solução de problemas complexos, mas iniciou a era da matemática moderna.

Referências

- [1] ANDRADE, R. J. M. B. *Resolução de uma equação do quinto grau*. Bauru: Revista Eletrônica Paulista de Matemática, 2019. v. 3. 196-205 p. Disponível em: <<https://www.fc.unesp.br/Home/Departamentos/Matematica/revistacqd2228/v16a12-resolucao-de-uma-equacao-do-quinto-grau.pdf>>. Acesso em: 25 de jan. de 2021.
- [2] BERLINGHOFF, W. P.; GOUVÊA, F. Q. *Matemática através dos tempos: um guia fácil e prático para professores e entusiastas*. 2. ed. São Paulo: Edgard Blücher Ltda., 2010.
- [3] BOYER, C. B. *História da Matemática*. 1. ed. São Paulo: Edgard Blücher Ltda., 1974.
- [4] BRANDEMBERG, J. C. *Sobre o uso da história da matemática no ensino de equações algébricas*. Pará: Revista Cocar, 2017. v. 3. 167-186 p. Disponível em: <<https://periodicos.uepa.br/index.php/cocar/article/view/1168>>. Acesso em: 07 de nov. de 2021.
- [5] DOMINGUES, H. H.; IEZZI, G. *Álgebra Moderna*. 2. ed. São Paulo: Atual, 1979.
- [6] FRALEIGH, J. B. *A first course in Abstract Algebra*. 7. ed. University of Rhode Island: Addison Wesley World Student Edition, 2002.
- [7] HEFEZ, A.; VILLELA, M. L. T. *Polinômios e Equações Algébricas*. 2. ed. Rio de Janeiro: Sociedade Brasileira de Matemática - SBM, 2018.
- [8] NOBRE, S. R. *O problema das 100 aves*. Revista do professor de Matemática - RPM, 2014. Disponível em: <<https://www.rpm.org.br/cdrpm/85/1.html>>. Acesso em: 04 de out. de 2021.

-
- [9] PONTE, J. P. d.; BRANCO, N.; MATOS, A. *Álgebra no ensino básico*. [S.l.]: DGIDC, 2009.
- [10] REZENDE, F. S. *Equações do Terceiro e do Quarto Graus*. Departamento de Matemática - UFMG, 2002. Disponível em: <<https://docplayer.com.br/87638110-Equacoes-do-terceiro-e-do-quarto-graus.html>>. Acesso em: 07 de nov. de 2021.
- [11] ROQUE, T.; CARVALHO, J. B. P. de. *Tópicos de História da Matemática*. 2. ed. Rio de Janeiro: Sociedade Brasileira de Matemática - SBM, 2019.